Université de Genève – cours de 3e et 4e années – hiver 2005/06

REPRÉSENTATIONS DES GROUPES FINIS

Pierre de la Harpe

Version du 24 février 2006

Table des matières

Il existe des expositions bien établies de la théorie élémentaire des représentations des groupes finis. Le livre de Serre est une référence obligée, en français [Serre–67] ; nous recommandons aussi [Vinbe–89]. Citons encore [AleBe–95] et [CurRe–62].

On trouve également des chapitres traitant de ce sujet dans de nombreux livres consacrés au moins en partie à d'autres domaines des mathématiques, par exemple la géométrie différentielle [Wolf–67, chapitre 4, pages 138 à 154], les probabilités et la statistique [Diaco–88, chapitre 2, pages 5 à 16], des problèmes de combinatoire liés aux groupes symétriques [Sagan–91, chapitre 1, pages 1 à 51] ou à des graphes remarquables [DaSaV–03, § 3.4], divers chapitres de physique [Stern–94, chapitre 2, pages 48 à 93], et bien sûr des livres envisageant les représentations de groupes plus généraux, dont [Weil–40, chapitre V] et [FulHa–91, Part I].

Pour l'histoire ancienne du sujet, crée autour de 1900 par Georg Frobenius (1849–1917), William Burnside (1852–1927), Issaï Schur (1875–1941), Richard Brauer (1901–1977), et bien d'autres, voir [Curti–99].

Dans les chapitres I à V, la lettre G désigne un groupe dont, souvent, il importe peu qu'il soit fini ou infini. Aux chapitres VI et suivants, et sauf mention expresse du contraire,

G désigne un groupe fini. De nombreux exemples illustrent les notions traitées ; en particulier, une grande attention a été consacrée aux groupes de symétrie des polyèdres réguliers et à quelques groupes apparentés comme les sous–groupes finis de $S\mathcal{U}(2)$.

Ce texte, dactilographié pendant le semestre d'hiver 2005/06, reprend la matière d'un cours déjà donnés deux fois. Au cours des ans, j'ai bénéficié de nombreuses conversations qui m'ont beacoup appris, et pour lesquelles je remercie (parmi d'autres) Bachir Bekka, Vaughan Jones, Jan Saxl, Jacques Thévenaz et Thierry Vust. Une partie de ce qui suit n'a pas été exposée en 2005/06 ; c'est le cas de nombreux exercices (quelques solutions partielles apparaissent en dernière partie) ainsi que des chapitres X, XIV et XV.

I. Définitions et premiers exemples

Une *représentation linéaire* de G dans un espace vectoriel V sur un corps $\mathbf{K}$ est un homomorphisme π de G dans le *groupe général linéaire* $GL(V)$, qui est le groupe des automorphismes linéaires de l'espace V. Une telle représentation est *fidèle* si l'homomorphisme π est injectif.

Dans ce cours, et sauf mention expresse du contraire, nous nous intéressons au cas où l'espace V est de dimension finie, auquel cas cette dimension s'appelle le *degré* de π, et au cas où le corps $\mathbf{K}$ est de caractéristique nulle ; le plus souvent, ce sera même le corps $\mathbf{C}$ des nombres complexes.

Deux représentations $\pi_j : G \longrightarrow GL(V_j)$, $j = 1, 2$, d'un même groupe G sont dites *équivalentes* s'il existe un isomorphisme linéaire $S : V_1 \longrightarrow V_2$ qui est *G–équivariant,* c'est–à–dire tel que $S\pi_1(g) = \pi_2(g)S$ pour tout $g \in G$.

Rappelons que, lorsque V est de dimension finie, notée n, et muni d'une base, le groupe $GL(V)$ s'identifie au groupe $GL_n(\mathbf{K})$ des matrices n–fois–n inversibles à coefficients dans $\mathbf{K}$. On appelle donc aussi représentation linéaire de G de degré n un homomorphisme $\pi : G \longrightarrow GL_n(\mathbf{K})$. La définition d'équivalence ci–dessus se formule alors en terme d'une matrice inversible $S \in GL_n(\mathbf{K})$. Lorsque $n = 1$, l'usage est de noter $\mathbf{K}^*$, plutôt que $GL_1(\mathbf{K})$, le groupe multiplicatif du corps $\mathbf{K}$.

On peut penser à deux représentations $G \longrightarrow GL_n(\mathbf{K})$ qui sont équivalentes comme à une même représentation dans $\mathbf{K}^n$ écrite en termes de matrices relativement à deux bases de $\mathbf{K}^n$.

Soit V un espace *hermitien*, c'est–à–dire un espace vectoriel complexe de dimension finie muni d'un produit scalaire $(v, w) \longmapsto \langle v \mid w\rangle$, et de la norme associée $v \longmapsto \|v\| = \langle v \mid v\rangle^{\frac{1}{2}}$; par convention ici, le produit scalaire est antilinéaire en v et linéaire en w. Rappelons que tout endomorphisme linéaire A de V possède un *adjoint* A^*, bien défini par les égalités $\langle A^*v \mid w\rangle = \langle v \mid Aw\rangle$ pour tous $v, w \in V$. Un opérateur A est *unitaire* si $\|Av\| = \|v\|$ pour tout $v \in V$, ou de manière équivalente si $A^*A = I$, ou encore si $A^*A = AA^* = I$. Le *groupe unitaire* de V est le groupe $\mathcal{U}(V)$ constitué des opérateurs unitaires de V.

Une représentation π d'un groupe G dans V est alors *unitaire* si l'image de l'homomorphisme π est dans le sous–groupe $\mathcal{U}(V)$ de $GL(V)$.

Deux représentations unitaires $\pi_j : G \longrightarrow GL(V_j)$, $j = 1, 2$, d'un même groupe G dans des espaces hermitiens sont dites *unitairement équivalentes* s'il existe une isométrie linéaire surjective $S : V_1 \longrightarrow V_2$ qui est G–équivariante.

Comme plus haut, on peut aussi définir une représentation unitaire de degré n comme un homomorphisme dans le groupe $\mathcal{U}(n)$ des matrices complexes n–fois–n unitaires. De même que $GL_1(\mathbf{K})$ s'identifie au groupe multiplicatif $\mathbf{K}^*$, le groupe $\mathcal{U}(1)$ s'identifie au groupe multiplicatif des nombres complexes de module 1.

On peut penser à deux représentations unitaires $G \longrightarrow \mathcal{U}(n)$ qui sont unitairement équivalentes comme à une même représentation unitaire dans $\mathbf{C}^n$ écrite en termes de matrices relativement à deux bases orthonormales de $\mathbf{C}^n$.

I.1. Exemple. Soit G un sous–groupe de $GL(V)$. L'inclusion de G dans $GL(V)$ fournit une représentation de G, dite parfois "tautologique".

I.2. Exemple : représentations de premutation. Soit G un groupe agissant (on dit aussi "opérant") sur un ensemble X non vide ; convenons que l'action est à gauche. Rappelons qu'une telle *action* est une application

$$G \times X \longrightarrow X, \quad (g, x) \longmapsto gx$$

telle que $g(hx) = (gh)x$ et $1x = x$ pour tous $g, h \in G$ et $x \in X$. Notons $V = \mathbf{K}^{(X)}$ l'espace vectoriel des fonctions à supports finis de X dans $\mathbf{K}$. Pour tout $g \in G$, on définit un automorphisme linéaire $\pi(g)$ de V par

$$(1) \qquad (\pi(g)\varphi)(x) = \varphi(g^{-1}x) \qquad \text{pour tous} \quad \varphi \in \mathbf{K}^{(X)} \quad \text{et} \quad x \in X \ ;$$

on vérifie que $\pi(g)$ est inversible d'inverse $\pi(g^{-1})$ et que $\pi : G \longrightarrow GL(V)$ est bien un homomorphisme ; on l'appelle la *représentation de permutation* associée à l'action donnée de G sur X. [Si G agit fidèlement sur X, alors G s'identifie à un sous–groupe de $GL(V)$, et on peut voir ceci comme un cas particulier de l'exemple précédent.] Pour $x \in X$, notons $\epsilon_x \in V$ la fonction qui vaut 1 en x et 0 ailleurs. On vérifie que $(\epsilon_x)_{x \in X}$ est une base de V et que

$$(2) \qquad \pi(g)\epsilon_x = \epsilon_{gx}$$

pour tous $g \in G$ et $x \in X$.

L'espace V est de dimension finie si et seulement si l'ensemble X est fini. Supposons désormais que ce soit le cas et écrivons $\mathbf{K}^X$ au lieu de $\mathbf{K}^{(X)}$; notons que le degré de π est la cardinalité de X.

Supposons de plus que $\mathbf{K} = \mathbf{C}$. On définit un produit scalaire sur V en posant

$$\langle \varphi \mid \psi \rangle = \sum_{x \in X} \overline{\varphi(x)} \psi(x) \qquad \text{pour tous} \quad \varphi, \psi \in \mathbf{C}^X.$$

La base $(\epsilon_x)_{x \in X}$ est alors orthonormale, et la représentation π est unitaire.

Lorsque X est un ensemble avec une certaine structure préservée par l'action de G, l'espace V possède parfois des sous–espaces vectoriels W dans lesquels G opère linéairement de manière intéressante. Par exemple, si G opère par homéomorphismes sur un espace topologique compact X, la formule (1) définit une action linéaire de G sur l'espace (de dimension infinie) des fonctions continues sur X ; un cas particulier abondamment étudié est celui de l'action du groupe des rotations $G = \mathcal{SO}(3)$ sur la sphère unité $\mathbf{S}^2$ de l'espace usuel. Ce type d'exemple peut fournir des représentations de dimension finie ; en voici une illustration.

Considérons deux entiers $k \geq 2$, $d \geq 0$, l'espace vectoriel $X = \mathbf{R}^k$, et l'espace vectoriel $W = \mathcal{P}^{(d)}(\mathbf{R}^k)$ des fonctions polynomiales $\mathbf{R}^k \longrightarrow \mathbf{C}$ qui sont homogènes de degré d, c'est–à–dire des fonctions de la forme

$$(x_1, \ldots, x_k) \longmapsto \sum_{\substack{0 \leq d_1, \ldots, d_k \leq d \\ d_1 + \cdots + d_k = d}} c_{d_1, \ldots, d_k} x_1^{d_1} \cdots x_k^{d_k}$$

où les $c_{d_1,\ldots,d_k}$ sont des nombres complexes. Soit G un sous–groupe de $GL(X)$. La représentation naturelle de G dans W est définie par la formule suivante, formellement identique à (1) :

$$(\pi(g)\varphi)(x) = \varphi(g^{-1}x) \qquad \text{pour tous} \quad \varphi \in W, g \in G, x \in X.$$

Nous revenons à une construction de ce type ci–dessous à l'exercice V.E9.

I.3. Exemple : représentation régulière. Particularisons l'exemple précédent au cas où le groupe G agit sur lui–même ($X = G$) par multiplications à gauche. Un usage fréquent, que nous adoptons, est d'écrire alors $\mathbf{K}[G]$ au lieu de $\mathbf{K}^{(G)}$. (Cet espace possède plusieurs structures supplémentaires, dont un *produit de convolution* qui en fait la $\mathbf{K}$–*algèbre du groupe* G ; nous y reviendrons au chapitre X.) Nous obtenons la *représentation régulière gauche*

$$\lambda_G : G \longrightarrow GL(\mathbf{K}[G])$$

définie par

$$(*) \qquad (\lambda_G(g)\varphi)(x) = \varphi(g^{-1}x)$$

pour toute fonction φ à support fini sur G et pour tous $g, x \in G$. Notons que cette représentation est fidèle, comme cela résulte par exemple de la relation $\lambda_G(g)\epsilon_1 = \epsilon_g$, cas particulier de (2).

De même, la *représentation régulière droite*

$$\rho_G : G \longrightarrow GL(\mathbf{K}[G])$$

est définie par $(\rho_G(g)\varphi)(x) = \varphi(xg)$ pour toute fonction φ à support fini sur G et pour tous $g, x \in G$.

Les représentations λ_G et ρ_G sont équivalentes. En effet, si $S : \mathbf{K}[G] \longrightarrow \mathbf{K}[G]$ est l'isomorphisme linéaire défini par $(S\varphi)(x) = \varphi(x^{-1})$ pour tout $x \in G$, il est immédiat de vérifier que $(S\lambda_G(g)\varphi)(x) = (\rho_G(g)S\varphi)(x)$ pour tous $g, x \in G$ et $\varphi \in \mathbf{K}[G]$.

Soit H un sous–groupe de G. L'action naturelle de G sur l'ensemble quotient $X = G/H$ fournit la *représentation quasi-régulière*

$$\lambda_{G/H} : G \longrightarrow GL\left(\mathbf{K}^{(G/H)}\right)$$

définie par l'analogue des formules (*). On retrouve λ_G si $H = \{1\}$.

I.4. Exemple : caractères linéaires, caractère principal. Un *caractère linéaire* d'un groupe G est un homomorphisme de G dans le groupe multiplicatif $\mathbf{C}^*$ des nombres complexes non nuls. C'est une représentation de degré 1.

(Les "caractères linéaires" introduits ici sont des cas particulier des "caractères" du chapitre V ; voir la remarque V.2.ii. Ceux-ci seront associés à des représentations de degrés *quelconques*, et les représentations de degré *un* fourniront les caractères *linéaires*.)

Par exemple, si V est un espace vectoriel réel ou complexe, le déterminant fournit un caractère linéaire $\det : GL(V) \longrightarrow \mathbf{C}^*$; il est surjectif si V est complexe, et d'image $\mathbf{R}^*$ si V est réel. Plus généralement, pour toute représentation linéaire $\pi : G \longrightarrow GL(V)$, la composition de π et du déterminant fournit un caractère linéaire $g \longmapsto \det(\pi(g))$ de G.

Lorsque le groupe G est fini, un caractère linéaire prend pour valeurs des racines de l'unité ; un tel caractère linéaire est donc nécessairement une représentation unitaire.

En particulier, la *représentation unité*, ou *caractère principal* d'un groupe G est le caractère noté 1_G défini par $1_G(g) = 1$ pour tout $g \in G$.

A toute représentation π de G de degré 1, on associe le caractère linéaire $\chi : G \longrightarrow \mathbf{C}^*$ défini[1] par $\chi(g) = \det(\pi(g))$. Ce caractère peut être vu comme une représentation $G \longrightarrow GL_1(\mathbf{C})$ dans l'espace vectoriel $\mathbf{C}$, dont on vérifie qu'elle est équivalente à π ; de fait, dans ce cas, on identifie souvent (abusivement !) π et χ.

I.5. Exemple : représentations et groupes quotients. Soient G un groupe et N un sous–groupe normal de G. Notons Q le groupe quotient et $p : G \longrightarrow Q$ la projection canonique. Toute représentation $\underline{\pi} : Q \longrightarrow GL(V)$ fournit par composition avec p une représentation $\pi : G \longrightarrow GL(V)$.

Il y a ainsi une correspondance naturelle entre représentations de Q et représentations de G dont le noyau contient N.

I.6. Exemple : représentations et automorphismes. Soient G un groupe, $\pi : G \longrightarrow GL(V)$ une représentation et α un automorphisme de G. Alors $\pi\alpha$ est encore une représentation de G dans V.

Si l'automorphisme α est intérieur, c'est–à–dire s'il existe $s \in G$ tel que $\alpha(g) = sgs^{-1}$ pour tout $g \in G$, les représentations π et $\pi\alpha$ sont équivalentes. Pour le S de la définition, l'automorphisme $\pi(s)$ de V convient.

Si G est le sous–groupe de $\mathbf{C}^*$ des racines cubiques de l'unité, π la représentation tautologique de G dans $\mathbf{C}$ (exemple I.1) et α l'automorphisme qui échange $\exp(2i\pi/3)$ avec $\exp(-2i\pi/3)$, les représentations π et $\pi\alpha$ ne sont pas équivalentes.

I.7. Exemple : la contragédiente. Soient V un espace vectoriel, $\mathcal{L}(V)$ l'espace de ses endomorphismes linéaires V' son dual, G un groupe et $\pi : G \longrightarrow GL(V)$ une représentation linéaire. Pour tout endomorphisme linéaire A de V, notons $A' \in \mathcal{L}(V')$ l'endomorphisme dual, défini par $(A'\varphi)(v) = \varphi(Av)$ pour toute forme linéaire φ sur V (c'est–à–dire pour tout $\varphi \in V'$) et pour tout $v \in V$. On vérifie que l'application $\check{\pi} : G \longrightarrow GL(V')$ définie par

$$\check{\pi}(g) \;=\; \pi(g^{-1})'$$

est une représentation de G dans V'. On l'appelle la *représentation contragrédiente* de π.

Noter que la représentation contragrédiente de $\check{\pi}$ est canoniquement équivalente à π.

[1] Noter que $\det(\pi(g)) = \mathrm{trace}(\pi(g))$, puisque $\pi(g)$ est un endomorphisme d'un espace de dimension 1.

I.8. Exemples arithmétiques et préhistoire du sujet. Soit m un nombre entier impair. Posons

$$\epsilon(m) \equiv \frac{m-1}{2} \pmod 2 = \begin{cases} 0 & \text{si} \quad m \equiv 1 \pmod 4 \\ 1 & \text{si} \quad m \equiv -1 \pmod 4 \end{cases}$$

et

$$\omega(m) \equiv \frac{m^2-1}{8} \pmod 2 = \begin{cases} 0 & \text{si} \quad m \equiv \pm 1 \pmod 8 \\ 1 & \text{si} \quad m \equiv \pm 3 \pmod 8). \end{cases}$$

L'application $m \longmapsto (-1)^{\epsilon(m)}$ peut être vue comme un caractère linéaire du groupe multiplicatif $(\mathbf{Z}/4\mathbf{Z})^*$ des éléments invesibles de l'anneau $\mathbf{Z}/4\mathbf{Z}$. De même, $m \longmapsto (-1)^{\omega(m)}$ peut être vu comme un caractère linéaire $(\mathbf{Z}/8\mathbf{Z})^* \longrightarrow \{\pm 1\}$.

Soit p un nombre premier impair. A tout $x \in \mathbf{Z}/p\mathbf{Z}$ est associé son *symbole de Legendre*

$$\left(\frac{x}{p}\right) = \begin{cases} x^{\frac{p-1}{2}} & \text{si} \quad x \neq 0 \\ \quad 0 & \text{si} \quad x = 0. \end{cases}$$

Pour $x \in (\mathbf{Z}/p\mathbf{Z})^*$, on observe que $x^{\frac{p-1}{2}} \in \{\pm 1\}$, et $x^{\frac{p-1}{2}} = 1$ si et seulement si x est un carré dans $(\mathbf{Z}/p\mathbf{Z})^*$. Quitte à identifier (abusivement !) le 1 de $(\mathbf{Z}/p\mathbf{Z})^*$ et celui de $\mathbf{C}^*$, on peut considérer le symbole de Legendre $x \longmapsto \left(\frac{x}{p}\right)$ comme un homomorphisme $(\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \mathbf{C}^*$ à valeurs dans $\{\pm 1\}$; c'est alors un caractère linéaire.

Pour $y \in \mathbf{Z}$ de classe $x \in \mathbf{Z}/p\mathbf{Z}$, on pose $\left(\frac{y}{p}\right) = \left(\frac{x}{p}\right)$. Alors $\left(\frac{y}{p}\right) = 1$ si et seulement si $y \in \mathbf{Z}$ est un carré modulo p. Les égalités

$$\left(\frac{1}{p}\right) = 1, \qquad \left(\frac{-1}{p}\right) = (-1)^{\epsilon(p)}, \qquad \left(\frac{2}{p}\right) = (-1)^{\omega(p)}$$

sont classiques. Rappelons encore la *loi de réciprocité quadratique*[2] : si ℓ, p sont deux nombres premiers impairs distincts, alors

$$\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)(-1)^{\epsilon(\ell)\epsilon(p)}.$$

Pour tout ceci (et bien plus), voir par exemple le chapitre I de [Serre–70].

La théorie de la représentation des groupes finis, qui fut crée par G. Frobenius dans des articles de 1896 et 1897, doit beaucoup à l'usage (plus ou moins explicite) de caractères linéaires en théorie des nombres par les illustres prédécesseurs des XVIIIe (Lagrange) et XIXe siècles (Legendre, Gauss, Dirichlet) [Curti–99].

---

[2]Loi énoncée par Euler, discutée par Legendre et démontrée par Gauss dans ses *Disquisitiones arithmeticae* de 1801, ... excusez du peu !

I.9. Proposition. *Soient π_1, π_2 deux représentations unitaires d'un même groupe G. Si π_1, π_2 sont équivalentes, alors π_1, π_2 sont unitairement équivalentes.*

Démonstration. Soient V_1, V_2 les espaces de π_1, π_2 et $S : V_1 \longrightarrow V_2$ un isomorphisme linéaire G–équivariant.

Notons $S^* : V_2 \longrightarrow V_1$ l'adjoint de S, et rappelons que l'opérateur $S^*S : V_1 \longrightarrow V_1$ possède une unique *racine carrée* positive, qui est un opérateur autoadjoint inversible ; nous le notons $\sqrt{S^*S}$. Posons $U = S(\sqrt{S^*S})^{-1}$; comme S, c'est un opérateur de source V_1 et de but V_2. Le calcul

$$\langle S(\sqrt{S^*S})^{-1}v \mid S(\sqrt{S^*S})^{-1}v'\rangle \;=\; \langle(\sqrt{S^*S})^{-1}S^*S(\sqrt{S^*S})^{-1}v \mid v'\rangle \;=\; \langle v \mid v'\rangle$$

(pour $v, v' \in V_1$) montre que U une isométrie, qui est de plus surjective puisque les dimensions de V_1 et V_2 sont égales.

On vérifie successivement que les opérateurs S^*, $\sqrt{S^*S}$ et U sont G–équivariants, d'où l'affirmation. $\square$

Exercices

I.E1 Pour un entier $m \geq 1$, notons $\mu(m)$ le groupe des racines m–ièmes de l'unité ; c'est un sous–groupe du groupe multiplicatif $\mathbf{C}^*$.

Vérifier que, pour tout entier $j \in \{0, 1, \ldots, m-1\}$, l'application $\mu(m) \longrightarrow \mathbf{C}^*$, $\omega \longmapsto \omega^j$ est un caractère linéaire de $\mu(m)$. Montrer que tout caractère de $\mu(m)$ est l'un de ceux–ci.

En particulier, avec des notations insipirées de celles de l'exemple I.8, les trois caractères du groupe $(\mathbf{Z}/8\mathbf{Z})^*$ distincts du caractère unité sont $(-1)^\epsilon$, $(-1)^\omega$ et $(-1)^{\epsilon+\omega}$.

I.E2 Soient G un groupe abélien fini, H un sous–groupe de G et $\chi : H \longrightarrow \mathbf{C}^*$ un caractère linéaire. Montrer qu'il existe un caractère linéaire $\chi' : G \longrightarrow \mathbf{C}^*$ qui prolonge χ.

[Indication : on peut procéder par récurrence sur l'indice de H dans G.]

I.E3 Pour tout entier $k \geq 2$, écrire 2^k caractères linéaires distincts du 2–groupe élémentaire $(\mathbf{Z}/2\mathbf{Z})^k$. Montrer qu'il n'y a pas d'autre caractère.

I.E4 Soient $\mathbf{k}$ un corps fini, $n \geq 2$ un entier, et $GL_n(\mathbf{k})$ le groupe linéaire correspondant ; on suppose le corps $\mathbf{k}$ distinct du corps à deux éléments. Ecrire un caractère linéaire de $GL_n(\mathbf{k})$ distinct du caractère unité. [Rappel : tout sous–groupe fini du groupe multiplicatif d'un corps est un groupe cyclique.]

I.E5 Pour tout entier $k \geq 2$, écrire un caractère linéaire du groupe symétrique de k objets distinct du caractère unité.

II.E6 Consulter l'encyclopédie WikipediA à "group representation" et aux entrées adjacentes — ou toute autre encycopédie raisonnable.

II. Sous–représentations et sommes directes

Soit $\pi : G \longrightarrow GL(V)$ une représentation d'un groupe G dans un espace vectoriel V. Un sous–espace vectoriel W de V est dit *invariant* ou *stable* par π si $\pi(g)(W) \subset W$ pour tout $g \in G$. Dans ce cas, l'homomorphisme

$$G \longrightarrow GL(W),\ g \longmapsto \pi(g)|_W$$

est une *sous–représentation* de π.

Les sous–espaces $\{0\}$ et V sont évidemment toujours invariants ; ce sont les sous–espaces invariants *triviaux.*

II.1. Exemple. Soient $G \times X \longrightarrow X$ une action, $V = \mathbf{K}^{(X)}$ et $\pi : G \longrightarrow GL(V)$ la représentation de permutation associée, comme à l'exemple I.2.

Le sous–espace V_{cst} des fonctions constantes est évidemment invariant par π. Si X est infini, ce sous–espace est réduit à $\{0\}$. Si X est fini, ce sous–espace est de dimension 1 et la sous–représentation correspondante π_{cst} est équivalente au caractère principal (exemple I.4).

Soient Y un sous–ensemble de X et W le sous–espace de V formé des fonctions à supports dans Y. Alors l'espace W est invariant par π si et seulement si l'ensemble Y est invariant par G, c'est–à–dire si et seulement si $g(Y) = Y$ pour tout $g \in G$.

Le sous–espace V_0 des fonctions à supports finis φ de X dans $\mathbf{K}$ telles que $\sum_{x\in X} \varphi(x) = 0$ est aussi invariant et fournit une sous–représentation π_0 de π.

II.2. Rappel et définition. Soient V un espace vectoriel et V_1, V_2 deux sous–espaces vectoriels de V. On dit que V est *somme directe* de V_1 et V_2 si tout vecteur $v \in V$ s'écrit de manière unique sous la forme $v = v_1 + v_2$ avec $v_1 \in V_1$ et $v_2 \in V_2$; on écrit alors $V = V_1 \oplus V_2$. Le sous–espace V_2 est dit *supplémentaire* du sous–espace V_1. L'application

$$p_1 : \begin{cases} V \longrightarrow V_1 \\ v \longmapsto v_1 \end{cases}$$

est la *projection* de V sur V_1 correspondant à la décomposition $V = V_1 \oplus V_2$ (attention ! p_1 dépend de V_1 ET de V_2). On vérifie que

p_1 est une application linéaire telle que $p_1(v) = v$ pour tout $v \in V_1$,
$V_1 = \mathrm{Im}(p_1)$,
$V_2 = \mathrm{Ker}(p_1)$.

Réciproquement, soit $p \in \mathcal{L}(V)$ une application *idempotente*, c'est–à–dire telle que $p^2 = p$, ou de manière équivalente telle que $p(v) = v$ pour tout $v \in \mathrm{Im}(p)$. Si $V_1 = \mathrm{Im}(p)$ et $V_2 = \mathrm{Ker}(p)$, alors V est la somme directe $V_1 \oplus V_2$, car tout vecteur $v \in V$ s'écrit $v = p(v) + (v - p(v))$, et $V_1 \cap V_2 = \{0\}$.

Lorsque V est de dimension finie, deux sous–espaces V_1, V_2 de V fournissent une décomposition en somme directe $V = V_1 \oplus V_2$ si et seulement si $V_1 \cap V_2 = \{0\}$ et $\dim(V) = \dim(V_1) + \dim(V_2)$.

Une représentation π d'un groupe G dans un espace vectoriel V est dite *somme directe* de deux sous–représentations π_1 et π_2, et on écrit $\pi = \pi_1 \oplus \pi_2$, s'il existe deux sous–espaces vectoriels V_1, V_2 de V invariants par π tels que $V = V_1 \oplus V_2$, les notations étant telles que $\pi_j(g)$ soit la restriction de $\pi(g)$ à V_j pour tout $g \in G$ et pour $j = 1, 2$.

II.3. Exemple. Soient X un ensemble fini, n le nombre de ses éléments, G un groupe de permutations de X et $\pi : G \longrightarrow GL(\mathbf{K}^X)$ la représentation correspondante ; on reprend les notations de l'exemple II.1. Alors π est somme directe des sous–représentations π_{cst} de degré 1 et π_0 de degré $n-1$.

Voir les numéros VII.7 à VII.9 pour des décompositions plus fines de π en sommes directes de sous–représentations.

II.4. Exemple. Soit π la représentation du groupe additif[3] $\mathbf{Z}$ dans $\mathbf{C}^2$ définie par

$$\pi(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \qquad \text{pour tout} \quad t \in \mathbf{Z}.$$

L'espace $\mathbf{C}^2$ possède un sous–espace invariant "évident" V_1 formé des vecteurs $\begin{pmatrix} x \\ 0 \end{pmatrix}$ avec $x \in \mathbf{C}$. Il n'y a pas de sous–espace invariant de V autre que V_1 et les deux sous–espaces triviaux (qui sont $\{0\}$ et $\mathbf{C}^2$ tout entier).

En effet, supposons qu'il existe un sous–espace W non réduit à $\{0\}$, distinct de V_1, et invariant par π. Il existe donc dans W un vecteur $\begin{pmatrix} x \\ y \end{pmatrix}$ tel que $y \neq 0$. Alors W contient aussi le vecteur

$$\begin{pmatrix} x \\ y \end{pmatrix} - \pi(1)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} x+y \\ y \end{pmatrix} = \begin{pmatrix} -y \\ 0 \end{pmatrix}$$

et par suite $W \supset V_1$, dont on déduit que $W = V$. Ainsi, le sous–espace invariant V_1 de V *n'admet pas* de supplémentaire invariant par π.

Le théorème qui suit (dans lequel il est important que $\mathbf{K}$ soit de caractéristique 0) montre que cette circonstance n'apparaît pas lorsque le groupe G est fini.

La propriété de la représentation π à noter est que les matrices $\pi(t)$ sont *unipotentes*, c'est–à–dire que la seule valeur propre des matrices $\pi(t) - \mathrm{id}_V$ est 0, et non pas le fait que les matrices $\pi(t)$ sont triangulaires. Pour s'en assurer, on peut considérer une autre représentation du même groupe $\mathbf{Z}$ dans le même espace $\mathbf{C}^2$, par exemple la représentation ρ définie par

$$\rho(t) = \begin{pmatrix} e^t & e^t - 1 \\ 0 & 1 \end{pmatrix} \qquad \text{pour tout} \quad t \in \mathbf{Z}.$$

L'espace $\mathbf{C}^2$ possède cette fois deux sous–espaces invariants, à savoir V_1 et le sous–espace V_2 formé des vecteurs $\begin{pmatrix} y \\ -y \end{pmatrix}$ avec $y \in \mathbf{C}$. En fait, tous les vecteurs de V_2 sont fixes par G. Par suite, la représentation ρ est somme directe du caractère linéaire défini par V_1 et du caractère principal (correspondant à V_2).

[3] L'exemple vaut aussi pour une représentation du groupe additif $\mathbf{R}$ ou $\mathbf{C}$ définie par la même formule.

II.5. Théorème. *Soient G un groupe fini et $\pi : G \longrightarrow GL(V)$ une représentation de dimension finie. Tout sous–espace de V invariant par π admet un supplémentaire invariant.*

Première démonstration. Soit V_1 un sous–espace de V invariant par π. Soit W' un supplémentaire quelconque de V_1 dans V est soit q la projection de V sur V_1 de noyau W'. Posons

$$p \;=\; \frac{1}{|G|}\sum_{h \in G} \pi(h)q\pi(h^{-1}) \;\in\; \mathcal{L}(V).$$

Il est immédiat que l'image de p est dans V_1 et que $p(v) = v$ pour tout $v \in V_1$; par suite, $\mathrm{Im}(p) = V_1$ et p est une projection linéaire de V sur V_1. Pour tout $g \in G$, le calcul[4]

$$p\pi(g) \;=\; \frac{1}{|G|}\sum_{h \in G} \pi(h)q\pi(h^{-1}g) \;\overset{x=g^{-1}h}{=}\; \frac{1}{|G|}\sum_{x \in G} \pi(gx)q\pi(x^{-1}) \;=\; \pi(g)p$$

montre que le sous–espace $\mathrm{Ker}(p)$ de V est invariant par π ; c'est donc un supplémentaire invariant de V_1. $\square$

Seconde démonstration, qui vaut lorsque $\mathbf{K}$ est le corps des réels ou celui des complexes : elle résulte immédiatement des deux propositions suivantes, par ailleurs intéressantes en elles–mêmes.

II.6. Proposition. *Soient G un groupe, V un espace hermitien, $\pi : G \longrightarrow \mathcal{U}(V)$ une représentation unitaire et W un sous–espace de V invariant par π. L'orthogonal de W est aussi invariant par π.*

Démonstration. Toute opérateur unitaire sur V qui laisse un sous–espace W invariant laisse aussi invariant l'orthogonal de W. $\square$

II.7. Proposition. *Soient G un groupe fini, V un espace vectoriel complexe de dimension finie, et π une représentation linéaire de G dans V. Il existe une structure hermitienne sur V pour laquelle π est une représentation unitaire.*

Démonstration. Soit $V \times V \longrightarrow \mathbf{C},\ (v,w) \longmapsto \langle v \mid w\rangle$ un produit scalaire arbitraire sur V. Pour $v, w \in V$, posons

$$\langle\langle v \mid w \rangle\rangle \;=\; \frac{1}{|G|}\sum_{h \in G} \langle \pi(h)v \mid \pi(h)w\rangle.$$

On vérifie d'une part que $\langle\langle \cdot \mid \cdot \rangle\rangle$ est un produit scalaire sur V et d'autre part (par un calcul analogue à celui de la première démonstration du théorème II.5) qu'il est invariant par π au sens où

$$\langle\langle \pi(g)v \mid \pi(g)w \rangle\rangle \;=\; \langle\langle v \mid w \rangle\rangle$$

pour tous $g \in G$ et $v, w \in V$. Il en résulte que la représentation π est unitaire sur l'espace V muni du produit scalaire $\langle\langle \cdot \mid \cdot \rangle\rangle$. $\square$

Une variante de cet argument est esquissée à l'exercice II.E8.

[4] Noter l'analogie avec un changement de variable sous un signe d'intégration.

II.8. Exemple. Soient $\pi_j : G \longrightarrow GL(V_j)$, $j = 1, 2$, deux représentations d'un même groupe G. Notons $\mathcal{L}(V_1, V_2)$ l'espace vectoriel des applications linéaires de V_1 dans V_2 et posons

$$(\pi(g)\alpha)(v_1) \;=\; \pi_2(g)\left(\alpha(\pi_1(g^{-1})v_1)\right)$$

pour tous $g \in G$, $\alpha \in \mathcal{L}(V_1, V_2)$ et $v_1 \in V_1$. On vérifie que (exercice !) :

(i) $\pi(g)$ est inversible d'inverse $\pi(g^{-1})$ pour tout $g \in G$;
(ii) l'application $\pi : G \longrightarrow GL(\mathcal{L}(V_1, V_2))$ est une représentation de G ;
(iii) l'ensemble $\mathcal{L}(V_1, V_2)^G$ des applications linéaires $\alpha : V_1 \longrightarrow V_2$ qui sont G–équivariantes, c'est–à–dire telles que $\alpha\pi_1(g) = \pi_2(g)\alpha$ pour tout $g \in G$, ou de manière équivalente telles que $\pi(g)\alpha = \alpha$ pour tout $g \in G$, est un sous–espace vectoriel de $\mathcal{L}(V_1, V_2)$ invariant par π ;
(iv) il existe un isomorphisme linéaire dans $\mathcal{L}(V_1, V_2)^G$ si et seulement si les représentations π_1 et π_2 sont équivalentes.
(v) Pour la lectrice[5] connaissant le produit tensoriel (voir le chapitre XII), préciser et montrer l'énoncé suivant : si V_1 est de dimension finie, la représentation π est équivalente au produit tensoriel de la contragrédiente de π_1 avec π_2.

II.9. Exemple. Conservons les notations de l'exemple précédent. Notons de plus V la somme directe $V_1 \oplus V_2$ et $p_j : V \longrightarrow V_j$ la projection canonique ($j = 1, 2$).

Soit Γ l'ensemble des sous–espaces vectoriels W de V tels que la restriction de p_1 soit un isomorphisme de W sur V_1 et soit

$$\gamma \,:\, \begin{cases} \mathcal{L}(V_1, V_2) \longrightarrow & \Gamma \\ \quad\alpha \qquad\longmapsto & \{(x, y) \in V_1 \oplus V_2 \mid y = \alpha(x)\} \end{cases}$$

l'application qui associe à un opérateur linéaire son graphe. Le groupe G agit sur l'espace $\mathcal{L}(V_1, V_2)$ par la représentation π et sur l'ensemble Γ par

$$(g, W) \longmapsto (\pi_1(g) \oplus \pi_2(g))(W).$$

On vérifie que γ est une bijection G–équivariante.

II.10. Exemple. Soient $n \geq 1$ un entier, $\mathbf{K}$ un corps et λ la représentation du groupe général linéaire $GL_n(\mathbf{K})$ dans l'algèbre de matrices $M_n(\mathbf{K})$ définie par la multiplication à gauche : $\lambda(g)(a) = ga$ pour tous $g \in GL_n(\mathbf{K})$ et $a \in M_n(\mathbf{K})$.

Pour tout $j \in \{1, \ldots, j\}$, notons V_j le sous–espace de $M_n(\mathbf{K})$ constitué des matrices dont les colonnes autres que la j–ième sont nulles. Alors V_j est un sous–espace invariant de $M_n(\mathbf{K})$; la sous–représentation correspondante λ_j de λ est équivalente à la représentation tautologique de $GL_n(\mathbf{K})$ dans $\mathbf{K}^n$, et $\lambda = \bigoplus_{j=1}^n \lambda_j$.

Plus généralement, la multiplication à gauche de $GL_n(\mathbf{K})$ dans l'espace $M_{n,n'}(\mathbf{K})$ des matrices à n lignes et n' colonnes fournit une représentation de $GL_n(\mathbf{K})$ équivalente à la somme directe de n' copies de la représentation tautologique.

II.11. Digression différentiable. L'idée à la base des démonstrations II.5 et II.7, qui est le procédé de moyenne par un groupe fini, est utile en dehors du cadre linéaire. Considérons par exemple un groupe fini G de difféomorphismes d'un espace $\mathbf{R}^n$ préservant l'origine.

[5] L'usage du féminin est notamment un clin d'oeil admiratif vers le beau livre de T.W. Körner [Körne–88].

Assertion : il existe des voisinages G–invariants $\mathcal{U}$ et $\mathcal{V}$ de l'origine dans $\mathbf{R}^n$ et un difféomorphisme $\varphi : \mathcal{V} \longrightarrow \mathcal{U}$ tels que $\varphi g \varphi^{-1}$ soit la restriction à $\mathcal{U}$ d'un automorphisme linéaire de $\mathbf{R}^n$, de sorte que $g \longmapsto \varphi g \varphi^{-1}$ est une représentation de G dans $\mathbf{R}^n$.

En effet, si g'_0 désigne la dérivée à l'origine du difféomorphisme $g \in G$, la règle de dérivation des fonctions composées montre que l'application

$$\pi \, : \, G \longrightarrow GL(\mathbf{R}^n), \quad g \longmapsto g'_0$$

est une représentation linéaire et le théorème des fonctions implicites que l'application

$$\varphi \, : \, \mathbf{R}^n \longrightarrow \mathbf{R}^n, \quad x \longmapsto \frac{1}{|G|} \sum_{h \in G} h'_0 \left(h^{-1}(x) \right)$$

est un difféomorphisme local ; de plus, $g'_0 \varphi = \varphi g$ pour tout $g \in G$. En restreignant convenablement φ une première fois, on obtient un difféomorphisme d'un voisinage $\mathcal{V}'$ sur un voisinage $\mathcal{U}'$ de l'origine. En restreignant une seconde fois φ à $\mathcal{V} = \bigcap_{g \in G} g(\mathcal{V}')$, on obtient un difféomorphisme, encore noté φ, d'un voisinage $\mathcal{V}$ de l'origine invariant par l'action donnée sur un voisinage $\mathcal{U}$ de l'origine invariant par la représentation π, tel que

$$g'_0 \, = \, \varphi g \varphi^{-1} \qquad \text{pour tout} \quad g \in G.$$

Il en résulte notamment que, au voisinage de l'origine, l'ensemble

$$\{x \in \mathbf{R}^n \mid gx = x \quad \text{pour tout} \quad g \in G\}$$

des points fixes est une *sous–variété différentiable* de $\mathbf{R}^n$.

Exercices

II.E1 Soient X l'ensemble des faces d'un cube centré à l'origine de $\mathbf{R}^3$ et $V = \mathbf{C}^X$. Notons G_C le *groupe du cube*[6], c'est–à–dire le groupe des isométries de $\mathbf{R}^3$ laissant le cube invariant ; c'est un sous–groupe du groupe orthogonal $\mathcal{O}(3)$ qui, à conjugaison près, ne dépend pas du choix du cube. Notons $\pi : G_C \longrightarrow GL(V)$ la représentation de permutation associée à l'action naturelle de G_C sur X et π_{pair} [respectivement π_{imp}] la sous–représentation de π sur l'espace des fonctions paires [resp. impaires] de V.

Vérifier que π est somme directe de π_{pair} et π_{imp}, et décomposer π_{pair} en somme directe de deux sous–représentations.

II.E2 Soient ω_1, ω_2 deux nombres complexes non nuls distincts, et $\pi : \mathbf{Z} \longrightarrow GL_2(\mathbf{C})$ la représentation définie par

$$\pi(j) \, = \, \begin{pmatrix} \omega_1^j & 0 \\ 0 & \omega_2^j \end{pmatrix} \qquad \text{pour tout} \quad j \in \mathbf{Z}.$$

Dresser la liste de tous les sous–espaces invariants de $\mathbf{C}^2$.

---

[6]Rappel du cours d'algèbre linéaire : G_C est un groupe à 48 éléments, isomorphe au produit direct du groupe symétrique de 4 objets et d'un groupe d'ordre deux.

Observer que, s'il existe un entier $k \geq 2$ tel que ω_1 et ω_2 sont des racines k–ièmes de l'unité, alors l'homomorphisme π peut être vu comme une représentation du groupe cyclique fini $\mathbf{Z}/k\mathbf{Z}$.

II.E3 Soient $\omega_1, \ldots, \omega_n$ des nombres complexes. Vérifier que

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ \omega_1 & \omega_2 & \omega_3 & \ldots & \omega_n \\ \omega_1^2 & \omega_2^2 & \omega_3^2 & \ldots & \omega_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \omega_1^{n-1} & \omega_2^{n-1} & \omega_3^{n-1} & \ldots & \omega_n^{n-1} \end{vmatrix} = \prod_{i>j}(\omega_i - \omega_j)$$

(*déterminant de Vandermonde*).

II.E4 Soit n un entier, $n \geq 2$. Soient $\omega_1, \ldots, \omega_n$ des nombres complexes non nuls distincts deux à deux, $\pi : \mathbf{Z} \longrightarrow GL_n(\mathbf{C})$ la représentation définie par

$$\pi(j) = \operatorname{diag}((\omega_1)^j, \ldots, (\omega_n)^j) \qquad \text{pour tout} \quad j \in \mathbf{Z}$$

(où "diag$(\cdots)$" désigne une matrice diagonale) et $v \in \mathbf{C}^n$ un vecteur de coordonnées non nulles. Déduire de (iii) que tout sous–espace de $\mathbf{C}^n$ contenant v et invariant par π est l'espace $\mathbf{C}^n$ tout entier.

II.E5 Formuler un analogue de l'exercice II.E2 pour des représentations dans $\mathbf{C}^n$, pour tout $n \geq 2$.

Pour une autre perspective sur les exercices II.E2 et II.E5, voir la remarque (ii) qui suit la proposition III.3.

II.E6 On considère un entier $k \geq 2$, le groupe symétrique $\mathrm{Sym}(k)$, la signature σ : $\mathrm{Sym}(k) \longrightarrow \{1, -1\}$ et la droite $V \subset \mathbf{C}[\mathrm{Sym}(k)]$ engendrée par σ.

Vérifier que V est un sous–espace de $\mathbf{C}[\mathrm{Sym}(k)]$ invariant par la représentation régulière gauche, et que la sous–représentation correspondante est équivalente à σ.

Rédiger un énoncé général pour un caractère linéaire d'un groupe fini dont l'énoncé ci–dessus soit un cas particulier.

II.E7 Vérifier les assertions suivantes, concernant les sous–espaces invariants dans les situations des exemples I.5, I.6 et I.7, dont on reprend les notations.

Un sous–espace de V est invariant pour la représentation $\underline{\pi} : G/N \longrightarrow GL(V)$ si et seulement s'il est invariant par la représentation $\pi : G \longrightarrow GL(V)$.

Un sous–espace de V est invariant par la représentation $\pi \circ \alpha : G \longrightarrow GL(V)$ si et seulement s'il est invariant par la représentation π.

Pour un sous–espace vectoriel W de V, posons[7] $W^\circ = \{\varphi \in V' \mid \varphi(W) = \{0\}\}$. Alors W° est invariant par la représentation contragrédiente $\check{\pi}$ si et seulement si W est invariant par π.

[7] Si V est un espace hermitien, l'application linéaire $v \longmapsto (u \longmapsto \langle v \mid u \rangle)$ est un isomorphisme de V sur V' par lequel $W^\perp$ corresond â W°.

II.E8 Soient G un groupe fini, V un espace hermitien et $\pi : G \longrightarrow GL(V)$ une représentation. Montrer qu'il existe un opérateur inversible $S \in GL(V)$ tel que $S\pi(g)S^{-1} \in \mathcal{U}(V)$ pour tout $g \in G$.

Reformulation : tout sous–groupe fini de $GL_n(\mathbf{C})$ est conjugué à un sous–groupe de $\mathcal{U}(n)$. De même, tout sous–groupe fini de $SL_n(\mathbf{C})$ est conjugué à un sous–groupe de $S\mathcal{U}(n)$.

[Indication. Choisir pour S un opérateur positif tel que $S^2 = \frac{1}{|G|}\sum_{x\in G}\pi(x)^*\pi(x)$.

Rappel: un opérateur linéaire T sur un espace hermitien V est *positif* si $\langle v \mid Tv\rangle \geq 0$ pour tout $v \in V$. Un opérateur positif est nécessairement hermitien. Un opérateur hermitien est positif si et seulement si toutes ses valeurs propres sont positives, et positif inversible si et seulement si toutes ses valeurs propres sont strictement positives. Un opérateur positif possède une unique racine carrée positive.]

III. Représentations irréductibles

Une représentation linéaire $\pi : G \longrightarrow GL(V)$ est *irréductible* si V n'est pas réduit à $\{0\}$ et si V ne possède aucun sous–espace invariant par π distinct de $\{0\}$ et V.

Par exemple, toute représentation de degré 1 est irréductible.

La représentation naturelle, dite aussi *tautologique*, de $GL_2(\mathbf{K})$ dans $\mathbf{K}^2$ est irréductible (car l'action de $GL_2(\mathbf{K})$ sur le complémentaire de l'origine dans $\mathbf{K}^2$ est transitive). De même, la représentation naturelle du groupe unitaire $\mathcal{U}(2)$ dans $\mathbf{C}^2$ est irréductible.

Pour un groupe G et un quotient $Q = G/N$ comme à l'exemple I.5, la correspondance entre représentations de G de noyau contenant N et représentations de Q préserve l'irréductibilité.

Si π est α sont comme aux exemples I.6 et I.7, alors les trois conditions suivantes sont équivalentes : π est irréductible, $\pi\alpha$ est irréductible, $\check{\pi}$ est irréductible. (Voir l'exercice II.E7.)

III.1. Théorème. *Toute représentation linéaire d'un groupe fini est somme directe de représentations irréductibles.*

Démonstration. Soient G un groupe fini, V un espace vectoriel de dimension n finie et $\pi : G \longrightarrow GL(V)$ une représentation linéaire. Nous allons raisonner par récurrence sur n en utilisant le théorème II.5.

Si $n = 0$, il n'y a rien à montrer (une somme directe d'espaces vectoriels indexés par l'ensemble vide est l'espace réduit à $\{0\}$!). Si $n = 1$, il n'y a rien à montrer non plus (π est irréductible).

Supposons donc $n \geq 2$ et le théorème déjà montré pour les dimensions strictement inférieures. Si π est irréductible, il n'y a rien à montrer. Sinon, il existe un sous–espace invariant V_1 distinct de $\{0\}$ et V, et le théorème II.5 montre que π est somme de deux représentations de dimensions strictement inférieures à n. L'assertion à montrer résulte alors de l'hypothèse de récurrence. □

Remarques. (i) En général, on peut avoir des décompositions π–invariantes $V = V_1 \oplus \cdots \oplus V_k = W_1 \oplus \cdots \oplus W_l$ telles que les restrictions de π aux V_i et aux W_j soient toutes irréductibles, *sans que* $\{V_1, \ldots, V_k\} = \{W_1, \ldots, W_l\}$. (Penser à une représentation du groupe à un élément.) Nous verrons toutefois plus bas qu'on a nécessairement $k = l$; voir aussi la remarque (i) suivant la proposition III.3.

(ii) L'exemple II.4 montre que l'assertion du théorème est en défaut pour les groupes infinis.

(iii) L'hypothèse implicite que la caractéristique du corps de référence est nulle ne peut pas non plus être omise.

(iv) Considérons exceptionellement un espace vectoriel V de dimension infinie, ainsi qu'une représentation π d'un groupe fini dans V. Si v est un vecteur non nul de V, le sous–espace de V engendré par les transformés $\pi(g)v$, pour $g \in G$, est d'une part invariant par π et d'autre part de dimension finie (donc distinct de V). La représentation π est donc réductible.

En d'autres termes, toute représentation irréductible d'un groupe fini est de dimension finie.

III.2. Corollaire. *Soit G un groupe fini.*

(i) Pour tout $g \in G$, $g \neq 1$, il existe une représentation irréductible π de G dans un espace vectoriel V telle que $\pi(g) \neq \mathrm{id}_V$.

(ii) Si G n'est pas commutatif, il existe au moins une représentation irréductible de G de degré ≥ 2.

Démonstration. Les deux assertions résultent de ce que la représentation régulière de G est d'une part fidèle et d'autre part une somme directe de représentations irréductibles. □

Une représentation π d'un groupe G dans un espace vectoriel V est *complètement réductible* si tout sous–espace de V qui est invariant par G possède un supplémentaire invariant. La proposition II.5 établit que toute représentation d'un groupe fini est complètement réductible. Ceci *ne s'étend pas*[8] aux groupes infinis, comme le montre l'exemple II.4 pour le groupe cyclique infini. La proposition qui suit montre quelques propriétés simples des représentations complètement réductibles ; pour en savoir plus, voir par exemple les numéros 2.4.1 et 3.1.4 de [GooWa–98].

III.3. Proposition. *Soit G un groupe (fini ou infini !).*

(i) Toute sous–représentation d'une représentation complètement réductible de G est complètement réductible.

(ii) Toute représentation complètement réductible de G est somme directe de sous–représentations irréductibles.

(iii) Toute somme directe de représentations irréductibles de G est complètement réductible.

Démonstration. (i) Soient $\pi : G \longrightarrow GL(V)$ une représentation complètement réductible de G et π_1 une sous–représentation de π, dans un sous–espace vectoriel V_1 de V. Soit V_2 un sous–espace invariant de V_1. Il s'agit de montrer qu'il existe un sous–espace invariant W_2 de V_1 tel que $V_1 = V_2 \oplus W_2$. On peut supposer V_2 strictement contenu dans V_1.

Nous affirmons qu'il existe un sous–espace invariant non nul W_2' de V_1 tel que $V_2 \cap W_2' = \{0\}$. En effet, comme π est complètement réductible, il existe un sous–espace invariant W' de V tel que $V_2 \oplus W' = V$. Mais $\dim(V_2) < \dim(V_1)$, donc W' est de codimension strictement supérieure à $\dim(V_1)$, et il suffit de poser $W_2' = V_1 \cap W'$.

[8]Ceci s'étend à *certains* groupes infinis, par exemple aux groupes $SL_d(\mathbf{R})$ et $SL_d(\mathbf{C})$, au moins si on ne considère que des représentations qui sont *continues* dans un sens approprié.

Si $V_2 \oplus W_2' = V_1$, la preuve est achevée. Sinon, on peut répéter l'argument pour le sous–espace invariant $V_2 \oplus W_2' \subset V_1$. Après un nombre fini de pas, on obtient un supplémentaire invariant de V_2 dans V_1.

(ii) Procédons par récurrence sur le degré n d'une représentation complètement réductible $\pi : G \longrightarrow GL(V)$. Si $n = 1$, la représentation π est irréductible et il n'y a rien à montrer. Supposons donc $n \geq 2$ et l'assertion (ii) établie jusqu'à $n-1$. Si π est irréductible, il n'y a rien à montrer non plus. Supposons donc de plus que π est réductible, c'est–à–dire qu'il existe un sous–espace invariant V_1 de V tel que $\{0\} \subsetneqq V_1 \subsetneqq V$; on peut supposer V_1 minimal pour ces propriétés, c'est–à–dire que la sous–représentation π_1 de π correspondant à V_1 est irréductible.

Par hypothèse de complète réductibilité, il existe un supplémentaire invariant W de V_1 ; la représentation de G dans W est complètement réductible, par l'assertion (i). La dimension de W étant strictement inférieure à celle de V, il résulte de l'hypothèse de récurrence que la sous–représentation de π correspondant à W est somme directe de représentations irréductibles $\pi_2, \ldots, \pi_k$. L'assertion (ii) résulte de ce que $\pi = \bigoplus_{j=1}^k \pi_j$.

(iii) Considérons une suite $\pi_j : G \longrightarrow GL(V_j)$, $j = 1, \ldots, k$, de représentations irréductibles de G, ainsi que la représentation somme directe $\pi = \bigoplus_{j=1}^k \pi_j$ de G dans l'espace $V = \bigoplus_{j=1}^k V_j$. Soit W un sous–espace invariant V ; il s'agit de montrer que W possède un supplémentaire invariant W' dans V, et nous allons procéder par récurrence sur la codimension de W. Si $\mathrm{codim}(W) = 0$, il n'y a rien à montrer. Supposons donc $\mathrm{codim}(W) > 0$, et l'assertion démontrée pour les codimensions strictement inférieures.

Par hypothèse, il existe $i \in \{1, \ldots, k\}$ tel que V_i n'est pas inclus dans W ; il résulte de l'irréductibilité de V_i que $V_i \cap W = \{0\}$, et donc que la somme $U = W + V_i$ est directe. Par hypothèse de récurrence, il existe un sous–espace supplémentaire invariant U' de U dans V, et il suffit de poser $W' = V_i \oplus U'$. □

Remarques. (i) Soit π une représentation complètement réductible d'un groupe G. Soient $\pi = \bigoplus_{i=1}^k \pi_i$ et $\pi = \bigoplus_{j=1}^\ell \pi_j'$ deux décompositions de π en sommes directes de sous–représentations irréductibles. Il est naturel de se demander si on a nécessairement $l = k$ et si, après renumérotation convenable des π_j', les représentations π_i et π_i' sont équivalentes.

La réponse est oui ; lorsque G est fini, voir le corollaire VII.4 et le théorème IX.9 ci–dessous. Pour une démonstration du cas général, voir par exemple le théorème 4 du chapitre 3 de [Vinbe–89], ou la proposition 3.1.6 de [GooWa–98], ou le *théorème de Krull–Schmidt* dans un livre exposant la théorie des modules sur les anneaux (qu'on peut appliquer ici au sous–anneau de $\mathcal{L}(V)$ engendré par l'image de π).

(ii) La proposition précédente et le corollaire IV.2 (selon lequel les représentations d'un groupe abélien sont les représentations de degré 1), particularisés au groupe $\mathbf{Z}$, fournissent une solution de l'exercice II.E5.

(iii) Avec les notations de l'exemple II.4, la représentation π de $\mathbf{Z}$ n'est pas complètement réductible alors que la représentation ρ l'est.

III.4. Corollaire. *Toute somme directe de représentations complètement réductibles est encore complètement réductible.*

On sait de même que, en caractéristique zéro, tout produit tensoriel (voir le chapitre XII) de représentations complètement réductibles est encore complètement réductible ; voir [Cheva–55], chapitre IV, § 5, proposition 2. Mais la démonstration de Chevalley utilise des outils de géométrie algébrique (topologie de Zariski). L'assertion ne s'étend en charactéristique p que pour p assez grand, relativement aux dimensions des G–modules impliqués ; voir la page 17 des *Moursund Lectures* de Serre (1998).)

Exercices

III.E1 Soient $k \geq 3$ un entier, r une rotation d'ordre k du plan euclidien et s une symétrie de ce plan relativement à une droite, de sorte que les transformations

$$1, r, \ldots, r^{k-1}, s, sr, \ldots, sr^{k-1}$$

constituent un *groupe diédral d'ordre* $2k$, noté[9] D_{2k}. C'est aussi le groupe des isométries du plan laissant invariant un polygone régulier à k côtés centré à l'origine ; noter que le groupe D_6 opère sur les trois sommets d'un triangle et qu'il est isomorphe au groupe symétrique Sym(3).

Soit ω une racine $k$ième de l'unité ; on suppose que $\omega \neq 1$ et $\omega \neq -1$ (la seconde hypothèse est automatique si k est impair). Vérifier qu'on définit une représentation π_ω de D_{2k} dans $\mathbf{C}^2$ en posant

$$\pi_\omega(r^j) = \begin{pmatrix} \omega^j & 0 \\ 0 & \overline{\omega}^j \end{pmatrix} \qquad \text{et} \qquad \pi_\omega(sr^j) = \begin{pmatrix} 0 & \overline{\omega}^j \\ \omega^j & 0 \end{pmatrix} \qquad (j = 0, \ldots, k-1).$$

Montrer que cette représentation est irréductible. [Utiliser l'exercice II.E2.]

Soit ω' une seconde racine $k$ième de l'unité. Si $\omega' \neq \omega$ et $\omega' \neq \overline{\omega}$, vérifer que les représentations π_ω et $\pi_{\omega'}$ ne sont pas équivalentes. [Utiliser pour cela la théorie du chapitre V.]

Nous verrons au chapitre IX que les seules représentations irréductibles du groupe D_{2k} sont, à équivalence près, des caractères linéaires et des représentations de degré deux du type ci–dessus.

Que devient ce qui précède si $k = 1$ ou $k = 2$?

III.E2 Notons Q le groupe des quaternions, et $\{\pm 1, \pm i, \pm j, \pm k\}$ ses éléments.

Vérifier qu'on définit une représentation π de Q dans $\mathbf{C}^2$ en posant

$$\pi(\pm 1) = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \pi(\pm i) = \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$
$$\pi(\pm j) = \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad \pi(\pm k) = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Montrer que cette représentation est irréductible.

III.E3 Vérifier que le groupe $D(Q)$ des commutateurs de Q est le groupe à deux éléments $\{1, -1\}$ et que l'abélianisé de Q, c'est–à–dire le quotient $Q/D(Q)$, s'identifie à $(\mathbf{Z}/2\mathbf{Z})^2$. En déduire que le groupe Q possède quatre caractères linéaires (voir l'exercice I.E3).

Rappel : le *groupe dérivé* ou *groupe des commutateurs* d'un groupe G est le sous–groupe $D(G)$ engendré par les commutateurs, c'est–à–dire par les éléments de la forme $g^{-1}h^{-1}gh$. *L'abélianisé* de G est le groupe quotient $G_{\text{ab}} = G/D(G)$.

[9]Certains auteurs notent D_k le groupe diédral d'ordre $2k$.

Nous verrons (exercice XI.E2) que le groupe Q possède, à équivalence près, exactement cinq représentations irréductibles qui sont la représentation de III.E2 et ces quatre caractères.

III.E4 Soient $m \geq 2$ un entier, C_m le groupe cyclique d'ordre m et t un générateur de C_m. Soient V un espace vectoriel complexe et $\pi : C_m \longrightarrow GL(V)$ une représentation. Pour $k \in \{0, \ldots, m-1\}$, on définit un endomorphisme linéaire p_k de V par

$$p_k(v) \;=\; \frac{1}{m} \sum_{j=0}^{m-1} \exp(-2i\pi jk/m)\pi(t^j)v.$$

Montrer que

$$\begin{aligned} p_j^2 \;&=\; p_j \qquad \text{pour tout} \quad j \in \{0, \ldots, m-1\} \;; \\ p_j p_k \;&=\; 0 \qquad \text{pour tous} \quad j, k \in \{0, \ldots, m-1\} \quad \text{avec} \quad j \neq k \;; \\ \sum_{j=0}^{m-1} p_j \;&=\; \mathrm{id}_V \;; \\ p_j \pi(t^\ell) \;&=\; \pi(t^\ell) p_j \qquad \text{pour tous} \quad j, \ell \in \{0, \ldots, m-1\}. \end{aligned}$$

Pour $j \in \{0, \ldots, m-1\}$, l'espace $V_j = \mathrm{Im}(p_j)$ est donc $\pi(C_m)$–invariant ; la restriction de π à V_j est la représentation π_j telle que $\pi_j(t^\ell) = \exp(2i\pi j\ell/m)\,\mathrm{id}_V$ pour tout $t^\ell \in C_m$. La représentation π est somme directe des π_j.

Noter que cet argument vaut en toutes dimensions (finies ou non). Si V est de dimension finie, il fournit une preuve du théorème III.1 lorsque $G = C_m$. Si V est un espace de Banach, noter que les endomorphismes p_j sont continus et que les sous–espaces V_j sont fermés dans V.

IV. Lemme de Schur

On suppose désormais que le corps de référence est celui des nombres complexes : $\mathbf{K} = \mathbf{C}$ (ce qui suit s'étend à un corps algébriquement clos de caractéristique nulle). L'énoncé suivant est connu sous le nom de **lemme de Schur**. Rappelons qu'une *homothétie* d'un espace vectoriel V est un automorphisme linéaire de la forme $\mu\,\mathrm{id}_V$, où μ est un nombre du corps de base.

IV.1. Théorème. *Soient G un groupe, $\pi_j : G \longrightarrow GL(V_j)$, $j = 1, 2$, deux représentations irréductibles et $S : V_1 \longrightarrow V_2$ une application linéaire G–équivariante.*

(i) *Si $S \neq 0$, alors S est un isomorphisme. De plus, toute application linéaire G–équivariante $T : V_1 \longrightarrow V_2$ est un multiple scalaires de S.*
(ii) *Si $V_1 = V_2$ et $\pi_1 = \pi_2$, alors S est une homothétie.*
(iii) *Si les représentations π_1 et π_2 ne sont pas équivalentes, alors $S = 0$.*

Démonstration. Il est facile de vérifier que le noyau de S est $\pi_1(G)$–invariant et que son image est $\pi_2(G)$–invariante (c'est un exercice !).

(i_a) Si $S \neq 0$, alors $\mathrm{Ker}(S) \neq V_1$ et $\mathrm{Im}(S) \neq \{0\}$. Comme les représentations π_1 et π_2 sont irréductibles, nous avons nécessairement $\mathrm{Ker}(S) = \{0\}$ et $\mathrm{Im}(S) = V_2$, ce qui montre l'assertion.

(ii) Soit μ une valeur propre de S dans $\mathbf{C}$. L'application linéaire $T = S - \mu\,\mathrm{id}$ est G–équivariante et non inversible. Il résulte de (i) qu'elle est nulle, d'où l'assertion (ii).

(i_b) Par (ii), il existe $\mu \in \mathbf{C}$ tel que $S^{-1}T = \mu\,\mathrm{id}_{\mathrm{V}_1}$. Donc $T = \mu S$.

(iii) Cette assertion est une forme de la contraposée de (i). □

IV.2. Corollaire. *Soit $\pi : G \longrightarrow GL(V)$ une représentation irréductible d'un groupe G.*

(i) Si G est abélien, π est de degré 1.

(ii) Si π est de degré au moins 2, il existe $g, h \in G$ tels que $\pi(g)$ et $\pi(h)$ ne commutent pas.

Remarques. (i) Comparer avec le corollaire III.2.

(ii) Pour le lemme de Schur et le corollaire IV.2, il n'est pas utile de supposer G fini. Dans le cadre adopté dans ce cours, la dimension de V est finie ; toutefois, le lemme de Schur et le corollaire IV.2 sont vrais dans d'autres contextes, par exemple celui des représentations unitaires continues des groupes topologiques dans les espaces de Hilbert. (Une représentation est alors *irréductible* si les seuls sous–espaces invariants *fermés* sont $\{0\}$ et l'espace tout entier.)

(iii) L'hypothèse que le corps de base, ici $\mathbf{C}$, est algébriquement clos ne peut être omise. En effet, pour tout entier $n \geq 3$, la représentation $\pi : \mathbf{Z}/n\mathbf{Z} \longrightarrow GL_2(\mathbf{R})$ définie par

$$\pi(j) \;=\; \begin{pmatrix} \cos(2\pi/j) & -\sin(2\pi/j) \\ \sin(2\pi/j) & \cos(2\pi/j) \end{pmatrix}, \qquad j \in \{0, 1, \ldots, n-1\},$$

est irréductible de degré 2.

Démonstration du corollaire IV.2. (i) Vu le lemme de Schur, $\pi(g)$ est une homothétie pour tout $g \in G$, et l'assertion est alors évidente.

(ii) Soit $g \in G$ tel que $\pi(g)$ commute à $\pi(h)$ pour tout $h \in G$. Alors $\pi(g)$ est une homothétie par le lemme de Schur. Si cela était le cas pour tout $g \in G$, tout sous–espace de V serait invariant par G, ce qui est absurde pour une représentation complexe, irréductible, de degré deux ou davantage ; il existe donc $g, h \in G$ tels que $\pi(g^{-1})\pi(h^{-1})\pi(g)\pi(h) \neq \mathrm{id}_V$, et il en résulte que π est de degré au moins 2. □

IV.3. Corollaire. *Soient V un espace hermitien et $\pi : G \longrightarrow \mathcal{U}(V)$ une représentation unitaire irréductible d'un groupe G. Toute forme hermitienne $\Phi : V \times V \longrightarrow \mathbf{C}$ telle que $\Phi(\pi(g)v, \pi(g)w) = \Phi(v, w)$ pour tous $g \in G$ et $v, w \in V$ est un multiple réel du produit scalaire.*

Démonstration. Notons comme d'habitude $\langle\cdot|\cdot\rangle$ le produit scalaire sur V. Pour tout $v \in V$, la forme linéaire $w \longmapsto \Phi(v, w)$ peut s'écrire $w \longmapsto \langle u_v \mid w\rangle$, où u_v est un vecteur de V dépendant de v. On s'assure que cette dépendance est linéaire, de sorte qu'il existe un endomorphisme linéaire A de V tel que $\Phi(v, w) = \langle Av \mid w\rangle$ pour tous $v, w \in V$.

Soit $g \in G$; nous avons

$$\begin{aligned} \Phi(\pi(g)v, \pi(g)w) \;&=\; \langle A\pi(g)v \mid \pi(g)w\rangle \;=\; \langle \pi(g)^* A\pi(g)v \mid w\rangle \\ &=\; \Phi(v, w) \;=\; \langle Av \mid w\rangle \end{aligned}$$

pour tous $v, w \in V$, de sorte que $\pi(g)^* A \pi(g) = A$, ou encore $A\pi(g) = \pi(g)A$ par unitarité de π. Il résulte donc du lemme de Schur qu'il existe un nombre complexe μ tel que $A = \mu\,\mathrm{id}_V$, et par suite que $\Phi(v, w) = \overline{\mu}\langle v \mid w\rangle$ pour tous $v, w \in V$.

Notons pour terminer que $\Phi(v, v) = \overline{\mu}\langle v \mid v\rangle$ pour tout $v \in V$, d'où il résulte que le nombre μ est réel. □

IV.4. Remarque. Voici une nouvelle preuve de la proposition I.9, pour le cas de deux représentations unitaires π_1, π_2 qui sont *irréductibles*.

Par hypothèse, il existe un isomorphisme linéaire S de V_1 sur V_2 tel que $S\pi_1(g) = \pi_2(g)S$ pour tout $g \in G$. La forme sesquilinéaire

$$\Phi \,:\, V_1 \times V_1 \longrightarrow \mathbf{C}, \qquad (v, w) \longmapsto \langle Sv \mid Sw\rangle_2$$

est hermitienne, positive, non nulle, et $\pi_1(G)$–invariante. Par le corollaire IV.3, il existe un nombre réel $\mu > 0$ tel que $\langle Sv \mid Sw\rangle_2 = \mu\langle v \mid w\rangle_1$ pour tous $v, w \in V_1$. Notons T l'isomorphisme linéaire $(1/\sqrt{\mu})S$; alors T est encore équivariant ($T\pi_1(g) = \pi_2(g)T$ pour tout $g \in G$) et c'est une isométrie (car $\langle Tv \mid Tw\rangle_2 = \langle v \mid w\rangle_1$ pour tous $v, w \in V$) ; c'est une isométrie surjective (car $\dim(V_1) = \dim(V_2)$), et ceci achève la démonstration.

IV.5. Corollaire. *Soit G un groupe fini possédant une représentation irréductible fidèle. Alors le centre $Z(G)$ de G est cyclique.*

Démonstration. Soit $\pi : G \longrightarrow GL(V)$ une représentation irréductible de G. Par le lemme de Schur, la restriction de π au centre de G est de la forme $g \longmapsto z_g\,\mathrm{id}_V$, où l'application $g \longmapsto z_g$ de $Z(G)$ dans $\mathbf{C}^*$ est un caractère linéaire. Si la représentation π est fidèle, $Z(G)$ s'identifie à un sous–groupe fini de $\mathbf{C}^*$. Or tout sous–groupe fini de $\mathbf{C}^*$ (plus généralement du groupe multiplicatif d'un corps) est cyclique. □

IV.6. Corollaire. *Soient G un groupe fini et H un sous–groupe abélien de G. Alors le degré de toute représentation irréductible complexe de G est majoré par l'indice $[G : H]$.*

Démonstration. Soit $\pi : G \longrightarrow GL(V)$ une représentation irréductible de G. Comme la restriction de π à H se décompose en une somme directe de sous–représentations de degré 1, on peut choisir une droite D de V qui est $\pi(H)$–invariante.

Notons n l'indice $[G : H]$ et choisissons des représentants $t_1, \ldots, t_n$ des classes de G/H, de sorte que G est une réunion disjointe $\sqcup_{j=1}^n t_j H$. Soit W le sous–espace vectoriel de V somme sur $g \in G$ des espaces $\pi(g)D$. (Attention : il faut bien lire "somme", et non pas "somme directe" !) Le sous–espace W de V est d'une part invariant par $\pi(G)$, donc égal à V par irréductiblité. Ce sous–espace est d'autre part la somme sur $j \in \{1, \ldots, n\}$ des espaces $\pi(t_j)D$, et donc de dimension au plus n. □

Remarque. Nous verrons au chapitre X une autre contrainte sur le degré de ρ : il doit diviser l'ordre de G. On sait même qu'il doit diviser l'ordre du quotient de G par un sous-groupe abélien normal (par exemple l'ordre du quotient de G par son centre).

IV.7. Exemple, séries de Fourier. Notons $\mathbf{T}$ le groupe multiplicatif des nombres complexes de module 1 ; c'est un groupe abélien compact, déjà rencontré au chapitre

I avec la notation $\mathcal{U}(1)$. Il résulte du lemme de Schur (corollaire IV.2) que toutes ses représentations irréductibles sont de degré un.

Pour tout nombre réel k, l'homomorphisme

$$\pi_k \,:\, \mathbf{R} \longrightarrow \mathbf{T}, \qquad t \longmapsto e^{2i\pi kt}$$

est une représentation unitaire continue de $\mathbf{R}$, de dimension un et donc irréductible. (On peut montrer que toute représentation unitaire continue irréductible de $\mathbf{R}$ est l'une de celles-ci.) Lorsque k est entier, le noyau de π_k contient $\mathbf{Z}$, de sorte qu'on peut voir π_k comme une représentation unitaire continue du quotient $\mathbf{R}/\mathbf{Z}$. (On peut montrer que toute représentation unitaire continue irréductible de $\mathbf{R}/\mathbf{Z}$ est l'une de celles-ci.)

Ces représentations jouent un rôle clé dans la théorie des séries de Fourier, puisque les coefficients de Fourier d'une fonction continue $f : \mathbf{R}/\mathbf{Z} \longrightarrow \mathbf{C}$ sont définis par

$$c_k(f) \;=\; \int_{\mathbf{R}/\mathbf{Z}} e^{-2i\pi kt} f(t)dt.$$

L'usage de la série de Fourier $\sum_{k\in\mathbf{Z}} c_k(f)e^{2i\pi kt}$ pour étudier la fonction continue f remonte au moins à Euler et doit son nom au mémoire de Fourier, *Théorie analytique de la chaleur,* de 1822. Mais il semble qu'il ait fallu attendre 1927 pour qu'Hermann Weyl établisse un lien quelconque entre l'analyse harmonique classique et la théorie des représenttions de groupes [Macke–80, page 603]. Voir aussi la remarque IX.11 ci-dessous.

Exercices

IV.E1 Soient G un groupe fini, $\pi : G \longrightarrow GL_n(\mathbf{R})$ une représentation réelle telle que[10] la composition $G \longrightarrow GL_n(\mathbf{R}) \subset GL_n(\mathbf{C})$ est irréductible, et $Q : \mathbf{R}^n \longrightarrow \mathbf{R}$ une forme quadratique $\pi(G)$–invariante, c'est–à–dire telle que $Q(\pi(g)v) = Q(v)$ pour tous $g \in G$ et $v \in \mathbf{R}^n$. Montrer que Q est ou bien positive, c'est–à–dire telle que $Q(v) \geq 0$ pour tout $v \in \mathbf{R}^n$, ou bien négative, c'est–à–dire telle que $-Q$ est positive.

[Indication. Soient B la forme bilinéaire sur $\mathbf{R}^n$ définie par $B(v,w) = \frac{1}{2}(Q(v+w) - Q(v) - Q(w))$. Montrer qu'il existe un produit scalaire sur $\mathbf{R}^n$ invaratiant par $\pi(G)$ en adaptant la démonstration de la proposition II.7 et que B est un multiple de ce produit scalaire en adaptant la démonstration du corollaire IV.3.]

IV.E2 Soient G un groupe fini, $\pi_j : G \longrightarrow GL(V_j)$, $j = 1, 2$, deux représentations linéaires complexes irréductibles et $S : V_2 \longrightarrow V_1$ une application linéaire. Soit T l'application linéaire définie par

$$T \;=\; \frac{1}{|G|} \sum_{x\in G} \pi_1(x) S \pi_2(x^{-1}).$$

Si $V_2 = V_1 = V$ et $\pi_1 = \pi_2$, montrer que T est une homothétie de rapport $\frac{1}{\dim V}\,\mathrm{trace}(S)$. Si π_1 et π_2 ne sont pas équivalentes, montrer que $T = 0$.

En particulier, si π est une représentation irréductible de G dans un espace V et si on applique ce qui précède à $S = \pi(a)$, on obtient d'abord

$$\frac{1}{|G|} \sum_{x\in G} \pi(xax^{-1}) \;=\; \frac{1}{\mathrm{degré}(\pi)}\, \mathrm{trace}(\pi(a))\, \mathrm{id}_V \,.$$

[10] On dit que π est *absolument irréductible.*

puis, en multipliant à droite par $\pi(b)$ et en prenant les traces :

$$\frac{1}{|G|}\sum_{x\in G}\operatorname{trace}(\pi(xax^{-1}b)) \;=\; \frac{1}{\text{degré}(\pi)}\operatorname{trace}(\pi(a))\operatorname{trace}(\pi(b))$$

pour tous $a, b \in G$. Nous revenons sur cette équation à l'exercice X.E3.

V. Caractères des représentations

Soit $\pi : G \longrightarrow GL(V)$ une représentation d'un groupe G. Le *caractère* de π est la fonction $\chi_\pi : G \longrightarrow \mathbf{K}$ définie par

$$\chi_\pi(g) \;=\; \operatorname{trace}(\pi(g))$$

pour tout $g \in G$.

Nous notons V^G le sous–espace de V formé des vecteurs invariants par G, c'est–à–dire des vecteurs $v \in V$ tels que $\pi(g)v = v$ pour tout $g \in G$. (Notation déjà utilisée à l'exemple II.8.) La dimension de V^G s'appelle la *multiplicité de la représentation unité dans la représentation* π. (Voir aussi la terminologie définie au corollaire VII.3.)

V.1. Proposition. *Soient π une représentation de degré n d'un groupe G (fini ou infini) et χ_π son caractère. Alors :*

(i) $\chi_\pi(1) = n$ *;*
(ii) $\chi_\pi(xgx^{-1}) = \chi_\pi(g)$ *pour tous* $x, g \in G$ *;*
(iii) $\chi_{\pi'} = \chi_\pi$ *pour toute représentation π' de G équivalente à π.*

Si $\pi = \pi_1 \oplus \pi_2$, alors

(iv) $\chi_\pi(g) = \chi_{\pi_1}(g) + \chi_{\pi_2}(g)$ *pour tout $g \in G$.*

Supposons de plus que G est un groupe fini et que π est une représentation dans un espace complexe *; notons $\check{\pi}$ la représentation contragrédiente de π. Alors :*

(v) $\chi_\pi(g^{-1}) = \overline{\chi_\pi(g)} = \chi_{\check{\pi}}(g)$ *pour tout $g \in G$;*
(vi) $|\chi_\pi(g)| \le n$ *pour tout $g \in G$;*
(vii) $\chi_\pi(g) = n$ *si et seulement si g est dans le noyau de π ;*
(viii) $|\chi_\pi(g)| = n$ *si et seulement si $\pi(g)$ est une homothétie ;*
(ix) $\dim_{\mathbf{C}}(V^G) = \frac{1}{|G|}\sum_{g\in G}\chi_\pi(g)$.

Démonstration. Les assertions (i) à (iv) résultent des propriétés de la trace. Dans la situation des assertions (v) à (ix), l'endomorphisme $\pi(g)$ est d'ordre fini pour tout $g \in G$. Il est donc diagonal relativement à une base convenable : $\pi(g) = \operatorname{diag}(\mu_1, \ldots, \mu_n)$, où $\mu_1, \ldots, \mu_n$ sont des racines complexes de l'unité. Par suite

$$\chi_\pi(g^{-1}) \;=\; \frac{1}{\mu_1} + \cdots + \frac{1}{\mu_n} \;=\; \overline{\mu_1} + \cdots + \overline{\mu_n} \;=\; \overline{\chi_\pi(g)},$$

ce qui montre la première égalité de (v). Le caractère de la représentation contragrédiente est donné par $\chi_{\check{\pi}}(g) = \chi_\pi(g^{-1})$, d'où la seconde égalité de (v). Les assertions (vi) et (vii) sont (encore plus...) immédiates. L'assertion (viii) résulte de ce qu'une somme de

n nombres compleses de module 1 est de valeur absolue n si et seulement si ces nombres complexes sont tous égaux.

Pour (ix), posons $p = \frac{1}{|G|}\sum_{x\in G}\pi(x) \in \mathcal{L}(V)$. Un calcul standard (voir par exemple la preuve du théorème II.5) montre que $\pi(g)p = p$ pour tout $g \in G$, et par suite que $p^2 = p$; par ailleurs, il est immédiat de vérifier que l'image de p coïncide avec V^G. Donc p est un projecteur de V sur V^G, et la décomposition $V = V^G \oplus \mathrm{Ker}(p)$ est G–invariante. Dans une base de V adaptée à cette décomposition, la matrice de p est diagonale, avec $\dim_{\mathbf{C}}(V^G)$ coefficients diagonaux 1 et les autres coefficients diagonaux nuls. Par suite $\dim_{\mathbf{C}}(V^G) = \mathrm{trace}(p) = \frac{1}{|G|}\sum_{g\in G}\chi_\pi(g)$. □

V.2. Remarques. (i) Le caractère d'une représentation de degré un est un caractère linéaire au sens de l'exemple I.4. Pour une représentation $\pi : G \longrightarrow \mathbf{K}^*$ de degré un, il n'y a pas lieu de distinguer entre π et son caractère. Répétons que, plus généralement (et abusivement), pour une représentation de degré un, on identifie souvent l'espace de π au corps de base, et donc la représentation à son caractère ; ceci s'applique en particulier au caractère unité du groupe G, noté parfois 1_G et parfois χ_1 (voir l'exemple I.4).

Soient G un groupe, π une représentation de degré n et χ son caractère. Si χ ne prend pas la valeur 0 et si $\chi : G \longrightarrow \mathbf{K}^*$ est un homomorphisme de groupes, alors $n = 1$, c'est–à–dire χ est un caractère linéaire. (C'est une conséquence immédiate de l'égalité $n^2 = \chi(1)^2 = \chi(1) = n$.)

(ii) En général, il reste indispensable de bien distinguer une représentation π d'un groupe G et son caractère χ_π.

(iii) Une fonction φ définie sur un groupe G est dite *centrale* si $\varphi(g_1g_2) = \varphi(g_2g_1)$ pour tous $g_1, g_2 \in G$, c'est–à–dire si φ est constante sur les classes de conjugaison. L'assertion (ii) dit que les caractères des représentations sont des fonctions centrales.

Noter que le caractère principal d'un groupe G appartient à $\mathbf{K}[G]$ si et seulement si le groupe G est fini. Pour un groupe infini, les caractères ne sont en général pas à supports finis (voir les exercices V.E4 à V.E6).

Les fonctions de G dans $\mathbf{K}$ qui sont centrales et à supports finis constituent un sous–espace vectoriel de $\mathbf{K}[G]$ que nous notons $\mathbf{K}[G]^G$. (La notation est justifiée par l'exercice V.E3.)

(iv) Vu l'importance de la représentation régulière (gauche ou droite ...) d'un groupe fini G, notons ici que son caractère χ est donné par $\chi(1) = |G|$ et $\chi(g) = 0$ si $g \neq 1$.

De même, si H est un sous–groupe de G, le caractère χ de la représentation quasi-régulière $\lambda_{G/H}$ définie à l'exemple I.3 est donné par $\chi(g) = |G/H|$ si $g \in H$ et $\chi(g) = 0$ sinon. (Pour cet exemple, il suffit de supposer H d'indice fini dans G.)

(v) C'est une conséquence des assertions (i) et (vii) que, pour un groupe fini, la représentation complexe de dimension n définie par $\pi(g) = 1$ est caractérisée par son caractère.

V.3. Exemple. Soient G un groupe fini opérant sur un ensemble fini X. Notons V l'espace $\mathbf{C}^X$ et $\pi : G \longrightarrow GL(V)$ la représentation de permutation associée. Rappelons que V possède une structure hermitienne naturelle pour laquelle la représentaiton π est unitaire, ainsi qu'une base canonique $(\epsilon_x)_{x\in X}$ qui est orthonormale. (Voir les exemples I.2 et II.1.) Notons χ le caractère de π.

Pour tout $g \in G$, notons X^g l'ensemble des points de X fixes par g, et $|X^g|$ le nombre de ses éléments. Le caractère de π est donné par

$$\chi(g) \,=\, |X^g| \qquad \text{pour tout} \quad g \in G$$

car ϵ_x contribue à la trace de $\pi(g)$ si et seulement si $gx = x$.

Soit $n \geq 2$ un entier. Le groupe G opère sur X^n par *l'action diagonale*, $g(x_1, \ldots, x_n) = (gx_1, \ldots, gx_n)$, à laquelle on peut associer une représentation de permutation que nous notons ici $\pi^{\otimes n}$ (au sens du chapitre XII, c'est le produit tensoriel de n copies de π). Soit $g \in G$; un point $(x_1, \ldots, x_n) \in X^n$ est fixe par g si et seulement si chacun des x_j l'est, de sorte que $(X^n)^g = (X^g)^n$. Il en résulte que le caractère de $\pi^{\otimes n}$ est donné par

$$\chi_{\pi^{\otimes n}}(g) \,=\, \chi(g)^n \qquad \text{pour tout} \quad g \in G$$

et qu'il n'y a pas d'ambiguïté à écrire χ^n le caractère de $\pi^{\otimes n}$.

V.4. Exemple. Soit G un groupe fini non réduit à un élément. Alors G est simple si et seulement si $\chi_\pi(g) \neq \chi_\pi(1)$ pour toute représentation irréductible π de G non équivalente à la représentation unité et pour tout $g \in G$ distinct de 1.

En effet, supposons d'abord G simple. Comme $\mathrm{Ker}(\pi) \neq G$ par hypothèse sur π, la représentation π est fidèle, et $\chi_\pi(g) \neq \chi_\pi(1)$ par la proposition V.1.vii.

Supposons au contraire G non simple. Soit[11] N un sous–groupe normal de G distinct de $\{1\}$ et de G. Soit $\underline{\pi}$ une représentation irréductible du quotient G/N, distincte de la représentation unité, et soit π la composition de $\underline{\pi}$ avec la projection canonique de G sur G/N. Alors $\chi_\pi(g) = \chi_\pi(1)$ pour tout $g \in N$.

Associons à tout caractère χ d'une représentation irréductible d'un groupe fini G le sous–groupe normal $K_\chi = \{g \in G \mid \chi(g) = \text{degré}(\chi)\}$. Plus généralement, on montre que tout sous–groupe normal de G est de la forme $K_{\chi_1} \cap \cdots \cap K_{\chi_k}$; voir la proposition 7 de la section 15 dans [AlpBe–95]. Signalons encore que la connaissance des caractères d'un groupe fini permet de déterminer si ce groupe est "résoluble" ou "nilpotent" ; voir les corollaires 9 et 14 de la section 15 de [AlpBe–95].

V.5. Proposition. *Soient G un groupe (fini ou infini) et $\pi_j : G \longrightarrow GL(V_j)$, $j = 1, 2$, deux représentations complexes*[12] *de G. On considère la représentation π de G dans l'espace $\mathcal{L}(V_1, V_2)$, définie comme à l'exemple II.8 par*

$$(\pi(g)\alpha)\,(v_1) \,=\, \pi_2(g)\Big(\alpha\big(\pi_1(g^{-1})v_1\big)\Big)$$

pour tous $g \in G$, $\alpha \in \mathcal{L}(V_1, V_2)$ et $v_1 \in V_1$. Alors

$$\chi_\pi(g) \,=\, \chi_{\check{\pi}_1}(g)\, \chi_{\pi_2}(g) \qquad \textit{pour tout} \quad g \in G$$

[11] Rappelons que, par définition, un groupe est simple si $\{1\}$ et G sont ses seuls sous–groupes normaux. Un groupe cyclique fini $\mathbf{Z}/n\mathbf{Z}$, avec $n \geq 2$, est simple si et seulement si n est premier. On peut montrer que tout groupe fini simple non cyclique d'ordre au plus 200 est isomorphe soit au groupe alterné Alt(5), d'ordre 60, soit au groupe $PSL_2(\mathbf{F}_7)$, d'ordre 168. L'exercice VII.E7 indique une méthode pour montrer que le groupe Alt(5) est simple.

[12] Cette hypothèse n'est pas nécessaire pour la proposition, mais la preuve que nous en donnons utilise le fait que toute transformation linéaire d'un espace vectoriel complexe est trigonalisable.

où $\chi_{\check\pi_1}$ désigne le caractère de la représentation contragrédiente de π_1.

Démonstration. Soit $g \in G$. On peut choisir une base $(a_1, \dots, a_m)$ de V_1 telle que la matrice représentant $\pi_1(g)$ soit triangulaire inférieure, avec $\mu_1, \dots, \mu_m$ sur la diagonale, ainsi qu'une base $(b_1, \dots, b_n)$ de V_2 telle que la matrice représentant $\pi_2(g)$ soit triangulaire inférieure, avec $\nu_1, \dots, \nu_n$ sur la diagonale. L'espace vectoriel $\mathcal{L}(V_1, V_2)$ possède une base $(e_{j,i})_{1\le i\le m, 1\le j\le n}$, où $e_{j,i}$ est l'application de V_1 dans V_2 définie par $e_{j,i}(a_i) = b_j$ et $e_{j,i}(a_k) = 0$ si $k \neq i$. On calcule

$$\begin{aligned}
(\pi(g)e_{j,i})\,(a_l) &= \pi_2(g)\Big(e_{j,i}\big(\pi_1(g)^{-1}a_l\big)\Big) = \pi_2(g)\Big(e_{j,i}\big(\mu_l^{-1}a_l + \sum_{m>l}\cdots a_m\big)\Big) \\
&= \pi_2(g)\Big(\big(\mu_l^{-1}\delta_{i,l} + \sum_{m>l}\cdots \delta_{i,m}\big)b_j\Big) \\
&= \nu_j\mu_i^{-1}\delta_{i,l}b_j + \sum_{k>j}\cdots b_k.
\end{aligned}$$

Par suite $\pi(g)e_{j,i} \equiv \mu_i^{-1}\nu_j e_{j,i}$ (mod autres vecteurs de la base $e_{*,*}$) et

$$\chi_\pi(g) = \sum_{i=1}^{m}\mu_i^{-1}\sum_{j=1}^{n}\nu_j = \chi_{\check\pi_1}(g)\chi_{\pi_2}(g),$$

ce qu'il fallait montrer. □

V.6. Conséquence. L'espace $\mathbf{C}^G$ des fonctions de G dans $\mathbf{C}$ est un anneau[13] pour les opérations ponctuelles. L'espace des fonctions centrales de G dans $\mathbf{C}$ est un sous–anneau. Les propositions V.1.iv et V.5 montrent que l'ensemble des combinaisons linéaires de caractères de représentations est lui–même un sous–anneau de l'anneau des fonctions centrales ; en particulier, si ρ et σ sont deux représentations de G, la proposition V.5 avec π_1 la contragrédiente de ρ et $\pi_2 = \sigma$ montre que le produit des caractères χ_ρ et χ_σ est encore un caractère de représentation.

De même, l'espace $\mathbf{C}[G]$ des fonctions à supports finis est un sous–anneau de $\mathbf{C}^G$. (Attention : la multiplication ponctuelle des fonctions *n'est pas* le produit de convolution évoqué à l'exemple I.3 et défini au chapitre X ; l'espace $\mathbf{C}[G]$ possède donc *deux* structures d'anneaux à distinguer soigneusement, l'une étant toujours commutative, l'autre ne l'étant que si G est commutatif.) L'espace $\mathbf{C}[G]^G$ des fonctions centrales à supports finis est un sous–anneau de $\mathbf{C}[G]$.

Nous verrons plus tard que, pour un groupe fini, l'ensemble des combinaisons linéaires de caractères de représentations complexes *coïncide* avec l'anneau $\mathbf{C}[G]^G$ des fonctions centrales.

Exercices

Dans les exercices V.E1 à V.E3, G désigne un groupe (fini ou infini) et $\mathbf{K}$ un corps (toujours de caractéristique nulle, selon nos conventions courantes).

V.E1 Soient $\rho : G \longrightarrow \mathbf{K}^*$ un caractère et $\pi : G \longrightarrow GL(V)$ une représentation de G.

[13] C'est même une algèbre complexe. Voir le numéro X.9.

Vérifier que l'application $\rho\pi : G \longrightarrow GL(V)$ définie par $(\rho\pi)(g) = \rho(g)\pi(g)$ est une représentation dont le caractère $\rho\chi_\pi$ est le produit ponctuel de ρ et du caractère de π.

Vérifier que $\rho\pi$ est irréductible si et seulement si π l'est.

[L'analogue de $\rho\pi$ pour deux représentations quelconques de G est le produit tensoriel, voir le chapitre XII.]

V.E2 Pour tout caractère $\rho : G \longrightarrow \mathbf{K}^*$, montrer que la représentation régulière λ_G et le produit $\rho\lambda_G$ sont équivalentes.

[Indication. Définir un automorphisme linéaire S de $\mathbf{K}[G]$ par $(S\varphi)(x) = \rho(x)\varphi(x)$ pour tous $\varphi \in \mathbf{K}[G]$ et $x \in G$, et vérifier que $(\rho\lambda_G)(g)S = S\lambda_G(g)$ pour tout $g \in G$.]

[Remarque. Lorsque G est fini et $\mathbf{K} = \mathbf{C}$, on peut aussi observer que $\rho\lambda_G$ a le même caractère que λ_G et anticiper le corollaire VII.5.]

V.E3 On définit une représentation γ de G sur $\mathbf{K}[G]$ en posant $(\gamma(g)\varphi)(x) = \varphi(g^{-1}xg)$ pour tous $\varphi \in \mathbf{K}[G]$ et $g, x \in G$.

(i) Vérifier qu'une fonction $\varphi \in \mathbf{K}[G]$ est invariante par G pour cette représentation si et seulement si elle est centrale, c'est–à–dire si et seulement si $\varphi \in \mathbf{K}[G]^G$.

(ii) Vérifier que les fonctions caractéristiques des classes de conjugaison finies de G constituent une base de $\varphi \in \mathbf{K}[G]^G$.

En particulier, lorsque G est fini, la dimension de $\mathbf{K}[G]^G$ est égale au nombre des classes de conjugaison de G.

Remarque : lorsque G est fini, le caractère de γ associe à $g \in G$ l'ordre du centralisateur $Z_G(g) = \{h \in G \mid hg = gh\}$.

V.E4 Soient G un groupe infini, V un espace hermitien, $\pi : G \longrightarrow \mathcal{U}(V)$ une représentation unitaire et χ son caractère. Montrer que le support $\{g \in G \mid \chi(g) \neq 0\}$ de χ est un sous–ensemble infini de G.

[Indication. Distinguer deux cas, selon que le noyau de π est d'indice fini ou infini dans G. Dans le second cas, montrer que id_V est un point d'accumulation de l'ensemble $\pi(G)$.]

V.E5*[14] Soit a une matrice complexe n–fois–n. Si $\mathrm{trace}(a^\ell) = 0$ pour tout ℓ assez grand, alors la matrice a est nilpotente.

Rappel : une matrice carrée a est *nilpotente* s'il existe un entier ℓ tel que $a^\ell = 0$. Une matrice complexe étant triangularisable, elle est nilpotente si et seulement si 0 est sa seule valeur propre.

V.E6 Soient $\pi : \mathbf{Z} \longrightarrow GL_n(\mathbf{C})$ une représentation du groupe cyclique infini $\mathbf{Z}$ et χ son caractère. Déduire de l'exercice précédent que χ n'est pas à support fini.

Soient G un groupe, $\pi : G \longrightarrow GL_n(\mathbf{C})$ une représentation et χ son caractère. Si G contient un élément d'ordre infini, il résulte du cas précédent que χ n'est pas à support fini. Sinon, G est localement fini, c'est–à–dire réunion de ses sous–groupes finis ; c'est un théorème de Schur, voir par exemple le théorème 9.2 de [Dixon–71].

[14] Pour les exercices marqués d'un astérisque, voir aussi les indications et les solutions rédigées à la fin de ces notes.

V.E7 Le groupe $\mathcal{O}(2)$ est constitué des rotations centrées à l'origine et des symétries orthogonales d'axes passant par l'origine dans le plan euclidien $\mathbf{R}^2$. Choisissons une symétrie particulière $s \in \mathcal{O}(2)$. Pour tout angle θ, notons r_θ la rotation d'angle θ et sr_θ la symétrie dont l'axe fait un angle de $\theta/2$ avec celui de s. Ainsi $\mathcal{O}(2) = \{r_\theta\}_{0\le\theta<2\pi} \sqcup \{sr_\theta\}_{0\le\theta<2\pi}$.

Pour tout entier $\ell \in \mathbf{Z}$, $\ell \neq 0$, vérifier que l'application $\pi_\ell : \mathcal{O}(2) \longrightarrow GL_2(\mathbf{C})$ définie par

$$\pi_\ell(r_\theta) = \begin{pmatrix} \cos(\ell\theta) & \sin(\ell\theta) \\ -\sin(\ell\theta) & \cos(\ell\theta) \end{pmatrix} \quad \text{et} \quad \pi_\ell(sr_\theta) = \begin{pmatrix} \cos(\ell\theta) & \sin(\ell\theta) \\ \sin(\ell\theta) & -\cos(\ell\theta) \end{pmatrix}$$

est une représentation irréductible.

Montrer que les représentations π_ℓ et $\pi_{\ell'}$ sont équivalentes si et seulement si $\ell' = \pm\ell$.

V.E8 Vérifier que le groupe $\mathcal{SU}(2)$ des matrices 2–fois–2 complexes unitaires de déterminant 1 coïncide avec le groupe

$$\mathcal{SU}(2) = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in M_2(\mathbf{C}) \;\middle|\; |a|^2 + |b|^2 = 1 \right\}.$$

V.E9* Considérons un entier $n \geq 0$ et l'espace $V_n = \mathcal{P}^{(n)}(\mathbf{C}^2)$ des fonctions polynomiales homogènes de degré n de $\mathbf{C}^2$ dans $\mathbf{C}$ (voir l'exemple I.2). Ainsi V_n est un espace vectoriel de dimension $n+1$; si ξ et η désignent les deux projections canoniques de $\mathbf{C}^2$ sur $\mathbf{C}$, alors $(\xi^n, \xi^{n-1}\eta, \xi^{n-2}\eta^2, \ldots, \eta^n)$ est une base de V_n. Notons π_n la représentation naturelle du groupe $SL_2(\mathbf{C})$ dans V_n :

$$\left(\pi_n \begin{pmatrix} a & b \\ c & d \end{pmatrix} \varphi\right) \begin{pmatrix} x \\ y \end{pmatrix} = \varphi\left(\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right)$$

pour tous $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{C})$, $\varphi \in V_n$, et $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{C}^2$.

Calculer la valeur du caractère χ_n de π_n sur une matrice diagonale $\mathrm{diag}(t, t^{-1}) \in SL_2(\mathbf{C})$. En utilisant l'exercice II.E5 (voir aussi la proposition III.3), montrer que la représentation π_n est irréductible.

Montrer que la restriction de π_n au sous–groupe $SL_2(\mathbf{R})$ de $SL_2(\mathbf{C})$ est également irréductible. Idem pour la restriction de π_n au sous–groupe $\mathcal{SU}(2)$.

V.E10 Soient G un groupe fini, H un sous–groupe d'ordre $[G : H] = m$ et $\psi \in \mathbf{C}[H]^H$ une fonction centrale sur H. Noter que, en général, la fonction $\tilde{\psi} \in \mathbf{C}[G]$ obtenue en prolongeant ψ par zéro hors de H n'est pas centrale, car deux éléments de H peuvent être conjugués dans G sans l'être dans H.

Vérifier que la fonction $\varphi : G \longrightarrow \mathbf{C}$ définie par

$$\varphi(g) = \frac{1}{|H|}\tilde{\psi}(xgx^{-1}), \quad g \in G$$

est centrale sur G et que $\varphi(1) = m\psi(1)$.

[Si ψ est le caractère d'une représentation ρ de H dans un espace de dimension $n = \psi(1)$, il se trouve que φ est le caractère d'une représentation $\pi = \mathrm{Ind}_H^G(\rho)$ de G, dite *l'induite de ρ de H à G*, dans un espace de dimension mn.]

VI. Produits scalaires de coefficients

Soient $\pi : G \longrightarrow GL(V)$ une représentation d'un groupe G dans un espace hermitien[15] V et v, w deux vecteurs de V. Le *coefficient* correspondant est la fonction $\varphi_{v,w}$ à valeurs complexes sur G définie par

$$\varphi_{v,w}(g) \;=\; \langle v \mid \pi(g)w\rangle.$$

Supposons que V soit muni d'une base orthonormale $(e_1, \ldots, e_n)$, de sorte qu'on peut voir π comme un homomorphisme $g \longmapsto (\pi(g)_{j,k})_{1\le j,k\le n}$ de G dans $GL_n(\mathbf{C})$. Dans le cas particulier où $v = e_j$ et $w = e_k$, avec $j, k \in \{1, \ldots, n\}$, le coefficient correspondant s'écrit

$$\varphi_{e_j,e_k}(g) \;=\; \langle e_j \mid \pi(g)e_k\rangle \;=\; \pi(g)_{j,k}.$$

Il s'agit donc bien du (j, k)–ième coefficient de la matrice $\pi(g)$ au sens usuel.

Si $\mathbf{C}(G, \pi)$ désigne le sous–ensemble de $\mathbf{C}^G$ des coefficients de π, nous avons $\mathbf{C}(G, \pi') = \mathbf{C}(G, \pi)$ pour toute représentation π' unitairement équivalente à π.

Désormais G désigne **un groupe fini** dont $|G|$ désigne l'ordre.

On définit un produit scalaire sur l'espace $\mathbf{C}[G]$ des fonctions à valeurs complexes sur G par

$$\text{(PS)} \qquad \langle \varphi \mid \psi\rangle \;=\; \frac{1}{|G|}\sum_{g\in G}\overline{\varphi(g)}\psi(g).$$

Notons que, si $\mathbf{1}$ désigne la fonction constante de valeur 1, alors $\langle \mathbf{1} \mid \mathbf{1}\rangle = 1$.

On pourrait aussi poser $\langle \varphi \mid \psi\rangle = \sum_{g\in G}\overline{\varphi(g)}\psi(g)$, ce qui aurait l'avantage de définir un produit scalaire sur $\mathbf{C}[G]$ dans tous les cas (groupes finis et infinis). Mais il faut d'une part noter que, pour les groupes infinis, les coefficients $\varphi_{v,w}$ ne sont en général pas des fonctions à supports finis ; or le produit scalaire introduit ci-dessus sera évalué dans ce cours essentiellement sur des coefficients ou des caractères (qui sont des sommes de coefficients). D'autre part et surtout, une autre normalisation que celle adoptée dans (PS) rendrait plus compliquées un grand nombre de formules apparaissant ci-dessous.

Dans les chapitres qui suivent, le théorème qui suit n'est utilisé que pour le théorème IX.10 et pour la *deuxième* démonstration du théorème VII.1. C'est donc un choix possible pour la lectrice de paser en première lecture d'ici au chapitre suivant.

VI.1. Théorème. *(i) Soient V un espace hermitien de dimension n et $\pi : G \longrightarrow \mathcal{U}(V)$ une représentation unitaire irréductible d'un groupe G dans V. Alors*

$$\langle \varphi_{v,w} \mid \varphi_{v',w'}\rangle \;=\; \frac{1}{n}\overline{\langle v \mid v'\rangle}\langle w \mid w'\rangle$$

pour tous $v, v', w, w' \in V$.

(ii) Soient $\pi_j : G \longrightarrow \mathcal{U}(V_j)$, $j = 1, 2$, deux représentations unitaires irréductibles inéquivalentes. Alors

$$\langle \varphi_{v_1,w_1} \mid \varphi_{v_2,w_2}\rangle \;=\; 0$$

---

[15] Lorsque V est un espace vectoriel sans structure hermitienne donnée, il existe encore des coefficients : à une *forme linéaire* ν sur V et un vecteur $w \in V$ correspond le coefficient défini par $\varphi_{\nu,w}(g) = \nu\big(\pi(g)w\big)$.

pour tous $v_1, w_1 \in V_1$ *et* $v_2, w_2 \in V_2$.

Démonstration. Nous découpons la preuve de (i) en quatre pas.

Premier pas : définition des opérateurs $K_{v',v}$. Soient $v, v', w' \in V$. L'expression

$$(1) \qquad \langle \varphi_{v,w} \mid \varphi_{v',w'} \rangle \;=\; \frac{1}{|G|} \sum_{x \in G} \overline{\langle v \mid \pi(x) w \rangle} \langle v' \mid \pi(x) w' \rangle$$

est antilinéaire en w. Il existe donc un unique vecteur $u_{v',v,w'} \in V$ tel que

$$\langle \varphi_{v,w} \mid \varphi_{v',w'} \rangle \;=\; \langle w \mid u_{v',v,w'} \rangle \qquad \text{pour tout} \quad w \in V.$$

L'égalité (1) étant linéaire en w', l'application $K_{v',v} : V \longrightarrow V$, $w' \longmapsto u_{v',v,w}$ est linéaire et telle que

$$\langle \varphi_{v,w} \mid \varphi_{v',w'} \rangle \;=\; \langle w \mid K_{v',v}(w') \rangle \qquad \text{pour tous} \quad v, w, v', w' \in V.$$

Deuxième pas : équivariance. Pour $v, w, v', w' \in V$ et $g, h \in G$, nous avons

$$\begin{aligned} \langle \pi(h) w \mid K_{\pi(g)v', \pi(g)v}(\pi(h) w') \rangle \;&=\; \langle \varphi_{\pi(g)v, \pi(h)w} \mid \varphi_{\pi(g)v', \pi(h)w'} \rangle \\ &=\; \frac{1}{|G|} \sum_{x \in G} \overline{\langle v \mid \pi(g)^* \pi(xh) w \rangle} \langle v' \mid \pi(g)^* \pi(xh) w' \rangle \\ &=\; \langle \varphi_{v,w} \mid \varphi_{v',w'} \rangle \;=\; \langle w \mid K_{v',v}(w') \rangle \end{aligned}$$

de sorte que

$$(2) \qquad \pi(h)^* K_{\pi(g)v', \pi(g)v} \pi(h) \;=\; K_{v',v} \qquad \text{pour tous} \quad v', v \in V \quad \text{et} \quad g, h \in G.$$

Troisième pas : conséquence de l'irréductibilité. L'égalité (2) avec $g = 1$ montre que $K_{v',v}$ commute à $\pi(h)$ pour tout $h \in G$; le lemme de Schur implique donc qu'il existe pour toute paire v', v de vecteurs de V un nombre complexe $\mu_{v',v}$ tel que

$$K_{v',v} \;=\; \mu_{v',v} \, \mathrm{id}_V \, .$$

Notons que l'application

$$(3) \qquad \begin{cases} V \times V \;\longrightarrow\; \mathbf{C} \\ \;(v', v) \;\longmapsto\; \mu_{v',v} \end{cases}$$

est une forme hermitienne sur l'espace V.

La même égalié (2) avec $h = 1$ montre que $\mu_{\pi(g)v', \pi(g)v} = \mu_{v',v}$ pour tous $g \in G$ et $v, v' \in V$, c'est–à–dire que la forme hermitienne (3) est invariante par π. Le corollaire IV.3 (donc a travers lui encore le lemme de Schur) implique qu'il existe un nombre réel μ tel que $\mu_{v',v} = \mu \langle v' \mid v \rangle$ pour tous $v, v' \in V$. Par suite,

$$\langle \varphi_{v,w} \mid \varphi_{v',w'} \rangle \;=\; \mu \overline{\langle v \mid v' \rangle} \langle w \mid w' \rangle \qquad \text{pour tous} \quad v, w, v', w' \in V.$$

Quatrième pas : calcul de μ. Soient $e_1, \dots, e_n$ une base orthonormale de V et $w \in V$ un vecteur unité. Nous avons

$$\mu \;=\; \mu \langle e_j \mid e_j \rangle \langle w \mid w \rangle \;=\; \langle \varphi_{e_j,w} \mid \varphi_{e_j,w} \rangle \;=\; \frac{1}{|G|} \sum_{x \in G} \left| \langle e_j \mid \pi(x) w \rangle \right|^2$$

pour tout $j = 1, \dots, n$. Par suite

$$n\mu \;=\; \sum_{j=1}^{n} \frac{1}{|G|} \sum_{x \in G} \left| \langle e_j \mid \pi(x) w \rangle \right|^2 \;=\; \frac{1}{|G|} \sum_{x \in G} \sum_{j=1}^{n} \left| \langle e_j \mid \pi(x) w \rangle \right|^2 \;=\; \|w\|^2$$

et donc $\mu = \frac{1}{n}$.

Cinquième pas : démonstration de (ii). Soit $S : V_2 \longrightarrow V_1$ un opérateur linéaire. L'opérateur $\sum_{x \in G} \pi_1(x^{-1}) S \pi_2(x)$ est G-équivariant, comme on le vérifie par un calcul analogue à celui de la preuve du théorème II.5, donc est l'opérateur nul, par le lemme de Schur. Par suite

$$\sum_{x \in G} \langle \pi_1(x) w_1 \mid S \pi_2(x) w_2 \rangle \;=\; 0 \qquad \text{pour tous} \quad w_1 \in V_1 \quad \text{et} \quad w_2 \in V_2.$$

En particulier, si S est de la forme

$$V_2 \longrightarrow V_1, \quad u \longmapsto \langle v_2 \mid u \rangle v_1$$

avec $v_1 \in V_1$ et $v_2 \in V_2$, nous obtenons

$$\sum_{x \in G} \langle \pi_1(x) w_1 \mid v_1 \rangle \langle v_2 \mid \pi_2(x) w_2 \rangle \;=\; \sum_{x \in G} \overline{\langle v_1 \mid \pi_1(x) w_1 \rangle} \langle v_2 \mid \pi_2(x) w_2 \rangle \;=\; 0,$$

comme annoncé. □

VI.2. Remarques. Malgré le peu d'usage fait dans ce cours du théorème VI.1 et des opérateurs $K_{v',v}$ introduits dans sa démonstration, indiquons comment ceux-ci sont utiles à d'autres fins.

Soient G un groupe et $\pi : G \longrightarrow \mathcal{U}(V)$ une représentation unitaire (irréductible ou non). Pour tous $v, v' \in B$, les deux premiers pas de la preuve précédente montrent qu'il existe un opérateur $K_{v',v} \in \mathcal{L}(V)$ tel que

$$\begin{aligned}
\langle w \mid K_{v',v}(w') \rangle \;&=\; \frac{1}{|G|} \sum_{x \in G} \overline{\langle v \mid \pi(x) w \rangle} \langle v' \mid \pi(x) w' \rangle \\
&=\; \overline{\frac{1}{|G|} \sum_{x \in G} \overline{\langle v' \mid \pi(x) w' \rangle} \langle v \mid \pi(x) w \rangle} \\
&=\; \overline{\langle w' \mid K_{v,v'}(w) \rangle} \;=\; \langle w \mid \left(K_{v,v'}\right)^* (w') \rangle
\end{aligned}$$

pour tous $w, w' \in V$. En particulier :

(4) $$\left(K_{v,v'}\right)^* \;=\; K_{v',v} \qquad \text{et} \qquad K_{v,v} \quad \text{est autoadjoint.}$$

La relation (2) de la preuve du théorème VI.1 montre que $K_{v,v}$ commute à $\pi(h)$ pour tout $h \in G$. En particulier :

(5) tout sous–espace propre de $K_{v,v}$ est invariant par G.

La relation de définition de $K_{v,v}$ peut aussi s'écrire

$$K_{v,v}(w') \;=\; \frac{1}{|G|}\sum_{x\in G}\langle v \mid \pi(x)w'\rangle \pi(x^{-1})v \;\in\; V \qquad \text{pour tout} \quad w' \in V$$

de sorte que

(6) l'image par $K_{v,v}$ de la boule unité de V est dans l'enveloppe convexe du sous–ensemble $\pi(G)v$ de V.

Considérons alors un *groupe compact* G, muni d'une *mesure de Haar* dx normalisée par $\int_G dx = 1$. Ainsi, une fonction continue f de G à valeurs dans $\mathbf{C}$ ou dans un espace vectoriel convenable E possède une *intégrale* $\int_G f(x)dx \in E$. Lorsque G est fini, $\int_G F(x)dx = \frac{1}{|G|}\sum_{x\in X} f(x)$. Soient $\mathcal{H}$ un *espace de Hilbert* complexe et $\pi : G \longrightarrow \mathcal{U}(\mathcal{H})$ une représentation unitaire *continue*. On définit pour tout $v \in \mathcal{H}$ un opérateur linéaire borné autoadjoint $K_{v,v}$ sur $\mathcal{H}$ par

$$K_{v,v}(w') \;=\; \int_G \langle v \mid \pi(x)w'\rangle \pi(x^{-1})v dx \;\in\; \mathcal{H}. \tag{7}$$

L'analogue de (6) est encore vrai, de sorte que l'opérateur $K_{v,v}$ est compact (conséquence de la compacité de l'image $\pi(G)v$ du groupe compact G par l'application continue $g \longmapsto \pi(g)v$ de G dans $\mathcal{H}$). L'opérateur $K_{v,v}$ n'est pas nul, car $\langle v \mid K_{v,v}(v)\rangle = \int_G |\langle v \mid \pi(x)v\rangle|^2 dx > 0$. Or les espaces propres des opérateurs auto-adjoints compacts correspondant à des valeurs propres non nulles sont de dimension finie ; il résulte donc de (5) que $\mathcal{H}$ possède un sous–espace invariant de dimension finie strictement positive. Nous avons en particulier montré :

(i) *toute représentation unitaire irréductible d'un groupe compact est de dimension finie.*

On pourrait poursuivre ainsi et montrer les résultats standard concernant les représentations continues des groupes compacts dans les espaces de Hilbert qui constituent la *théorie de Peter-Weyl* (l'article original date de 1927). Notamment :

(ii) *toute représentation est unitarisable ;*
(iii) *toute représentation continue est somme directe de sous–représentations irréductibles ;*
(iv) *toute représentation irréductible est équivalente à une sous–représentation de la représentation régulière de G dans $L^2(G)$, où elle apparaît avec une multiplicité égale à son degré.*

Dans le cas particulier des groupes finis, voir respectivement la proposition II.7, le théorème III.1 et le théorème IX.1.

Certains groupes non compacts possèdent certaines représentations unitaires irréductibles[16] de dimension infinie dont les coefficients sont des fonctions L^2 et satisfont les relations du théorème VI.1 (pour un nombre réel $n > 0$ appelé la *dimension formelle de la représentation* ; ces représentations sont celles de la *série discrète*. Par exemple, $SL_2(\mathbf{R})$ possède une série discrète, et $SL_2(\mathbf{C})$ n'en possède pas.

VII. Relations d'orthogonalité des caractères

Rappelons (encore une fois) que, désormais, G désigne un **groupe fini** dont $|G|$ désigne l'ordre, et que les espaces des représentations sont des espaces vectoriels **complexes**. L'espace $\mathbf{C}[G]$ des fonctions à valeurs complexes sur G est muni du produit scalaire défini au chapitre VI.

[16]Il s'agit de groupes topologiques et de représentations continues dans des espaces de Hilbert. L'irréductibilité consiste alors en l'absence de sous–espaces invariants *fermés* non triviaux.

VII.1. Théorème (relations d'orthonormalité des caractères irréductibles). *Soient $\pi_j : G \longrightarrow GL(V_j)$, $j = 1, 2$, deux représentations irréductibles et χ_1, χ_2 leurs caractères.*

Si π_1 et π_2 sont équivalentes, alors $\langle \chi_1 \mid \chi_2 \rangle = 1$. [Rappel : dans ce cas, $\chi_1 = \chi_2$.]

Si π_1 et π_2 sont non équivalentes, alors $\langle \chi_1 \mid \chi_2 \rangle = 0$.

Première démonstration. Soit π la représentation naturelle de G dans $\mathcal{L}(V_1, V_2)$, définie à l'exemple II.8, et χ son caractère, calculé à la proposition V.5. Par le lemme de Schur, la multiplicité de la représentation unité dans π est la dimension de $\mathcal{L}(V_1, V_2)^G$, c'est–à–dire 1 ou 0 selon que les représentation π_1 et π_2 sont équivalentes ou non. Il résulte de la proposition V.1.ix que $\frac{1}{|G|} \sum_{g \in G} \overline{\chi_1(g)} \chi_2(g)$ vaut 1 ou 0 selon le cas. □

Remarque. Même sans supposer les représentations π_1 et π_2 irréductibles, nous avons

$$\dim_{\mathbf{C}} \left(\mathcal{L}(V_1, V_2)^G \right) \ = \ \langle 1_G \mid \chi \rangle \ = \ \langle 1_G \mid \chi_{\check{\pi}_1} \chi_{\pi_2} \rangle \ = \ \langle \chi_{\pi_1} \mid \chi_{\pi_2} \rangle,$$

où $\check{\pi}_1$ désigne la représentation contragrédiente de π_1.

Deuxième démonstration. Grâce à la proposition II.7, nous pouvons supposer π_1 et π_2 unitaires, de sorte que nous allons pouvoir invoquer le théorème VI.1. Soient $a_1, \ldots, a_m$ une base orthonormale de V_1 et $b_1, \ldots, b_n$ une base orthonormale de V_2.

(i) Il suffit de considérer le cas $V_2 = V_1$, $\pi_2 = \pi_1$, $\chi_2 = \chi_1$. Par définition de χ_1 et du produit scalaire sur $\mathbf{C}[G]$,

$$\chi_1(g) \ = \ \mathrm{trace}(\pi_1(g)) \ = \ \sum_{k=1}^{m} \langle a_k \mid \pi_1(g) a_k \rangle$$

pour tout $g \in G$ et

$$\begin{aligned} \langle \chi_1 \mid \chi_1 \rangle \ &= \ \frac{1}{|G|} \sum_{g \in G} \sum_{k=1}^{m} \overline{\langle a_k \mid \pi_1(g) a_k \rangle} \sum_{l=1}^{m} \langle a_l \mid \pi_1(g) a_l \rangle \\ &= \ \sum_{k,l=1}^{m} \frac{1}{|G|} \sum_{g \in G} \overline{\varphi_{a_k, a_k}(g)} \varphi_{a_l, a_l}(g). \end{aligned}$$

En conséquence du théorème VI.1, nous avons

$$\sum_{k,l=1}^{m} \frac{1}{|G|} \sum_{g \in G} \overline{\varphi_{a_k, a_k}(g)} \varphi_{a_l, a_l}(g) \ = \ \sum_{k,l=1}^{m} \frac{1}{m} \delta_{k,l} \ = \ 1.$$

(ii) On vérifie que

$$\begin{aligned} \langle \chi_1 \mid \chi_2 \rangle \ &= \ \frac{1}{|G|} \sum_{g \in G} \sum_{k=1}^{m} \overline{\langle a_k \mid \pi_1(g) a_k \rangle} \sum_{l=1}^{n} \langle b_l \mid \pi_2(g) b_l \rangle \\ &= \ \sum_{k=1}^{m} \sum_{l=1}^{n} \frac{1}{|G|} \sum_{g \in G} \overline{\varphi_{a_k, a_k}(g)} \varphi_{b_l, b_l}(g) \ = \ 0 \end{aligned}$$

en utilisant le même théorème. □

Troisième démonstration. Voir ci–dessous le numéro IX.10. □

VII.2. Corollaire. *Le nombres des représentations irréductibles d'un groupe fini, à équivalence près, est un nombre fini.*

Plus précisément, le théorème précédent montre que les caractères des classes d'équivalence de représentations irréductibles d'un groupe fini G sont des fonctions orthonormales dans l'espace des fonctions centrales de G dans $\mathbf{C}$. Par suite, le nombre de ces classes d'équivalence est majoré par la dimension de $\mathbf{C}[G]^G$, qui est le nombre de classes de conjugaison du groupe G.

Nous verrons plus loin que ces nombres sont de fait égaux (théorème IX.4).

VII.3. Corollaire. *Soient π une représentation de G et $\pi = \rho_1 \oplus \cdots \oplus \rho_k$ une décomposition de π en sous–représentations irréductibles comme au théorème III.1. Soit ρ une représentation irréductible de G.*

Alors la multiplicité de ρ dans π, *c'est–à–dire le nombre des indices j dans $\{1, \ldots, k\}$ pour lesquels ρ_j est équivalente à ρ, est égale au produit scalaire $\langle \chi_\rho \mid \chi_\pi \rangle$.*

Démonstration. Si χ_k désigne le caractère de ρ_k, nous avons $\chi_\pi = \sum_{j=1}^{k} \chi_k$, et le théorème est une conséquence immédiate du théorème VII.1. □

VII.4. Corollaire. *Avec les notations du corollaire précédent, le nombre des ρ_j équivalents à ρ ne dépend pas de la décomposition de π choisie.*

Par exemple, la multiplicité du caractère principal χ_1 dans une représentation $\pi : G \longrightarrow GL(V)$, qui est la dimension du sous–espace V^G de V invariant par G, est donnée par le produit scalaire $\langle \chi_1 \mid \chi_\pi \rangle$, comme nous l'avons déjà établi à la proposition V.1.ix.

VII.5. Corollaire. *Deux représentations de même caractère sont équivalentes.*

Remarque. Soient π, π' deux représentations complexes irréductibles de dimension finie d'un même groupe G, fini *ou infini* ; alors π et π' sont équivalentes *si et seulement si* leurs caractères sont égaux. L'assertion apparaît dans Selberg, Collected Papers, Volume I, page 478, Lemma 4 ; pour le lemme 3 du même article, qui dit que $\pi(G)$ engendre linéairement $\mathcal{L}(V)$, voir ci–dessous l'assertion (d) de l'exercice X.E2.

Il résulte par exemple du corollaire VII.5 que, pour une représentation π d'un groupe fini G, la représentation contragrédiente $\check{\pi}$ est équivalente à π si et seulement si les valeurs du caractère χ_π sont toutes réelles (voir la proposition V.1.v).

VII.6. Corollaire. *Soient $\rho_1, \ldots, \rho_k$ un système de représentants des classes d'équivalence de représentations irréductibles d'un groupe fini G et $\chi_1, \ldots, \chi_k$ leurs caractères.*

Toute représentation π de G est équivalente à une représentation de la forme

$$m_1\rho_1 \oplus \cdots \oplus m_k\rho_k,$$

où $m_1, \ldots, m_k$ sont des entiers positifs ou nuls, et le caractère de π est alors égal à

$$m_1\chi_1 + \cdots + m_k\chi_k.$$

Les relations d'orthonormalité des caractères (théorème VII.1) impliquent que

$$\langle \chi_\pi \mid \chi_\pi \rangle = \sum_{i=1}^{k} m_i^2.$$

En particulier, le nombre $\langle \chi_\pi \mid \chi_\pi \rangle$ est toujours un entier positif ou nul, et ce nombre vaut 1 si et seulement si la représentation π est irréductible.

Représentations de permutation

Considérons la situation des exemple I.2, II.1 et V.3, dont nous conservons les notations : G opère sur X, d'où une représentation $\pi : G \longrightarrow GL(V = \mathbf{C}^X)$ de caractère π, et χ_1 désigne le caractère principal.

VII.7. Exemple. Notons de plus m le nombre des orbites de G dans X. Le sous–espace V^G des fonctions G–invariantes dans V s'identifie aux fonctions sur X constantes sur les orbites ; sa dimension, qui est m, est aussi la multiplicité de la représentation unité dans π. Nous avons donc

$$(*) \qquad m = \langle \chi_1 \mid \chi \rangle = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

VII.8. Exemple. Continuons avec la situation de l'exemple VII.7, en supposant désormais de plus que l'action de G sur X est transitive, c'est–à–dire que $m = 1$. Notons d'abord une conséquence qualitative de la formule (*) ci–dessus : si $|X| \geq 2$, il existe au moins un élément $g_0 \in G$ qui agit sans point fixe (avec $|X^{g_0}| = 0$) ; en effet, la formule montre que 1 est la moyenne des quantités $|X^g|$, et l'une d'entre elles (pour $g = 1$) est strictement supérieure à 1.

Par définition, le *rang* de l'action de G sur X est le nombre des orbites de l'action diagonale de G sur $X \times X$; notons–le r. (Pour d'autres définitions, équivalentes, voir la proposition VIII.4.) L'analogue de la relation (*) pour la représentation de permutation associée à l'action diagonale de G sur X^2, c'est–à–dire pour la représentation notée $\pi^{\otimes 2}$ à l'exemple V.3, est

$$r = \langle \chi_1 \mid \chi^2 \rangle = \frac{1}{|G|} \sum_{g \in G} |X^g|^2.$$

La fonction χ étant à valeurs réelles (même entières !), nous avons

$$\langle \chi_1 \mid \chi^2 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)^2 = \langle \chi \mid \chi \rangle,$$

de sorte que

$$(**) \qquad r = \langle \chi \mid \chi \rangle = \frac{1}{|G|} \sum_{g \in G} |X^g|^2.$$

Soit $\pi = \chi_1 \oplus (\bigoplus_{j=2}^k m_j \pi_j)$ une décomposition de π en sous–représentations irréductibles ; $m_2, \ldots, m_k$ sont des entiers strictement positifs et $\pi_1 = \chi_1, \pi_2, \ldots, \pi_k$ des représentations irréductibles inéquivalentes deux à deux. Nous avons donc

$$(***) \qquad r = \langle \chi \mid \chi \rangle = 1 + \sum_{j=2}^{k} m_j^2$$

par le corollaire VII.6. (Voir aussi le numéro VII.15.)

En particulier, si $r \leq 4$, alors $k \leq 4$ et chaque m_j est égal à 1 ; la représentation π est dite *sans multiplicité*. Vu l'importance de ces cas, nous allons les reformuler dans la proposition suivante.

Une action d'un groupe G sur un ensemble X est dite *doublement transitive* si, pour tous $u, v, x, y \in X$ tels que $u \neq v$ et $x \neq y$, il existe $g \in G$ tel que $x = gu$ et $y = gv$. Si X est de cardinal au moins 2 une action est doublement transitive si et seulement si elle est de rang 2. Nous laissons à la lectrice le soin de définir une action *m–transitive* pour tout entier $m \geq 2$; pour $m = 3, 4, \ldots$, on écrit aussi *triplement transitive, quadruplement transitive, ...*

VII.9. Proposition. *Soit G un groupe fini agissant transitivement sur un ensemble X non réduit à un élément ; notons r le rang de l'action. Soit π la représentation de permutation correspondante et π_0 la sous–représentation de π agissant sur l'espace des fonctions de $\mathbf{C}^X$ de somme nulle, comme à l'exemple II.1.*

(i) Pour que la représentation π_0 soit irréductible, il faut et il suffit que l'action de G sur X soit doublement transitive.

(ii) Si $r = 3$ [respectivement $r = 4$], alors la représentation π_0 est une somme directe de deux [resp. trois] sous–représentations irréductibles distinctes de la représentation unité et non équivalentes deux à deux.

Remarques. Plus généralement, pour une action transitive de G sur X de rang $r \leq 5$, la représentation de permutation π est sans multiplicité ; voir l'exercice X.E1.

L'action du groupe Sym(3) sur lui-même par multiplication à gauche est de rang 6, et la représentation de permutation correspondante, qui est la représentation régulière de Sym(3), a de la multiplicité.

Il existe des actions de rang arbitrairement grand dont les représentations de permutation associées sont sans multiplicité ; voir l'exercice VII.E17.

L'exercice VIII.E11 indique pour $m \geq 3$ des conditions en terme du caract'ere de π dont chacune est nécessaire et suffisante pour que l'action soit m–transitive.

Démonstration. Rappelons que, dans tous les cas, π est somme directe de la représentation unité et de π_0. Avec les notations de l'exemple VII.8, nous avons donc $\pi_0 = \bigoplus_{j=2}^{k} m_j \pi_j$ et $r - 1 = \sum_{j=2}^{k} m_j^2$. Pour (i), il suffit de remarquer que $r = 2$ si et seulement si $k = 2$ et $m_2 = 1$. Comme déjà indiqué, l'assertion (ii) résulte de ce que $m_j = 1$ pour tout j lorsque $r \leq 4$. $\square$

VII.10. Exemple. Pour tout entier $k \geq 2$, l'action naturelle du groupe symétrique Sym(k) sur l'ensemble $\{1, \ldots, k\}$ est doublement transitive, et fournit donc une représentation irréductible de degré $k - 1$; c'est la représentation naturelle du groupe Sym(k) dans l'hyperplan de $\mathbf{C}^k$ d'équation $x_1 + \cdots + x_k = 0$.

Lorsque $k \geq 4$, la restriction de cette représentation au groupe alterné Alt(k) est encore irréductible.

Supposons de plus que $k \geq 4$. L'action naturelle du groupe Sym(k) sur l'ensemble X des sous–ensembles à deux éléments de $\{1, \ldots, k\}$ est de rang 3, car les orbites sur le complémentaire de la diagonale dans $X \times X$ sont représentées respectivement par $(\{1, 2\}, \{1, 3\})$ et $(\{1, 2\}, \{3, 4\})$.

Pour $k = 4$, les valeurs du caractère χ de la représentation π correspondante sont

$$\chi(\mathrm{id}) = 6 \quad \chi((1,2)) = 2 \quad \chi((1,2,3)) = 0 \quad \chi((1,2,3,4)) = 0 \quad \chi((1,2)(3,4)) = 2$$

et on vérifie sans peine que $\frac{1}{24}\sum_{g\in \mathrm{Sym}(4)} |X^g|^2 = 3$. Il n'est pas difficile de déduire de la table de caractères XI.3 ci-dessous quelles sont les composantes irréductibles de π.

A titre d'exercice, la lectrice pourra vérifier l'égalité correspondante pour $k = 5$, à savoir $\frac{1}{120}\sum_{g\in \mathrm{Sym}(5)} |X^g|^2 = 3$.

VII.11. Exemple. Soit SG_I le *groupe spécial de l'icosaèdre,* qui est le groupe des rotations de $\mathbf{R}^3$ laissant invariant un icosaèdre régulier I centré à l'origine. Notons π la représentation obtenue en composant les inclusions $SG_I \subset SO(\mathbf{R}^3) \subset GL(\mathbf{R}^3) \subset GL(\mathbf{C}^3)$.

Rappelons d'abord que l'ordre de SG_I est égal au produit du nombre des sommets de l'icosaèdre par le nombre des arêtes issues de chaque sommet, c'est–à–dire à $12 \times 5 = 60$. L'icosaèdre contient 10 paires de faces opposées, 15 paires d'arêtes opposées et 6 paires de sommets opposés. Le groupe SG_I contient donc, en plus de l'indentité, 20 rotations d'un tiers de tour, 15 rotations d'un demi tour, 12 rotations d'un cinquième de tour et 12 rotations de deux cinquièmes de tour. La trace d'une rotation d'angle θ de $\mathbf{R}^3$ étant $1 + 2\cos\theta$, les valeurs du caractère χ_π sont :

$$\begin{array}{ccccccc}
1 & + & 2\cos(0) & = & 3 & \text{avec multiplicité} & 1 \;; \\
1 & + & 2\cos(\frac{2\pi}{3}) & = & 0 & \text{avec multiplicité} & 20 \;; \\
1 & + & 2\cos(\pi) & = & -1 & \text{avec multiplicité} & 15 \;; \\
1 & + & 2\cos(\frac{2\pi}{5}) & = & \frac{1}{2}(1+\sqrt{5}) & \text{avec multiplicité} & 12 \;; \\
1 & + & 2\cos(\frac{4\pi}{5}) & = & \frac{1}{2}(1-\sqrt{5}) & \text{avec multiplicité} & 12 \;.
\end{array}$$

(Nous rappelons ci-dessous comment on peut calculer $\cos(2\pi/5)$ et $\cos(4\pi/5)$.) Par suite

$$\sum_{g\in SG_I} \chi_\pi(g)^2 \;=\; 9 \;+\; 12 \times \frac{3+\sqrt{5}}{2} \;+\; 12 \times \frac{3-\sqrt{5}}{2} \;+\; 15 \;=\; 60$$

et

$$\langle \chi_\pi \mid \chi_\pi \rangle \;=\; 1.$$

Il résulte en particulier du corollaire VII.6 que la représentation π est irréductible.

Il existe de ce dernier fait des preuves moins calculatoires et plus courtes ! En effet, si la représentation π de dimension 3 était réductible, il existerait un sous–espace de $\mathbf{C}^3$ de dimensions 1 invariant. Or une inspection rapide montre que les rotations qui constituent SG_I n'ont pas d'espace propre commun. Donc π est bien irréductible.

Posons $\omega = \exp(2i\pi/5)$. Les nombres ω et ω^2 sont deux des quatre racines du polynôme cyclotomique

$$\frac{T^5-1}{T-1} \;=\; T^4 + T^3 + T^2 + T + 1 \;=\; T^2\left(\left(T+\frac{1}{T}\right)^2 + \left(T+\frac{1}{T}\right) - 1\right).$$

Donc $2\cos(2\pi/5)$ et $2\cos(4\pi/5)$ sont les deux racines du polynôme U^2+U-1. Comme de plus $0 < 2\pi/5 < \pi/2$, nous avons $1 > \cos(2\pi/5) > 0$; par suite

$$\cos\frac{2\pi}{5} \;=\; \frac{-1+\sqrt{5}}{4} \qquad \text{et} \qquad \cos\frac{4\pi}{5} \;=\; \frac{-1-\sqrt{5}}{4}.$$

Voici une illustration tirée du très riche livre de Kirillov. Elle peut servir “de modèle d'application de la théorie des représentations à divers problèmes des mathématiques, de mécanique et de physique ayant une symétrie quelconque” (§ 16 de [Kirill–74]).

VII.12. Un problème de calcul.

Considérons comme à l'exercice II.E1 l'ensemble X des faces d'un cube centré à l'origine de $\mathbf{R}^3$, l'espace $V = \mathbf{C}^X$ et la représentation π du groupe du cube G_C dans l'espace V. Considérons de plus le "laplacien"

$$L : V \longrightarrow V, \qquad (L\varphi)(x) = \frac{1}{4} \sum_{\text{voisins de } x} \varphi(y)$$

qui consiste à remplacer la valeur $\varphi(x)$ d'une fonction de V en une face x par la moyenne des valeurs sur les quatre faces voisines.

Etant donné une fonction $\tau \in V$ numérotant les faces d'un cube de 1 à 6, on se propose de déteminer la fonction $L^{30}(\tau)$ à 10^{-6} près.

VII.13. La solution.

Convenons qu'une fonction de V est *paire* [respectivement *impaire*] si ses valeurs sur deux faces opposées du cube sont égales [resp. opposées]. L'espace V a manifestement trois sous–espaces invariants qui sont

le sous–espace V_1 des fonctions constantes, de dimension 1,
le sous–espace V_2 des fonctions paires de somme nulle, de dimension 2,
le sous–espace V_3 des fonctions impaires, de dimension 3.

Notons $\pi = \pi_1 \oplus \pi_2 \oplus \pi_3$ la décomposition correspondante de π. Le G_C–espace X est de rang trois, et la relation (***) de l'exemple VII.8 montre que π possède exactement trois sous–représentations irréductibles ; les représentations π_1, π_2 et π_3 sont donc irréductibles.

Comme $L\pi(g) = \pi(g)L$ pour tout $g \in G_C$, chacun des espaces V_j est invariant par L. Il résulte du lemme de Schur que la restriction de L à V_j est une homothétie ; notons–en μ_j le rapport. Il est évident que $\mu_1 = 1$. Pour calculer μ_j, il suffit de calculer $L\varphi$ pour *une* fonction non nulle de V_j. En choisissant une fonction paire prenant les trois valeurs 1, -1 et 0, on trouve facilement $\mu_2 = -\frac{1}{2}$. En choisissant une fonction impaire prenant les valeurs 1 et -1 sur deux faces opposées et la valeur 0 sur les quatre autres faces, on trouve $\mu_3 = 0$. Par suite, pour une fonction $\varphi \in V$ de composantes $\varphi_j \in V_j$, $j = 1, 2, 3$, nous avons

$$L^k\varphi = \varphi_1 + \left(-\frac{1}{2}\right)^k \varphi_2$$

pour tout entier $k \geq 1$.

Dans le cas particulier de la fonction τ donnée, nous avons pour toute face x du cube[17] $\tau_1(x) = 7/2$, donc $(L^{30}\tau)(x) - 7/2 = 2^{-30}\tau_2(x)$. De plus, $1 \leq \tau(x) \leq 6$ et $3/2 \leq \frac{\tau(x)+\tau(-x)}{2} \leq 11/2$, donc aussi $-2 \leq \tau_2(x) = \frac{\tau(x)+\tau(-x)}{2} - \frac{7}{2} \leq 2$; par suite $\max_{x\in X} |\tau_2(x)| \leq 2$ et

$$\sup_{x\in X} |L^{30}\tau(x) - 7/2| \leq 2 \times 2^{-30} < 2 \times 10^{-9}.$$

La fonction $L^{30}\tau$ est donc la fonction constante de valeur $\frac{7}{2}$, à 2×10^{-9} près.

[17] Pour certains dés à jouer, la fonction τ est telle que $\tau_2 = 0$, de sorte que $L^k\tau = \tau_1$ pour tout $k \geq 1$. Nous n'en tenons pas compte ici.

VII.14. Commutant. Soient G un groupe et $\pi : G \longrightarrow GL(V)$ une représentation complexe. Le *commutant* de π est le sous–espace vectoriel

$$\pi(G)' = \{S \in \mathcal{L}(V) \mid \pi(g)S = S\pi(g) \quad \text{pour tout} \quad g \in G\}$$

de $\mathcal{L}(V)$; quitte à anticiper sur la termiologie du numéro X.9, notons que c'est une sous–algèbre de $\mathcal{L}(V)$.

Proposition. *On conserve les notations ci–dessus et on écrit $\pi = \bigoplus_{j=1}^{s} m_j\rho_j$ une décomposition de π en somme directe de représentations irréductibles, les ρ_j étant irréductibles non équivalentes deux à deux et les m_j étant des entiers strictement positifs. Alors le commutant $\pi(G)'$ est isomorphe à l'algèbre $\bigoplus_{j=1}^{s} M_{m_j}(\mathbf{C})$.*

En particulier, pour que π soit sans multiplicité, il faut et il suffit que son commutant soit abélien.

Démonstration. Pour éviter des lourdeurs de notation, considérons le cas particulier d'une représentation $\pi = \rho_1 \oplus 2\rho_2$; l'argument s'étend au cas général.

Soit $V = V_1 \oplus V_2 \oplus V_3$ une décomposition de V en somme directe de sous–espaces $\pi(G)$–invariants telle que la restriction de π à V_1, V_2, V_3 soit la représentation irréductible ρ_1, ρ_2, ρ_2 respectivement, l'espace V_3 étant une copie de V_2. Tout endomorphisme linéaire S de V possède une écriture en matrices par blocs de la forme $S = (S_{i,j})_{1\le i,j\le 3}$, avec $S_{i,j} \in \mathcal{L}(V_j, V_i)$. Pour que S soit dans $\pi(G)'$, c'est–à–dire pour que S et $\begin{pmatrix} \rho_1(g) & 0 & 0 \\ 0 & \rho_2(g) & 0 \\ 0 & 0 & \rho_2(g) \end{pmatrix}$ commutent pour tout $g \in G$, il faut et il suffit que $S_{1,1}\rho_1(g) = \rho_1(g)S_{1,1}$, $\quad S_{1,2}\rho_2(g) = \rho_1(g)S_{1,2}$, $\quad$ etc. Il résulte donc du lemme de Schur que

$$S = \begin{pmatrix} aI_1 & 0 & 0 \\ 0 & bI_2 & cI_2 \\ 0 & dI_2 & eI_2 \end{pmatrix} = aI_1 \oplus \left(\begin{pmatrix} b & c \\ d & e \end{pmatrix} \otimes I_2 \right).$$

Ici, I_1 et I_2 désignent l'identité de V_1 et V_2 respectivement. Le coefficient I_2 qui apparaît à la 2e ligne et la 3e colonne de la matrice a un sens car nous avons identifié les sous–espaces V_2 et V_3 de V. Le signe de produit tensoriel $\otimes$ anticipe sur le chapitre XII.

Il en résulte que le commutant $\pi(G)'$ est isomorphe à la somme directe des algèbres de matrices $M_1(\mathbf{C}) \oplus M_2(\mathbf{C})$, ce qu'il fallait montrer.

L'exercice VII.E15 est consacré à un autre cas particulier. □

Particularisons au cas d'une représentation $\pi : G \longrightarrow GL(\mathbf{C}^X)$ associée à une action de G sur un ensemble fini X. Soit $(\epsilon_x)_{x\in X}$ la base de $\mathbf{C}^X$ formée des fonctions catactéristiques des points. Pour toute paire (x, y) de points de X, notons $E_{x,y}$ l'endomorphisme de $\mathbf{C}^X$ appliquant ϵ_z sur ϵ_x si $z = y$ et sur 0 sinon ; ainsi $(E_{x,y})_{x,y\in X}$ est une base de $\mathcal{L}(\mathbf{C}^X)$. Notons $\Delta_1, \ldots, \Delta_k$ les orbites de G dans $X \times X$ pour l'action diagonale ; pour $j \in \{1, \ldots, k\}$, posons

$$E_j = \sum_{(x,y)\in\Delta_j} E_{x,y}.$$

Un calcul de routine montre que $\pi(g)E_{x,y}\pi(g^{-1}) = E_{gx,gy}$ pour tous $x, y \in X$ et $g \in G$; il en résulte que $(E_j)_{1\le j\le k}$ est une base de l'espace vectoriel $\pi(G)'$, et en particulier que *le rang de l'action de G sur X est égal à la dimension du commutant $\pi(G)'$.*

La formule (***) précédant la proposition VII.9 est alors une conséquence immédiate de l'isomorphisme $\pi(G)' \simeq \bigoplus_{j=1}^{s} M_{m_j}(\mathbf{C})$.

VII.15. Action généreusement transitive. L'action de G sur X est dite *généreusement transitive* si, pour toute paire (x, y) de points de X, il existe $g \in G$ tel que $gx = y$ et $gy = x$. Voici une condition équivalente : pour tout $j \in \{1, \ldots, k\}$, l'orbite Δ_j est invariante par la transformation $(x, y) \longmapsto (y, x)$ de $X \times X$.

VII.16. Proposition. *Pour que la représentation $\pi : G \longrightarrow GL(\mathbf{C}^X)$ soit sans multiplicité, il suffit que l'action de G sur X soit généreusement transitive.*

Démonstration. Nous conservons les notations du numéro VII.14. Pour $w, x, y, z \in X$, il est immédiat que $E_{w,x}E_{y,z}$ est égal à $E_{w,z}$ si $x = y$ et à zéro sinon. Il en résulte que, pour $i, j \in \{1, \ldots, k\}$, nous avons

$$E_i E_j \;=\; \sum_{x,z \in X} \Big| \{y \in X \mid (x, y) \in \Delta_i \quad \text{et} \quad (y, z) \in \Delta_j\} \Big| E_{x,z}.$$

Si l'action est généreusement transitive, Δ_i et Δ_j sont invariants par $(u, v) \longmapsto (v, u)$; donc

$$\{y \in X \mid (z, y) \in \Delta_j \quad \text{et} \quad (y, x) \in \Delta_i\} \;=\; \{y \in X \mid (x, y) \in \Delta_i \quad \text{et} \quad (y, z) \in \Delta_j\},$$

et donc aussi

$$E_j E_i \;=\; \sum_{x,z \in X} \Big| \{y \in X \mid (x, y) \in \Delta_j \quad \text{et} \quad (y, z) \in \Delta_i\} \Big| E_{x,z} \;=\; E_i E_j.$$

Ceci étant vrai pour tous les couples (i, j), le commutant $\pi(G)'$ est abélien. □

VII.17. Paires de Gelfand. Soient G un groupe fini et H un sous–groupe de G. La paire (G, H) est dite *de Gelfand* si la représentation de permutation π de G dans l'espace $\mathbf{C}^{G/H}$ est sans multiplicité ; ou, de manière équivalente (proposition VII.14), si le commutant $\pi(G)'$ est abélien.

Par exemple, soit G un groupe agissant transitivement sur un ensemble X et soit H le groupe d'isotropie d'un point de X. Si l'action de G est généreusement transitive, alors (G, H) est une paire de Gelfand (proposition VII.16). Si l'action de G est de rang au plus 5, alors (G, H) est une paire de Gelfand (proposition VII.9 et exercice X.E1). En particulier, si l'action de G est doublement transitive (donc à la fois généreusement transitive et de rang $2 \leq 5$), alors (G, H) est une paire de Gelfand. Si (G, H) est une paire de Gelfand, alors (G, gHg^{-1}) est une paire de Gelfand pour tout $g \in G$.

Voici une famille d'exemples plus spécifiques. Considérons deux entiers k, n tels que $1 \leq k \leq n - 1$ et la paire

$$G \;=\; \mathrm{Sym}(n) \;\supset\; H \;=\; \mathrm{Sym}(k) \times \mathrm{Sym}(n - k).$$

L'espace homogène G/H s'identifie à l'ensemble $\mathcal{B}_k(n)$ des k–blocs, c'est–à–dire des sous–ensembles à k éléments de $\{1, \ldots, n\}$. Il est facile de vérifier (exercice VII.E17) d'une part que l'action naturelle de $\mathrm{Sym}(n)$ sur $\mathcal{B}_k(n)$ est généreusement transitive, donc que la paire (G, H) est de Gelfand, et d'autre part que cette action est de rang $r = \min\{k, n-k\} + 1$. La représentation de permutation $\mathrm{Sym}(n) \longrightarrow GL(\mathbf{C}^{\mathcal{B}_k(n)})$ a donc un commutant abélien isomorphe à $\mathbf{C}^r$.

De même, si $\mathbf{F}_q$ est un corps fini, et si $PGL_n(\mathbf{F}_q)$ est le groupe défini à l'exercice VIII.E4 du chapitre suivant, l'action naturelle de $PGL_n(\mathbf{F}_q)$ sur l'ensemble $\mathcal{G}_k(n)$ des sous–espaces de dimension k dans $\mathbf{F}_q^n$ est généreusement transitive et donne lieu à une paire de Gelfand.

Il existe des paires de Gelfand (G, H) telles que l'action de G sur G/H *n'est pas* généreusement transitive (voir l'exercice VII.E18 et l'exemple XV.10).

La notion de paire de Gelfand se définit plus généralement pour des paires (G, H) formées d'un groupe localement compact et d'un sous–groupe compact.

VII.18. Exemple. Soit X un *espace métrique* ; notons $d(x, y)$ la distance entre deux points $x, y \in X$. Une *isométrie* de X est une bijection $\gamma : X \longrightarrow X$ telle que $d(\gamma(x), \gamma(y)) = d(x, y)$ pour toute paire (x, y) de points de X. Soit G un groupe agissant sur X ; l'action est *isométrique* si $x \longmapsto gx$ est une isométrie pour tout $g \in G$, et *homogène à deux points* si, de plus, pour tous $(x, y), (x', y') \in X \times X$ tels que $d(x, y) = d(x', y')$, il existe $g \in G$ tel que $gx = x'$ et $gy = y'$. En d'autres termes, l'action de G est homogène à deux points si G opère transitivement sur les paires de points équidistants. Une telle action est évidemment généreusement transitive.

Par exemple, l'action canonique du groupe des rotations $S\mathcal{O}(3)$ sur la sphère unité $\mathbf{S}^2$ de $\mathbf{R}^3$ est homogène à deux points.

Soit P un polytope de l'espace euclidien $\mathbf{R}^3$. Notons G_P le *groupe de P,* c'est–à–dire le groupe des isométries de $\mathbf{R}^3$ laissant P invariant, et $SG_P = G_P \cap S\mathcal{O}(3)$ le *groupe spécial de P,* qui est le sous–groupe des rotations de G_P. L'action de SG_P sur l'ensemble des sommets de P est homogène à deux points.

Soit X un espace métrique fini ; notons n le nombre des points et $D = \max_{x,y \in X} d(x, y)$ le diamètre de X. Supposons pour la suite de ce numéro que la distance $d : X \times X \longrightarrow \mathbf{R}_+$ est à valeurs entières et que, pour tout entier $j \in \{0, \ldots, D\}$, il existe des points $x, y \in X$ tels que $d(x, y) = j$. Soit G un sous–groupe du groupe des isométries de X (par exemple le groupe de toutes les isométries de X). Il résulte des définitions que le rang de l'action de G sur X est au moins $D + 1$, et qu'il est égal à $D + 1$ si et seulement si l'action de G sur X est homogène à deux points.

Soient à nouveau P et SG_P comme ci–dessus. Notons X_P l'ensemble des sommets de P et définissons la distance entre deux de ces sommets comme le nombre minimum d'arêtes de P d'un chemin les connectant dans le graphe constitué des sommets et des arêtes du polytope. L'action de G sur X_P est alors un exemple de la situation considérée dans ce numéro. Il est (presqu'...) immédiatement visible que le rang de l'action de SG_P sur X_P est égal à 2 [respectivement 3, 4, 4, 5] si P est un tétraèdre régulier [resp. un octaèdre, un cube, un icosaèdre, un dodécaèdre régulier]. Voir l'exercice VII.E3.

VII.19. Proposition. *Soient X un ensemble fini, G un groupe fini agissant sur X par isométries et $\pi : G \longrightarrow GL(\mathbf{C}^X)$ la représentation de permutation associée.*

Si l'action de G sur X est homogène à deux points, alors la représentation π est sans multiplicité.

Démonstration. C'est un cas particulier de la proposition VII.16. □

Exercices

VII.E1 Soient $k \geq 3$ et $D_{2k} = \{1, r, \ldots, r^{k-1}, s, sr, \ldots, sr^{k-1}\}$ le groupe diédral d'ordre $2k$. Soit $\pi_\ell : D_{2k} \longrightarrow GL_2(\mathbf{C})$ la représentation irréductible définie à l'exercice III.E1 en termes de la racine de l'unité $\omega = \exp(2i\pi\ell/k)$; on suppose que $\omega \neq 1, -1$. Le caractère χ_ℓ de π_ℓ est donné par

$$\chi_\ell(r^j) \;=\; 2\cos(j\pi\ell/k) \quad \text{et} \quad \chi_\ell(sr^j) \;=\; 0 \qquad (0 \leq j \leq k-1).$$

Vérifier explicitement la relation du théorème VII.1, c'est–à–dire la relation

$$\frac{1}{2k} \sum_{g \in D_{2k}} \overline{\chi_\ell(g)} \chi_{\ell'}(g) \;=\; \delta_{\ell,\ell'}$$

pour tous $\ell, \ell' \in \{1, \ldots, k-1\}$, $\ell + \ell' \neq k$.

VII.E2 On définit l'intégrale d'une fonction continue f sur le groupe $\mathcal{O}(2)$ de l'exercice V.E7 par

$$\int_{\mathcal{O}(2)} f(g)dg \;=\; \frac{1}{4\pi}\int_0^{2\pi} f(r_\theta)d\theta \;+\; \frac{1}{4\pi}\int_0^{2\pi} f(sr_\theta)d\theta$$

(dg est la "mesure de Haar normalisée" sur le groupe compact $\mathcal{O}(2)$).

Pour $\ell \in \mathbf{Z}$, $\ell \neq 0$, soit χ_ℓ de caractère de la la représentation π_ℓ définie à l'exercice V.E7. Pour $\ell, \ell' \in \mathbf{Z}$, montrer que

$$\int_{\mathcal{O}(2)} \overline{\chi_\ell(g)} \chi_{\ell'}(g) dg \;=\; \delta_{\ell,\ell'}$$

et interpréter. [Voir le théorème VII.1.]

VII.E3 Calculer le rang de l'action de G_P sur l'ensemble des sommets de P lorsque P est un polytope régulier (tétraèdre, cube, octaèdre, dodécaèdre, icosaèdre) centré à l'origine de $\mathbf{R}^3$. Calculs analogues pour SG_P.

Remarque. Soit k un entier, $k \geq 3$. Considérons un polygone régulier $P(k)$ à k sommets situés sur un équateur de la sphère unité de $\mathbf{R}^3$. Le groupe *spécial* $SG_{P(k)} = \{g \in S\mathcal{O}(3) \mid g(P(k)) = P(k)\}$ contient les rotations d'ordre k d'axe perpendiculaire au plan de $P(k)$ et des demi–tours d'axes passant par des sommets et des milieux de côtés du polygone. C'est un groupe diédral d'ordre $2k$ contenu dans $S\mathcal{O}(3)$.

Notons que le groupe $\mathcal{O}(3)$ contient deux types de sous–groupes, isomorphes mais non conjugués : le groupe ci–dessus, et le groupe $D_{2k} \subset \mathcal{O}(2) \subset O(3)$ des exercices III.E1 et VII.E1. (Une isométrie dans $\mathcal{O}(2)$ est identifiée à l'isométrie de $\mathcal{O}(3)$ dont la restriction à l'axe perpendiculaire à $P(k)$ est l'identité.)

VII.E4* Soit C un cube centré à l'origine, comme en VII.12 et VII.13, et soient T, T' les deux tétraèdres réguliers dont les sommets sont des sommets de C.

(i) Montrer les isomorphismes

$$\begin{aligned} SG_T &\simeq \mathrm{Alt}(4), \qquad & G_T &\simeq \mathrm{Sym}(4) \\ SG_C &\simeq \mathrm{Sym}(4), \qquad & G_C &\simeq \mathrm{Sym}(4) \times C_2 \end{aligned}$$

où C_2 désigne le groupe à deux éléments $\{\pm id\}$.

[Indication : considérer les actions naturelles de SG_T et G_T sur l'ensemble des sommets du tétraèdre, ainsi que l'action de SG_C sur les quatres diagonales du cube.]

(ii) Interpréter en termes des groupes SG_T et SG_C les suites exactes courtes

$$\{1\} \longrightarrow \mathbf{V} \longrightarrow \mathrm{Alt}(4) \longrightarrow \mathrm{Alt}(3) \longrightarrow \{1\}$$

et

$$\{1\} \longrightarrow \mathbf{V} \longrightarrow \mathrm{Sym}(4) \longrightarrow \mathrm{Sym}(3) \longrightarrow \{1\}$$

où $\mathbf{V}$ désigne un groupe d'ordre 4 non cyclique.

[Indication. Le groupe SG_T [respectivement le groupe SG_C] agit sur l'ensemble à trois éléments des axes orthonormaux passant par les milieux des arêtes du tétraèdre [resp. par les centres des faces du cube].]

(iii) Définissons des homomorphismes $\epsilon_j : G_C \longrightarrow \{1, -1\}$, $j = 1, 2$, par

$$\epsilon_1(g) = \begin{cases} 1 & \text{si } g \text{ est une rotation de } \mathbf{R}^3, \\ -1 & \text{si } g \text{ renverse l'orientation de } \mathbf{R}^3, \end{cases}$$

et

$$\epsilon_2(g) = \begin{cases} 1 & \text{si } g(T) = T, \\ -1 & \text{si } g(T) = T'. \end{cases}$$

Décrire les noyaux de ϵ_1, ϵ_2 et $\epsilon_1\epsilon_2$. Parmi ces trois, y a–t–il des paires de sous–groupes qui sont isomorphes ? conjugués dans G_C ?

(iv) Construire un modèle en carton d'un icosaèdre régulier. Dessiner sur ses faces les arêtes d'un cube C dont les sommets sont certains sommets de l'icosaèdre, et marquer les sommets d'un tétraèdre régulier T inscrit dans ce cube.

En déduire que SG_T est un sous–groupe de SG_C et de SG_I. Vérifier que SG_C n'est pas un sous–groupe de SG_I.

VII.E5* Notons Y l'ensemble des sommets du cube introduit en VII.12 et posons $W = \mathbf{C}^Y$. Notons $\rho : G_C \longrightarrow GL(W)$ la représentation de permutation du groupe des symétries du cube dans l'espace W et considérons le laplacien $L : W \longrightarrow W$ défini *formellement* comme au numéro VII.12, c'est–à–dire par

$$(L\psi)(y) = \frac{1}{3} \sum_{\text{voisins de } y} \psi(y).$$

Vérifier que l'action de G_C sur Y est de rang quatre, décrire les quatres sous–espaces vectoriels correspondants de W invariants par G_C, et calculer l'effet de L dans chacun d'eux.

VII.E6 Soit SG_I le *groupe spécial de l'icosaèdre*, groupe des rotations laissant invariant un icosaèdre régulier I centré à l'origine, comme à l'exemple VII.11, et soit D l'ensemble des six diagonales de l'icosaèdre, c'est–à–dire des six droites déterminées par les paires de sommets opposés.

Vérifier que l'action naturelle de SG_I sur D est doublement transitive, de sorte que SG_I possède une représentation irréductible de degré 5 (proposition VII.9.i).

Voir aussi l'exercice XI.E5.

VII.E7 Soit SG_I le groupe de l'exercice précédent. Montrer que les sous–ensembles de SG_I décrits à l'exemple VII.11, respectivement à $1, 20, 15, 12$ et 12 éléments, sont les classes de conjugaison de SG_I.

En déduire que le groupe SG_I est simple. [Indication. L'ordre d'un sous–groupe normal non réduit à un élément est un diviseur de 60 de la forme $n = 1 + 12a + 15b + 20c$, où a, b, c sont des entiers positifs non tous nuls. Il en résulte que $n = 60$.]

Vérifier que le groupe G_I des isométries de l'icosaèdre est isomorphe au produit direct de SG_I et du groupe $\{\pm id\}$ d'ordre 2.

VII.E8 Le groupe SG_I de l'exercice VII.E6 est aussi le groupe des rotations de $\mathbf{R}^3$ laissant invariant un dodécaèdre régulier centré à l'origine (le dodécaèdre dont les sommets sont aux centres des faces de l'icosaèdre). En choisissant[18] convenablement 8 des 12 sommets du dodécaèdre, on obtient un cube, et il y a exactement cinq tels cubes ; ce qui fournit[19] une action naturelle de SG_I sur un ensemble à cinq éléments, autrement dit un homomorphisme φ de SG_I vers le groupe symétrique Sym(5).

(i) Vérifier que l'action décrite ci–dessus est de rang deux, de sorte que SG_I possède une représentation irréductible de degré 4.

(ii) En utilisant le résultat de l'exercice précédent, vérifier que φ induit un *isomorphisme* de SG_I avec le groupe alterné Alt(5).

VII.E9 On considère le groupe symétrique Sym(5), la permutation $c_5 = (1, 2, 3, 4, 5)$, et son centralisateur dans Sym(5), noté $Z(c_5)$.

Montrer que $Z(c_5)$ coïncide avec le groupe cyclique engendré par c_5.

En déduire que la restriction α au groupe alterné Alt(5) de la conjugaison par la transposition $(1, 2)$ n'est pas un automorphisme intérieur.

[Indication : S'il existe $s \in \mathrm{Sym}(5)$ tel que $\alpha(g) = s^{-1}gs$ pour tout $g \in \mathrm{Alt}(5)$, alors $(1, 2)s \in Z(c_5) \subset \mathrm{Alt}(5)$ et $s \notin \mathrm{Alt}(5)$.]

VII.E10 Soit π la représentation complexe du groupe SG_I obtenue en composant une inclusion de SG_I dans $GL_3(\mathbf{R})$ et l'inclusion canonique de $GL_3(\mathbf{R})$ dans $GL_3(\mathbf{C})$; la représentation π est irréductible (exemple VII.11). On considère désormais π comme une représentation du groupe Alt(5).

Soit α l'automorphisme de Alt(5) de l'exercice VII.E9. Déduire de la comparaison de leurs caractères que les représentations irréductibles π et $\pi\alpha$ (voir l'exemple I.6) sont non équivalentes.

Noter que α échange les deux classes de conjugaison à 12 éléments.

---

[18]Voici, en coordonnées cartésiennes, les sommets d'un dodécaèdre régulier rendant l'un des 5 cubes évidemment “visible” :

$$(0, \pm\tau^{-1}, \pm\tau), \quad (\pm\tau, 0, \pm\tau^{-1}), \quad (\pm\tau^{-1}, \pm\tau, 0), \quad (\pm 1, \pm 1, \pm 1)$$

où $\tau = \frac{1}{2}(1 + \sqrt{5})$. Ce sont les formules $3 \cdot 76$ de [Coxet–73].

[19]Certaines lectrices considéreront plutôt l'action par conjugaison de Alt(5) sur ses cinq 2-Sylow.

En revanche, si π' est une des représentations irréductibles de SG_I de dimension 1, 4 ou 5 (voir les exercices VII.E6 et VII.E8), alors $\pi'\alpha$ et π' sont équivalentes.

VII.E11 Soient G un groupe fini, c un élément de G et $Z_G(c) = \{g \in G \mid gc = cg\}$ son centralisateur, qui est un sous–groupe de G. Montrer que le nombre d'éléments de la classe de conjugaison C de c est égal à l'indice de $Z_G(c)$ dans G.

[Indication : l'action $G \times C \longrightarrow C, (g, x) \longmapsto gxg^{-1}$ de G sur C est transitive, et fournit une bijection de l'espace quotient $G/Z_G(c)$ sur C.]

VII.E12 Soient G un groupe fini, H un sous–groupe d'indice deux, et k un élément de G qui n'est pas dans H. Soient C une classe de conjugaison de G contenue dans H et c un élément de C. Soit $Z_G(c)$ le centralisateur de c dans G, c'est–à–dire $\{g \in G \mid gc = cg\}$; notons que la classe C s'identifie à l'espace homogène $G/Z_G(c)$. Vérifier les assertions suivantes, selon que $Z_G(c)$ n'est pas contenu ou est contenu dans H.

(i) Cas de $Z_G(c) \not\subset H$. Pour tout $g \in G$, il existe $h \in H$ tel que $hch^{-1} = gcg^{-1}$, de sorte que C est une classe de conjugaison de H.

(ii) Cas de $Z_G(c) \not\subset H$. La classe C est réunion de deux classes de conjugaison de H représentées par c et kck^{-1}.

Que pouvez-vous dire des classes de conjugaison du groupe alterné $\mathrm{Alt}(k)$ pour $k \leq 5$?

VII.E13 Reprenons les notations de l'exemple VII.8 : l'action du groupe G sur l'ensemble X est transitive de rang r et la représentation de permutation correspondante possède une décomposition en irréductibles $\pi = \chi_1 \oplus \left(\bigoplus_{j=2}^k m_j \pi_j\right)$, avec $r = 1 + \sum_{j=2}^k m_j^2$.

Montrer que, si la restriction de l'action au groupe des commutateurs $D(G)$ est transitive, alors les degrés de $\pi_2, \ldots, \pi_k$ sont tous strictement supérieurs à 1.

[Indication : la restriction à $D(G)$ d'une représentation de degré 1 de G est l'identité.]
Remarque. Grâce au théorème de réciprocité de Frobenius, on peut montrer la réciproque : s'il existe $j \in \{2, \ldots, k\}$ tel que le degré de π_j soit 1, alors $D(G)$ n'est pas transitif sur X.[20]

VII.E14 Soit $k \geq 2$ un entier. Pour tout $j \in \{0, 1, \ldots, k\}$, on désigne par a_j le nombre de permutations de k objets ayant exactement j points fixes. Montrer que

$$2\sum_{j=1}^{k} j a_j = \sum_{j=1}^{k} j^2 a_j.$$

[Indication : si π_0 désigne la sous–représentation irréductible de degré $k-1$ de la représentation définie par l'action du groupe $\mathrm{Sym}(k)$ sur $\{1, \ldots, k\}$, le produit scalaire par lui-même de son caractère vaut 1.]

[20] La représentation π est l'induite $\mathrm{Ind}_H^G(1_H)$. Convenons d'écrire $\langle \rho \mid \sigma \rangle$ le produit scalaire des caractères de deux représentations ρ, σ. Supposons que la retriction de l'action de G à $D(G)$ n'est pas transitive. Alors $\langle \mathrm{Res}_{D(G)}^G \mathrm{Ind}_H^G 1_H \mid 1_{D(G)} \rangle \geq 2$. Par réciprocité de Frobenius, le membre de gauche de cette inégalité est égal à $\langle \mathrm{Ind}_H^G 1_H \mid \mathrm{Ind}_{D(G)}^G 1_{D(G)} \rangle$, de sorte qu'il existe une sous-représentation irréductible σ de $\mathrm{Ind}_{D(G)}^G 1_{D(G)}$ qui apparaît dans π. Or $\mathrm{Ind}_{D(G)}^G 1_{D(G)}$ s'identifie à la représentation régulière du groupe abélien $G/D(G)$, donc σ est de degré 1.

VII.E15 Soient G un groupe de permutation doublement transitif d'un ensemble fini X à n éléments et π la représentation de permutation correspondante. Conformément aux notations du numéro VII.15, on pose

$$E_1 \;=\; \sum_{x \in X} E_{x,x} \quad \text{et} \quad E_2 \;=\; \sum_{(y,z) \in X \times X, y \neq z} E_{y,z}.$$

Montrer que

$$E_1^2 = E_1, \quad E_1(E_1 + E_2) = (E_1 + E_2)E_1 = E_1 + E_2 \quad \text{et} \quad (E_1 + E_2)^2 = E_1 + E_2.$$

Si $U_1 = \left(1 + \frac{1}{n}\right) E_1 - \frac{1}{n} E_2$ et $U_2 = \frac{1}{n} E_2$, vérifier que l'algèbre $\pi(G)'$ est linéairemenet engendrée par les éléments U_1 et U_2, qui satisfont

$$U_1^2 = U_1, \quad U_2^2 = U_2, \quad U_1 U_2 = U_2 U_1 = 0, \quad U_1 + U_2 = 1.$$

(Ici, 1 désigne l'unité de l'algèbre $\pi(G)'$, c'est–à–dire l'identité de V.)

VII.E16 Soient $k \geq 1$ un entier, D_{2k} le groupe diédral d'ordre $2k$, vu comme groupe des isométries d'un polygone régulier à k côtés, et σ une symétrie du polygone. On note C_2 le sous–groupe $\{1, \sigma\}$ de D_{2k}. Montrer que (D_{2k}, C_2) est une paire de Gelfand.

[Indication : considérer l'action de D_{2k} sur l'ensemble des sommets du polygone.]

VII.E17 Avec les notations du numéro VII.17, montrer que l'action du groupe symétrique $\mathrm{Sym}(n)$ sur l'ensemble des k–blocs $\mathcal{B}_k(n)$ est généreusement transitive. Vérifier que le rang de cette action est $\min\{k, n-k\} + 1$.

Il résulte donc de la proposition VII.16 que la représentation de permutation correspondante est sans multiplicité, et plus précisément qu'elle est somme directe de $\min\{k, n-k\}+1$ sous-représentations irréductibles non équivalentes deux à deux. (Voir aussi les nos 29.12 à 29.14 de [JamLi–01].)

Observer que $\mathcal{B}_k(n)$ est un espace métrique pour la distance définie par $d(x,y) = k - |x \cap y|$. L'action naturelle du groupe $\mathrm{Sym}(n)$ est alors une action par isométries, qui est de plus homogène à deux points (voir VII.18).

De même, montrer que l'action du groupe projectif linéaire $PGL_n(\mathbf{F}_q)$ sur la grassmannienne $\mathcal{G}_k(n)$ des sous–espaces de dimension k dans $\mathbf{F}_q^n$ est généreusement transitive, et déterminer son rang.

VII.E18 Soient $q = p^a$ une puissance d'un nombre premier ($a \geq 1$) et $\mathbf{F}_q$ le corps à q éléments. Pour $k \geq 1$, le groupe symétrique $\mathrm{Sym}(k)$ agit sur l'espace vectoriel $\mathbf{F}_q^k$ par permutation des coordonnées. Notons $\mathbf{F}_q^k \rtimes \mathrm{Sym}(k)$ le produit semi–direct correspondant ; rappelons que le produit s'y écrit $(x, \sigma)(y, \tau) = (x + \sigma(y), \sigma\tau)$.

Le groupe $\mathbf{F}_q^k \rtimes \mathrm{Sym}(k)$ agit sur $\mathbf{F}_q^k$ par

$$((x, \sigma), z) \;=\; x + \sigma(z).$$

L'action est transitive, et le groupe d'isotropie de l'origine s'identifie au sous–groupe $\mathrm{Sym}(k)$ de $\mathbf{F}_q^k \rtimes \mathrm{Sym}(k)$. On peut observer que cette action est isométrique pour la *distance de Hamming*, définie sur $\mathbf{F}_q^k$ par $d(x,y) = |\{j \in \{1, \ldots, k\} \mid x_j \neq y_j\}|$.

Si $p = 2$, vérifier que l'action de $\mathbf{F}_q^k \rtimes \mathrm{Sym}(k)$ sur $\mathbf{F}_q^k$ est généreusement transitive.

[Indication : pour $y, z \in \mathbf{F}_q^k$, la translation $x \longmapsto x + z - y$ échange y et z. Remarque : si $q = 2$, on peut observer que l'action est homogène à deux points.]

Si p est impair, montrer que cette action n'est pas généreusement transitive.

Nous verrons toutefois à l'exemple XV.10 que la paire $(\mathbf{F}_q^k \rtimes \mathrm{Sym}(k), \mathrm{Sym}(k))$ est de Gelfand dans tous les cas.

VII.E19 Soient G un groupe fini et H un sous–groupe de G. Si φ est une fonction sur G, on définit $\check{\varphi}$ par $\check{\varphi}(g) = \varphi(g^{-1})$; on vérifie que l'endomorphisme $J : \varphi \longmapsto \check{\varphi}$ est un antiautomorphisme de l'algèbre du groupe $\mathbf{C}[G]$. Montrer que les conditions suivantes sont équivalentes

(i) l'action de G sur G/H est généreusement transitive ;
(ii) $g^{-1} \in HgH$ pour tout $g \in G$;
(iii) $\mathbf{C}[H \setminus G/H]$ est contenu dans l'algèbre des points fixes de J.

Ces conditions impliquent que (G, H) est une paire de Gelfand (proposition VII.16). Comparer avec la proposition XV.9.

Une paire de Gelfand est dite *symétrique* si elle satisfait les conditions ci–dessus.

VIII. Digression : le lemme de Cauchy–Frobenius–Burnside

Soit G un groupe fini opérant sur un ensemble fini X. Le but de ce chapitre est d'une part d'offrir une autre preuve des égalités

$$m \;=\; \frac{1}{|G|}\sum_{g \in G} |X^g| \qquad \text{et} \qquad r \;=\; \frac{1}{|G|}\sum_{g \in G} |X^g|^2$$

du chapitre précédent, indépendante de la théorie des représentations[21], et d'autre part d'exposer plusieur exemples (notamment dans les exercices).

Voici d'abord quelques notations et rappels (pour lesquels il n'est pas nécessaire que G et X soient finis). Le *groupe d'isotropie* d'un point x de X est le sous–groupe

$$G_x \;=\; \{h \in G \mid hx = x\}$$

de G. L'*orbite* de x est

$$Gx \;=\; \{y \in X \mid \text{il existe } g \in G \text{ tel que } y = gx\}.$$

Pour $x \in X$, le groupe G opère naturellement sur l'orbite Gx ; l'application $G \longrightarrow Gx$, $g \longmapsto gx$ "passe au quotient" et fournit une *bijection* $G/G_x \longrightarrow Gx$, $gG_x \longmapsto gx$. Si G et X sont finis, il en résulte en particulier que

$$|G| \;=\; |G_x|\,|Gx|$$

pour tout $x \in X$.

Les groupes d'isotropie de deux points x et $y = gx$ d'une même G–orbite sont conjugés : $G_y = gG_xg^{-1}$; en particulier, ils ont même ordre.

Pour la suite, **on suppose à nouveau systématiquement le groupe G et l'ensemble X finis.** Le résultat suivant, souvent appelé "lemme de Burnside", semble être dû à Cauchy et Frobenius [Neuma–79]. Comparer avec l'égalité (*) de l'exemple VII.7.

[21] Voir (*) et (**) aux exemples VII.7 et VII.8, ainsi que VIII.1 et VIII.5 ci-dessous.

VIII.1. Lemme de Cauchy–Frobenius–Burnside. *Si G possède m orbites sur X, alors*

$$m|G| \;=\; \sum_{g\in G} |X^g|.$$

VIII.2. Exemple. Soit SG_T le groupe spécial du tétraèdre, c'est–à–dire (voir VII.E3) le groupe des rotations laissant invariant un tétraèdre régulier centré à l'origine de $\mathbf{R}^3$, vu comme opérant sur l'ensemble X des sommets du tétraèdre. Alors $m = 1$, car SG_T opère transitivement sur X. Le groupe SG_T a 12 éléments qui sont

l'identité laissant fixe les 4 points de X,
trois rotations d'ordre 2 ne laissant fixe aucun point de X,
huit rotations d'ordre 3 laissant fixe un point de X chacune.

On vérifie que $12 = 1 \times 4 + 3 \times 0 + 8 \times 1$.

Démonstration du lemme VIII.1. Notons $\mathcal{F}$ l'ensemble des paires $(g, x) \in G \times X$ telles que $gx = x$. Il est d'une part évident que

$$|\mathcal{F}| \;=\; \sum_{g\in G} |X^g|.$$

D'autre part

$$|\mathcal{F}| \;=\; \sum_{x\in X} |G_x| \;=\; |G| \sum_{x\in X} \frac{1}{|Gx|}.$$

Or la somme sur X est aussi la somme sur les orbites de la somme sur les points de chaque orbite, de sorte que

$$\sum_{x\in X} \frac{1}{|Gx|} \;=\; \sum_{\mathcal{O}} \sum_{x\in\mathcal{O}} \frac{1}{|Gx|} \;=\; \sum_{\mathcal{O}} 1 \;=\; m.$$

Le "lemme" résulte de ces égalités. □

Nous avons déjà observé en VII.8 que, vu le lemme VIII.1, il existe dans G des éléments agissant sans point fixe. Le corollaire suivant précise cela.

VIII.3. Corollaire. *Si le groupe G est transitif sur X et si $|X| = n \geq 2$, alors il existe dans G au moins $n - 1$ éléments sans point fixe.*

Démonstration. Soit t le nombre d'éléments de G sans point fixe. En séparant dans la somme $\sum_{g\in G} |X^g|$

l'identité,
les autres éléments avec points fixes,
les éléments sans point fixe,

on obtient

$$|G| \;=\; n + \sum_{g\in G, |X^g|\geq 1} |X^g| \;\geq\; n + (|G| - 1 - t)$$

et par suite $1 + t \geq n$. □

Raffinement plus récent : il existe un premier p et un entier $a \geq 1$, et il existe dans G un élément sans point fixe d'ordre p^a [FeKaS–81]. (La démonstration utilise la complétude de la "classification des groupes finis simples".)

Avant de formuler un second corollaire du lemme de Cauchy–Frobenius–Burnside, revenons à la notion de rang, définie dans l'exemple VII.8, pour une action transitive d'un groupe fini G sur un ensemble $X = G/H$. La proposition suivante montre que c'est à la fois le nombre des G–orbites de $X \times X$, le nombre des H–orbites de X, ainsi que le nombre $|H \setminus G/H|$ des doubles classes de G modulo H.

Notons que, de même que G/H peut être interprété comme l'ensemble des H–orbites pour l'action de H sur G par multiplication à droite, de même $H \setminus G/H$ "est" l'ensemble des H–orbites pour l'action naturelle (à gauche) de H sur G/H (ou pour l'action à droite de H sur $H \setminus G$!).

VIII.4. Proposition. *Soit G un groupe opérant transitivement sur un ensemble X. Soit $x_0 \in X$; notons H le groupe d'isotropie de x_0 dans G. Il existe des bijections naturelles entre*

(i) *l'ensemble des orbites de G dans $X \times X$ (pour l'action diagonale),*
(ii) *l'ensemble des orbites de H dans X,*
(iii) *l'ensemble $H \setminus G/H$ des doubles classes de G modulo H.*

Démonstration. A toute orbite Δ de G dans $X \times X$, associons le sous–ensemble

$$\Delta(x_0) \;=\; \{y \in X \mid (x_0, y) \in \Delta\}.$$

Notons que

$\Delta(x_0)$ est une H–orbite dans X,
$\Delta(x_0) = \{x_0\}$ si Δ est la diagonale de $X \times X$.

A toute orbite $\mathcal{O}$ de H dans X, associons

$$\Delta_{\mathcal{O}} \;=\; \{(x, y) \in X \times X \mid \text{il existe } g \in G \text{ tel que } gx = x_0 \text{ et } gy \in \mathcal{O}\};$$

si y_0 désigne un point de $\mathcal{O}$, l'ensemble $\Delta_{\mathcal{O}}$ est la G–orbite de (x_0, y_0). Notons que

$\Delta_{\mathcal{O}}$ est une G–orbite dans $X \times X$,
$\Delta_{\mathcal{O}}$ est la diagonale si $\mathcal{O} = \{x_0\}$.

Les applications $\Delta \longmapsto \Delta(x_0)$ et $\mathcal{O} \longmapsto \Delta_{\mathcal{O}}$ sont inverses l'une de l'autre ; elles établissent une bijection entre les ensembles de (i) et (ii).

La bijection entre les ensembles de (ii) et (iii) résulte de la définition de l'ensemble des classes doubles $H \setminus G/H$. □

VIII.5. Corollaire (du lemme de Cauchy–Frobenius–Burnside). *Si G est un groupe fini transitif sur X, de rang r, alors*

$$r|G| \;=\; \sum_{g \in G} |X^g|^2.$$

Il convient de comparer avec l'égalité (**) de l'exemple VII.8.

Démonstration. C'est une conséquence immédiate de VIII.1 appliqué à l'action de G sur $X \times X$ et des égalités $(X \times X)^g = X^g \times X^g$, pour tout $g \in G$. □

Voici une autre démonstration du corollaire VIII.5, en termes de l'action du groupe d'isotropie G_x d'un point x de X. En appliquant le lemme VIII.1 à l'action de G_x sur X, on obtient

$$r|G_x| \;=\; \sum_{h \in G_x} |X^h|.$$

Le membre de gauche de cette égalité est égal à $r|G|/|X|$. Pour le membre de droite, et vu que G_y est conjugé à G_x pour tout $y \in X$, nous avons[22]

$$|X| \sum_{h \in G_x} |X^h| \;=\; \sum_{y \in X} \sum_{g \in G_y} |X^g| \;\stackrel{*}{=}\; \sum_{g \in G} \sum_{y \in X^g} |X^g| \;=\; \sum_{g \in G} |X^g|^2.$$

Le corollaire VIII.5 résulte des égalités ci–dessus.

VIII.6. Exemple. Dans la situation de l'exemple VIII.2 (groupe SG_T des rotations d'un tétraèdre sur l'ensemble des 4 sommets, de rang 2), on vérifie que $2 \times 12 = 1 \times 4^2 + 3 \times 0^2 + 8 \times 1^2$.

Signalons pour terminer un type standard d'application de VIII.1 à d'autres problèmes que des problèmes de représentation.

.

VIII.7. Dénombrement. Le lemme de Cauchy–Frobenius–Burnside permet parfois de dénombrer des ensembles. Voici un exemple simple.

On se donne un entier $k \geq 1$. Notons S_k l'ensemble des suites de 0 et de 1 de longueur k ; c'est un ensemble à 2^k éléments. Le groupe cyclique d'ordre k, noté ici $C_k = \{1, 2, \ldots, k\}$, agit sur S_k par $j(x_1, \ldots, x_k) = (x_{1+j}, \ldots, x_{k+j})$, où les sommes sont à prendre modulo k. Notons T_k l'ensemble quotient, qui est un modèle de *l'ensemble des colliers circulaires à k perles blanches ou noires.* On se propose de compter le nombre N_k des éléments de l'ensemble T_k. Il est facile de vérifier que $N_1 = 2$, $N_2 = 3$, $N_3 = 4$, $N_4 = 6$, …, mais le calcul de N_k devient plus délicat à mesure que k augmente.

Soit $j \in C_k$. Rappelons que j est d'ordre k/d_j où d_j désigne le plus grand commun diviseur de k et j (vu cette fois comme un entier). Les éléments de S_k fixés par j sont exactement les suites de période d_j, qui sont au nombre de 2^{d_j}. Pour un diviseur d de k, le nombre des éléments j de C_k tels que $d_j = d$ est donné par la valeur en k/d de la fonction φ d'Euler. [Rappel : $\varphi(m)$ désigne le nombre des entiers entre 1 et m (inclus) qui sont premiers à m. Ainsi $\varphi(p^a) = p^a - p^{a-1}$ pour p premier et $a \geq 1$, et $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$ si m_1 et m_2 sont premiers entre eux.]

C'est une conséquence du lemme de Cauchy–Frobenius–Burnside que

$$N_k \;=\; \frac{1}{k} \sum_{j=1}^{k} 2^{d_j} \;=\; \frac{1}{k} \sum_{d|k} \varphi\left(\frac{k}{d}\right) 2^d.$$

On obtient par exemple

$$\begin{aligned}
N_4 \;&=\; \frac{1}{4}\Big(\varphi(4)2 + \varphi(2)4 + \varphi(1)16\Big) \;=\; \frac{1}{4}\Big(4 + 1 + 16\Big) \;=\; 6, \\
N_5 \;&=\; \frac{1}{5}\Big(\varphi(5)2 + \varphi(1)32\Big) \;=\; \frac{1}{5}\Big(8 + 32\Big) \;=\; 8, \\
N_6 \;&=\; \frac{1}{6}\Big(\varphi(6)2 + \varphi(3)4 + \varphi(2)8 + \varphi(1)64\Big) \;=\; \frac{1}{6}\Big(4 + 8 + 8 + 64\Big) \;=\; 14.
\end{aligned}$$

[22] Noter l'analogie de l'égalité $\stackrel{*}{=}$ avec un changement de l'ordre des intégrations dans une intégrale double.

On pourrait bien sûr remplacer l'action du groupe cyclique C_k par celle du groupe diédral D_{2k} (décalages et symétries des suites de S_k) ; ce serait un autre modèle de "l'ensemble des colliers à k perles", fournissant d'autres nombres N'_k.

Pour d'autres exemples et informations sur cette méthode de Polya, voir par exemple le chapitre 36 de [VLiWi–92] et les pages 58–62 de [Rotma–95].

Exercices et compléments

VIII.E1 Soient k un nombre entier, $k \geq 3$, et $I_k = \{1, \dots, k\}$. Calculer le nombre des orbites des actions naturelles de $\mathrm{Sym}(k)$ et $\mathrm{Alt}(k)$ sur $(I_k)^3$.

VIII.E2 Soit G un groupe fini ; notons k le nombre des classes de conjugaison de G. Montrer que

$$|\{(g,h) \in G \times G \mid gh = hg\}| \; = \; k|G|.$$

[Considérer l'action de G sur lui–même par conjugaison.]

VIII.E3* Soits $\mathbf{K}$ un corps. Le *groupe affine* de $\mathbf{K}$ est le groupe $\mathrm{Aff}(\mathbf{K})$ des transformations de $\mathbf{K}$ de la forme $x \longmapsto ax + b$, avec $a \in \mathbf{K}^*$ et $b \in \mathbf{K}$. Il est isomorphe au groupe des matrices de la forme $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. Le sous–groupe $\mathrm{Transl}(\mathbf{K})$ des translations $x \longmapsto x + b$ correspond au groupe des matrices pour lesquelles $a = 1$; c'est un sous–groupe normal de $\mathrm{Aff}(\mathbf{K})$.

Le calcul

$$\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c^{-1} & -c^{-1}d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & (1-a)d + cb \\ 0 & 1 \end{pmatrix}$$

montre que deux affinités $x \longmapsto ax + b$ et $x \longmapsto a'x + b'$ sont conjuguées dans $\mathrm{Aff}(\mathbf{K})$ si et seulement si l'une des trois situations suivantes est réalisée : (i) $a = a' \neq 1$, (ii) $a = a' = 1$ et $b \neq 0 \neq b'$, (iii) $a = a' = 1$ et $b = b' = 0$. En particulier, si $\mathbf{K} = \mathbf{F}_q$ est fini, le nombre des classes de conjugaison du groupe $\mathrm{Aff}(\mathbf{K})$ est $q + 1$.

Le commutateur de deux éléments de $\mathrm{Aff}(\mathbf{K})$ est dans $\mathrm{Transl}(\mathbf{K})$. Le calcul

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (1-a^{-1})b \\ 0 & 1 \end{pmatrix}$$

montre que, si $\mathbf{K}$ n'est pas le corps à deux éléments, le groupe dérivé de $\mathrm{Aff}(\mathbf{K})$ coïncide avec $\mathrm{Transl}(\mathbf{K})$. Par suite, si $\mathbf{K} \neq \mathbf{F}_2$, l'homomorphisme

$$\begin{cases} \mathrm{Aff}(\mathbf{K}) \longrightarrow \mathbf{K}^* \\ (x \mapsto ax + b) \longmapsto a \end{cases}$$

induit un isomorphisme de l'abélianisé de $\mathrm{Aff}(\mathbf{K})$ sur $\mathbf{K}^*$. Par ailleurs, $\mathrm{Aff}(\mathbf{F}_2) \simeq \mathbf{F}_2$.

(i) Vérifier que l'action naturelle de $AGL_1(\mathbf{K})$ sur $\mathbf{K}$ est doublement transitive.

Dans (ii) à (iv), on suppose que $\mathbf{K} = \mathbf{F}_q$ est fini et que $q > 2$.

(ii) Pour l'action naturelle de $\mathrm{Aff}(\mathbf{F}_q)$ sur $\mathbf{F}_q$, vérifier l'égalité du lemme de Cauchy–Frobenius–Burnside ainsi que l'égalité du corollaire VIII.5.

(iii) Montrer que la liste complète (à équivalence près) des représentations complexes irréductibles de $\mathrm{Aff}(\mathbf{F}_q)$ est constituée de $q-1$ caractères linéaires et d'une représentation de degré $q-1$.

(iv) Lorsque $\mathbf{K} = \mathbf{F}_q$ avec q premier impair et $q > 3$, investiguer l'analogue de (iii) pour le sous–groupe $B_2(\mathbf{F}_q)$ de $\mathrm{Aff}(\mathbf{F}_q)$ constitué des affinités de la forme $x \longmapsto a^2x + b$. [Rappel : dans un corps fini $\mathbf{F}_q$ d'ordre impair, le sous–groupe $(\mathbf{F}_q^*)^2$ de $\mathbf{F}_q^*$ formé des carrés est d'indice deux dans $\mathbf{F}_q$.]

(v) Pour tout entier $n \geq 1$, définir un groupe affine $\mathrm{Aff}_n(\mathbf{K})$ généralisant $\mathrm{Aff}(\mathbf{K}) = \mathrm{Aff}_1(\mathbf{K})$ et vérifier que son action naturelle sur $\mathbf{K}^n$ est doublement transitive.

(vi) Vérifier que le groupe $\mathrm{Aff}_2(\mathbf{F}_2)$ est isomorphe au groupe symétrique de quatre objets.

VIII.E4* Soit V un espace vectoriel sur un corps $\mathbf{K}$. L'*espace projectif* associé à V est l'ensemble $\mathbf{P}(V)$ des droites de V ; la *projection canonique* $p : V \setminus \{0\} \longrightarrow \mathbf{P}(V)$ associe à tout vecteur $v \neq 0$ de V la droite passant par v. Notons que, si V est de dimension 1, l'espace $\mathbf{P}(V)$ est réduit à un point ; en général, si V est de dimension $n+1$, on dit que $\mathbf{P}(V)$ est de *dimension n*. Ainsi, $\mathbf{P}(\mathbf{K}^2)$ est la *droite projective* de $\mathbf{K}$, souvent notée $\mathbf{P}^1_{\mathbf{K}}$.

Le groupe général linéaire $GL(V)$ de V agit naturellement sur $V \setminus \{0\}$, et aussi sur l'ensemble quotient $\mathbf{P}(V)$. Identifions le groupe multilicatif $\mathbf{K}^*$ au groupe des homothéties de V ; c'est un sous–groupe central de $GL(V)$, a fortiori normal, qui agit trivialement sur $\mathbf{P}(V)$. On désigne par $PGL(V)$ le quotient du groupe $GL(V)$ par ce sous–groupe normal ; c'est un groupe qui agit naturellement sur $\mathbf{P}(V)$.

Pour $V = \mathbf{K}^{n+1}$, on écrit aussi $GL_{n+1}(\mathbf{K})$ au lieu de $GL(V)$ et $PGL_{n+1}(\mathbf{K})$ au lieu de $PGL(V)$, ainsi que $\mathbf{P}^n_{\mathbf{K}}$ au lieu de $\mathbf{P}(\mathbf{K}^{n+1})$.

Lorsque $V = \mathbf{K}^2$, on peut identifier $\mathbf{P}(V)$ à l'ensemble $\mathbf{P}_{\mathbf{K}} = \mathbf{K} \sqcup \{\infty\}$ obtenu en ajoutant à $\mathbf{K}$ un "point à l'infini" ; une droite d'équation $x = ty$ dans $\mathbf{K}^2$ correspond au point $t \in \mathbf{K} \sqcup \{\infty\}$, et la droite d'équation $x = 0$ correspond au point ∞. Pour l'action naturelle, la classe $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PGL_2(\mathbf{K})$ d'une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{K})$ applique un point $t \in \mathbf{P}_{\mathbf{K}}$ sur le point $\frac{at+b}{ct+d}$. (On adopte les conventions usuelles pour les opérations faisant intervenir ∞, c'est–à–dire $\infty + a = \infty$, $\frac{a}{0} = \infty$ si $a \neq 0$, ainsi que $\frac{a}{\infty} = 0$ et $\frac{\infty}{a} = \infty$ si $a \neq \infty$.)

(i) Montrer que l'action de $PGL_2(\mathbf{K})$ sur $\mathbf{P}_{\mathbf{K}}$ est *triplement transitive* (il a été fait allusion à la définition de ce terme juste avant la proposition VII.9).

(ii) Montrer qu'elle est de plus *simplement triplement transitive*[23] au sens où, pour deux triples ordonnés de points distincts (a, b, c) et (a', b', c') dans $\mathbf{P}_{\mathbf{K}}$, il existe un unique élément $g \in PGL_2(\mathbf{K})$ tel que $ga = a'$, $gb = b'$, et $gc = c'$.

(iii) Expliciter $g \in PGL_2(\mathbf{K})$ tel que $ga = \infty$, $gb = 0$ et $gc = 1$.

[23]La classification des groupes finis de permutation qui sont simplement triplement transitifs est due à Zassenhaus (1936). Il existe deux telles familles : d'une part les groupes $PGL_2(\mathbf{K})$ agissant sur $\mathbf{P}_{\mathbf{K}}$ (avec $\mathbf{K}$ fini), comme ci–dessus, et d'autre part des "variantes tordues", agissant également sur $\mathbf{P}_{\mathbf{K}}$, lorsque $\mathbf{K}$ est un corps à p^{2a} éléments, avec p un premier impair et $a \geq 1$, comme exposé au § 7.6 de [DixMo–96]. Bien mieux pour comrendre cette famille d'exemples (ajouté fin mars) : B. Huppert et N. Blackburn, *Finite groups III,* Grundlehren 243, Springer 1982, paragraphe XI.1, exemple 1.3.c.

(iv) En revanche, pour $n \geq 2$, l'action naturelle de $PGL_{n+1}(\mathbf{K})$ sur $\mathbf{P}^n_{\mathbf{K}}$ n'est pas triplement transitive.

(v) Calculer l'ordre du groupe $PGL_2(\mathbf{F}_2)$. [Noter que $\mathbf{F}_2^*$ n'a qu'un élément, donc que $PGL_2(\mathbf{F}_2) = GL_2(\mathbf{F}_2)$.]

Vérifier dans ce cas l'égalité du lemme de Cauchy–Frobenius–Burnside ainsi que l'égalité du corollaire VIII.5.

Calculer l'ordre du groupe $PGL_2(\mathbf{F}_q)$ pour $q \in \{3, 4, 5\}$.

VIII.E5* Le noyau du déterminant det : $GL_{n+1}(\mathbf{K}) \longrightarrow \mathbf{K}^*$ est le *groupe spécial linéaire* $SL_{n+1}(\mathbf{K})$. On note $PSL_{n+1}(\mathbf{K})$ le quotient de ce groupe par le sous–groupe des matrices diagonales de la forme diag$(a, \ldots, a)$ avec $a \in \mathbf{K}$ et $a^{n+1} = 1$. C'est un sous–groupe de $PGL_{n+1}(\mathbf{K})$; il possède donc une action naturelle sur $\mathbf{P}^n_{\mathbf{K}}$.

Remarques. (i) Si $\mathbf{K}$ est algébriquement clos, alors $PSL_{n+1}(\mathbf{K}) = PGL_{n+1}(\mathbf{K})$.

(ii) Pour la topologie naturelle, le groupe $PSL_2(\mathbf{R})$ est la composante connexe de $PGL_2(\mathbf{R})$; c'est un sous–groupe d'indice 2.

(iii) Nous avons des égalités

$$PSL_2(\mathbf{F}_2) = SL_2(\mathbf{F}_2) = PGL_2(\mathbf{F}_2) = GL_2(\mathbf{F}_2) \qquad \text{et} \qquad PSL_2(\mathbf{F}_4) = SL_2(\mathbf{F}_4).$$

Le groupe $GL_2(\mathbf{F}_2)$ peut aussi être vu comme le groupe des automorphismes du Viergruppe $\mathbf{V} = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Montrer qu'il existe des isomorphismes

$PSL_2(\mathbf{F}_2) \approx \mathrm{Sym}(3)$,
$PSL_2(\mathbf{F}_3) \approx \mathrm{Alt}(4)$,
$PSL_2(\mathbf{F}_4) \approx \mathrm{Alt}(5)$.

Indication : Le groupe $PSL_2(\mathbf{F}_q)$ agit naturellement sur la droite projective $\mathbf{F}_q \sqcup \{\infty\}$; l'action est transitive. L'image de l'homomorphisme correspondant

$$PSL_2(\mathbf{F}_q) \longrightarrow \mathrm{Sym}(\mathbf{F}_q \sqcup \{\infty\})$$

contient :

pour $q = 2$ les transpositions, donc tout le groupe symétrique,
pour $q = 3$ les 3–cycles, donc tout le groupe alterné,
et pour $q = 4$ les 3–cycles, donc tout le groupe alterné [autre argument : l'image contient les permutations de la forme $(a, b)(c, d)$, donc tout le groupe alterné].

(Rappel : le groupe alterné $\mathrm{Alt}(k)$ est engendré par les 3–cycles pour tout $k \geq 3$; si $k \geq 5$, il est également engendré par les produits $(a, b)(c, d)$ de deux transpositions à supports disjoints.)

Complément. Les groupes $SG_T \approx \mathrm{Alt}(4)$, $SG_C \approx \mathrm{Sym}(4)$ et $SG_I \approx \mathrm{Alt}(5)$ ont été vus plus haut comme des sous–groupes de $\mathcal{SO}(3) \approx \mathcal{SU}(2)/\{\pm\,\mathrm{id}\}$; voir les exercices VII.E4 et VII.E8, ainsi que le rappel XIII.1 ci–dessous. On peut bien sûr aussi les voir comme des sous–groupes de $PSL_2(\mathbf{C}) = SL_2(\mathbf{C})/\{\pm\,\mathrm{id}\} = PGL_2(\mathbf{C}) = GL_2(\mathbf{C})/\mathbf{C}^*$. On peut ensuite se demander à quelles conditions, pour un corps $\mathbf{K}$, ce sont des sous–groupes de $PGL_2(\mathbf{K})$. La réponse est donnée au n° 2.5 de [Serre–72].

VIII.E6 Soient $\mathbf{K}$ un corps et $a, b, c, d \in \mathbf{P}^1_{\mathbf{K}}$ quatre points dont les trois premiers sont distincts deux à deux. Le *birapport* $[a, b, c, d]$ de ces quatre points est le "nombre" $t \in \mathbf{K} \sqcup \{\infty\}$ tel qu'il existe $g \in PGL_2(\mathbf{K})$ avec

$$g(a) = \infty, \quad g(b) = 0, \quad g(c) = 1 \quad \text{et} \quad g(d) = t \;;$$

le birapport est bien défini parce que l'action de $PGL_2(\mathbf{K})$ sur la droite projective est simplement triplement transitive (voir l'exercice[24] VIII.E4.ii). Notons que

$$[a, b, c, d] \ = \begin{cases} \infty & \text{si et seulement si} \quad d = a, \\ 0 & \text{si et seulement si} \quad d = b, \\ 1 & \text{si et seulement si} \quad d = c. \end{cases}$$

Supposons désormais que **la caractéristique du corps K n'est pas** 2. Les points a, b, c, d sont dits être *en division harmonique* si $[a, b, c, d] = -1$.

Le groupe $PGL_2(\mathbf{K})$ contient l'homothétie de rapport -1, qui fixe 0 et ∞, et qui échange 1 et -1. Il en résulte d'abord que $[\infty, 0, -1, 1] = [\infty, 0, 1, -1]$, et plus généralement que, pour quatre points a, b, c, d distincts deux à deux, a, b, d, c sont en division harmonique si et seulement si a, b, c, d sont en division harmonique.

Le groupe $PGL_2(\mathbf{K})$ contient aussi $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, qui échange 0 et ∞, et qui fixe 1 et -1. Il en résulte d'abord que $[0, \infty, 1, -1] = [\infty, 0, 1, -1]$, et plus généralement que, pour quatre points a, b, c, d distincts deux à deux, b, a, c, d sont en division harmonique si et seulement si a, b, c, d sont en division harmonique.

Le groupe $PGL_2(\mathbf{K})$ contient encore $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, qui échange d'une part ∞ et 1, et d'autre part 0 et -1. Il en résulte d'abord que $[1, -1, \infty, 0] = [\infty, 0, 1, -1]$, et plus généralement que, pour quatre points a, b, c, d distincts deux à deux, c, d, a, b sont en division harmonique si et seulement si a, b, c, d sont en division harmonique.

Il résulte de ce qui précède que, pour $a, b, c, d \in \mathbf{P}^1_{\mathbf{K}}$ distincts deux à deux, il est sensé d'écrire que $\{a, b\}$ et $\{c, d\}$ sont en division harmonique, ou encore que *les paires* $\{a, b\}$ *et* $\{c, d\}$ *sont harmoniquement conjuguées.* (Ne comptent ni l'ordre des paires ni l'ordre des points dans chaque paire.)

Supposons de plus que $\mathbf{K} = \mathbf{F}_5$ est le corps premier à 5 éléments. Le groupe $PGL_2(\mathbf{F}_5)$ contient l'homothétie de rapport 2, qui fixe 0 et ∞, et qui applique 1 et -1 sur 2 et -2. Il en résulte d'abord que $[\infty, 0, 2, -2] = [\infty, 0, 1, -1]$. Plus généralement, si a, b, c, d, e, f est une énumération des six points de la droite projective sur $\mathbf{F}_5$, il en résulte que les trois conditions suivantes sont équivalentes :

$$(*) \qquad \begin{array}{l} \text{les paires } \{a, b\} \text{ et } \{c, d\} \text{ sont harmoniquement conjuguées,} \\ \text{les paires } \{a, b\} \text{ et } \{e, f\} \text{ sont harmoniquement conjuguées,} \\ \text{les paires } \{c, d\} \text{ et } \{e, f\} \text{ sont harmoniquement conjuguées.} \end{array}$$

L'exercice proprement dit consiste à justifier les assertions suivantes.

(i) Il existe 15 manières de distribuer les éléments d'un ensemble à six éléments en trois sous–ensembles à deux éléments.

(ii) Il existe 5 manières de distribuer les six points de la droite projective sur $\mathbf{F}_5$ en trois sous–ensembles à deux éléments satisfaisant les conditions de (*).

[24]Nous évitons ci-dessous d'utiliser le résultat de l'exercice VIII.E4.iii, selon lequel le birapport est donné $[a, b, c, d] = \frac{c-a}{c-b} : \frac{d-a}{d-b}$. On peut bien sûr fort bien utiliser cette dernière fomule, ou même la prendre comme une définition du birapport, et raccourcir ce qui suit.

(iii) Il résulte de ce qui précède que le groupe $PSL_2(\mathbf{F}_5)$ est isomorphe au groupe alterné Alt(5).

(iv) Voici le début d'un argument plus court pour démontrer que les groupes $PSL_2(\mathbf{F}_5)$ et Alt(5) sont isomorphes.

Dans $PSL_2(\mathbf{F}_5)$, qui est d'ordre 60, l'élément $\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$ est d'ordre 2. Son centralisateur est constitué des éléments $\begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix}$ et $\begin{bmatrix} 0 & y \\ -y^{-1} & y \end{bmatrix}$, avec x et y dans $\mathbf{F}_5^*$; en particulier, ce centralisateur est d'ordre 4, c'est–à–dire d'indice 15 (c'est aussi un 2–Sylow). Par suite, $PSL_2(\mathbf{F}_5)$ contient 15 éléments d'ordre 2. (Il résulte de ce qui suit qu'il n'a a pas d'autre éléments d'ordre 2, mais peut importe ici.)

Par le théorème de Sylow, le nombre de 2–Sylow de $PSL_2(\mathbf{F}_5)$ est un nombre congru à 1 modulo 5 qui divise 60.

Vu ce qui précède que le nombre des 2–Sylow dans $PSL_2(\mathbf{F}_5)$ est exactement 5. Donc $PSL_2(\mathbf{F}_5)$ agit naturellement, par conjugaison, sur cet ensemble à 5 éléments ; d'où un homomorphisme $PSL_2(\mathbf{F}_5) \longrightarrow \mathrm{Sym}(5)$.

On peut alors montrer que cet homomorphisme est injectif d'image Alt(5).

VIII.E7* Soient $\mathbf{K}$ un corps. D'une part, le groupe Sym(4) opère naturellement sur l'ensemble des quadruples de points de $\mathbf{P}^1_{\mathbf{K}}$ distincts deux à deux ; notons $(a^\sigma, b^\sigma, c^\sigma, d^\sigma)$ le résultat de l'action de $\sigma \in \mathrm{Sym}(4)$ sur un tel quadruple (a,b,c,d). D'autre part, le groupe $PGL_2(\mathbf{K})$ agit par action diagonale sur l'ensemble de ces quadruples. Ces deux actions commutent :

$$((ga)^\sigma, (gb)^\sigma, (gc)^\sigma, (gd)^\sigma) \;=\; (g(a^\sigma), g(b^\sigma), g(c^\sigma), g(d^\sigma))$$

pour tous quadruple (a,b,c,d) de points de $\mathbf{P}^1_{\mathbf{K}}$ distincts deux à deux, $g \in PGL_2(\mathbf{K})$ et $\sigma \in \mathrm{Sym}(4)$.

(i) Si $\sigma \in \mathbf{V} = \{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, montrer que

$$[a^\sigma, b^\sigma, c^\sigma, d^\sigma] \;=\; [a,b,c,d]$$

pour tout quadruple (a,b,c,d) de points de $\mathbf{P}^1_{\mathbf{K}}$ distincts deux à deux.

(ii) Si $[a,b,c,d] = t \in \mathbf{P}^1_{\mathbf{K}} \setminus \{0,1\}$, montrer que

$$[a^\sigma, b^\sigma, c^\sigma, d^\sigma] \;\in\; \left\{ t, \frac{1}{t}, 1-t, \frac{1}{1-t}, 1-\frac{1}{t}, \frac{t}{t-1} \right\}$$

pour tout $\sigma \in \mathrm{Sym}(4)$.

(iii) Montrer qu'on définit une action du groupe Sym(4) sur l'ensemble $\mathbf{P}^1_{\mathbf{K}} \setminus \{0,1\}$ en posant

$$\sigma([a,b,c,d]) \;=\; [a^\sigma, b^\sigma, c^\sigma, d^\sigma].$$

Cette action n'est pas fidèle mais factorise par une action du quotient $\mathrm{Sym}(4)/\mathbf{V} \approx \mathrm{Sym}(3)$. Examiner les orbites dans le cas de $\mathbf{K} = \mathbf{C}$.

VIII.E8 Vérifier que les groupes $PSL_2(\mathbf{F}_7)$ et $PSL_3(\mathbf{F}_2)$ sont tous deux d'ordre 168.

VIII.E9 : quelques groupes simples. Terminons par quelques affirmations culturelles. On peut montrer que les groupes $PSL_2(\mathbf{F}_7)$ et $PSL_3(\mathbf{F}_2)$ sont isomorphes. Voir par exemple [Dieud–54].

Les groupes $PSL_n(\mathbf{F}_q)$ sont simples, à deux exceptions près qui sont $PSL_2(\mathbf{F}_2)$ et $PSL_2(\mathbf{F}_3)$. Pour une preuve de la simplicité de $PSL_2(\mathbf{F}_q)$ lorsque $q \geq 4$, voir le théorème 3.2.2 de [DaSaV–03] ; cette preuve a l'avantage d'être remarquablement courte lorsque $q \neq 5$. Pour $PSL_2(\mathbf{F}_5)$, voir aussi l'exercice précédent ainsi que les exercices VII.E7 et VII.E8.

Les groupes simples $PSL_3(\mathbf{F}_4)$ et $PSL_4(\mathbf{F}_2)$ sont isomorphes d'ordre 20160. Les groupes simples $PSL_3(\mathbf{F}_4)$ et $PSL_4(\mathbf{F}_2)$ sont de même ordre et ne sont pas isomorphes. Voir la fin du chapitre 4 dans [Artin–62], ou [Artin–55] pour un traitement plus exhaustif.

Les groupes $PSL_n(\mathbf{F}_q)$ constituent la première de plusieurs familles infinies de groupes finis simples qui, outre les groupes cycliques d'ordres premiers, les groupes alternés $\mathrm{Alt}(k)$, $k \geq 5$, et un nombre fini (les experts disent 26) de "groupes sporadiques", constituent apparemment la totalité des groupes finis simples.

VIII.E10 : actions multiplement transitives. Soient $m \geq 2$ un entier, X un ensemble fini contenant au moins m éléments et G un groupe fini agissant X de manière m–transitive.

Si $m \geq 6$, alors (G, X) est l'une des paires $(\mathrm{Sym}(k), \{1, \ldots, k\})$, $(\mathrm{Alt}(k), \{1, \ldots, k\})$ (action naturelle). Supposons désormais que (G, X) ne soit pas l'une de ces paires.

Si $m = 5$, il n'existe que deux pairs (G, X) possibles. Pour l'une, X a 24 éléments et G est le *groupe de Mathieu* M_{24} d'ordre $2^{10} \times 3^3 \times 5 \times 7 \times 11 \times 23 = 244\,823\,040$. Pour l'autre, X a 12 éléments et G est le groupe de Mathieu M_{12} d'ordre $2^6 \times 3^3 \times 5 \times 11 = 95\,040$. De même, si $m = 4$, il n'y a que deux paires possibles, l'une avec le groupe de Mathieu M_{23} d'ordre $2^7 \times 3^2 \times 5 \times 7 \times 11 \times 23 = 10\,200\,960$ (sous–groupe d'indice 24 de M_{24}) et l'autre avec le groupe de Mathieu M_{11} d'ordre $2^4 \times 3^2 \times 5 \times 11 = 7920$ (sous–groupe d'indice 12 de M_{12}). La première description de ces groupes, et d'un cinquième *groupe de Mathieu* M_{22}, remonte à deux articles de 1861 et 1873.

Dans la mesure où on croit la *classification des groupes finis simples*, on peut classer les actions 3–transitives et 2–transitives. Voir des exemples aux exercices VIII.E4 et VIII.E3, et une description de la classification des actions 2–transitives au § 7.7 de [DixMo–96].

Les groupes M_{12}, M_{24}, M_{11}, M_{23} et un cinquième groupe M_{22} sont les premiers des *groupes simples finis sporadiques*. La liste fut prolongée de 21 autres groupes découverts dans les années 1965–1975. Il semble que la plupart des spécialistes pensent que cette liste de 26 groupes sporadiques est désormais complète.

VIII.E11 Soit $m \geq 2$ un entier. Notons $\tau(m)$ le nombre des orbites de l'action diagonale naturelle du groupe $\mathrm{Sym}(k)$ sur $\{1, \ldots, \}^m$ lorsque $k \geq m$; en particulier

$$\tau(2) = 2, \quad \tau(3) = 5, \quad \tau(4) = 15 \quad \text{et} \quad \tau(5) = 52.$$

Considérons un groupe fini G qui agit transitivement sur un ensemble X à au moins m éléments, la représentation de permutation π correspondante et son caractère χ. Montrer que les quatre conditions suivantes sont équivalentes :

— l'action de G sur X est m–transitive ;
— le nombre d'orbites de l'action diagonale de G sur X^m est $\tau(m)$;
— $\langle \chi^m \mid \chi_1 \rangle = \frac{1}{|G|} \sum_{g \in G} |X^g|^m = \tau(m)$;
— $\frac{1}{|G|} \sum_{g \in G} \chi(g)(\chi(g) - 1) \cdots (\chi(g) - m + 1) = 1$.

Voir [Livre de B. Huppert, Endliche Gruppen, sans doute I, § 20, réf. à contrôler].

IX. Décomposition de la représentation régulière

Dans ce chapitre, nous adoptons les notations suivantes :

— G est un groupe fini ;
— $\rho_1, \ldots, \rho_k$ est une énumération des représentations irréductibles de G, à équivalence près (on sait que ce nombre est fini par le corollaire VII.2), avec $\rho_1 = 1_G$ la représentation unité ;
— χ_j désigne le caractère de ρ_j et n_j son degré $(1 \leq j \leq k)$;
— λ_G désigne la représentation régulière gauche de G dans $\mathbf{C}[G]$ et χ son caractère, dont on rappelle que $\chi(1) = |G|$ et $\chi(g) = 0$ si $g \neq 1$;
— $\mathbf{C}[G]^G$ désigne l'espace des fonctions centrales de G dans $\mathbf{C}$, muni du produit scalaire défini au chapitre VI.

IX.1. Théorème. *(i) La mutliplicité d'une représentation irréductible ρ_j dans λ_G est égale à son degré n_j.*

(ii) Les degrés des caractères irréductibles vérifient la relation

$$\sum_{j=1}^{k} n_j^2 \; = \; |G|.$$

Démonstration. Si χ_G désigne le caractère de λ_G, la multiplicité de ρ_j dans λ_G est donnée par (corollaire VII.3) :

$$\langle \chi_j \mid \chi \rangle \; = \; \frac{1}{|G|} \sum_{g \in G} \overline{\chi_j(g)} \chi_G(g) \; = \; \overline{\chi_j(1)} \; = \; n_j.$$

L'assertion (ii) résulte du décompte des degrés des représentations équivalentes λ_G et $\bigoplus_{j=1}^{k} n_j \rho_j$. □

Remarque. Nous verrons au chapitre suivant que, de plus, chacun des n_j divise $|G|$.

Soient $\pi : G \longrightarrow GL(V)$ une représentation et $\varphi \in \mathbf{C}[G]$ une fonction sur G. On définit un endomorphisme linéaire $\pi(\varphi)$ de V par

$$\pi(\varphi) \; = \; \sum_{g \in G} \varphi(g) \pi(g).$$

Par exemple, si ϵ_h désigne la fonction caractéristique d'un élément $h \in G$, alors $\pi(\epsilon_h) = \pi(h)$.

Notons que $\pi(\varphi) \in \mathcal{L}(V)$ dépend linéairement de φ ; nous y revenons à l'exercice X.E2. Notons aussi que $\pi(\varphi)$ dépend additivement de π : si π_1 et π_2 sont deux représentations de G, alors $(\pi_1 \oplus \pi_2)(\varphi) = \pi_1(\varphi) \oplus \pi_2(\varphi)$.

IX.2. Lemme. *Soient π une représentation irréductible de G de degré n et $\varphi \in \mathbf{C}[G]^G$ une fonction centrale sur G. Alors $\pi(\varphi)$ est une homothétie dont le rapport μ est donné par*

$$\mu \;=\; \frac{1}{n}\sum_{g\in G}\varphi(g)\chi_\pi(g) \;=\; \frac{|G|}{n}\langle\overline{\varphi}\mid\chi_\pi\rangle.$$

Démonstration. Pour tout $g \in G$, nous avons

$$\pi(g)^{-1}\pi(\varphi)\pi(g) \;=\; \sum_{x\in G}\varphi(x)\pi(g^{-1}xg) \;=\; \sum_{y\in G}\varphi(gyg^{-1})\pi(y) \;=\; \sum_{y\in G}\varphi(y)\pi(y) \;=\; \pi(\varphi).$$

Il existe donc $\mu \in \mathbf{C}$ tel que $\pi(\varphi) = \mu\,\mathrm{id}_V$ par le lemme de Schur. On obtient μ en calculant les traces :

$$\mathrm{trace}(\pi(g)) \;=\; \sum_{g\in G}\varphi(g)\chi_\pi(g) \;=\; \langle\overline{\varphi}\mid\chi_\pi\rangle \;=\; \mathrm{trace}(\mu\,\mathrm{id}_V) \;=\; \mu n. \qquad \square$$

IX.3. Théorème. *Les caractères irréductibles χ_j constituent une base orthonormale de l'espace $\mathbf{C}[G]^G$ des fonctions centrales.*

Démonstration. Comme nous savons déjà que les χ_j sont orthonormaux (théorème VII.1), il reste à montrer qu'ils engendrent l'espace $\mathbf{C}[G]^G$ tout entier. Soit $\varphi \in \mathbf{C}[G]^G$ une fonction orthogonale à tous les χ_j ; il s'agit de montrer que $\varphi = 0$.

Pour tout $j \in \{1,\ldots,k\}$, le lemme précédent s'applique à la représentation irréductible ρ_j et montre que $\rho_j(\overline{\varphi}) = 0$. Toute représentation π de G étant somme directe de copies des ρ_j, nous avons encore $\pi(\overline{\varphi}) = 0$. En particularisant π à la représentation régulière gauche λ_G, on trouve $\lambda_G(\overline{\varphi}) = 0$, et *a fortiori*

$$\lambda_G(\overline{\varphi})(\epsilon_1) \;=\; \sum_{g\in G}\overline{\varphi(g)}\lambda_G(g)\epsilon_1 \;=\; \sum_{g\in G}\overline{\varphi(g)}\epsilon_g \;=\; 0.$$

Comme les fonctions caractéristiquen ϵ_g sont linéairement indépendantes dans $\mathbf{C}[G]$, la dernière égalité implique $\varphi(g) = 0$ pour tout $g \in G$, ce qu'il fallait montrer. $\square$

IX.4. Théorème. *Le nombre des représentations complexes irréductibles de G, à équivalence près, est égal au nombre des classes de conjugaison.*

Démonstration. Cela résulte de l'exercice V.E3, du théorème IX.3 et du fait que deux bases de $\mathbf{C}[G]^G$ ont le même nombre d'éléments. $\square$

Attention. En général, pour un groupe G, il n'existe pas de bijection *naturelle* entre les classes de conjugaison de G et les classes d'équivalence de représentations irréductibles de G. De telles bijections existent toutefois dans des cas particuliers, par exemple si G est un groupe symétrique $\mathrm{Sym}(k)$; voir par exemple la leçon 4 de [FulHa–91].

Il résulte des corollaires III.2 et IV.2 qu'un groupe fini G est abélien si et seulement si toutes ses représentations irréductibles sont de degré 1. Il résulte du théorème IX.1 que, lorsque le groupe est abélien, le nombre des représentations irréductibles de G coïncide avec l'ordre de G. En un sens, le corollaire qui suit est une généralisation de ce fait.

IX.5. Corollaire. *Soit G un groupe fini. Le nombre des représentations irréductibles de G de degré 1, à équivalence près, est égal à l'ordre de l'abélianisé G_{ab}.*

Démonstration. Il résulte du corollaire IV.2 que les représentations irréductibles de G dont le noyau contient $D(G)$ sont exactement les représentations de degré 1, et de l'exemple I.5 qu'elles sont en bijection naturelle avec les représentations irréductibles de l'abélianisé G_{ab}. □

IX.6. Exemple. Les considérations qui précèdent permettent parfois de trouver simplement les degrés n_j.

Considérons par exemple le groupe Sym(3). Il est d'ordre 6 et possède trois classes de conjugaison. Le seul triple (n_1, n_2, n_3) d'entiers strictement positifs dont la somme des carrés vaut 6 et tels que $1 \leq n_1 \leq n_2 \leq n_3$ est le triple $(1, 1, 2)$. A titre de vérification, on observe que le groupe dérivé $D(\mathrm{Sym}(3))$ est bien d'indice 2 dans Sym(3), conformément au corollaire IX.5.

Le groupe alterné Alt(4) est d'ordre 12. Il possède une représentation irréductible de degré trois (exemple VII.10 et proposition VII.9). La relation $12 = \sum_{j=1}^{k} n_j^2$ montre qu'il possède exactement quatre représentations complexes irréductibles dont les degrés sont $1, 1, 1, 3$. C'est une conséquence du théorème IX.4 qu'il possède par ailleurs quatre classes de conjugaison.

Ces quatre classes sont représentées par l'identité, $(1, 2, 3)$, $(1, 3, 2)$ et $(1, 2)(3, 4)$. L'une des manières de le vérifier consiste à tirer profit de l'isomorphisme de $\mathrm{Alt}(4) \simeq SG_T$ avec le groupe des rotations d'un tétraèdre régulier (exercice VII.E4) ; une autre manière est indiquée à l'exercice VII.E12. Le sous–groupe $\mathbf{V} = \{\mathrm{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ est normal et le quotient $\mathrm{Alt}(4)/\mathbf{V}$ est un groupe d'ordre trois. Par ailleurs, $\mathbf{V}$ coïncide avec le groupe dérivé de Alt(4), et donc $\mathrm{Alt}(4)/\mathbf{V} \simeq \mathrm{Alt}(3)$ avec l'abélianisé de Alt(4).

Pour le groupe Sym(4), la relation du théorème IX.1 s'écrit $\sum_{j=1}^{5} n_j^2 = 24$. Nous savons de plus que $n_1 = 1$ (caractère principal) et $n_2 = 2$ (homomorphisme signature). Il en résulte que $(n_1, n_2, n_3, n_4, n_5) = (1, 1, 2, 3, 3)$. Nous connaissons d'ailleurs déjà de Sym(4) une représentation irréductible de degré 3 (exemple VII.10). Nous revenons sur ces représentations en XI.3.

IX.7. Exemple. Reprenons les notations de l'exercice III.E1 pour le groupe diédral D_{2k} d'ordre $2k$, avec $k \geq 1$. Notons que le déterminant fournit un homomorphisme surjectif $\delta : D_{2k} \longrightarrow \{1, -1\}$, dont le noyau est le sous–groupe C_k des k rotations de D_{2k} ; ce déterminant est donc un caractère linéaire de D_{2k} distinct du caractère principal. Notons que le groupe dérivé de D_{2k} est contenu dans C_k.

Considérons une rotation r d'angle $2\pi/k$ du plan euclidien, une symétrie s d'axe une droite d, et la symétrie rsr^{-1}, d'axe la droite $r(d)$. On vérifie que

$$(*) \qquad rsr^{-1}s \,=\, r^2.$$

Si k est impair, il résulte de (*) que le groupe dérivé de D_{2k} coïncide avec C_k, donc que D_{2k} possède exactement deux représentations irréductibles de degré 1. Les représentations de l'exercice III.E1, de degré 2, fournissent $(k-1)/2$ représentations irréductibles inéquivalentes. La formule

$$2 \times 1^2 + \frac{k-1}{2} \times 2^2 \,=\, 2k$$

montre que les représentations ainsi décrites fournissent une liste complète des représentations irréductibles de D_{2k}.

Si k est pair, D_{2k} est le groupe des symétries d'un polygone P_k du plan qui est régulier à k sommets. Ces k sommets se partagent en ceux de deux polygones réguliers P et P' à $k/2$ sommets chacuns. L'application $\epsilon : D_{2k} \longrightarrow \{1, -1\}$ définie par $\epsilon(g) = 1$ si $g(P) = P$ et $\epsilon(g) = -1$ si $g(P) = P'$ est un caractère linéaire. Le groupe dérivé de D_{2k} est contenu dans l'intersection des noyaux de δ et de ϵ, c'est–à–dire dans le sous–groupe d'indice deux $C_{k/2}$ de C_k, et la formule (*) montre qu'il y a égalité. Il en résulte que l'abélianisé de D_{2k} est isomorphe au groupe[25] $\mathbf{V} = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, d'ordre 4, et donc que D_{2k} possède exactement quatre représentations irréductibles de degré 1. Comme ci-dessus, la formule

$$4 \times 1^2 + \frac{k-2}{2} \times 2^2 \;=\; 2k$$

montre que D_{2k} possède quatre représentations de degré 1 et $(k-2)/2$ représentations irréductibles de degré 2, inéquivalentes deux à deux, décrites à l'exercice III.E2.

Nous désignons ci–dessous par $C(g)$ la classe de conjugaison d'un élément $g \in G$.

IX.8. Théorème. *Pour les caractères irréductibles $\chi_1, \ldots, \chi_k$ de G et pour toute paire g, h d'éléments de G, nous avons*

$$\frac{1}{|G|} \sum_{j=1}^{k} \overline{\chi_j(g)} \chi_j(h) \;=\; \begin{cases} \dfrac{1}{|C(g)|} & \textit{si } g \textit{ et } h \textit{ sont conjugués,} \\ 0 & \textit{sinon.} \end{cases}$$

Cas particulier. Lorsque G est abélien et $g = 1$, la relation du théorème IX.8 s'écrit

$$\sum_{j=1}^{k} \chi_j(h) \;=\; \begin{cases} |G| & \text{si} \quad h = 1 \\ 0 & \text{sinon.} \end{cases}$$

Première démonstration. Notons φ la fonction caractéristique de $C(g)$ et posons $\mu_j = \langle \chi_j \mid \varphi \rangle$ pour tout $j \in \{1, \ldots, k\}$; le théorème IX.3 implique $\varphi = \sum_{j=1}^{k} \mu_j \chi_j$. Par définition du produit scalaire dans $\mathbf{C}[G]^G$, nous avons aussi $\mu_j = \frac{1}{|G|} \overline{\chi_j(g)} |C(g)|$. Par suite,

$$\varphi(h) \;=\; \frac{|C(g)|}{|G|} \sum_{j=1}^{k} \overline{\chi_j(g)} \chi_j(h) \qquad \text{pour tout} \quad h \in G.$$

La proposition résulte de ce que $\varphi(h)$ vaut 1 ou 0 selon que h est conjugué ou non à g. □

Seconde démonstration. Choisissons des représentants $g_1, \ldots, g_k$ des classes de conjugaison de G ; c'est en vertu du théorème IX.4 que leur nombre est égal à celui des caractères irréductibles. Les relations d'orthogonalité des caractères (théorème VII.1) s'écrivent

$$\frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \chi_j(g) \;=\; \sum_{l=1}^{k} \overline{\chi_i(g_l)} \chi_j(g_l) \frac{|C(g_l)|}{|G|} \;=\; \delta_{i,j} \qquad \text{pour tous} \quad i, j \in \{1, \ldots, k\}.$$

[25] Ce groupe est, à isomorphisme près, l'unique groupe non cyclique d'ordre 4. C'est le *Viergruppe* de F. Klein.

En d'autres termes : les lignes de la matrice carrée $\left(\sqrt{\frac{|C(g_l)|}{|G|}}\chi_i(g_l)\right)_{1\leq i,l\leq k}$ sont orthonormales dans $\mathbf{C}^k$ pour le produit hermitien canonique ; ou encore : cette matrice est unitaire. On peut donc écrire que les colonnes de cette même matrice sont orthonormales, ce qui est l'assertion du théorème. $\square$

Soit $\pi : G \longrightarrow GL(V)$ une représentation. Choisissons une décomposition

$$\text{(Irrep)} \qquad \pi = \bigoplus_{\alpha\in A} \pi_\alpha \ : \ G \longrightarrow GL\left(V \ = \ \bigoplus_{\alpha\in A} V_\alpha\right)$$

en sous–représentations irréductibles ; pour tout $\alpha \in A$, notons χ_α le caractère de la sous–représentation π_α. Pour $j \in \{1, \ldots, k\}$, notons V_j la somme directe des V_α pour lesquels π_α est équivalente à ρ_j. Nous obtenons une décomposition en somme directe

$$\text{(Isot)} \qquad \pi = \bigoplus_{j=1}^{k} \pi_j \ : \ G \longrightarrow GL\left(V \ = \ \bigoplus_{j=1}^{k} V_j\right).$$

Par définition, les sous–représentations π_j sont les *composantes isotypiques* de π, et de même les sous–espaces V_j sont les *composants isotypiques* de V. Noter que certains des V_j peuvent être réduits à $\{0\}$.

IX.9. Théorème. *On conserve les notations ci–dessus.*

(i) La décomposition (Isot) *ne dépend pas du choix de la décomposition* (Irrep).

(ii) Pour tout $j \in \{1, \ldots, k\}$, la projection p_j de V sur V_j de noyau $\bigoplus_{1\leq i\leq k, i\neq j} V_i$ est donnée par

$$p_j \ = \ \frac{n_j}{|G|} \sum_{h\in G} \overline{\chi_j(h)}\pi(h).$$

Démonstration. Il suffit de montrer (ii), dont l'assertion (i) est une conséquence immédiate.

Notons d'abord que $p_j = \frac{n_j}{|G|}\pi(\overline{\chi_j})$. Le lemme IX.2 montre que la restriction de p_j à un sous–espace invariant irréductible de V de caractère χ_i est une homothétie de rapport

$$\frac{n_j}{|G|}\frac{|G|}{n_i}\langle \chi_j \mid \chi_i \rangle \ = \ \delta_{j,i}.$$

En d'autres termes, la restriction de p_j à un sous–espace invariant irréductible W de V dont la représentation correspondante est équivalente à ρ_i est l'inclusion de W dans V si $i = j$ et l'application zéro si $i \neq j$. L'espace V_i est donc bien la somme directe des V_α tels que $\chi_\alpha = \chi_j$. $\square$

IX.10. Composantes isotypiques de la représentation régulière. Pour j dans $\{1, \ldots, k\}$, supposons la représentation ρ_j unitaire. Notons $\mathbf{C}[G, \rho_j]$ le sous–espace de $\mathbf{C}[G]$ linéairement engendré par les coefficients de la représentation ρ_j, c'est–à–dire par les fonctions $\varphi_{v,w} : g \longrightarrow \langle v \mid \rho_j(g)w\rangle$, où v, w sont deux vecteurs de l'espace de ρ_j. Il résulte du théorème VI.1 que $\mathbf{C}[G, \rho_j]$ est un sous–espace de $\mathbf{C}[G]$ de dimension n_j^2 et que les $\mathbf{C}[G,\rho_j]$ sont orthogonaux deux à deux ; en particulier, leur somme est directe. De plus

$$\mathbf{C}[G] \;=\; \bigoplus_{j=1}^{k} \mathbf{C}[G,\rho_j]\,;$$

c'est une conséquence immédiate du théorème IX.1, et cela résulte également de l'argument ci–dessous, que nous aurions pu donner au chapitre VI déjà.

Troisième démonstration du théorème IX.1. Posons $V = \bigoplus_{j=1}^{k} \mathbf{C}[G,\rho_j]$; il s'agit de montrer que l'orthogonal $V^{\perp}$ est réduit à $\{0\}$. Supposons que ce ne soit pas vrai ; choisissons un sous–espace G–invariant irréductible $V_0 \subset V^{\perp}$, définissant une sous–représentation irréductible ρ_0 de λ_G, et une fonction $\varphi_0 \neq 0$ dans V_0 ; nous allons aboutir à une contradiction.

Définissons $\psi \in \mathbf{C}[G]$ par

$$\psi(g) \;=\; \langle \varphi_0 \mid \rho_G(g)\varphi_0\rangle \;=\; \frac{1}{|G|}\sum_{x\in G} \overline{\varphi_0(x)}\varphi_0(xg).$$

(Rappel : ρ_G désigne la représentation régulière droite de G.) C'est une fonction non nulle, car $\psi(1) = \|\varphi_0\|^2 > 0$. La fonction ψ est orthogonale à tout coefficient $\varphi_{v,w}$ de toute représentation ρ_j (notation comme plus haut) ; en effet :

$$\begin{aligned}
\langle \psi \mid \varphi_{v,w}\rangle \;&=\; \frac{1}{|G|^2}\sum_{x,g\in G} \varphi_0(x)\overline{\varphi_0(xg)}\langle v \mid \rho_j(g)w\rangle \\
&=\; \frac{1}{|G|^2}\sum_{x,y\in G} \varphi_0(x)\overline{\varphi_0(y)}\langle \rho_j(x)v \mid \rho_j(y)w\rangle \\
&=\; \frac{1}{|G|}\sum_{x\in G} \varphi_0(x)\langle \varphi_0 \mid \varphi_{\rho_j(x)v,w}\rangle \\
&=\; 0,
\end{aligned}$$

la dernière égalité résultant de ce que la fonction φ_0 est orthogonale à $\varphi_{\rho_j(x)v,w} \in \mathbf{C}[G,\rho_j]$. Par suite, la fonction ψ est orthogonale à V. Or ψ est un coefficient de la représentation ρ_0, équivalente à l'une des représentations ρ_j, de sorte que $\psi \in V$. Donc $\psi = 0$, contrairement à ce qui précède. Ceci achève la preuve. $\square$

IX.11. Remarque sur la transformation de Fourier. Le résultat du numéro précédent montre en particulier que

toute fonction à valeurs complexes sur G est une combinaison linéaire
de coefficients de représentations irréductibles.

Dans le cas particulier d'un groupe G commutatif, on obtient l'énoncé suivant (qui résulte aussi du théorème IX.3) :

toute fonction à valeurs complexes sur G s'écrit de manière unique
comme combinaison linéaire de caractères.

Ce dernier énoncé, qui convenablement formulé vaut pour tout groupe abélien localement compact (et pas seulement fini), généralise le cas bien connu des séries de Fourier déjà évoqué à l'exemples IV.7. Appliqué au groupe abélien fini des éléments inversibles dans un anneau $\mathbf{Z}/m\mathbf{Z}$, c'est un ingrédient important de la preuve du *théorème de Dirichlet* qui est l'objet du chapitre XIV.

Il existe également des formulations de la transformée de Fourier pour les groupes localement compacts en général (c'est–à–dire non nécessairement abéliens).

Revenons au numéro IX.10. Il est immédiat de vérifier que chacun des sous–espaces $\mathbf{C}[G,\rho_j]$ de $\mathbf{C}[G]$ est invariant *à la fois* par la représentation régulière gauche λ_G et la représentation régulière droite ρ_G de G. Définissons une représentation π du groupe produit direct $G\times G$ dans $\mathbf{C}[G]$ par

$$\big(\pi(g,h)\varphi\big)(x) \;=\; \varphi(g^{-1}xh) \qquad \text{pour tous} \quad g,h,x\in G \quad \text{et} \quad \varphi\in\mathbf{C}[G].$$

Ce qui précède montre que les sous–espaces $\mathbf{C}[G,\rho_j]$ sont invariants par π. Signalons le résultat suivant, dont nous repoussons la démonstration à l'exemple XV.10 (à choix, voir le chapitre 5 de [Rober–83]).

IX.12. Théorème. *Pour la représentation π de $G \times G$, les sous–espaces $\mathbf{C}[G, \rho_j]$ de $\mathbf{C}[G]$ sont irréductibles et les sous–représentations correspondantes non équivalents deux à deux.*

En particulier, la représentation π est sans multiplicité, et le nombre de ses sous–représentations irréductibles est égal au nombre des classes de conjugaison de G (voir aussi l'exercice IX.E3).

Exercices

IX.E1 Soit m un entier. Notons C_m le groupe cyclique fini $\mathbf{Z}/m\mathbf{Z}$. Ecrire les fonctions caractéristiques des points comme combinaisons linéaires de caractères de C_m.

Soit $G(m)$ le groupe des éléments inversibles dans l'anneau $\mathbf{Z}/m\mathbf{Z}$. Ecrire de même les fonctions caractéristiques des points comme combinaisons linéaires de caractères de $G(m)$.

Particulariser aux cas $m = 4$ et $m = 8$. (Voir l'exemple I.8.)

IX.E2* On considère un corps fini $\mathbf{k}$ d'ordre q et le *groupe de Heisenberg* $H(\mathbf{k})$ des matrices

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

à coefficients dans $\mathbf{k}$.

Montrer que l'abélianisé de $H(\mathbf{k})$ est isomorphe à $\mathbf{k}^2$, et que le nombre des classes de conjugaison de $H(\mathbf{k})$ est $q^2 + q - 1$.

Lorsque $q = 3$, calculer les degrés des représentations complexes irréductibles de $H(\mathbf{k})$. Même question pour $q = 4$ et $q = 5$ (pour $q = 5$, utiliser le résultat du théorème X.1, ou à choix celui du corollaire IV.6).

IX.E3 Pour un groupe fini G, considérons l'action de $G \times G$ sur G définie par $\big((g, h), x\big) \longmapsto gxh^{-1}$. Montrer que le rang de cette action est égal au nombre des classes de conjugaison de G.

[Indication : pour l'action diagonale de $G \times G$ sur $G \times G$, toute orbite contient un élément de la forme $(1, y)$.]

IX.E4 Soient G un groupe fini, π une représentation de G et χ son caractère ; soit $g \in G$. Vérifier que $\pi(g)$ est central dans $\pi(G)$ si et seulement si $|\chi(g)| = \chi(1)$. En particulier, lorsque π est fidèle, g est central dans G si et seulement si $|\chi(g)| = \chi(1)$.

[Indication : utiliser le lemme de Schur et la proposition V.1.viii.]

IX.E5 Soient G un groupe fini, $\chi_1, \ldots, \chi_k$ ses caractères irréductibles et $g \in G$. Montrer que g est central si et seulement si $\sum_{j=1}^{k} |\chi_j(g)|^2 = |G|$.

[Indication : utiliser le théorème IX.1 et l'exercice précédent.]

X. Intégralité et algèbres de groupes

X.1. Théorème. *Le degré de toute représentation irréductible d'un groupe fini divise l'ordre du groupe.*

Nous avons déjà vérifié plusieurs fois cette propriété (exemple IX.6, entre autres). Sa démonstration nécessite quelques préliminaires algébriques.

Soit R un anneau commutatif avec unité. Un élément $\xi \in R$ est un *entier algébrique* s'il existe un entier naturel $k \geq 0$ et des entiers $a_1, \ldots, a_k \in \mathbf{Z}$ tels que

$$(*) \qquad \xi^k + a_1\xi^{k-1} + \cdots + a_k \;=\; 0.$$

Par exemple, dans $R = \mathbf{C}$, les nombres $\exp(2i\pi/k)$, $\sqrt{2}$ et $\frac{1}{2}(1+\sqrt{5})$ sont des entiers algébriques, respectivement racines des polynômes $X^k - 1$, $X^2 - 2$ et $X^2 - X - 1$ de $\mathbf{Z}[X]$.

X.2. Exemple. Nous laissons à la lectrice le soin de vérifier les trois assertions suivantes.

(i) Dans le corps $\mathbf{Q}$ des nombres rationnels, un nombre ξ est un entier algébrique si et seulement s'il est dans $\mathbf{Z}$. [C'est pour cela que $\mathbf{Z}$ s'appelle l'anneau des *entiers rationnels* !]

(ii) Dans le corps $\mathbf{C}$ des nombres complexes, pour qu'un nombre $p/q \in \mathbf{Q}$ soit un entier algébrique, il faut et il suffit qu'il soit dans $\mathbf{Z}$.

(iii) Dans $\mathbf{C}$, le nombre $\sqrt{2}/2$ n'est pas un entier algébrique. Ceci est une illustration de ce que, pour un nombre complexe ξ qui est un entier algébrique (par exemple $\exp(i\pi/4)$), la partie réelle de ξ n'est pas nécessairement un entier algébrique.

Il est vrai, mais non évident, que la somme et le produit de deux entiers algébriques sont encore des entiers algébriques. Avant de le montrer, nous allons établir les équivalences suivantes. Pour $\xi_1, \ldots, \xi_l \in R$, nous notons $\mathbf{Z}[\xi_1, \ldots, \xi_l]$ le sous–anneau de R engendré par $\xi_1, \ldots, \xi_l$, qui est aussi le sous–groupe additif de R engendré par les produits $\prod_{j=1}^{l} \xi_j^{n_j}$, avec $n_1, \ldots, n_l \in \mathbf{N}$.

Pour $k \geq 1$, nous notons $M_k(R)$ l'anneau des matrices k–fois–k à coefficients dans R et $\det : M_k(R) \longrightarrow R$ l'application déterminant. Rappelons que toute matrice $b \in M_k(R)$ possède une *matrice adjointe* $\mathrm{ad}(b) \in M_k(R)$ telle que $\mathrm{ad}(b)b = b\,\mathrm{ad}(b)$ soit le produit de $\det(b)$ par la matrice unité.

X.3. Proposition. *Pour un élément ξ d'un anneau commutatif R avec unité, les propriétés suivantes sont équivalentes :*

(i) *ξ est un entier algébrique ;*
(ii) *$\mathbf{Z}[\xi]$ est un $\mathbf{Z}$–module de type fini ;*
(iii) *$\mathbf{Z}[\xi]$ est contenu dans un sous–$\mathbf{Z}$–module de type fini.*

Démonstration. Supposons que ξ possède la propriété (i) ; soient $a_1, \ldots, a_k \in \mathbf{Z}$ tels que l'équation (*) soit satisfaite. On vérifie par récurrence sur $n \geq k$ que

$$\xi^n \;=\; -a_1\xi^{n-1} - \cdots - a_k\xi^{n-k}$$

est dans le $\mathbf{Z}$–module de type fini[26] engendré par $1, \xi, \ldots, \xi^{k-1}$, de sorte que la propriété (ii) est satisfaite.

L'implication de (iii) par (ii) est immédiate.

Supposons la propriété (iii) satisfaite. Nous proposons deux rédactions montrant que la propriété (i) en découle.

(1) Soient $\epsilon_1, \ldots, \epsilon_k$ un système fini de générateurs d'un sous–$\mathbf{Z}$–module de type fini de R contenant $\mathbf{Z}[\xi]$. Par hypothèse, il existe une matrice $a = (a_{i,j})_{1 \leq i,j \leq k} \in M_k(\mathbf{Z})$ telle que

[26]Nous écrivons indifféremment "$\mathbf{Z}$–module" ou "groupe abélien".

$\xi\epsilon_j = \sum_{i=1}^k a_{i,j}\epsilon_i$ pour tout $j \in \{1, \dots, k\}$. Notons $b \in M_k(R)$ la matrice de coefficients $\xi\delta_{i,j} - a_{i,j}$. Alors $b\epsilon_j = 0$, donc $\det(b)\epsilon_j = ad(b)b\epsilon_j = 0$ pour tout $j \in \{1, \dots, k\}$. Soient $\mu_1, \dots, \mu_k \in \mathbf{Z}$ tels que $1 = \sum_{j=1}^k \mu_j\epsilon_j$. Nous avons aussi $\det(b) = \sum_{j=1}^k \mu_j \det(b)\epsilon_j = 0$. Ceci achève l'argument car l'égalité $\det(b) = 0$ peut s'écrire sous la forme $\xi^k + a_1\xi^{k-1} + \cdots + a_k = 0$, avec $a_1, \dots, a_k \in \mathbf{Z}$.

(2) Le sous–$\mathbf{Z}$–module S de R engendré par $(\xi^n)_{n\geq 0}$ est contenu dans un $\mathbf{Z}$–module de type fini de R, donc est lui–même de type fini. Soit $\{s_1, \dots, s_l\}$ un système fini de générateurs de S. Chaque s_j peut s'écrire comme une $\mathbf{Z}$–combinaison linéaire finie de puissances de ξ. Notons $k - 1$ le maximum des exposants intervenant dans ces écritures des s_j. Alors ξ^k est une $\mathbf{Z}$–combinaison linéaire des ξ^i pour $0 \leq i \leq k-1$, ce qui achève l'argument. $\square$

X.4. Corollaire. *Dans un anneau commutatif R avec unité, les entiers algébriques constituent un sous–anneau.*

Démonstration. Si $\xi, \eta \in R$ sont des entiers algébriques, alors $\mathbf{Z}[\xi, \eta]$ est un $\mathbf{Z}$–module de type fini qui contient $\xi + \eta$ et $\xi\eta$. $\square$

X.5. Corollaire. *Les valeurs des caractères des représentations complexes d'un groupe fini sont des entiers algébriques.*

Démonstration. Soit π une représentation complexe d'un groupe fini dans un espace vectoriel V. Pour tout $g \in G$, l'endomorphisme $\pi(g)$ est d'ordre fini ; il existe donc une base de V relativement à laquelle $\pi(g)$ s'écrit comme une matrice diagonale dont les coefficients diagonaux sont des racines de l'unité. Ces racines étant toutes des nombres algébriques, leur somme $\chi_\pi(g)$ est aussi un entier algébrique en vertu du corollaire précédent. $\square$

X.6. Proposition. *Soient R, R' deux anneaux commutatifs avec unité et $\alpha : R \longrightarrow R'$ un homorphisme d'anneaux tel que $\alpha(1) = 1$. Si $\xi \in R$ est un entier algébrique, alors $\alpha(\xi) \in R'$ est un entier algébrique.*

Démonstration : immédiate, avec chacune des propriétés de la proposition X.3. $\square$

X.7. Produit de convolution. Soient $\mathbf{K}$ un corps et G un groupe fini. Le *produit de convolution* de deux fonctions $\varphi, \psi \in \mathbf{K}[G]$ est la fonction de $\mathbf{K}[G]$ définie par

$$(\varphi * \psi)(g) = \sum_{x,y\in G, xy=g} \varphi(x)\psi(y) = \sum_{x\in G} \varphi(x)\psi(x^{-1}y).$$

Par exemple, si ϵ_a désigne comme d'habitude la fonction caractéristique d'un élément $a \in G$, alors $e_a * e_b = e_{ab}$; en particulier, $\psi * \varphi \neq \varphi * \psi$ en général (sauf si G est abélien).

La $\mathbf{K}$–*algèbre de G* est l'espace vectoriel $\mathbf{K}[G]$ muni du produit de convolution.

X.8. Propriétés du produit de convolution.

(i) *Le produit* $(\varphi, \psi) \longmapsto \varphi * \psi$ *est bilinéaire ;*
(ii) *il est associatif :* $(\varphi * \psi) * \omega = \varphi * (\psi * \omega)$ *;*
(iii) *il possède une unité :* $\varphi * \epsilon_1 = \epsilon_1 * \varphi = \varphi$ *;*
(iv) *si* V *est un* $\mathbf{K}$*–espace vectoriel et si* $\pi : G \longrightarrow GL(V)$ *est une représentation, alors* $\pi(\varphi * \psi) = \pi(\varphi)\pi(\psi) \in \mathcal{L}(V)$ *;*

ceci pour tous $\varphi, \psi, \omega \in \mathbf{K}[G]$*. De plus, pour* $\varphi \in \mathbf{K}[G]$*,*

(v) $\varphi * \psi = \psi * \varphi$ *pour tout* $\psi \in \mathbf{K}[G]$ *si et seulement si* $\varphi \in \mathbf{K}[G]^G$*.*

Démonstration et remarques. Les vérifications sont immédiates. Par exemple, la vérification de (iii) résulte de ce que $(\epsilon_a * \epsilon_b) * \epsilon_c = \epsilon_a * (\epsilon_b * \epsilon_c)$ pour tous $a, b, c \in G$ (ces produits étant tous les deux égaux à ϵ_{abc}, par associativité de la multiplication dans G).

Rappelons que l'endomorphisme $\pi(\psi)$ de V a été défini au début du chapitre IX. La propriété (iv) exprime que $\pi : \mathbf{K}[G] \longrightarrow \mathcal{L}(V)$ est un homomorphisme d'algèbres.

La propriété (v) exprime que $\mathbf{K}[G]^G$ est le centre de l'algèbre de convolution $\mathbf{K}[G]$. $\square$

Dans le cas du corps $\mathbf{C}$, on définit pour toute fonction $\varphi \in \mathbf{C}[G]$ la fonction φ^* par $\varphi^*(g) = \overline{\varphi(g^{-1})}$. Pour une représentation unitaire $\pi : G \longrightarrow \mathcal{U}(V)$, on vérifie alors que

(vi) $\pi(\varphi^*) = \pi(\varphi)^*$,

c'est–à–dire que $\pi : \mathbf{C}[G] \longrightarrow \mathcal{L}(V)$ est un homomorphisme de $*$–algèbres complexes (la lectrice qui tiendrait à lire une définition formelle de ce terme en trouverait une dans N. Bourbaki, *Théories spectrales, chapitres 1 et 2* (Hermann 1967), chapitre I, § 6, no 1).

X.9. Terminologie : algèbres, G–modules. Une *algèbre* sur un corps $\mathbf{K}$ (sous–entendu ici : algèbre *associative*) est un $\mathbf{K}$–espace vectoriel A muni d'une application linéaire

$$A \times A \longrightarrow A, \qquad (a, b) \longmapsto ab,$$

appeleée *multiplication*, telle que $(ab)c = a(bc)$ pour tous $a, b, c \in A$. (En particulier, l'addition de la structure d'espace vectoriel et la multiplication munissent toute algèbre d'une structure sous–jacente d'anneau.) Une *unité* dans une algèbre A est un élément 1 tel que $1a = a1 = a$ pour tout $a \in A$; un argument standard montre qu'il existe au plus une telle unité. Si A, A' sont deux $\mathbf{K}$–algèbres, une application linéaire $\alpha : A \longrightarrow A'$ est un *homomorphisme d'algèbres* si $\alpha(ab) = \alpha(a)\alpha(b)$ pour tous $a, b \in A$. Voici quelques exemples de $\mathbf{K}$–algèbres :

l'espace $\mathbf{K}^X$ des fonctions à valeurs dans $\mathbf{K}$ sur un ensemble X (produit ponctuel) ;
le sous–espace $\mathbf{K}^{(X)}$ des fonctions à supports finis (produit ponctuel) ;
la $\mathbf{K}$–algèbre $\mathbf{K}[G]$ d'un groupe[27] G (convolution) ;
l'espace $\mathcal{L}(V)$ des endomorphismes d'un $\mathbf{K}$–espace vectoriel (composition) ;
le commutant $\pi(G)'$ dans $\mathcal{L}(V)$, défini pour $\pi : G \longrightarrow GL(V)$ comme en VII.14 ;
l'espace $M_n(\mathbf{K})$ des matrices n–fois–n à coefficients dans $\mathbf{K}$;
le sous–espace des matrices triangulaires supérieures.

Lorsque $\mathbf{K} = \mathbf{C}$, mentionnons encore :

l'espace $\mathcal{C}(\Omega)$ des fonctions continues à valeurs complexes sur un espace topologique Ω ;
le sous–espace $\mathcal{C}_c(\Omega)$ des fonctions à supports compacts.

[27] Noter que $\mathbf{K}[G]$ possède *deux structures* (au moins) de $\mathbf{K}$–algèbre, en général non isomorphes.

On laisse à la lectrice le soin d'expliciter la multiplication et de décider s'il existe une unité, dans chaque cas.

L'homomorphisme π de $\mathbf{K}[G]$ dans $\mathcal{L}(V)$ défini ci-dessus fait de l'espace vectoriel V un *module* sur l'algèbre $\mathbf{K}[G]$; en d'autres termes, V est un $\mathbf{K}[G]$–module ou, plus brièvement, un G–module. Réciproquement, comme G s'identifie à un sous–ensemble de $\mathbf{K}[G]$, toute structure de G–module (c'est–à–dire de $\mathbf{K}[G]$–module) sur un espace vectoriel V fournit une représentation linéaire $G \longrightarrow GL(V)$.

Etant donné un groupe G et un corps $\mathbf{K}$, on écrit et on dit donc indifféremment "soit V un espace vectoriel muni d'une représentation $\pi : G \longrightarrow GL(V)$" ou "soit V un G–module".

X.10. Proposition. *Soient G un groupe fini, C_0 une classe de conjugaison, π une représen tation complexe irréductible de G dans un espace vectoriel V de dimension n et χ_π son caractère.*

Alors le nombre complexe $\frac{1}{n}\sum_{g\in C_0}\chi_\pi(g)$ est un entier algébrique.

Remarque. Soit $g_0 \in C_0$. Les valeurs $\chi_\pi(g)$ apparaissant ci–dessus sont toutes égales entre elles et

$$\frac{1}{n}\sum_{g\in C_0}\chi_\pi(g) \;=\; \frac{1}{n}|C_0|\chi_\pi(g_0).$$

Démonstration. Notons $\mathbf{Z}[G]$ et $\mathbf{Z}[G]^G$ les sous–anneaux de $\mathbf{C}[G]$ et $\mathbf{C}[G]^G$ formé des fonctions sur G à valeurs dans $\mathbf{Z}$. Notons $\mathcal{C}$ l'ensemble des classes de conjugaison de G. Pour toute classe $C \in \mathcal{C}$, posons $\epsilon_C = \sum_{g\in C}\epsilon_g$. Alors $(\epsilon_C)_{C\in\mathcal{C}}$ est une base de l'espace vectoriel $\mathbf{C}[G]^G$ et aussi du $\mathbf{Z}$–module libre de type fini $\mathbf{Z}[G]^G$; en particulier, les éléments ϵ_C sont entiers algébriques dans $\mathbf{C}[G]^G$.

Pour tout élément central φ de $\mathbf{C}[G]$, le lemme de Schur montre que $\pi(\varphi)$ est une homothétie de V ; notons–en $\mu(\varphi)$ le rapport, de sorte que π fournit par restriction un homomorphisme d'anneaux $\mu : \mathbf{C}[G]^G \longrightarrow \mathbf{C}$ tel que $\pi(\varphi) = \mu(\varphi)\,\mathrm{id}_V$ pour tout $\varphi \in \mathbf{C}[G]^G$. Il résulte de la proposition X.3 que $\mu(\epsilon_C)$ est un entier algébrique pour tout $C \in \mathcal{C}$.

Comme la trace de $\pi(\epsilon_{C_0})$ peut s'écrire de deux manières,

$$\mathrm{trace}\,(\pi(\epsilon_{C_0}) \;=\; n\mu(\epsilon_{C_0}) \;=\; \sum_{g\in C_0}\chi_\pi(g),$$

la proposition en résulte. □

X.11. Corollaire. *Dans la situation de la proposition précédente, supposons de plus les entiers $|C_0|$ et n premiers entre eux. Alors $\frac{\chi_\pi(g_0)}{n}$ est un entier algébrique.*

Démonstration. Par le théorème de Bézout, il existe des entiers $a, b \in \mathbf{Z}$ tels que $a|C_0| + bn = 1$. Par suite

$$\frac{\chi_\pi(g_0)}{n} \;=\; a\,\frac{|C_0|\chi_\pi(g_0)}{n} + b\chi_\pi(g_0).$$

Le premier terme du membre de droite est un entier algébrique par la proposition X.10 et le second par le corollaire X.5. □

Preuve du théorème X.1. Soit χ le caractère d'une représentation complexe irréductible de degré n d'un groupe fini G. Alors

$$\langle \chi \mid \chi \rangle \;=\; \frac{1}{|G|}\sum_{g\in G}\chi(g^{-1})\chi(g) \;=\; 1$$

par le théorème VII.1, donc

$$\frac{|G|}{n} \;=\; \sum_{g\in G}\chi(g^{-1})\frac{\chi(g)}{n} \;=\; \sum_{C\in\mathcal{C}}\chi\left((h_C)^{-1}\right)\sum_{g\in C}\frac{\chi(g)}{n},$$

où $\chi\left((h_C)^{-1}\right)$ désigne la valeur commune $\chi\left(h^{-1}\right)$ lorsque h parcourt la classe C.

Or, pour toute classe C, le nombre $\chi\left((h_C)^{-1}\right)$ est un entier algébrique par le corollaire X.5 et le nombre $\sum_{g\in C}\frac{\chi(g)}{n}$ en est aussi un par la proposition X.10. Donc $\frac{|G|}{n}$ est un entier algébrique par le corollaire X.4. Il résulte de l'exemple X.2.ii que n divise $|G|$. $\square$

Raffinement. Soit $Z(G)$ le centre de G ; on peut montrer que n divise $|G/Z(G)|$. Mieux : pour tout sous–groupe abélien normal A de G, on peut montrer que n divise $|G/A|$. Voir [Serre–67], § 6.4 et § 9.1.

La proposition suivante est due à Burnside. Voir le théorème 3.6 du chapitre III dans [Curti–99].

X.12. Proposition. *Soient G un groupe d'ordre impair et χ un caractère irréductible de G distinct du caractère unité. Alors χ prend des valeurs complexes non réelles.*

Démonstration. Un groupe d'ordre impair ne contient pas d'élément d'ordre deux. On peut donc choisir un sous–ensemble A de G tel que G soit la réunion disjointe de $\{1\}$, A et A^{-1}. La relation d'orthogonalité de χ avec le caractère principal peut s'écrire

$$(*) \qquad -\frac{1}{2}\chi(1) \;=\; \frac{1}{2}\sum_{a\in A}\left(\chi(a)+\chi(a^{-1})\right) \;=\; \mathrm{Re}\left(\sum_{a\in A}\chi(a)\right).$$

Le degré $\chi(1)$ est un nombre impair par le théorème X.1, de sorte que $-\frac{1}{2}\chi(1)$ n'est pas un entier algébrique (exemple X.2.ii). La proposition résulte de ce que, si χ ne prenait que des valeurs réelles, le nombre $\mathrm{Re}\left(\sum_{a\in A}\chi(a)\right) = \sum_{a\in A}\chi(a)$ serait un entier algébrique, ce qui est absurde au vu de l'égalité (*). $\square$

X.13. Théorème. *Soit p un nombre premier. Tout groupe d'ordre p^2 est abélien.*

Démonstration. Soient $n_1 = 1, n_2, \dots, n_k$ les degrés des représentations complexes irréductibles d'un groupe G d'ordre p^2. D'une part, $1+\sum_{j=2}^{k} n_j^2 = p^2$; d'autre part, chaque n_j divise p^2, donc est l'un de 1, p, p^2. Il en résulte que $n_2 = \cdots = n_k = 1$, donc que G est abélien par le corollaire III.2. $\square$

Exercices et compléments

X.E1 Soient G un groupe fini agissant sur un ensemble fini X et $\pi : G \longrightarrow GL(\mathbf{C}^X)$ la représentation correspondante. On suppose qu'il existe une représentation ρ de G, sans sous–représentation équivalente à 1_G, et un entier $k \geq 1$ tels que $\pi \approx 1_G \oplus k\rho$. Montrer que $k = 1$.

[Indication. La multiplicité de 1_G dans π étant 1, l'action de G sur X est transitive. Soit $g \in G$ un élément sans point fixe sur X (corollaire VIII.3). La relation $\chi_\pi(g) = 0 = 1 + k\chi_\rho(g)$ implique $\chi_\rho(g) = -1/k$, et le corollaire X.5 implique $k = 1$.]

En déduire que, si l'action de G sur X est de rang $r \leq 5$, alors la représentation π est sans multiplicité.

X.E2 Soient G un groupe fini et $\rho_j : G \longrightarrow GL(V_j)$, $1 \leq j \leq \ell$, des représentations complexes irréductibles de G, non équivalentes deux à deux ; on a donc $\ell \leq k$ si k est comme au début du chapitre X.

(a) Montrer que l'homomorphisme d'algèbres

$$\rho = \bigoplus_{j=1}^{\ell} \rho_j \ : \ \mathbf{C}[G] \longrightarrow \bigoplus_{j=1}^{\ell} \mathcal{L}(V_j)$$

est surjectif.

(b) Si, de plus, $\ell = k$, montrer que l'homomorphisme d'algèbres ρ est un isomorphisme.

(c) Constater qu'il existe des paires (G_1, G_2) de groupes non isomorphes telles que les algèbres $\mathbf{C}[G_1]$ et $\mathbf{C}[G_2]$ sont isomorphes.

[Indication pour (a). On peut supposer les représentations ρ_j unitaires. Pour $j = 1, \ldots, \ell$, soit $\big(e_i^{(j)}\big)_{1 \leq i \leq \dim(V_j)}$ une base orthonormale de V_j. Si l'application linéaire ρ n'était pas surjective, il existerait des nombres complexes $\big(\lambda_{i,i'}^{(j)}\big)_{1 \leq j \leq \ell, 1 \leq i,i' \leq \dim(V_j)}$ tels que l'image de ρ soit dans le noyau de la forme linéaire α définie sur $\bigoplus_{j=1}^{\ell} \mathcal{L}(V_j)$ par

$$\alpha\Big(\bigoplus_{j=1}^{\ell} S_j\Big) = \sum_{j=1}^{\ell} \sum_{i,i'=1}^{\dim(V_j)} \lambda_{i,i'}^{(j)} \langle e_i^{(j)} \mid S_j e_{i'}^{(j)} \rangle,$$

ce qui contredirait la conclusion du théorème VI.1.

Indication pour (c). Considérer deux groupes abéliens non isomorphes de même ordre.]

(d) Soient G un groupe (fini *ou infini*) et $\rho : G \longrightarrow GL(V_j)$ une représentation complexe. Notons $\langle \rho(G) \rangle_{\text{lin}}$ le sous–espace vectoriel de $\mathcal{L}(V)$ engendré par $\rho(G)$. Supposons que $\rho = \bigoplus_{j=1}^{\ell} \rho_j$ soit une somme directe de représentations $\rho_j : G \longrightarrow GL(V_j)$; alors $\langle \rho(G) \rangle_{\text{lin}}$ est une sous–algèbre de la sous–algèbre $\bigoplus_{j=1}^{\ell} \mathcal{L}(V_j)$ de $\mathcal{L}(V)$ correspondant à la décomposition $V = \bigoplus_{j=1}^{\ell} V_j$. Voici une reformulation de l'assertion de (a) :

si G est fini, et si les ρ_j sont irréductibles et non équivalentes deux à deux, alors $\langle \rho(G) \rangle_{\text{lin}} = \mathcal{L}(V)$.

Sous cette forme, l'assertion est encore vraie pour un groupe infini. Voir par exemple le théorème 2.7A de [Dixon–71].

X.E3 : complément sur *l'équation fonctionnelle des caractères* (voir [Weil–40], § 24). Il s'agit de l'équation

$$\text{(EFC)} \qquad \frac{1}{|G|}\sum_{x\in G}\psi(xax^{-1}b) \;=\; \psi(a)\psi(b) \qquad \text{pour tous} \quad a,b\in G.$$

Soient π une représentation irréductible de G et χ son caractère ; nous avons vu à l'exercice IV.E2 que la fonction

$$\text{(SOL)} \qquad \psi = \frac{1}{\text{degré}(\pi)}\chi$$

est solution de (EFC), et $\psi(1) = 1$.

Réciproquement, si ψ est une solution non identiquement nulle de (EFC), nous allons montrer que ψ est de la forme (SOL). Nous laissons à la lectrice le soin de vérifier que $\psi(1) = 1$ et que ψ est une fonction centrale sur G. Par l'exercice précédent, il existe une représentation irréductible π de G telle que $\check{\pi}(\psi) \neq 0$, où $\check{\pi}$ désigne la représentation contragrédiente de π. Notons n le degré et χ le caractère de π ; rappelons que le caractère de $\check{\pi}$ est $\overline{\chi}$. Le calcul

$$\begin{aligned}
\psi(a)\check{\pi}(\psi) \;&=\; \frac{1}{|G|}\sum_{b\in G}\psi(a)\psi(b)\check{\pi}(b) \\
&=\; \frac{1}{|G|^2}\sum_{b,x\in G}\psi(xax^{-1}b)\check{\pi}(b) && \text{par (EFC)} \\
&=\; \frac{1}{|G|^2}\sum_{b,x\in G}\psi(xb)\check{\pi}(xa^{-1}b) && \text{en remplaçant } (x,b) \text{ par } (x,xa^{-1}b) \\
&=\; \frac{1}{|G|^2}\sum_{b,x\in G}\psi(b)\check{\pi}(xa^{-1}x^{-1})\check{\pi}(b) && \text{en remplaçant } (x,b) \text{ par } (x,x^{-1}b) \\
&=\; \frac{1}{|G|}\sum_{x\in G}\check{\pi}(xa^{-1}x^{-1})\check{\pi}(\psi) && \text{par définition de } \pi(\psi) \\
&=\; \frac{1}{n}\overline{\chi}(a^{-1})\check{\pi}(\psi) && \text{par l'exercice IV.1} \\
&=\; \frac{1}{n}\chi(a)\check{\pi}(\psi),
\end{aligned}$$

pour tout $a \in G$, montre qu'on a bien $\psi = \frac{1}{n}\chi$.

Nous avons montré que les *fonctions sphériques* de la paire de Gelfand $(G\times G, \Delta G)$ associée à G comme à l'exemple XV.10.iv correspondent bijectivement, par (SOL), aux caractères irréductibles de G.

X.E4 Soit G un groupe fini d'ordre n. Le problème suivant a été résolu dans les années 1890 par Frobenius, qui a fondé du même coup la théorie des représentations des groupes ; il s'agit de décomposer le polynôme

$$F \;=\; \det\big((X_{gh^{-1}})_{g,h\in G}\big)$$

en produit de polynômes irréductibles. Nous suivons d'assez près [FulHa–91, pages 39 et 518].

Notons A l'algèbre commutative $\mathbf{C}[(X_g)_{g\in G}]$ des polynômes à coefficients complexes en n variables, indexées par les éléments de G. Si M est un A–module libre de type fini, le *déterminant* det : $\mathcal{L}_A(M) \longrightarrow A$ est défini comme dans le cas des espaces vectoriels.

La *A–algèbre du groupe* G est le A–module libre A^G de rang n, muni du produit de convolution défini comme en X.7. Comme en I.3, il possède une base $(\epsilon_g)_{g\in G}$, et la représentation régulière de G dans $A[G]$ munit le A–module libre $A[G]$ d'une structure de G–module.

La convolution à gauche par $\sum_{y\in G} X_y\epsilon_y$ est un endomorphisme A–linéaire de $A[G]$; pour tout $h \in G$, il applique ϵ_h sur $\left(\sum_{y\in G} X_y\epsilon_y\right)\epsilon_h = \sum_{g\in G} X_{gh^{-1}}\epsilon_g$. En d'autres termes, la matrice de cette convolution à gauche $L_{\sum X_y\epsilon_y}$ relativement à la base $(\epsilon_g)_{g\in G}$ est précisément la matrice

$$\big((X_{gh^{-1}})_{g,h\in G}\big)$$

dont le déterminant est F.

Si $n_1, \ldots, n_k$ désignent les degrés des représentations complexes irréductibles de G, nous savons du chapitre IX que la représentation régulière gauche de G dans $\mathbf{C}[G]$ est équivalente à une somme directe de la forme $\bigoplus_{j=1}^k n_j\rho_j$, où les ρ_j sont irréductibles ; de même, la représentation régulière gauche de G dans $A[G]$ est équivalente à une somme directe de la forme $\bigoplus_{j=1}^k n_jR_j$, où chaque R_j est une représentation irréductible de G dans un A–module libre de rang n_j. Il en résulte que F a une factorisation

$$F = \prod_{j=1}^{k} (F_j)^{n_j} \tag{*}$$

De plus, comme Frobenius l'a montré, les facteurs F_j sont irréductibles.

L'étincelle qui mit le feu à l'intérèt de Frobenius fut une lettre de Dedekind lui relatant ses calculs de F pour le groupe symétrique d'ordre 6 et le groupe des quaternions d'ordre 8. Pour Sym(3), les deux facteurs linéaires de (*) sont

$$\begin{aligned} F_1 &= X_{\mathrm{id}} + X_{(1,2,3)} + X_{(1,3,2)} + X_{(2,3)} + X_{(1,3)} + X_{(1,2)} \\ F_2 &= X_{\mathrm{id}} + X_{(1,2,3)} + X_{(1,3,2)} - X_{(2,3)} - X_{(1,3)} - X_{(1,2)} \end{aligned}$$

et le facteur F_3, qui est au carré, est un polynôme homogène de degré deux en les mêmes six variables et qu'on peut lire par exemple dans [Curti–99, page 52].

L'exercice qui suit offre un schéma de démonstration du théorème X.13 indépendant de la théorie de la représentation.

Comparer les assertions des deux exercices qui suivent avec le théorème de Burnside du chapitre XV, concernant les groupes d'ordres p^aq^b.

X.E5 Soit p un nombre premier. Montrer que tout groupe d'ordre p^2 et abélien, selon le schéma suivant. On désigne par $Z(G)$ le centre d'un groupe G.

(a) Rappel préliminaire : tout groupe d'ordre p est cyclique.

(b) Soit G un groupe tel que $G/Z(G)$ est cyclique. Montrer que G est abélien, et par suite cyclique. [Indication : il existe $x \in G$ tel que tout élément de G soit de la forme x^jz, avec $j \in \mathbf{Z}$ et $z \in Z(G)$.]

(c) Soit G un p–groupe fini, c'est–à–dire un groupe d'ordre une puissance de p ; on suppose G non réduit à un élément. Montrer que le centre de G n'est pas réduit à un élément. [Indication : contempler l'égalité $|G| = |Z(G)| + \sum_i [G : Z_G(x_i)]$, où $(x_i)_i$ est une famille de représentants des classes de conjugaison non centrales de G et où $Z_G(x)$ désigne le centralisateur de x dans G.]

(d) Montrer que tout groupe d'ordre p^2 est abélien. [Indication : si G n'était pas abélien, on aurait $1 < |Z(G)| < p^2$ par (c), d'où une contradiction avec (b).]

(e) = Complément. Montrer qu'un groupe d'ordre p^2 est ou bien cyclique ou bien produit direct de deux groupes cycliques d'ordre p. [Indication : si G n'est pas cyclique, il existe $x, y \in G$, chacun d'ordre p, tels que les sous–groupes engendrés $\langle x \rangle, \langle y \rangle$ ont une intersection réduite à l'identité, et l'application $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \longrightarrow G, (j,k) \longmapsto x^j y^k$ est un isomorphisme.]

X.E6 Soient p, q deux nombres premiers tels que $p > q$. Si G est d'ordre pq, montrer qu'il existe un sous–groupe normal cyclique d'ordre p, notons–le P, tel que G/P est cyclique d'ordre q. [Indication : en vertu du théorème de Sylow, G possède un unique p–Sylow, qui est donc normal.]

Complément. Si de plus q ne divise pas $p-1$, alors G est nécessairement cyclique ; voir par exemple la proposition 2.19 de [Humph–96]. Si G est d'ordre $2p$, avec p impair, alors G est ou bien cyclique ou bien diédral ; voir par exemple le début du chapitre 12 dans [Humph–96].

XI. Tables de caractères

Ce chapitre est consacré aux tables de caractères de quelques groupes de "petits" ordres. Nous laissons à la lectrice de soin de se confectionner une table pour le groupe à un élément.

XI.1. Le groupe symétrique de deux objets.

Le groupe Sym(2) possède deux caractères : le caractère principal χ_1 et la signature χ_{sign}. Nous écrivons comme suit sa table de caractères :

	1	1
	id	$(1,2)$
χ_1	1	1
χ_{sign}	1	-1

Sym(2) est une notation pompeuse pour le groupe (nécessairement cyclique) à deux éléments.

Il n'est pas difficile d'écrire les tables de caractères des autres groupes cycliques finis (exercice XI.E1).

XI.2. Le groupe symétrique de trois objets, ou groupe diédral d'ordre 6.

Le groupe Sym(3) possède trois classes de conjugaison, respectivement représentées par id, avec un seul élément, $(1,2)$, avec trois éléments, et $(1,2,3)$, avec deux éléments. Il possède donc trois représentations irréductibles, à savoir : le caractère principal χ_1 et la signature χ_{sign}, qui sont de degré un, et la représentation π_2 de l'exemple VII.10, qui est de degré deux, associée à l'action naturelle du groupe sur un ensemble à trois éléments. On vérifie que $1^2+1^2+2^2=6$. Si χ_2 désigne le caractère de π_2, la table des caractères de Sym(3) s'écrit comme suit :

	1	2	3
	id	$(1,2,3)$	$(1,2)$
χ_1	1	1	1
χ_{sign}	1	1	-1
χ_2	2	-1	0

Pour calculer les valeurs de la dernière ligne, l'une des méthodes consiste à utiliser le fait que $(\chi_1+\chi_2)(g)$ est le nombre de points fixes de g pour l'action de Sym(3) sur $\{1,2,3\}$, c'est–à–dire respectivement 3, 0 et 1 pour g l'identité, un 3–cycle, et une transposition. Une autre méthode consiste à résoudre le système linéaire des deux équations $\langle\chi_2 \mid \chi_1\rangle = 0$ et $\langle\chi_2 \mid \chi_{\mathrm{sign}}\rangle = 0$, où les deux inconnues sont $\chi_2(1,2,3)$ et $\chi_2(1,2)$.

Remarque. Le groupe Sym(3) est isomorphe au groupe diédral D_6 des isométries du plan laissant invariant un triangle équilatéral. La représentation π_2 apparaît donc aussi aux exercices III.E1 et VII.E1.

XI.3. Le groupe symétrique de quatre objets, ou groupe spécial du cube.

Le groupe Sym(4) possède cinq classes de conjugaison :

la classe de id, réduite à un élément ;
la classe de $(1,2)$, à six éléments ;
la classe de $(1,2,3)$, à huit éléments ;
la classe de $(1,2,3,4)$, à six éléments ;
la classe de $(1,2)(3,4)$, à trois éléments.

Rappelons qu'il existe un homomorphisme surjectif standard de Sym(4) sur Sym(3), dont le noyau est constitué de l'identité et de la classe de conjugaison de $(1,2)(3,4)$; voir l'exercice VII.E4.ii ou l'exercice VIII.E7. Le groupe Sym(4) possède cinq représentations irréductibles qui sont :

— le caractère principal χ_1 et la signature χ_{sign}, qui sont de degré un ;
— la représentation de permutation π_2 de l'exemple VII.10 pour le groupe Sym(3), considéré comme une représentation de Sym(4) comme à l'exemple I.5, représentation dont nous désignons le caractère par χ_2 ;
— la représentation de permutation de l'exemple VII.10 pour le groupe Sym(4), que nous notons π_3 ici, et le produit $\chi_{\mathrm{sign}}\pi_3$, comme à l'exercice V.E1.

La table des caractères s'écrit comme suit :

	1	3	8	6	6
	id	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4)$	$(1,2)$
	0	π	$2\pi/3$	$\pi/2$	π
χ_1	1	1	1	1	1
χ_{sign}	1	1	1	-1	-1
χ_2	2	2	-1	0	0
χ_3	3	-1	0	-1	1
$\chi_{\text{sign}}\chi_3$	3	-1	0	1	-1

Remarques. (i) Le caractère produit $\chi_{\text{sign}}\pi_2$ (voir l'exercice V.E1) coïncide avec le caractère χ_2, de sorte que les représentations $\chi_{\text{sign}}\pi_2$ et π_2 sont équivalentes.

(ii) Si on préfère penser à ce groupe comme au groupe SG_C des rotations d'un cube, la représentation π_2 s'obtient à partir de l'action du groupe sur l'ensemble des trois droites passant par les milieux de paires de faces opposées. La représentation π_3 s'obtient à partir de l'action du groupe sur l'ensemble des quatre droites passant par des paires de sommets opposés ; elle s'obtient bien sûr aussi comme la succession des inclusions $SG_C \subset S\mathcal{O}(3) \subset GL_3(\mathbf{C})$.

La troisième ligne de la table ci–dessus indique pour chaque classe de conjugaison l'angle des rotations du cube la constituant.

(iii) La table illustre l'observation suivante, valable pour tout groupe fini G dont l'ordre est un multiple de 4. Comme le carré d'un nombre impair est congru à 1 modulo 4, il résulte du théorème IX.1 que le nombre des classes d'équivalence de représentations irréductibles de degrés impairs est nécessairement un multiple de 4.

XI.4. Le groupe alterné de quatre objets.

Le groupe Alt(4) possède quatre classes de conjugaison, trois caractères de degré un (car l'abélianisé de Alt(4) est d'ordre 3) et une représentation irréductible π_3 de degré trois. Si ω désigne une racine cubique primitive de l'unité, nous laissons à la lectrice le soin de vérifier que la table des caractères s'écrit :

	1	3	4	4
	id	$(1,2)(3,4)$	$(1,2,3)$	$(1,3,2)$
	0	π	$2\pi/3$	$-2\pi/3$
χ_1	1	1	1	1
χ_1'	1	1	ω	ω^2
χ_1''	1	1	ω^2	ω
χ_3	3	-1	0	0

En relation avec l'isomorphisme $\text{Alt}(4) \simeq SG_T$, la troisième ligne de la table indique l'angle de la rotation correspondante du tétraèdre régulier, avec une convention de signe qu'on laisse à la lectrice le soin d'expliciter.

Remarque : la comparaison des tables XI.3 et XI.4 montre que la restriction au groupe Alt(4) de la représentation π_2 du groupe Sym(4) est la somme directe des caractères χ_1' et χ_1''.

XI.5. Le groupe spécial de l'icosaèdre régulier, ou groupe alterné de cinq objets.

Le groupe SG_I est isomorphe au groupe alterné Alt(5), comme établi à l'exercice VII.E8. C'est un groupe d'ordre 60 qui possède cinq classes de conjugaison (exemple VII.11 et exercice VII.E7).

Le groupe SG_I possède deux représentations irréductibles immédiatement visibles, qui sont l'indentité χ_1 et la représentation π_3 de degré 3 fournie par les inclusions $SG_I \subset S\mathcal{O}(3) \subset GL_3(\mathbf{C})$, comme à l'exemple VII.11. Nous connaissons également[28] une représentation irréductible π_4 de degré 4 associée à l'action de SG_I sur un ensemble de 5 cubes, comme à l'exercice VII.E8, et une représentation irréductible π_5 de degré 5 associée à l'action de SG_I sur un ensemble de 6 droites, comme à l'exercice VII.E6. Vu que SG_I possède 5 représentations irréductibles non équivalentes deux à deux, il existe encore une représentation irréductible, nécessairement de degré 3 (théorème IX.1) ; nous la notons π_3'. Notons encore χ_3, χ_3', χ_4 et χ_5 les caractères correspondants.

En utilisant systématiquement les égalités du type $\chi(g) = |X^g|$, voir l'exemple V.3, on obtient la table partielle suivante

	1	15	20	12	12
	0	π	$2\pi/3$	$2\pi/5$	$4\pi/5$
χ_1	1	1	1	1	1
χ_3	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3'	3	a	b	c	d
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

où a, b, c, d sont (provisoirement) des inconnues. [Rappelons de l'exemple VII.11 que $1 + 2\cos(2\pi/5) = (1+\sqrt{5})/2$ et $1 + 2\cos(4\pi/5) = (1-\sqrt{5})/2$].

Pour déterminer a, b, c, d, il y a plusieurs méthodes, dont les trois que voici.

(i) Résoudre le système linéaire

$$\langle \chi_3' \mid \chi_1 \rangle \;=\; \langle \chi_3' \mid \chi_3 \rangle \;=\; \langle \chi_3' \mid \chi_4 \rangle \;=\; \langle \chi_3' \mid \chi_5 \rangle \;=\; 0$$

fourni par les relations d'orthogonalité.

(ii) Utiliser l'isomorphisme de $SG_I \approx \mathrm{Alt}(5)$ et poser $\pi_3' = \pi_3\alpha$ comme à l'exercice VII.E10.

(iii) "Trouver" π_3' dans le produit tensoriel de π_3 et π_4 ; voir ci–dessous le dernier des exemples XII.11, ainsi que le théorème de Burnside cité en XIII.6.

La table des caractères de SG_I s'écrit donc :

[28] La représentation irréductible de degré 4 peut aussi être vue comme sous–représentation de la représentation de permutation de $SL_2(\mathbf{F}_4)$ sur $\mathbf{F}_4 \sqcup \{\infty\}$. De même pour la représentation irréductible de degré 5 et la représentation de permutation de $PSL_2(\mathbf{F}_5)$ sur $\mathbf{F}_5 \sqcup \{\infty\}$. Voir l'exercice VIII.E5.

	1	15	20	12	12
	0	π	$2\pi/3$	$2\pi/5$	$4\pi/5$
	id	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
χ_1	1	1	1	1	1
χ_3	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3'	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

En relation avec l'isomorphisme $SG_I \simeq \mathrm{Alt}(5)$, la deuxième ligne de la table indique l'angle des rotations correspondantes de l'icosaèdre régulier et la troisième un représentant de la classe de conjugaison dans le groupe alterné.

On peut aussi ne penser qu'au groupe alterné (sans penser à l'icosaèdre). Les représentations irréductibles de Alt(5) immédiatement visibles sont l'identité χ_1 et la représentation de degré 4, sous–représentation de la représentation de permutation associée à l'action du groupe sur $\{1,2,3,4,5\}$. On trouve une représentation de degré 5 en considérant l'action du groupe sur l'ensemble des sous–ensembles à deux éléments de $\{1,2,3,4,5\}$ (voir la solution de l'exercice XI.E7). Il n'y a qu'une représentation de degré 1, car l'abélianisé de Alt(5) est réduit à un élément, et quatre représentations de degrés impairs (remarque (iii) de XI.3). S'il n'existait pas de représentation de degré 3, la somme des carrés des degrés des représentations irréductibles serait au moins $1 + 4 \times 5^2 > 60$, ce qui est absurde ; il existe donc au moins une représentation irréductible de degré 3, et en fait deux (voir IX.1). Il existe plusieurs manières d'exhiber une représentation irréductible de degré 3 ; l'une consiste à utiliser (de manière plus ou moins apparente) l'isomorphisme $\mathrm{Alt}(5) \approx SG_I$; une autre consiste à considérer une décomposition en irréductibles du produit extérieur de la représentation de degré 4 par elle-même, mais les prérequis d'algèbre linéaire ne sont pas disponibles à ce stade de notre exposition (voir le § 3.1 de [FulHa–91]).

Pour compléter la table des caractères de Alt(5) à partir des lignes de χ_1, χ_4 et χ_5, il suffit d'utiliser les relations d'orthogonalité et quelques arguments simples ; pour les détails, voir l'exemple 9 du paragraphe 15 dans [AlpBe–95].

XI.6. A propos du groupe symétrique de cinq objets.

Le groupe Sym(5) possède sept classes de conjugaison. Il possède exactement deux représentations de degré 1, l'identité et la signature, la représentation de degré quatre de l'exemple VII.10, et son produit par la signature. Les degrés $n_1 = 1$, $n_2 = 1$, $n_3 = 4$, $n_4 = 4$, n_5, n_6, n_7 satisfont donc la relation $120 = 1+1+16+16+n_5^2+n_6^2+n_7^2$, ou encore $86 = n_5^2 + n_6^2 + n_7^2$ avec $2 \leq n_5 \leq n_6 \leq n_7$. On vérifie que ces relations n'ont qu'une seule solution : $n_5 = 5$, $n_6 = 5$ et $n_7 = 6$. (Suite à l'exercice XI.E7.)

XI.7. Les groupes diédraux.

Pour tout entier $k \geq 1$, rappelons que le groupe diédral d'ordre $2k$ est

$$D_{2k} = \{1, r, \dots, r^{k-1}, s, sr, \dots, sr^{k-1}\}$$

(exercices III.E1 et VII.E1). Selon que k est impair ou pair, ce groupe possède 2 ou 4 représentations irréductibles de degré un, dont nous noterons les caractères χ_1, χ_1' ou

$\chi_1, \chi_1', \chi_1'', \chi_1'''$, et $(k-1)/2$ ou $(k-2)/2$ représentations irréductibles de degré deux, dont nous notons les caractères $\chi_j^{(2)}$, avec $1 \leq j \leq (k-1)/2$ ou $1 \leq j \leq (k-2)/2$ selon le cas ; voir l'exercice III.E1 et l'exemple IX.7. Nous écrivons ici les tables de caractères sous une forme légèrement différente des exemples précédents.

Cas où k est impair

$$1 \leq j \leq \frac{k-1}{2}$$

	r^j	sr^j
χ_1	1	1
χ_1'	1	-1
$\chi_j^{(2)}$	$2\cos(2\pi j/k)$	0

Cas où k est pair

$$1 \leq j \leq \frac{k-2}{2}$$

	r^j	sr^j
χ_1	1	1
χ_1'	1	-1
χ_1''	$(-1)^j$	$(-1)^j$
χ_1'''	$(-1)^j$	$(-1)^{j+1}$
$\chi_j^{(2)}$	$2\cos(2\pi j/k)$	0

XI.8. Groupes dont les caractères sont à valeurs entières. Les tables précédentes montrent que les valeurs des caractères complexes irréductibles sont des entiers rationnels pour les groupes $\mathrm{Sym}(k)$, $k \leq 4$, mais pas pour les groupes $\mathrm{Alt}(k)$, $3 \leq k \leq 5$, ni pour les groupes D_{2k}, $k = 5$ ou $k \geq 7$. Indiquons le critère suivant, pour la démonstration duquel nous renvoyons au numéro 12.5 de la partie II dans [Serre–67].

Pour que tout caractère complexe irréductible d'un groupe fini G soit à valeurs dans[29] $\mathbf{Z}$, *il faut et il suffit que G vérifie la ocndition suivante :*

pour tous $g \in G$ et $m \in \mathbf{Z}$ premier à l'ordre de g, les éléments g et g^m sont conjugués.

Les groupes symétriques $\mathrm{Sym}(k)$ satisfont à cette condition pour tout $k \geq 1$.

XI.9. L'ATLAS. Il existe de nombreuses tables de caractères. Par exemple, [ATLAS] fournit les tables pour plus de 200 groupes simples, dont les ordres vont de 60, pour le groupe $\mathrm{Alt}(5)$, à environ 8×10^{54}, pour "le monstre de Griess-Fischer", ou même environ 2×10^{75}, pour "le groupe $E_8(2)$". L'ATLAS traite en particulier de tous les groupes simples non abéliens d'ordre au plus 10^{25}, à l'exception de quelques familles "bien connues" ; par exemple : les $PSL_2(\mathbb{F}_q)$ ne sont tabulés que pour les ordres inférieurs à 10^6.

XI.10. Un théorème de Brauer. Les exemples précédents de tables de caractères montrent que les valeurs prises appartiennent à des corps de nombres "de petits degrés". Rappelons qu'un *corps de nombre* est un sous–corps de $\mathbf{C}$ qui, vu comme espace vectoriel sur $\mathbf{Q}$, est de dimension finie ; cette dimension s'appelle son *degré.*

[29] Ou, de manière équivalente (corollaire X.5), dans $\mathbf{Q}$.

Pour un groupe fini G donné, il est naturel de demander quels sont les corps de nombres $\mathbf{K}$ tels que *toute* représentation complexe de G soit *réalisable sur* $\mathbf{K}$, c'est–à–dire équivalente à une représentation $G \longrightarrow GL_n(\mathbf{C})$ d'image dans $GL_n(\mathbf{K})$; il est évidemment nécessaire qu'un tel corps $\mathbf{K}$ contienne toutes les valeurs du caractère χ_π, mais il se trouve que ce n'est pas suffisant.

Citons sans démonstration un résultat de Brauer. Voir par exemple le no 12.2 de [Serre–67].

Théorème. *Soit G un groupe fini ; notons m le plus petit commun multiple des ordres des éléments de G. Alors toute représentation irréductible de G est réalisable sur le corps cyclotomique* $\mathbf{Q}[\exp(2i\pi/m)]$.

Remarque. Certains groupes ont toutes leurs représentations irréductibles complexes réalisables sur le corps $\mathbf{Q}$ des nombres rationnels. C'est par exemple le cas des groupes symétriques $\mathrm{Sym}(k)$.

XI.11. Un théorème de Frobenius et Schur. Il est également naturel de demander quand une représentation irréductible d'un groupe fini G est *réelle*, c'est–à–dire équivalente à une représentation $G \longrightarrow GL_n(\mathbf{C})$ d'image dans $GL_n(\mathbf{R})$. Enoncons, de nouveau sans démonstration, un résultat de Frobenius et Schur (1906). Voir par exemple le no 12.6 de [Serre–67].

Théorème. *Soient π une représentation irréductible d'un groupe fini G, et χ son caractère. Alors la quantité*

$$(*) \qquad \frac{1}{|G|} \sum_{g \in G} \chi(g^2)$$

prend nécessairement l'une des trois valeurs 1, 0, -1. *La représentation π est réelle si et seulement si cette quantité vaut* 1.

Le théorème de Frobenius et Schur caractérise de plus les *représentations quaternioniennes* (que nous n'avons pas définies) comme celles pour lesquelles la quantité (*) vaut -1.

Exercices

XI.E1 Ecrire la table des caractères des groupes cycliques d'ordre 3, 4 et 5. Vérifier les tables de l'exemple XI.7 concernant les groupes diédraux.

XI.E2 Ecrire la table des caractères du groupe diédral D_8 d'ordre huit avec cinq colonnes correspondant aux cinq classes de conjugaison, respectivement représentées par 1, r^2, r, s et sr. Ecrire de même la table du groupe des quaternions $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ de l'exercice III.E2, dont les cinq classes de conjugaison sont 1, -1, $\pm i$, $\pm j$ et $\pm k$. Constater que ces deux tables sont "égales", bien que les deux groupes ne sont pas isomorphes.

(On peut montrer *a priori* que c'est la table d'un groupe d'ordre 8 non abélien ; voir la page 158 de [AlpBe–95]. Par ailleurs, tout groupe d'ordre 8 non abélien est isomorphe à l'un de D_8 ou Q.)

XI.E3 On conserve les notations de l'exercice précédent. Observer que la représentation irréductible de D_8 de degré deux est réalisable sur les réels, c'est–à–dire est réalisable par un homomorphisme $D_8 \longrightarrow GL_2(\mathbf{R})$.

Montrer que, en revanche, la représentation irréductible $\pi : Q \longrightarrow GL_2(\mathbf{C})$ de l'exercice III.E1 n'est pas équivalente à une représentation d'image dans $GL_2(\mathbf{R})$. [Indication : observer que $\pi(Q) \subset \mathcal{SU}(2)$; si π était réalisable sur $\mathbf{R}$, il existerait $S \in GL_2(\mathbf{C})$ tel que $S\pi(g)S^{-1} \subset SO(2)$ pour tout $g \in G$, ce qui est absurde car Q n'est pas abélien.]

XI.E3bis Les formules de l'exercice III.E2 montrent que la représentation irréductible de Q de degré deux est réalisable sur le corps $\mathbf{Q}[i]$. Montrer qu'elle l'est aussi sur le corps quadratique $\mathbf{Q}[\exp(2i\pi/3)]$.

??????????? Indication, si c'est vrai !!!!!!!!!!!!!

XI.E4 Constater qu'il existe un homomorphisme de groupes $r : GL_2(\mathbf{C}) \longrightarrow GL_4(\mathbf{R})$. Sa composition avec la représentation $\pi : Q \longrightarrow GL_2(\mathbf{C})$ de l'exercice III.E1 fournit une représentation $Q \longrightarrow GL_4(\mathbf{C})$ réalisable sur les réels.

XI.E5 Le groupe alterné Alt(5) possède exactement six 5–Sylow, et agit donc par conjugaisons sur l'ensemble de ces six sous–groupes. La représentation de permutation associée est somme directe du caractère principal et d'une représentation π_0. Montrer que la représentation π_0 est équivalente à la représentation de l'exercice VII.E6.

XI.E6 Dessiner le graphe biparti pondéré étiqueté $B_{\mathrm{Sym}(2)}^{\mathrm{Sym}(3)}$ défini comme suit.

Rappelons d'abord qu'un graphe Γ est *biparti* s'il existe une partition de l'ensemble de ses sommets en deux parties non vides, $V = V' \sqcup V''$ telle que toute arête joigne un sommet de V' et un sommet de V''. Dans cet exercice, un graphe est *pondéré* lorsqu'il est donné avec une fonction à valeurs numériques définie sur l'ensemble de ses arêtes ; un graphe pondéré est *sans multiplicité* lorsque que cette fonction est constante de valeur 1. Un graphe est *étiqueté* lorsqu'il est donné avec une fonction à valeurs numériques définie sur l'ensemble des sommets.

Pour $k \geq 1$, notons $\hat{G}_k$ l'ensemble des classes d'équivalence de représentations irréductibles du groupe symétrique Sym(k). L'ensemble des sommets de $B_{\mathrm{Sym}(2)}^{\mathrm{Sym}(3)}$ est la réunion disjointe des ensembles $V' = \hat{G}_2$ et $V'' = \hat{G}_3$. Chaque sommet est étiqueté par le degré de la représentation correspondante. Soit $\rho \in V'' = \hat{G}_3$ une représentation irréductible de Sym(3) et soit $\rho|_2 = \bigoplus_{s=1}^t n_s\sigma_s$ une décomposition de la restriction de ρ à Sym(2) en représentations irréductibles, avec les $\sigma_s \in V' = \hat{G}_2$ non équivalentes deux à deux et les n_s des entiers strictement positifs. Alors $B_{\mathrm{Sym}(2)}^{\mathrm{Sym}(3)}$ contient une arête de multiplicité n_s liant ρ à σ_s pour tout $s \in \{1, \ldots, t\}$. Vérifier que le graphe $B_{\mathrm{Sym}(2)}^{\mathrm{Sym}(3)}$ est sans multiplicité.

Plus généralement, à toute paire (G, H) constituée d'un groupe fini G et d'un sous–groupe H, on associe le *graphe de Bratteli* B_H^G. La terminologie vient d'un graphe analogue défini pour les paires d'algèbres semi–simples complexes [Bratt–72] ; de fait, B_H^G est le graphe de Bratteli au sens premier pour la paire d'algèbres $\mathbf{C}[H] \subset \mathbf{C}[G]$.

Dessiner de même le graphe de Bratteli de la paire Sym(3) $\subset$ Sym(4) et vérifier qu'il est aussi sans multiplicté.

En revanche, ce n'est pas le cas du graphe de la paire Sym(2) $\subset$ Sym(4).

Noter que le graphe de Bratteli de la paire $\mathrm{Alt}(4) \subset \mathrm{Sym}(4)$ n'est pas connexe.

XI.E7* Calculer la table des caractères du groupe symétrique $\mathrm{Sym}(5)$. Dessiner le graphe de Bratteli de la paire $\mathrm{Sym}(4) \subset \mathrm{Sym}(5)$.

Dessiner le graphe de Bratteli de la paire $\mathrm{Alt}(5) \subset \mathrm{Sym}(5)$.

Remarque. Même pour les groupes finis dont on connaît la table des caractères, il est en général autrement plus difficile d'exhiber des modèles des représentations irréductibles. Pour les groupes $\mathrm{Sym}(n)$ *et* $\mathrm{Alt}(n)$*, de tels modèles sont connus depuis le début du XXe siècle. En revanche, pour les groupes* $SL_n(\mathbf{F}_q)$*, si les tables de caractères étaient connues avant 1910 (Frobenius, Schur, Jordan), il a fallu attendre les années 1950 pour commencer à comprendre les représentations elles–mêmes (Green et beaucoup d'autres, pour* $GL_n(\mathbf{F}_q)$*,* $SL_n(\mathbf{F}_q)$ *et les autres groupes finis "de type Lie").*

XII. Produits tensoriels

Les espaces vectoriels qui apparaissent ci-dessous sont tous définis sur un même corps $\mathbf{K}$*. Pour un autre exposé rapide de ce qui suit, voir l'appendice A2 de* [Vinbe–89].

XII.1. Définition. *Soient* U, V *deux espaces vectoriels de dimension finie. Un produit tensoriel de* U *et* V *est un espace vectoriel* W *muni d'une application bilinéaire*

$$\begin{cases} U \times V & \longrightarrow \quad W \\ (u,v) & \longmapsto u \otimes v \end{cases}$$

telle que, si $\mathcal{B} = (b_1, \ldots, b_m)$ *est une base de* U *et* $\mathcal{C} = (c_1, \ldots, c_n)$ *est une base de* V*, alors* $(b_i \otimes c_j)_{1 \le i \le m, 1 \le j \le n}$ *est une base de* W*.*

Notons que, pour peu qu'il existe, l'espace W *est nécessairement de dimension égale au produit de celles de* U *et* V*.*

XII.2. Propriété universelle. *Si un tel produit tensoriel de* U *et* V *existe, alors, pour tout espace vectoriel* E *et pour toute application bilinéaire*

$$\varphi \,:\, U \times V \longrightarrow E$$

il existe une unique application linéaire

$$\Phi \,:\, W \longrightarrow E$$

telle que $\Phi(u \otimes v) = \varphi(u,v)$ *pour tous* $u \in U$ *et* $v \in V$*.*

Démonstration. Soient $\mathcal{B}$ et $\mathcal{C}$ comme ci-desssus. Alors Φ est l'unique application linéaire de W dans E telle que $\Phi(b_i \otimes c_j) = \varphi(b_i, c_j)$ pour tous $i \in \{1, \ldots, m\}$ et $j \in \{1, \ldots, n\}$. □

La proposition est résumée par l'égalité

$$\mathrm{Bil}(U, V; E) \approx \mathcal{L}(U \otimes V, E)$$

où $\mathrm{Bil}(U, V; E)$ désigne l'espace vectoriel des applications bilinéaires de $U \times V$ dans E.

XII.3. Proposition. *Le produit de deux espaces vectoriels existe ; il est unique à isomorphisme* canonique *près.*

Démonstration de l'existence. Soient U, V deux espaces vectoriels de dimensions finies ; notons U' le dual de U. Nous allons voir que l'espace $\mathcal{L}(U', V)$ et l'application bilinéaire

$$\begin{cases} U \times V \longrightarrow \mathcal{L}(U', V) \\ (u, v) \longmapsto (\psi \mapsto \psi(u)v) \end{cases}$$

démontrent l'existence du produit tensoriel de U et V.

Soient $\mathcal{B}$ et $\mathcal{C}$ comme ci-desssus. Rappelons que U' possède une *base duale* de $\mathcal{B}$, dont les vecteurs b'_i sont définis par $b'_{i'}(b_i) = \delta_{i',i}$. Comme

$$\dim(\mathcal{L}(U', V)) \;=\; \dim(U')\dim(V) \;=\; \dim(U)\dim(V) \;=\; mn,$$

il suffit de vérifier que la famille $(b_i \otimes c_j)_{1 \le i \le m, 1 \le j \le n}$ est libre.

Soit $(\lambda_{i,j})_{1 \le i \le m, 1 \le j \le n}$ une famille de nombres dans $\mathbf{K}$ telle que

$$\sum_{1 \le i \le m, 1 \le j \le n} \lambda_{i,j} b_i \otimes c_j \;=\; 0.$$

Pour tout $i' \in \{1, \ldots, m\}$, on peut évaluer cette relation de dépendance linéaire sur $b'_{i'}$:

$$\Big(\sum_{1 \le i \le m, 1 \le j \le n} \lambda_{i,j} b_i \otimes c_j \Big)(b'_{i'}) \;=\; \sum_{1 \le j \le n} \lambda_{i',j} c_j \;=\; 0,$$

et ceci implique $\lambda_{i',j} = 0$ pour tout $j \in \{1, \ldots, n\}$, ce qu'il fallait montrer.

Variante pour la démonstration de l'existence (esquisse). Si $U = \mathbf{K}^X$ et $V = \mathbf{K}^Y$, alors l'espace $W = \mathbf{K}^{X \times Y}$ et l'application bilinéaire $\mathbf{K}^X \times \mathbf{K}^Y \longrightarrow \mathbf{K}^{X \times Y}$ associant à un couple de fonctions (ψ_X, ψ_Y) la fonction $(x, y) \longmapsto \psi_X(x)\psi_Y(y)$ conviennent.

Démonstration de l'unicité. Soient $W, \tilde{W}$ deux produits tensoriels de U et V ; soient

$$\varphi : U \times V \longrightarrow W \qquad \text{et} \qquad \tilde{\varphi} : U \times V \longrightarrow \tilde{W}$$

les applications bilinéaires correspondantes. La propriété universelle montre qu'il existe des applications linéaires

$$\Phi : \tilde{W} \longrightarrow W \qquad \text{et} \qquad \tilde{\Phi} : W \longrightarrow \tilde{W}$$

telles que la restriction de $\Phi\tilde{\Phi}$ à une base de W est l'identité, et la restriction de $\tilde{\Phi}\Phi$ à une base de $\tilde{W}$ est l'identité ; il en résulte que Φ et $\tilde{\Phi}$ sont des *isomorphismes* linéaires inverses l'un de l'autre. □

XII.4. Notation et remarques. Nous écrivons désormais $U \otimes V$ "le" produit tensoriel de U et V et

$$\begin{cases} U \times V \longrightarrow U \otimes V \\ (u, v) \longmapsto u \otimes v \end{cases}$$

l'application canonique. La dimension de $U \otimes V$ est le produit des dimensions de U et V.

Les vecteurs de $U \otimes V$ de la forme $u \otimes v$ sont des vecteurs particuliers ! en général, un vecteur de $U \otimes V$ s'écrit comme une *somme* $\sum_i u_i \otimes v_i$ de tels vecteurs.

Nous laissons à la lectrice le soin de vérifier qu'il existe des isomorphismes naturels entre

(i) $\mathbf{K} \otimes U$ et U ;
(ii) $U \otimes \mathbf{K}$ et U ;
(iii) $U \otimes V$ et $V \otimes U$;
(iv) $(U \otimes V)'$ et $U' \otimes V'$;
(v) $(U_1 \otimes U_2) \otimes U_3$ et $U_1 \otimes (U_2 \otimes U_3)$.

La démonstration de la proposition XII.3 montre qu'il existe des isomorphismes naturels entre

(vi) $U' \otimes V$ et $\mathcal{L}(U, V)$, ou $U \otimes V$ et $\mathcal{L}(U', V)$;
(vii) $\mathbf{K}^{X \times Y}$ et $\mathbf{K}^X \otimes \mathbf{K}^Y$.

(Il est important pour ces derniers isomorphismes que U soit de dimension finie et que les ensembles X, Y soient finis.)

Démonstrations pour certains de ces isomorphismes. Il est conseillé de manipuler les produits tensoriels avant de lire dans tous leurs détails les justifications de leurs propriétés. Un cadre approprié et plus général que celui adopté ici est celui des produits tensoriels de modules sur un anneau commutatif ; voir par exemple le chapitre XVI de [Lang–65].

(i) Le dual $\mathbf{K}'$ de $\mathbf{K}$ étant canoniquement isomorphe à $\mathbf{K}$, l'espace $\mathcal{L}(\mathbf{K}', U)$ est canoniquement isomorphe à U.

(iii) Vu que le bidual U'' s'identifie à U, la transposition des homomorphismes fournit un isomorphisme de $\mathcal{L}(U', V)$ sur $\mathcal{L}(V', U)$.

(iv) L'espace $\mathrm{Bil}(U, V; \mathbf{K})$ est canoniquement isomorphe à $(U \otimes V)'$. Il suffit donc de vérifier que les espaces $\mathrm{Bil}(U, V; \mathbf{K})$ et $\mathcal{L}(U, V')$ sont isomorphes, ce dont on s'assure par exemple en contemplant les applications

$$\begin{cases} \mathcal{L}(U, V') & \longrightarrow \quad \mathrm{Bil}(U, V; \mathbf{K}) \\ \quad \alpha & \longmapsto \quad \Big((u, v) \mapsto (\alpha(u))(v)\Big) \end{cases}$$

et

$$\begin{cases} \mathcal{L}(U, V') & \longrightarrow \qquad \mathrm{Bil}(U, V; \mathbf{K}) \\ \quad \beta & \longmapsto \quad \left(u \longmapsto \begin{cases} V \longrightarrow \mathbf{K} \\ v \longmapsto \beta(u, v) \end{cases}\right), \end{cases}$$

inverses l'une de l'autre.

(v) L'espace $(U_1 \otimes U_2) \otimes U_3$ est isomorphe à $\mathcal{L}((U_1 \otimes U_2)', U_3)$, donc par (iv) à $\mathrm{Bil}(U_1', U_2'; U_3)$. L'espace $U_1 \otimes (U_2 \otimes U_3)$ est isomorphe à $\mathcal{L}(U_1', \mathcal{L}(U_2', U_3))$. L'application

$$\begin{cases} \qquad \mathrm{Bil}(U_1', U_2'; U_3) & \longrightarrow \quad \mathcal{L}(U_1', \mathcal{L}(U_2', U_3)) \\ \Big((\lambda_1', \lambda_2') \longmapsto \beta(\lambda_1', \lambda_2')\Big) & \longmapsto \quad \Big(\lambda_1' \longmapsto \big(\lambda_2' \mapsto \beta(\lambda_1', \lambda_2')\big)\Big) \end{cases}$$

est un isomorphisme.

(vi) L'approche des produits tensoriels choisie ici est basée sur l'isomoprhisme

$$\begin{cases} U \otimes V & \longrightarrow \ \mathcal{L}(U', V) \\ \ u \otimes v & \longmapsto \ (\psi \mapsto \psi(u)v). \end{cases}$$

Ecrivons l'isomorphisme inverse. Soient $(b_i)_{1 \leq i \leq m}$ une base de U et $\big(b_{i'}'\big)_{1 \leq i' \leq m}$ la base duale de U'. Alors

$$\begin{cases} \mathcal{L}(U', V) & \longrightarrow \qquad U \otimes V \\ \quad \alpha & \longmapsto \quad \displaystyle\sum_{i'=1}^{m} b_{i'} \otimes \alpha(b_{i'}') \end{cases}$$

convient.

□

XII.5. Produit tensoriel d'applications linéaires et fonctorialité. Soient $\alpha : U_1 \longrightarrow U_2$ et $\beta : V_1 \longrightarrow V_2$ deux applications linéaires. L'application *bilinéaire*

$$U_1 \times V_1 \longrightarrow U_2 \otimes V_2, \quad (u, v) \longmapsto (\alpha(u)) \otimes (\beta(v))$$

induit une application *linéaire*

$$\alpha \otimes \beta \, : \, U_1 \otimes V_1 \longrightarrow U_2 \otimes V_2, \quad u \otimes v \longmapsto (\alpha(u)) \otimes (\beta(v))$$

qui[30] est le *produit tensoriel* des applications α et β.

Pour des applications linéaires

$$U_1 \xrightarrow{\alpha_1} U_2 \xrightarrow{\alpha_2} U_3 \qquad \text{et} \qquad V_1 \xrightarrow{\beta_1} V_2 \xrightarrow{\beta_2} V_3,$$

il est facile de vérifier que

$$(\alpha_2\alpha_1) \otimes (\beta_2\beta_1) \; = \; (\alpha_2 \otimes \beta_2)\,(\alpha_1 \otimes \beta_1).$$

Par ailleurs, il est tout aussi facile de vérifier que le produit tensoriel de deux applications $\mathrm{id}_U : U \longrightarrow U$ et $\mathrm{id}_V : V \longrightarrow V$ est l'application identité $\mathrm{id}_{U\otimes V} : U \otimes V \longrightarrow U \otimes V$.

Il résulte des deux faits précédents que, pour deux applications linéaires inversibles $\alpha : U_1 \longrightarrow U_2$ et $\beta : V_1 \longrightarrow V_2$, le produit tensoriel est encore inversible et

$$(\alpha \otimes \beta)^{-1} \; = \; (\alpha^{-1}) \otimes (\beta^{-1}).$$

Soient U et V deux espaces vectoriels, m et n leurs dimensions, et $\alpha \in \mathcal{L}(U)$ et $\beta \in \mathcal{L}(V)$ deux endomorphismes linéaires, dont on note $z_1, \dots, z_m$ et $w_1, \dots, w_n$ les valeurs propres, répétées selon leurs multiplicités. Alors les valeurs propres de $\alpha \otimes \beta \in \mathcal{L}(U \otimes V)$ sont $(z_i w_j)_{1\le i\le m, 1\le j\le n}$, comme il résulte de la preuve de la proposition V.5.

XII.6. Traduction matricielle. Soient (U_j, V_j) deux paires d'espaces vectoriels, $j = 1, 2$. Choisissons des bases $\mathcal{B}^{(j)} = (b_1^{(j)}, \dots, b_{m^{(j)}}^{(j)})$ de U_j et $\mathcal{C}^{(j)} = (c_1^{(j)}, \dots, c_{n^{(j)}}^{(j)})$ de V_j, et notons $\left(b_k^{(j)} \otimes c_\ell^{(j)}\right)_{1\le k\le m^{(j)}, 1\le \ell\le n^{(j)}}$ la base correspondante de $U_j \otimes V_j$.

Soient $\mu : U_1 \longrightarrow U_2$ une application linéaire et M sa matrice relativement aux bases $\mathcal{B}^{(1)}$ et $\mathcal{B}^{(2)}$. Soient de même $\nu : V_1 \longrightarrow V_2$ une application linéaire et N sa matrice relativement aux bases $\mathcal{C}^{(1)}$ et $\mathcal{C}^{(2)}$.

Il résulte des définitions que la matrice P de $\mu \otimes \nu : U_1 \otimes V_1 \longrightarrow U_2 \otimes V_2$ relativement aux bases $\left(b_k^{(j)} \otimes c_\ell^{(j)}\right)_{1\le k\le m^{(j)}, 1\le \ell\le n^{(j)}}$, $j = 1, 2$, est donnée par

$$P_{(k',\ell'),(k,\ell)} \; = \; M_{k',k} N_{\ell',\ell}.$$

[30]Quitte à répéter une remarque de XII.4, insistons sur le fait que les vecteurs de la forme $u \otimes v$ sont des vecteurs *particuliers* de $U_1 \otimes V_1$. Toutefois, comme ils engendrent linéairement $U_1 \otimes V_1$, il suffisent à décrire précisément l'application linéaire $\alpha \otimes \beta$.

(On s'en assure de la manière usuelle, en considérant le vecteur image d'un vecteur du type $b_k^{(1)} \otimes b_\ell^{(1)}$, écrit comme combinaison linéaire des vecteurs $b_{k'}^{(2)} \otimes b_{\ell'}^{(2)}$ de la base de l'espace image.)

On définit naturellement le *produit tensoriel de deux matrices*, de telle sorte que, étant donné des bases appropriées, la matrice d'un produit tensoriel d'applications linéaires soit le produit tensoriel des matrices correspondantes.

XII.7. Produit tensoriel de deux représentations. Soient $\pi_j : G \longrightarrow GL(U_j)$, $j = 1, 2$, deux représentations d'un même groupe G. On définit le *produit tensoriel des représentations* π_1 *et* π_2 comme étant la représentation $\pi_1 \otimes \pi_2$ de G définie par

$$(\pi_1 \otimes \pi_2)(g) \;=\; (\pi_1(g)) \otimes (\pi_2(g))$$

pour tout $g \in G$. Le degré de $\pi_1 \otimes \pi_2$ est le produit des degrés de π_1 et π_2. (Pour cette définition, il importe peu que le groupe G soit fini ou infini.)

Attention : le produit tensoriel de deux représentations irréductibles n'est en général pas irréductible. Soit par exemple π la représentation complexe irréductible de degré 2 du groupe symétrique Sym(3). La représentation $\pi \otimes \pi$ est de degré 4. Comme les degrés des représentations complexes irréductibles de Sym(3) sont 1, 1 et 2, la représentation $\pi \otimes \pi$ ne saurait être irréductible (voir ci-dessous l'exemple XII.11)

XII.8. Cas des espaces hermitiens et des représentations unitaires. Soient U et V des espaces hermitiens. Il existe une unique forme sesquilinéaire

$$\langle \cdot \mid \cdot \rangle \;:\; (U \otimes V) \times (U \otimes V) \;\longrightarrow\; \mathbf{C}$$

telle que

$$\langle u_1 \otimes v_1 \mid u_2 \otimes v_2 \rangle \;=\; \langle u_1 \mid u_2 \rangle \, \langle v_1 \mid v_2 \rangle$$

pour tous $u_1, u_2 \in U$ et $v_1, v_2 \in V$, et cette forme est un produit scalaire sur $U \otimes V$. Pour la définir, il suffit par exemple de choisir des bases orthonormales $(b_1, \ldots, b_m)$ de U et $(c_1, \ldots, c_n)$ de V, et de décréter que la base $(b_i \otimes c_j)_{1 \leq i \leq m, 1 \leq j \leq n}$ de $U \otimes V$ est orthonormale.

Soient alors $\pi_j : G \longrightarrow \mathcal{U}(U_j)$, $j = 1, 2$, deux représentations unitaires d'un groupe G. Il est immédiat de vérifier que la représentation produit tensoriel $\pi_1 \otimes \pi_2$ est également unitaire.

XII.9. Exemples. (i) Soient $\pi_j : G \longrightarrow GL(V_j)$, $j = 1, 2$, deux représentations d'un groupe G ; notons $\check{\pi}_1$ la représentation contragrédiente de π_1. Alors la représentation produit tensoriel $\check{\pi}_1 \otimes \pi_2$ est équivalente à la représentation de G dans $V_1' \otimes V_2 \approx \mathcal{L}(V_1, V_2)$ qui apparaît aux numéros II.8, V.5 et VII.1.

(ii) Soit G un groupe agissant sur deux ensembles finis X et Y. Notons π_X et π_Y les représentations correspondantes de G, dans les espaces $\mathbf{K}^X$ et $\mathbf{K}^Y$ respectivement. Alors la représentation produit tensoriel $\pi_X \otimes \pi_Y$ est équivalente à la représentation de G dans $\mathbf{K}^{X \times Y}$ correspondant à l'action diagonale de G dans $X \times Y$ (action définie en V.3). En particulier, $\pi_X \otimes \pi_X$ est la représentation notée $(\pi_X)^{\otimes 2}$ à l'exemple VII.8.

(iii) Soient $\chi : G \longrightarrow \mathbf{K}^*$ un caractère linéaire et $\pi : G \longrightarrow GL(V)$ une représentation d'un même groupe G. Le produit tensoriel $\chi \otimes \pi$ est aussi noté $\chi\pi$, comme à l'exercice V.E2.

XII.10. Caractère d'un produit tensoriel. C'est une conséquence immédiate de la proposition V.5 (voir aussi XII.5), ou également du numéro XII.6, que la trace d'un produit tensoriel de deux matrices carrées (ou de deux endomorphismes linéaires) est le produit des traces des deux matrices (ou des deux endomorphismes). [Pour les lectrices allergiques à l'usage des bases, voir par exemple Bourbaki, *Algèbre linéaire*, chapitres 1 à 3 (Bourbaki, 1970), corollaire II de la page A.II.80.]

Il en résulte que le caractère d'un produit tensoriel est égal au produit des caractères des représentations facteurs du produit tensoriel,

$$\chi_{\pi_1 \otimes \pi_2} \,=\, \chi_{\pi_1}\chi_{\pi_2}$$

comme à la proposition V.5.

XII.11. Exemples de décompositions de produits tensoriels en représentations irréductibles. Considérons le groupe symétrique Sym(3) d'ordre 6. Désignons comme à l'exemple XI.2 par $\chi_1, \chi_{\mathrm{sign}}$ et π_2 ses représentations complexes irréductibles, respectivement de degrés 1, 1 et 2 ; notons χ_2 le caractère de π_2.

Considérons alors la représentation $\pi \,=\, \pi_2 \otimes \pi_2$. Son caractère est de la forme $\chi = a\chi_1 + b\chi_{\mathrm{sign}} + c\chi_2$, où a, b, c sont des entiers positifs. Le résultat du numéro précédent et la table de l'exemple XI.2 montrent que

$$\begin{aligned} \chi(1) \,&=\, 4 \,=\, a+b+2c \\ \chi(1,2) \,&=\, 0 \,=\, a-b \\ \chi(1,2,3) \,&=\, 1 \,=\, a+b-c. \end{aligned}$$

Il en résulte que $a = b = c = 1$, c'est–à–dire que

$$\pi_2 \otimes \pi_2 \,\approx\, \chi_1 \oplus \chi_{\mathrm{sign}} \oplus \pi_2.$$

Un calcul analogue pour le groupe alterné Alt(4) d'ordre 12 et sa représentation irréductible π_3 de degré 3 montre que

$$\pi_3 \otimes \pi_3 \,\approx\, \chi_1 \oplus \chi_1' \oplus \chi_1'' \oplus 2\pi_3$$

(les notations sont celles de l'exemple XI.4).

Considérons enfin les produits tensoriels des représentations irréductibles du groupe spécial SG_I de l'icosaèdre ; nous reprenons les notations de l'exemple XI.5. La table

	1	15	20	12	12
	0	π	$2\pi/3$	$2\pi/5$	$4\pi/5$
χ_1	1	1	1	1	1
χ_3	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3'	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0
χ_3^2	9	1	0	$\frac{3+\sqrt{5}}{2}$	$\frac{3-\sqrt{5}}{2}$
$\chi_3\chi_4$	12	0	0	$\frac{-1-\sqrt{5}}{2}$	$\frac{-1+\sqrt{5}}{2}$

montre par exemple que $\chi_3^2 = \chi_1 + \chi_3 + \chi_5$ et $\chi_3\chi_4 = \chi_3' + \chi_4 + \chi_5$, et par conséquent que

$$\pi_3 \otimes \pi_3 \;\approx\; \chi_1 \oplus \pi_3 \oplus \pi_5 \qquad \text{et} \qquad \pi_3 \otimes \pi_4 \;\approx\; \pi_3' \oplus \pi_4 \oplus \pi_5 .$$

Les autres produits se lisent dans la table suivante :

$$\begin{array}{ccc}
\chi_3^2 & = & \chi_1 + \chi_3 + \chi_5 \\
\chi_3\chi_3' & = & \chi_4 + \chi_5 \\
\chi_3\chi_4 & = & \chi_3' + \chi_4 + \chi_5 \\
\chi_3\chi_5 & = & \chi_3 + \chi_3' + \chi_4 + \chi_5 \\
\\
{\chi_3'}^2 & = & \chi_1 + \chi_3' + \chi_5 \\
\chi_3'\chi_4 & = & \chi_3 + \chi_4 + \chi_5 \\
\chi_3'\chi_5 & = & \chi_3 + \chi_3' + \chi_4 + \chi_5 \\
\\
\chi_4^2 & = & \chi_1 + \chi_3 + \chi_3' + \chi_4 + \chi_5 \\
\chi_4\chi_5 & = & \chi_3' + \chi_3 + \chi_4 + 2\chi_5 \\
\\
\chi_5^2 & = & \chi_1 + \chi_3' + \chi_3 + 2\chi_4 + 2\chi_5
\end{array}$$

Exercices

XII.E1 Notons $\{b_1, \ldots, b_m\}$ la base canonique de $\mathbf{C}^m$, $\{c_1, \ldots, c_n\}$ la base canonique de $\mathbf{C}^n$, et $(b_i \otimes c_j)_{1 \le i \le m, 1 \le j \le n}$ la base correspondante de $\mathbf{C}^m \otimes \mathbf{C}^n$. On ordonne lexicographiquement les couples (i,j) et on identifie $\mathbf{C}^m \otimes \mathbf{C}^n$ à $\mathbf{C}^{mn}$. On considère également deux matrices

$$M \;=\; \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \quad \text{vue comme une application} \quad \mathbf{C}^3 \longrightarrow \mathbf{C}^2,$$
$$N \;=\; \begin{pmatrix} p & q \\ r & s \\ t & u \end{pmatrix} \quad \text{vue comme une application} \quad \mathbf{C}^2 \longrightarrow \mathbf{C}^3.$$

Ecrire les matrices $MN \in M_2(\mathbf{C})$, $NM \in M_3(\mathbf{C})$, $M \otimes N \in M_6(\mathbf{C})$ et $N \otimes M \in M_6(\mathbf{C})$.

XII.E2 Avec les notations de l'exemple XI.2, vérifier que

$$\chi_1\pi_2 \;\approx\; \chi_1'\pi_2 \;\approx\; \pi_2$$

et

$$\pi_2 \otimes \pi_2 \otimes \pi_2 \;\approx\; \chi_1 \oplus \chi_{\mathrm{sign}} \oplus 3\pi_2 .$$

Plus généralement, vérifier que

$$\pi_2^{\otimes n} \;\approx\; a\chi_1 \oplus b\chi_1' \oplus c\pi_2$$

avec $a = b = \frac{1}{3}\left(2^{n-1} + (-1)^n\right)$ et $c = \frac{1}{3}\left(2^n + (-1)^{n+1}\right)$, pour tout $n \ge 1$.

XII.E3 Soient H, K deux groupes et $\rho : H \longrightarrow GL(V)$, $\sigma : K \longrightarrow GL(W)$ deux représentations. On définit une représentation π du produit direct $H \times K$ dans $V \otimes W$ par $\pi(h,k) = \rho(h) \otimes \sigma(k)$ pour tous $h \in H$ et $k \in K$. La représentation π est le *produit tensoriel extérieur* des représentations ρ et σ, et se note parfois $\rho \boxtimes \sigma$.

(i) Vérifier que les classes de conjugaison de $H \times K$ sont de la forme $C \times D$, où C [respectivement D] est une classe de conjugaison de H [resp. K]. En particulier, si H et K sont finis, *ce qu'on suppose désormais*, le nombre des classes de conjugaison de $H \times K$ est égal au produit des nombres correspondants pour H et K.

(ii) Vérifier que le caractère d'une représentation π comme ci–dessus est un produit au sens où $\chi_\pi(h,k) = \chi_\rho(h)\chi_\sigma(k)$.

(iii) Si ρ et σ sont irréductibles, montrer qu'il en est de même de π. [Indication : calculer $\langle \chi_\pi \mid \chi_\pi \rangle$. Remarque : il existe aussi des arguments valant pour des groupes finis *ou infinis* ; voir par exemple dans [Vinbe–89] le théorème 6 du chapitre 4.]

(iv) Soient ρ, ρ' *deux* représentations irréductibles de H et σ, σ' deux représentations irréductibles de K. Montrer que, pour que les représentations $\pi = \rho \boxtimes \sigma, \pi' = \rho' \boxtimes \sigma$ soient équivalentes, il faut et il suffit que $\rho \approx \rho'$ et $\sigma \approx \sigma'$. [Indication : comparer χ_π et $\chi_{\pi'}$.]

(v) Montrer que toute représentation irréductible de $H \times K$ est de la forme $\rho \boxtimes \sigma$.

XIII. Sous–groupes finis de $\mathcal{SU}(2)$ et graphes de McKay

XIII.1. Rappel concernant l'homomorphisme de $\mathcal{SU}(2)$ sur $\mathcal{SO}(3)$. Notons E l'espace vectoriel réel des matrices complexes 2–fois–2 qui sont hermitiennes de trace nulle, c'est–à–dire de la forme $\begin{pmatrix} x & y+iz \\ y-iz & -x \end{pmatrix}$, avec $x, y, z \in \mathbf{R}$. L'espace E est euclidien pour le produit scalaire défini par $\langle A \mid B \rangle = \frac{1}{2}\,\mathrm{trace}(AB)$; notons que le carré de la norme associée s'écrit aussi $A \longmapsto -\det(A)$.

L'algèbre de matrices $M_2(\mathbf{C})$ contient à la fois l'espace E et le groupe

$$\mathcal{SU}(2) = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in M_2(\mathbf{C}) \;\middle|\; |a|^2 + |b|^2 = 1 \right\}$$

de l'exercice V.E8. A toute matrice $g \in \mathcal{SU}(2)$ correspond une transformation linéaire $\Psi(g)$ de l'espace E définie par

$$\Psi(g)(A) = gAg^* \qquad \text{pour} \quad g \in \mathcal{SU}(2), A \in E \;;$$

la transformation $\Psi(g)$ est orthogonale, car

$$\|gAg^*\|^2 = \frac{1}{2}\,\mathrm{trace}\left((gAg^*)^2\right) = \frac{1}{2}\,\mathrm{trace}\left(A^2\right) = \|A\|^2 ,$$

et toujours de déterminant $+1$, car le groupe $\mathcal{SU}(2)$ est connexe ; en d'autres termes, $\Psi(g) \in \mathcal{SO}(3)$. L'application

$$\Psi : \mathcal{SU}(2) \longrightarrow \mathcal{SO}(3)$$

est un homomorphisme de groupes.

On montre que cet homomorphisme est surjectif et que son noyau est formé des deux matrices $\pm I_2$ constituant le centre du groupe $\mathcal{SU}(2)$. Si $h \in \mathcal{SO}(3)$ est une rotation de E d'angle θ, alors les deux éléments de $\Psi^{-1}(h)$ sont des matrices unitaires de valeurs propres $\exp(\pm i\theta/2)$ et $\exp(\pm i(\theta/2+\pi))$. Pour tout ceci, voir par exemple le chapitre IX des notes[31] du cours d'algèbre I.

Notons que, pour tout sous–groupe G de $\mathcal{SU}(2)$, l'inclusion de G dans $\mathcal{SU}(2)$ est une représentation unitaire (la représentation tautologique). Elle est irréductible si et seulement si G est non abélien (voir le corollaire IV.2).

XIII.2. Lemme. *Soit G^* un groupe possédant un sous–groupe normal d'ordre deux, noté ici $\{\pm \mathrm{id}\}$. Soient G le quotient $G^*/\{\pm \mathrm{id}\}$ et $\Psi : G^* \longrightarrow G$ la projection canonique.*

(i) Si C est une classe de conjugaison de G, alors $\Psi^{-1}(C)$ est ou bien une classe de conjugaison de G^* ou bien la réunion de deux classes de conjugaison de G^*.

(ii) Supposons G fini. Soient k^* et k les nombres des classes de conjugaison de G^* et G. Alors $k+1 \leq k^* \leq 2k$.

Démonstration. Pour toute classe C^* de conjugaison de G^*, l'image $\Psi(C^*)$ est une classe de conjugaison de G. Comme l'image inverse par Ψ de tout élément de G est constituée de deux éléments, ceci implique l'assertion (i). L'assertion (ii) résulte de (i) car le noyau $\Psi^{-1}(1)$ est la réunion de deux classes.

□

XIII.3. Lemme. *Soit* $\mathbf{V}$ *le sous–groupe de $\mathcal{SO}(3)$ constitué de l'identité et des trois matrices diagonales dont deux coefficients diagonaux sont -1 et le troisième* 1 *(c'est une incarnation du* Viergruppe *de Klein). Soit $\Psi : \mathcal{SU}(2) \longrightarrow \mathcal{SO}(3)$ comme en XIII.1.*

Alors $\Psi^{-1}(\mathbf{V})$ est le groupe des quaternions Q de l'exercice III.E2. En particulier, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ est un commutateur dans le groupe $\Psi^{-1}(\mathbf{V})$.

Démonstration. Il est par exemple immédiat de vérifier que

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} x & y+iz \\ y-iz & -x \end{pmatrix} \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} -x & y-iz \\ y+iz & x \end{pmatrix}.$$

Les calculs sont analogues pour les conjugaisons par $\pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ et $\pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. □

Pour la table des caractères de $\Psi^{-1}(\mathbf{V})$, voir l'exercice XI.E2.

XIII.4. Le groupe binaire du tétraèdre. Notons SG_T le groupe spécial du tétraèdre, comme à l'exemple VIII.2. Le *groupe binaire du tétraèdre* est le sous–groupe $G_T^* = \Psi^{-1}(SG_T)$ de $\mathcal{SU}(2)$. C'est un groupe fini d'ordre 24.

Les groupes associés à deux tétraèdres réguliers centrés à l'origine de $\mathbf{R}^3$ sont conjugués dans $\mathcal{SO}(3)$, et les deux sous–groupes correspondants de la forme G_T^* sont donc aussi conjugués dans $\mathcal{SU}(2)$. Nous considérons désormais un tétraèdre régulier T centré à l'origine de $\mathbf{R}^3$, fixé, de sorte que les notations SG_T et G_T^* ne sont pas ambiguës.

---

[31] Disponibles sur la toile : http://www.unige.ch/math/biblio/polycops/algebre

Les représentations irréductibles de SG_T fournissent par composition avec Ψ trois représentations irréductibles $\chi_1 = 1_{G_T^*}, \chi_1'$ et χ_1'' de degré un et une représentation irréductible π_3 de degré trois de G_T^*. Grâce au lemme XIII.3, on vérifie que G_T^* ne possède pas d'autre représentation de degré un. Comme G_T^* n'est pas abélien, la représentation tautologique $\pi_2^{\mathrm{taut}} : G_T^* \longrightarrow \mathcal{SU}(2)$ est irréductible. Notons χ_3 et χ_2^{taut} les caractères de π_3 et π_2^{taut}.

Soit $g \in G_T^*$ une matrice telle que $\Psi(g)$ soit un tiers de tour, et plus précisément telle que les valeurs propres de g soient $\exp(\pm i\pi/3)$; posons $\omega = \exp(i\pi/3)$. Alors $\chi_2^{\mathrm{taut}}(g) = 1$, $\chi_1'(g)\chi_2^{\mathrm{taut}}(g) = \omega$ et $\chi_1''(g)\chi_2^{\mathrm{taut}}(g) = \omega^2$ sont distincts, de sorte que les représentations π_2^{taut}, $\pi_2' = \chi_2'\pi_2^{\mathrm{taut}}$ et $\pi_2'' = \chi_2''\pi_2^{\mathrm{taut}}$ sont non équivalentes deux à deux. Notons χ_2' et χ_2'' les caractères de π_2' et π_2''.

Nous avons énuméré des représentations $\chi_1, \chi_1', \chi_1'', \pi_3, \pi_2^{\mathrm{taut}}, \pi_2'$ et π_2'' de G_T^*. L'égalité

$$24 \,=\, 1^2 + 1^2 + 1^2 + 3^2 + 2^2 + 2^2 + 2^2$$

montre que ces sept représentations irréductibles constituent une liste complète (à équivalence près) pour G_T^*. Ceci montre de plus que G_T^* possède exactement sept classes de conjugaison.

L'image inverse de la classe des demi–tours de SG_T constitue donc une seule classe de conjugaison dans G_T^*.

XIII.5. La table des caractères du groupe binaire du tétraèdre. Les considérations du numéro précédent permettent d'écrire cette table, que voici. Nous avons désigné par $(1,2,3)'$ et $(1,2,3)''$ les deux classes de conjugaison de G_T^* qui se projettent sur l'une des deux classes de tiers de tour de SG_T et par $(1,3,2)'$ et $(1,3,2)''$ les deux autres.

	1	1	6	4	4	4	4
	id	$-\mathrm{id}$	$\Psi^{-1}((1,2)(3,4))$	$(1,2,3)'$	$(1,2,3)''$	$(1,3,2)'$	$(1,3,2)''$
	1	-1	$\pm i$	$e(\pm i\pi/3)$	$e(\pm i2\pi/3)$	$e(\pm i\pi/3)$	$e(\pm i2\pi/3)$
χ_1	1	1	1	1	1	1	1
χ_2^{taut}	2	-2	0	1	-1	1	-1
χ_3	3	3	-1	0	0	0	0
χ_2'	2	-2	0	ω	$-\omega$	ω^2	$-\omega^2$
χ_1'	1	1	1	ω	ω	ω^2	ω^2
χ_2''	2	-2	0	ω^2	$-\omega^2$	ω	$-\omega$
χ_1''	1	1	1	ω^2	ω^2	ω	ω

La troisième ligne de la table indique les valeurs propres des éléments de la classe dans $\mathcal{SU}(2)$; on y écrit $e(\pm i\pi/3)$ pour $\exp(\pm i\pi/3)$.

La table permet de calculer facilement les décompositions en sommes d'irréductibles de produits tensoriels. Par exemple, pour les produits tensoriels avec π_2^{taut} :

$$(*)\qquad \begin{array}{rcl}
\chi_1 \otimes \pi_2^{\mathrm{taut}} & \approx & \pi_2^{\mathrm{taut}} \\
\pi_2^{\mathrm{taut}} \otimes \pi_2^{\mathrm{taut}} & \approx & \chi_1 \oplus \pi_3 \\
\pi_3 \otimes \pi_2^{\mathrm{taut}} & \approx & \pi_2^{\mathrm{taut}} \oplus \pi_2' \oplus \pi_2'' \\
\pi_2' \otimes \pi_2^{\mathrm{taut}} & \approx & \pi_3 \oplus \chi_1' \\
\chi_1' \otimes \pi_2^{\mathrm{taut}} & \approx & \pi_2' \\
\pi_2'' \otimes \pi_2^{\mathrm{taut}} & \approx & \pi_3 \oplus \chi_1'' \\
\chi_1'' \otimes \pi_2^{\mathrm{taut}} & \approx & \pi_2''
\end{array}$$

Notons d'une part que ces décompositions sont sans multiplicité, et d'autre part que σ apparaît dans $\rho \otimes \pi_2^{\mathrm{taut}}$ si et seulement si ρ apparaît dans $\sigma \otimes \pi_2^{\mathrm{taut}}$.

XIII.6. Graphes de McKay. Etant donné un groupe fini G et une représentation π de G, les décompositions en irréductibles des produits tensoriels par π sont encodées dans le *graphe de McKay* $\mathrm{MK}(G, \pi)$, défini comme suit. Soient $\rho_1, \ldots, \rho_k$ les représentations complexes irréductibles de G, à équivalence près. Les multiplicités $m_{i,j}$ sont définies par $\rho_i \otimes \pi \approx \bigoplus_{j=1}^k m_{i,j}\rho_j$. Le graphe $\mathrm{MK}(G, \pi)$ a pour sommets les ρ_j et, pour chaque paire (i, j) telle que $m_{i,j} \geq 1$, une arête orientée de poids $m_{i,j}$ de ρ_i vers ρ_j ; lorsque $m_{j,i} = m_{i,j} \geq 1$, l'usage est de remplacer les deux arêtes orientées correspondantes par une seule arête non orientée de poids $n_{\rho,\sigma}$. Voir [McKay–80] et [FoMcK–81].

Par exemple, les calculs (*) du numéro précédent montre que le graphe $\mathrm{MK}(G_T^*, \pi_2^{\mathrm{taut}})$ est un tripode dont chaque pied est long de deux arêtes. Il est connu sous le nom de "graphe de Dynkin de type $\tilde{E}_6$".

La dernière table de l'exemple XII.11 montre que $\mathrm{MK}(SG_I, \pi_3)$ est un graphe sans multiplicité, contrairement à $\mathrm{MK}(SG_I, \pi_5)$. Ces graphes possèdent des boucles ; par exemple, dans $\mathrm{MK}(SG_I, \pi_3)$, il existe des arêtes dont l'origine coïncide avec l'extrémité aux sommets correspondant à π_3, π_4 et π_5.

Le groupe simple $G_{168} = SL_2(\mathbf{F}_7)$ d'ordre 168 possède des représentations irréductibles χ_1, π_3, π_3', π_6, π_7, π_8 (les indices sont les degrés). Sa table des caractères est par exemple établie au chapitre 27 de [JamLi–01]. Elle permet de vérifier que le graphe de McKay $\mathrm{MK}(G_{168}, \pi_3)$ contient une arête dirigée de π_3 vers π_3', mais aucune de π_3' vers π_3.

Revenons au cas général d'un graphe de McKay $\mathrm{MK}(G, \pi)$.

Si la représentation π est fidèle, c'est un résultat de Burnside que le graphe $\mathrm{MK}(G, \pi)$ est connexe par chemins orientés. En voici la formulation classique : si la représentation π est fidèle, il existe pour toute représentation irréductible ρ de G un entier $n \geq 1$ tel que ρ soit équivalente à une sous–représentation de $\pi^{\otimes n}$. On peut d'ailleurs majorer l'entier n en terme du nombre N des valeurs prises par le caractère de π : il existe un entier $n \in \{0, 1, \ldots, N-1\}$ tel que ρ soit équivalente à une sous–représentation de $\pi^{\otimes n}$ [JamLi–01, théorème 19.10]. (Exemple : si π est la représentation régulière de G, alors $N = 2$; voir le théorème IX.1.)

Notons $\chi_1, \ldots, \chi_k$ les caractères de $\rho_1, \ldots, \rho_k$. Si le caractère χ de π ne prend que des valeurs réelles, alors $m_{j,i} = \langle \chi_j\chi \mid \chi_i \rangle = \langle \chi_j \mid \chi\chi_i \rangle = m_{i,j}$ et la matrice des multiplicités $(m_{i,j})_{1 \leq i,j \leq k}$ est symétrique. Il n'est pas difficile de vérifier que la réciproque est également vraie. Pour les quelques exemples de groupes étudiés dans ces notes (à l'exception de G_{168} évoqué ci–dessus), les caractères des représentations fidèles dont à valeurs réelles, et les graphes de McKay correspondants sont donc non dirigés.

XIII.7. Restrictions à G_T^* des représentations irréductibles de $\mathcal{SU}(2)$. Considérons un entier $n \geq 0$, l'espace $V_n = \mathcal{P}^{(n)}(\mathbf{C}^2)$ des fonctions polynomiales homogènes de degré n de $\mathbf{C}^2$ dans $\mathbf{C}$, et la représentation $\pi_n^{(\mathcal{SU}(2))}$ de $\mathcal{SU}(2)$ dans V_n, de degré $n+1$, comme à l'exercice V.E9. Rappelons que

$$\left(\pi_n^{(\mathcal{SU}(2))}\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}\varphi\right)\begin{pmatrix} x \\ y \end{pmatrix} = \varphi\left(\begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

pour tous $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathcal{SU}(2)$, $\varphi \in V_n$ et $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{C}^2$. En particulier, si ξ et η désignent comme en V.E9 les projections canoniques $\mathbf{C}^2 \longrightarrow \mathbf{C}$, alors $\left(\xi^{n-j}\eta^j\right)_{0\leq j\leq n}$ est une base de V_n et

$$\left(\pi_n^{(\mathcal{SU}(2))}\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}\right)\xi^{n-j}\eta^j \ = \ e^{i(-n+2j)\theta}\xi^{n-j}\eta^j, \qquad 0 \leq j \leq n.$$

Notons aussi que, si n est pair (c'est–à–dire si la dimension de V_n est impaire), alors $\pi_n^{(\mathcal{SU}(2))}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \mathrm{id}_{V_n}$, de sorte que $\pi_n^{(\mathcal{SU}(2))}$ factorise en une représentation du groupe quotient $\mathcal{SU}(2))/\{\pm 1\} \simeq \mathcal{SO}(3)$.

Toute matrice de $\mathcal{SU}(2)$ a deux valeurs propres $\exp(\pm i\theta)$, avec $\theta \in [0, \pi]$, et deux telles matrices sont conjuguées si et seulement si les angles correspondants sont égaux. Le caractère de $\pi_n^{(\mathcal{SU}(2))}$ est donc donné par la formule

$$\begin{aligned}\operatorname{trace}\left(\pi_n^{(\mathcal{SU}(2))}\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}\right) &= e^{in\theta} + e^{i(n-2)\theta} + \cdots + e^{-i(n-2)\theta} + e^{-in\theta} \\ &= \frac{\sin\big((n+1)\theta\big)}{\sin(\theta)} \ = \ U_n(\cos(\theta)).\end{aligned}$$

On reconnaît les *polynômes de Tchebichev de seconde espèce* U_n, dont les premiers sont

$$\begin{array}{lcclcc} U_0(\cos\theta) & = & 1 & U_2(\cos\theta) & = & 4\cos^2\theta - 1 \\ U_1(\cos\theta) & = & 2\cos\theta & U_3(\cos\theta) & = & 8\cos^3\theta - 4\cos\theta \end{array}$$

et qui satisfont à la relation de récurrence linéaire à trois termes

$$U_{n+1}(T) \ = \ 2TU_n(T) - U_{n-1}(T), \qquad n \geq 1.$$

En particulier, les restrictions à G_T^* des caractères des représentations $\pi_n^{(\mathcal{SU}(2))}$ sont données par la table suivante, où la troisième ligne indique les valeurs de $\cos\theta$.

	1	1	6	4	4	4	4
	id	$-$ id	$\Psi^{-1}((1,2)(3,4))$	$(1,2,3)'$	$(1,2,3)''$	$(1,3,2)'$	$(1,3,2)''$
	1	-1	0	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$
$U_0(\cos\theta)$	1	1	1	1	1	1	1
$U_1(\cos\theta)$	2	-2	0	1	-1	1	-1
$U_2(\cos\theta)$	3	3	-1	0	0	0	0
$U_3(\cos\theta)$	4	-4	0	-1	1	-1	1

La table permet de vérifier qu'on a bien

$$U_1(\cos\theta) \ = \ 2\cos\theta \ = \ \chi_2^{\mathrm{taut}}\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

et

$$U_2(\cos\theta) \;=\; 4\cos^2\theta - 1 \;=\; \chi_3\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta}\end{pmatrix}$$

(χ_2^{taut} et χ_3 comme dans la table XIII.5). En d'autres termes, la restriction de $\pi_1^{(\mathcal{SU}(2))}$ au groupe G_T^* est la représentation tautologique π_2^{taut} et la restriction de $\pi_2^{(\mathcal{SU}(2))}$ à G_T^* est la représentation π_3. (Voilà une manière bien détournée de montrer que la représentation $\pi_2^{(\mathcal{SU}(2))}$ est irréductible.) Le calcul

$$\frac{1}{|G_T^*|}\sum_{g\in G_T^*}\big(U_3(\cos\theta)\big)^2 \;=\; \frac{1}{24}\big(16+16+0+4+4+4+4\big) \;=\; 2$$

montre que la restriction à G_T^* de $\pi_3^{(\mathcal{SU}(2))}$ est une somme de deux représentations irréductibles inéquivalentes. En consultant la table des caractères de G_T^*, on vérifie que cette restriction est équivalente à la somme des deux représentations irréductibles de caractères χ_2' et χ_2''.

XIII.8. Réalisation matricielle. Bien que nous n'allons pas utiliser ceci dans ces notes, signalons la réalisation matricielle du groupe G_T^* calculée par Felix Klein [Klein–56]. C'est le groupe constitué des 24 matrices

$$\begin{pmatrix} i^k & 0 \\ 0 & (-i)^k\end{pmatrix}, \qquad \begin{pmatrix} 0 & -(-i)^k \\ i^k & 0\end{pmatrix},$$

$$\begin{pmatrix} i^k\,\frac{\epsilon+i}{2} & i^k\,\frac{-1+i}{2} \\ (-i)^k\,\frac{1+i}{2} & (-i)^k\,\frac{\epsilon-i}{2}\end{pmatrix}, \qquad \begin{pmatrix} -(-i)^k\,\frac{1+i}{2} & -(-i)^k\,\frac{\epsilon-i}{2} \\ i^k\,\frac{\epsilon+i}{2} & -i^k\,\frac{1-i}{2}\end{pmatrix}$$

où $k = 0,1,2,3$ et $\epsilon = 1,-1$. Le même livre contient des réalisations matricielles des groupes G_C^*, G_I^*, et plus généralement de tous les sous–groupes finis de $\mathcal{SU}(2)$ à conjugaison près.

XIII.9. Le groupe binaire du cube. Choisissons un cube C centré à l'origine de $\mathbf{R}^3$ et notons SG_C le groupe spécial de C. Le *groupe binaire du cube* est le sous–groupe $G_C^* = \Psi^{-1}(SG_C)$ de $\mathcal{SU}(2)$; à conjugaison près, il ne dépend pas du choix de C. C'est un groupe fini d'ordre 48, qui contient G_T^* comme sous–groupe d'indice 2.

Le groupe G_C^* n'est pas abélien ; la représentation tautologique $\pi_2^{\text{taut}} : G_C^* \longrightarrow \mathcal{SU}(2)$ est donc irréductible. Rappelons que, avec nos notations, c'est la restriction à G_C^* de la représentation $\pi_1^{(\mathcal{SU}(2))}$ de $\mathcal{SU}(2)$.

Affirmation : la restriction π_4 à G_C^* de la représentation irréductible $\pi_3^{(\mathcal{SU}(2))}$ de $\mathcal{SU}(2)$, de degré 4, est également irréductible. En effet, le groupe SG_C contient

1 rotation d'angle 0,
9 rotations d'angle π,
8 rotations d'angle $2\pi/3$,
6 rotations d'angle $\pi/2$.

Par suite, le groupe G_C^* contient

les matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}$ et $\begin{pmatrix} -1 & 0 \\ 0 & -1\end{pmatrix}$,

18 matrices de valeurs propres $\pm i = \pm\exp(\pm i\pi/2)$,
8 matrices de valeurs propres $\exp(\pm i\pi/3)$ et 8 de valeurs propres $\exp(\pm 2i\pi/3)$,
6 matrices de valeurs propres $\exp(\pm i\pi/4)$ et 6 de valeurs propres $\exp(\pm 3i\pi/4)$.

Notons χ_4 le caractère de π_4. Pour $g \in G_C^*$, notons $\theta_g \in [0,\pi]$ l'angle tel que les valeurs propres de g sont $\exp(\pm i\theta_g)$. Alors

$$\begin{aligned}\langle \chi_4 \mid \chi_4\rangle &= \frac{1}{48}\sum_{g\in G_C^*}(U_3(\cos(\theta_g)))^2 = \frac{1}{48}\sum_{g\in G_C^*}\left(8\cos^3(\theta_g) - 4\cos(\theta_g)\right)^2 \\ &= \frac{1}{48}\left(4^2 + (-4)^2 + 8(-1)^2 + 8(1)^2\right) = 1\end{aligned}$$

(on vérifie que $U_3(\cos\theta) = 0$ si θ est l'une des valeurs $\pi/2, \pi/4, 3\pi/4$). Ceci achève la démonstration de l'affirmation.

Les représentations irréductibles de SG_C fournissent par composition avec Ψ des représentations irréductibles $\chi_1 = 1_{G_C^*}, \chi_1', \pi_2, \pi_3$ et π_3' de G_C^*, respectivement de degrés $1, 1, 2$,3,3 et de caractères $\chi_1, \chi_1', \chi_2, \chi_3, \chi_3'$. (Nous écrivons ici χ_1' et χ_3' les caractères notés χ_{sign} et $\chi_{\mathrm{sign}}\chi_3$ en XI.1.)

Les représentations π_2^{taut} et $\chi_1'\pi_2^{\mathrm{taut}}$ ne sont pas équivalentes, car leurs caractères χ_2^{taut} et χ_2' sont distincts.

La somme des carrés des degrés des représentations ainsi répertoriées valant

$$\begin{aligned}\mathrm{degr}(\chi_1)^2 &+ \mathrm{degr}(\chi_1')^2 + \mathrm{degr}(\chi_2)^2 + \mathrm{degr}(\chi_3)^2 + \mathrm{degr}(\chi_3')^2 \\ &+ \mathrm{degr}(\chi_2^{\mathrm{taut}})^2 + \mathrm{degr}(\chi_2')^2 + \mathrm{degr}(\chi_4)^2 \\ &= 1^2 + 1^2 + 2^2 + 3^2 + 3^2 + 2^2 + 2^2 + 4^2 \\ &= 48,\end{aligned}$$

il n'y a pas d'autre représentation irréductible (à équivalence près).

XIII.10. La table des caractères de G_C^*. Il résulte du numéro précédent que le groupe G_C^* est réunion de 8 classes de conjugaison. Considérons une classe D du groupe quotient $SG_C = \Psi(G_C^*) = G_C^*/\{\pm I_2\}$.

Si D est la classe des demi–tours d'axes passant par les milieux de deux faces du cube, alors $\Psi^{-1}(D)$ est une seule classe dans G_C^* ; en effet, tout demi-tour $g \in SG_C$ de ce type est contenu dans un sous–groupe de SG_C isomorphe à SG_T, et les deux images inverses de g dans $\Psi^{-1}(g)$ sont déjà conjuguées dans $\Psi^{-1}(SG_T)$, comme nous l'avons vu en XIII.4. Si D est la classe des tiers de tour ou des quarts de tour, alors $\Psi^{-1}(D)$ est réunion de deux classes de G_C^* car, comme en XIII.4, $\Psi^{-1}(D)$ contient des matrices de valeurs propres distinctes. Il résulte de ce que G_C^* a 8 classes de conjugaison que, si D est la classe des demi–tours d'axes passant par les milieux de deux arêtes du cube, alors $\Psi^{-1}(D)$ est une classe dans G_C^*.

Il est maintenant facile d'écrire la table des caractères de G_C^*. La seconde ligne repère les classes de conjugaison dans G_C^* par leurs valeurs propres en tant que matrices de $\mathcal{SU}(2)$; leurs nombres d'éléments sont indiqués comme d'habitude à la première ligne. Si $e(\pm i\theta_g)$ est une telle paire de valeurs propres, la valeur correspondante $\chi_2^{\mathrm{taut}}(g)$ est $2\cos(\theta_g)$ et $\chi_4(g) = 8(\cos(\theta_g))^3 - 4\cos(\theta_g)$. A des permutations près des lignes et des colonnes, la table apparaît dans [FoMcK–81].

	1	1	6	8	8	6	6	12
	1	-1	$\pm i$	$e(\pm i\pi/3)$	$e(\pm i2\pi/3)$	$e(\pm i\pi/4)$	$e(\pm i3\pi/4)$	$\pm i$
χ_1	1	1	1	1	1	1	1	1
χ_2^{taut}	2	-2	0	1	-1	$\sqrt{2}$	$-\sqrt{2}$	0
χ_3'	3	3	-1	0	0	1	1	-1
χ_4	4	-4	0	-1	1	0	0	0
χ_2	2	2	2	-1	-1	0	0	0
χ_3	3	3	-1	0	0	-1	-1	1
χ_2'	2	-2	0	1	-1	$-\sqrt{2}$	$\sqrt{2}$	0
χ_1'	1	1	1	1	1	-1	-1	-1

Calculons comme en XIII.5 les décompositions en sommes d'irréductibles des produits tensoriels par π_2^{taut} :

$$\begin{array}{ccc}
\chi_1 \otimes \pi_2^{\text{taut}} & = & \pi_2^{\text{taut}} \\
\pi_2^{\text{taut}} \otimes \pi_2^{\text{taut}} & = & \chi_1 \oplus \pi_3' \\
\pi_3' \otimes \pi_2^{\text{taut}} & = & \pi_2^{\text{taut}} \oplus \pi_4 \\
\pi_4 \otimes \pi_2^{\text{taut}} & = & \pi_3' \oplus \pi_3 \oplus \pi_2 \\
\pi_2 \otimes \pi_2^{\text{taut}} & = & \pi_4 \\
\pi_3 \otimes \pi_2^{\text{taut}} & = & \pi_4 \oplus \pi_2' \\
\pi_2' \otimes \pi_2^{\text{taut}} & = & \pi_3 \oplus \chi_1' \\
\chi_1' \otimes \pi_2^{\text{taut}} & = & \pi_2'.
\end{array}$$

Il en résulte, comme en XIII.5–6, que le graphe de McKay $\mathrm{MK}(G_C^*, \pi_2^{\text{taut}})$ est à nouveau un tripode, dont les pieds sont cette fois longs de $3, 3, 1$ arêtes. Il est connu sous le nom de "graphe de Dynkin de type $\tilde{E}_7$".

XIII.11. Le groupe binaire de l'icosaèdre. Choisissons un icosaèdre I centré à l'origine de $\mathbf{R}^3$ et notons SG_I le groupe spécial de I. Le *groupe binaire de l'icosaèdre* est le sous–groupe $G_I^* = \Psi^{-1}(SG_I)$ de $SU(2)$, d'ordre 120.

Le Viergruppe $\mathbf{V}$ est un sous–groupe de SG_I, de sorte que le groupe des quaternions $Q = \Psi^{-1}(\mathbf{V})$ est un sous–groupe de G_I^* ; le lemme XIII.3 implique donc que $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ est un commutateur de G_I^*. Comme $SG_I \approx \mathrm{Alt}(5)$ est parfait (c'est–à–dire égal à son groupe dérivé), il en résulte que G_I^* est aussi parfait. Donc G_I^* possède un seul caractère linéaire.

Nous avons déjà énuméré à l'exemple VII.11 les éléments de SG_I ; ce sont

1 rotation d'angle 0,
15 rotations d'angle π,
20 rotations d'angle $2\pi/3$,
12 rotations d'angle $2\pi/5$,
12 rotations d'angle $4\pi/5$.

Par suite, le groupe G_I^* contient

les matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$,
30 matrices de valeurs propres $\pm i = \pm \exp(\pm i\pi/2)$,

20 matrices de valeurs propres $\exp(\pm i\pi/3)$ et 20 de valeurs propres $\exp(\pm 2i\pi/3)$,
12 matrices de valeurs propres $\exp(\pm i\pi/5)$ et 12 de valeurs propres $\exp(\pm 4i\pi/5)$,
12 matrices de valeurs propres $\exp(\pm 2i\pi/5)$ et 12 de valeurs propres $\exp(\pm 3i\pi/5)$.

On vérifie comme en XIII.10 d'abord que les 30 matrices de valeurs propres $\pm i$ constituent une seule classe de conjugaison et ensuite que G_I^* possède 9 classes de conjugaison.

Notons π_2^{taut}, π_4, π_6 les restrictions à G_I^* des représentations $\pi_1^{(\mathcal{SU}(2))}$, $\pi_3^{(\mathcal{SU}(2))}$, $\pi_5^{(\mathcal{SU}(2))}$ de $\mathcal{SU}(2)$, et χ_2^{taut}, χ_4, χ_6 leurs caractères. Les cinq représentations irréductibles de SG_I fournissent cinq représentations irréductibles de G_I^*, de degrés $1, 3, 3, 4, 5$; la représentation π_2^{taut} est irréductible de degré 2. Les degrés a, b, c des autres représentations irréductibles de G_I^* satisfont donc $a, b, c \geq 2$ et

$$1^2 + 3^2 + 3^2 + 4^2 + 5^2 + 2^2 + a^2 + b^2 + c^2 \;=\; 120.$$

Si les notations sont telles que $a \geq b \geq c$, ces conditions suffisent à déterminer $(a, b, c) = (6, 4, 2)$. En résumé, le groupe G_I^* possède des représentations irréductibles de degrés $1, 2, 3, 4, 5, 6, 4, 2, 3$.

Avec des notations comme en XIII.9, on peut vérifier que

$$\begin{aligned}
\langle \chi_2^{\text{taut}} \mid \chi_2^{\text{taut}} \rangle \;&=\; \frac{1}{120} \sum_{g \in G_I^*} (2\cos\theta_g)^2 \\
&=\; \frac{1}{120} \Bigg(2^2 + 2^2 + 20 + 20 + 12 \left(2\cos\frac{\pi}{5} \right)^2 + \\
&\qquad 12 \left(2\cos\frac{4\pi}{5} \right)^2 + 12 \left(2\cos\frac{2\pi}{5} \right)^2 + 12 \left(2\cos\frac{3\pi}{5} \right)^2 \Bigg) \\
&=\; 1,
\end{aligned}$$

c'est–à–dire que la représentation π_2^{taut} est irréductible (ce qu'on savait bien sûr déjà !). On peut surtout calculer

$$\begin{aligned}
\langle \chi_4 \mid \chi_4 \rangle \;&=\; \frac{1}{120} \sum_{g \in G_I^*} \left(8\cos^3\theta_g - 4\cos\theta_g \right)^2 \\
&=\; \cdots \;=\; 1
\end{aligned}$$

et

$$\begin{aligned}
\langle \chi_6 \mid \chi_6 \rangle \;&=\; \frac{1}{120} \sum_{g \in G_I^*} \left(32\cos^5\theta_g - 32\cos^3\theta_g + 6\cos\theta_g \right)^2 \\
&=\; \cdots \;=\; 1,
\end{aligned}$$

ce qui montre que π_4 et π_6 sont des représentations irréductibles. De plus, π_4 n'est pas équivalente à la représentation de degré deux factorisant par SG_I.

Avec encore un peu d'opiniâtreté, on arrive encore à calculer :

— la table des caractères de G_I^* (elle apparaît dans [FoMcK–81]) ; les caractères prennent leurs valeurs dans $\{0, \pm 1, \pm 2, 3, \pm 4, 5, \pm 6, \pm\frac{1}{2}(-1+\sqrt{5}), \pm\frac{1}{2}(-1-\sqrt{5})\}$;

— le graphe de McKay $MK(G_I^*, \pi_2^{\text{taut}})$, qui est un tripode dont les pieds sont longs de 5, 2, 1 arêtes et qui est connu sous le nom de “graphe de Dynkin de type $\tilde{E}_8$”.

Pour trouver la table des caractères dans [ATLAS], il faut savoir qu'un groupe que nous notons $PSL_2(\mathbf{F}_q)$ s'y note $L_2(q)$, donc $SG_I \approx \mathrm{Alt}(5) \approx PSL_2(\mathbf{F}_5) = L_2(5)$, et $SL_2(\mathbf{F}_q)$ s'y note $2 \cdot L_2(q)$, donc $G_I^* \approx SL_2(\mathbf{F}_5) = 2 \cdot L_2(5)$.

XIII.12. Programme. Voici un programme naturel.

— Énoncer et vérifier la classification des sous–groupes finis de $\mathcal{SU}(2)$, à conjugaison près. Pour ceux de $\mathcal{SO}(3)$, voir par exemple [Weyl, appendice A, pages 149–154]. Pour ceux de $\mathcal{SU}(2)$, voir par exemple [Wolf–67, théorème 2.6.7], ou [Lamot–86], ou l'exercice XIII.E2.

— Achever la liste ADE de McKay : les graphes $\tilde{D}_k$ pour les “groupes diédraux binaires” ou “groupes dicycliques” (indications à l'exercice XIII.E4) et les graphes $\tilde{A}_k$ pour les sous–groupes cycliques de $\mathcal{SU}(2)$. La liste ADE, constituée des deux familles infinies $\tilde{A}_k$, $\tilde{D}_k$ et des trois graphes $\tilde{E}_6$, $\tilde{E}_7$, $\tilde{E}_8$, se retrouve en de multiples domaines des mathématiques ; c'est un problème fascinant que de comprendre les raisons de son ubiquité [HaHSV–77].

XIII.13. Polytopes réguliers en dimension 4. Prenons le temps d'une digression géométrico–historique.

Considérons un entier $n \geq 2$ et un espace euclidien E de dimension n. Un *polytope* dans E est un sous–ensemble compact d'intérieur non vide qui est intersection d'un nombre fini de demi–espaces fermés ; de manière équivalente (mais il faut le montrer ...!), c'est l'enveloppe convexe d'un nombre fini de points qui engendrent affinement E. Un tel polytope possède des 0–facettes, ou sommets, des 1–facettes, ou arêtes, ..., et plus généralement des *j–facettes* pour $j \in \{0, \ldots, n-1\}$; on convient ici que les facettes sont des sous–ensembles fermés du polytope. Les $(n-1)$–facettes dont appelées des *faces*. Un *drapeau* d'un tel polytope est une suite $(F_0, F_1, \ldots, F_{n-1})$ où F_j est une j–facette et où $F_j \subset F_{j+1}$.

Le *groupe* G_P d'un polytope P est, comme en VII.18, le groupe des isométries de E laissant P invariant. C'est un groupe fini qui agit fidèlement sur l'ensemble des drapeaux de P et dont l'ordre est majoré par le nombre de ces drapeaux. Le polytope P est dit régulier si cette action est transitive. Il est facile de vérifier que cette définition du mot “régulier” est compatible avec son usage tel que pratiqué aux chapitres précédents dans le cadre des dimensions 2 et 3.

Pour toute dimension $n \geq 3$, il y a trois polytopes réguliers (à similitude près) qui sont le simplexe régulier, le cube et le cocube (en dimension 3, on dit “octaèdre” plutôt que “cocube”). Si $(e_1, \ldots, e_n)$ est une base orthonormale de $\mathbf{R}^n$, le *n–cube* est l'enveloppe convexe des 2^n sommets $\pm e_1 \pm e_2 \cdots \pm e_n$, le *$n$–cocube* est l'enveloppe convexe des $2n$ sommets $\pm e_1, \pm e_2, \ldots, \pm e_n$ et le *n–simplexe régulier* est l'enveloppe convexe des $n+1$ sommets $e_1, \ldots, e_{n+1}$ dans le sous–espace affine d'équation $x_1 + \cdots + x_{n+1} = 1$ de $\mathbf{R}^{n+1}$.

La *classification des polytopes réguliers* est due au Bernois Ludwig Schläfli, et remonte[32] aux années 1850, “un temps où Cayley, Grassmann et Möbius étaient les seuls autres personnes qui avaient jamais conçu la possibilité d'une géométrie en dimension supérieure à trois” (cité de la page 141 de [Coxet–73]). En dehors de la dimension deux, tout à fait particulière, il y a les “dimensions faciles”, c'est–à–dire les dimensions $n \geq 5$, où la liste simplexe–cube–cocube est complète. Les deux “dimensions difficiles” sont trois, où on

[32] Leur publication dut attendre 1901.

connaît l'icosaèdre et le dodécaèdre réguliers au moins depuis Pythagore et Platon, et la dimension quatre, où il existe trois polytopes réguliers exceptionnels ayant respectivement 24, 120 et 600 sommets. Une étude plus fine montre que les nombres N_j des j–facettes sont respectivement :

$N_0 = 24$, $N_1 = 96$, $N_2 = 96$, $N_3 = 24$ (les faces sont des octaèdres réguliers) ;
$N_0 = 120$, $N_1 = 720$, $N_2 = 1200$, $N_3 = 600$ (tétraèdres réguliers) ;
$N_0 = 600$, $N_1 = 1200$, $N_2 = 720$, $N_3 = 120$ (dodécaèdres réguliers).

Pour quelques notes sur l'attachante personalité de Schläfli, voir le § 7.X de [Coxet–73].

Il y a plusieurs procédés de construction pour ces 4–polytopes réguliers, dont celui que nous allons évoquer est directement lié à la matière de ce chapitre.

Comme au numéro XIII.1, le groupe $\mathcal{SU}(2)$ est un sous–ensemble de l'espace des matrices de la forme $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$, avec $a, b \in \mathbf{C}$, espace identifié ici à l'espace euclidien $\mathbf{R}^4$. Ainsi, à partir d'un sous–ensemble fini A de $\mathcal{SO}(3)$, on peut définir un polytope en dimension quatre qui est l'enveloppe convexe de $\Psi^{-1}(A)$. Dans le cas de $A = D_4$, il est facile de vérifier que l'enveloppe convexe de $\Psi^{-1}(A)$ est un 4–cocube (voir le lemme XIII.3). De même, si A est l'un des sous–groupes SG_T, SG_I de $\mathcal{SO}(3)$, on peut montrer que l'enveloppe convexe de $\Psi^{-1}(A)$ est respectivement un polytope régulier à 24 sommets, un polytope régulier à 120 sommets. L'enveloppe convexe des barycentres des faces d'un polytope régulier à 120 sommets est un polytope régulier à 600 sommets (et réciproquement). Voir par exemple [Lamot–86, § II.3].

Exercices et compléments

XIII.E1 (i) Vérifier que $SL_2(\mathbf{C})$ possède un unique élément d'ordre 2 ; il en est a fortiori de même pour $\mathcal{SU}(2)$.

[Indication : contempler l'égalité $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.]

Quels sont les corps $\mathbf{K}$ tels que le même énoncé vaille pour $SL_2(\mathbf{K})$?

(ii) Montrer que $SL_2(\mathbf{C})$ ne contient aucun sous–groupe isomorphe à $SL_2(\mathbf{F}_2)$ ni à $SL_2(\mathbf{F}_4)$. [Indication : dans $SL_2(\mathbf{F}_2)$, la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est de carré 1 et non centrale. Rappel de l'exercice VIII.E5 : $SL_2(\mathbf{F}_2) \approx \mathrm{Sym}(3)$ et $SL_2(\mathbf{F}_4) \approx \mathrm{Alt}(5)$ sont des sous–groupes de $PSL_2(\mathbf{C})$.]

(iii) Il se trouve que $SL_2(\mathbf{F}_3)$ et $SL_2(\mathbf{F}_5)$ sont des sous–groupes de $SL_2(\mathbf{C})$, respectivement isomorphes à G_T^* et G_I^*.

En effet, soit $G = SG_T \approx \mathrm{Alt}(4)$. On peut montrer que, à isomorphisme près, il existe exactement deux groupes $\tilde{G}$ possédant un sous–groupe central d'ordre deux C_2 tel que $\tilde{G}/C_2 \approx G$, le produit direct $G \times C_2$ et un autre groupe $\tilde{G}_1$. Comme chacun de G_T^* et $SL_2(\mathbf{F}_3)$ est une extension centrale de SG_T^* possèdant un unique élément d'ordre deux, ces groupes sont isomorphes (à $\tilde{G}_1$ et donc entre eux). Un argument analogue pour $G = SG_I \approx \mathrm{Alt}(5)$ montre que $G_I^* \approx SL_2(\mathbf{F}_5)$.

On peut aussi alculer la table des caractères de $SL_2(\mathbf{F}_3)$, qui possède des représentations irréductibles complexes de degrés 1, 1, 1, 3, 2, 2, 2 (voir par exemple [JamLi–01, page 440]). Il résulte de l'examen de cette table que les trois représentations de degré 2 sont fidèles et que l'une d'entre elles, dont le caractère est à valeurs réelles, a son image dans $SL_2(\mathbf{C})$. J'imagine qu'un tel argument est aussi possible pour $SL_2(\mathbf{F}_5)$.

XIII.E2 Soit G un sous–groupe de $\mathcal{SO}(3)$ contenant une rotation d'angle π. Montrer qu'il n'existe pas de sous–groupe H de $\mathcal{SU}(2)$ tel que la restriction de Ψ à H fournisse un isomorphisme de H sur G.

[Indication : si $g \in \mathcal{SU}(2)$ est tel que $\Psi(g)$ soit un demi–tour, alors g est conjugué à la matrice $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ et par suite $g^3 = -g$.]

Il résulte de cet exercice et de la classification des sous–groupes finis de $\mathcal{SO}(3)$ que tout sous–groupe fini non cyclique de $\mathcal{SU}(2)$ est l'image inverse par Ψ^{-1} d'un sous–groupe fini de $\mathcal{SO}(3)$. On obtient du même coup la classification des sous–groupes finis de $SL_2(\mathbf{C})$, à conjugaison près (voir l'exercice II.E8).

XIII.E3 Observer que, dans G_T^*, les éléments d'ordres 1, 2 et 4 constituent un sous–groupe isomorphe au groupe $Q = \Psi^{-1}(\mathbf{V})$ du lemme XIII.3 (c'est l'unique 2–Sylow de G_T^*). Déterminer le graphe de Bratteli de la paire (G_T^*, Q), et vérifier qu'il possède trois composantes connexes.

XIII.E4 Soit $k \geq 1$ un entier. Notons D_{2k}^* le sous–ensemble de $\mathcal{SU}(2)$ constitué des matrices

$$\begin{pmatrix} \omega & 0 \\ 0 & \overline{\omega} \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 0 & i\omega \\ i\overline{\omega} & 0 \end{pmatrix}$$

où ω parcourt les racines $(2k)$–ièmes de l'unité. Vérifier les assertions suivantes.

(i) D_{2k}^* est un sous–groupe d'ordre $4k$ de $\mathcal{SU}(2)$, engendré par les matrices

$$\begin{pmatrix} \exp(i\pi/k) & 0 \\ 0 & \exp(-i\pi/k) \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

(ii) Le groupe dérivé de D_{2k}^* est le groupe cyclique d'ordre k des matrices de la forme $\begin{pmatrix} \exp(2i\pi\ell/k) & 0 \\ 0 & \exp(-2i\pi\ell/k) \end{pmatrix}$, avec $\ell = 0, 1, \ldots, k-1$.

(iii) Le groupe D_{2k}^* possède, à conjugaison près, 4 représentations de degré 1 et $k-1$ représentations irréductibles de degré 2, ces dernières étant

$$\begin{pmatrix} \omega & 0 \\ 0 & \overline{\omega} \end{pmatrix} \longmapsto \begin{pmatrix} \omega^j & 0 \\ 0 & \overline{\omega}^j \end{pmatrix}$$
$$\begin{pmatrix} 0 & i\omega \\ i\overline{\omega} & 0 \end{pmatrix} \longmapsto \begin{pmatrix} 0 & i\omega^j \\ i\overline{\omega}^j & 0 \end{pmatrix},$$

pour $j = 1, \ldots, k-1$. En particulier, pour $j = 1$, on obtient la "représentation tautologique" π_2^{taut} de D_{2k}^*.

(iv) Si $k \geq 2$, le graphe de McKay $\mathrm{MK}(D_{2k}^*, \pi_2^{\mathrm{taut}})$ est constitué de deux segments longs de deux arêtes chacun, reliés par leurs milieux par un segment long de $k-2$ arêtes (deux sommets identifiés si $k = 2$). Il est connu sous le nom de "graphe de Dynkin de type $\tilde{D}_k$".

(v) Si $\Psi : \mathcal{SU}(2) \longrightarrow \mathcal{SO}(3)$ est l'homomorphisme décrit en XIII.1, alors $\Psi(D_{2k}^*)$ est un sous–groupe diédral d'ordre $2k$ de $\mathcal{SO}(3)$.

Lorsque $k = 2$, on retrouve la situation du lemme XIII.3, avec $D_4^* = Q$ et $\psi(D_4^*) = D_4 = \mathbf{V}$. Lorsque $k = 1$, le groupe D_2^* est un Viergruppe et $\Psi(D_2^*)$ un sous–groupe d'ordre 2 dans $\mathcal{SO}(3)$.

Les groupes D_{2k}^* sont parfois appelés les *groupes dicycliques* et, lorsque k est une puissance de 2, les *groupes de quaternions généralisés* (voir par exemple [Rotma–95], chapitre 11) ;

XIII.E5 Reprenons les notations du numéro XIII.1. Soient $g \in SL_2(\mathbf{C})$ et $A \in E$. La matrice gAg^* est encore hermitienne, mais n'est en général pas à trace nulle. Considérons l'espace F, isomorphe à $\mathbf{R}^4$, de toutes les matrices hermitiennes deux–fois–deux, c'est–à–dire de la forme $\begin{pmatrix} t+x & y+iz \\ y-iz & t-x \end{pmatrix}$, avec $t, x, y, z \in \mathbf{R}$. On le munit de la forme quadratique

$$q \, : \, B = \begin{pmatrix} t+x & y+iz \\ y-iz & t-x \end{pmatrix} \longmapsto \det(B) = t^2 - x^2 - y^2 - z^2$$

de signature $(1,3)$. On identifie $\mathbf{R}$ au sous–espace de F d'équation $x = y = z = 0$, de sorte que $F = \mathbf{R} \oplus E$.

Pour $g \in SL_2(\mathbf{C})$, la transformation $\tilde{\Psi}(g)$ de F définie par $\tilde{\Psi}(g)B = gBg^*$ préserve la forme quadratique q. Nous avons donc un homomorphisme $\tilde{\Psi}$ de $SL_2(\mathbf{C})$ vers le groupe orthogonal $\mathcal{O}(q)$ de la forme quadratique q. Cet homomorphisme passe au quotient en un homomorphisme de $PSL_2(\mathbf{C}) = SL_2(\mathbf{C})/\{\pm I_2\}$ vers la composante connexe $\mathcal{SO}^+(q) = \mathcal{SO}^+(1,3)$ de $\mathcal{O}(q)$.

On peut montrer que ce dernier homomorphisme est un isomorphisme du groupe de Lie réel sous-jacent à $PSL_2(\mathbf{C})$ sur $\mathcal{SO}^+(1,3)$.

La restriction de $\tilde{\Psi}$ au sous–groupe $\mathcal{SU}(2)$ de $SL_2(\mathbf{C})$ fournit un homomorphisme surjectif de noyau $\{\pm I_2\}$ et d'image le sous–groupe de $\mathcal{SO}^+(1,3)$ des transformations préservant la décomposition $F = \mathbf{R} \oplus E$ et égales à l'identité sur $\mathbf{R}$, sous–groupe qui s'identifie à $\mathcal{SO}(3)$. En d'autres termes, la restriction de $\tilde{\Psi}$ à $\mathcal{SU}(2)$ est l'homomoprhisme Ψ du numéro XIII.1.

Ce qui précède est une partie de ce qu'on trouve aux exercices du § 3 dans Bourbaki, *Groupes et algèbres de Lie*, chapitre III (Hermann 1972).

XIV. Le théorème de Dirichlet sur les nombres premiers dans les progressions arithmétiques

C'est en 1837 que Dirichlet a montré le théorème célèbre auquel est consacré ce chapitre. Aujourd'hui, la théorie des représentations des groupes finis abéliens apparaît comme l'un des ingrédients importants de sa très élégante démonstration. Dans les toutes dernières années du XIXe siècle, lors de la création de la théorie des représentations des groupes finis, les idées de Dirichlet furent pour Frobenius une source importante d'inspiration.

Pour la matière de ce chapitre, nous recommandons [Chand–68] et [Serre–70], ainsi que [Körne–88, chapitres 105 à 109].

XIV.a. Euclide, Euler, Riemann, Dirichlet

L'ensemble $\mathbf{P}$ des nombres premiers est infini ; les *Éléments* d'Euclide (Livre 9) en contiennent une démonstration. Euler a montré un résultat plus fort : la série $\sum_{p\in\mathbf{P}} \frac{1}{p}$ et le produit infini $\prod_{p\in\mathbf{P}} \left(1-\frac{1}{p}\right)^{-1}$ divergent.

La démonstration d'Euler est un bon prétexte pour introduire la *fonction zêta de Riemann* ζ, définie dans le demi–plan complexe $\{s \in \mathbf{C} \mid \mathrm{Re}(s) > 1\}$ par

$$\zeta(s) \;=\; \sum_{n=1}^{\infty} n^{-s}.$$

La série ci–dessus et le produit infinit de la proposition suivante convergent absolument et uniformément dans tout compact de ce demi–plan.

XIV.1. Identité d'Euler. *L'égalité*

$$\sum_{n=1}^{\infty} n^{-s} \;=\; \prod_{p\in\mathbf{P}} \frac{1}{1-p^{-s}}$$

vaut pour tout nombre complexe s tel que $\mathrm{Re}(s) > 1$.

Démonstration. Voir la proposition XIV.3. □

La fonction ζ est holomorphe dans le plan épointé $\mathbf{C} \setminus \{1\}$. Pour tout ceci, voir le cours d'analyse II ou, à défaut, les débuts des chapitres VII et X du livre de Chandrasekharan [Chand–68].

En 1837, Dirichlet a établi le résultat suivant.

XIV.2. Théorème. *Soient a, m deux entiers tels que $m > 0$ et $(a, m) = 1$. L'ensemble $\mathbf{P}_a$ des nombres premiers contenus dans la progression arithmétique $(a + mk)_{k=1,2,3,...}$ est infini.*

L'objet du présent chapitre est d'évoquer une démonstration de ce théorème, en ne détaillant que quelques pas où la théorie des caractères est utilisée. Dans toute la suite du chapitre, m désigne un entier strictement positif et a un entier positif premier à m.

Mertens (1874) a précisé le résultat d'Euler en montrant qu'il existe une constante C telle que

$$\sum_{p\in\mathbf{P}, p\leq x} \frac{1}{p} \;=\; \log\log x + C + O\left(\frac{1}{\log x}\right).$$

Rappelons la notation de Landau : $\alpha(x) = O(\beta(x))$ lorsque $x \to \infty$ s'il existe des constantes C_1, C_2 telles que $|\alpha(x)| \leq C_1\beta(x)$ pour tout $x \geq C_2$. De même, dans la situation du théorème XIV.2, on sait que

$$\sum_{p\in\mathbf{P}_a, p\leq x} \frac{1}{p} \;=\; \frac{1}{\varphi(m)} \log\log x + O(1).$$

Notons que le théorème de Dirichlet redonne le résultat d'Euclide pour $m = 1$, et l'infinitude de l'ensemble des nombres premiers impairs pour $m = 2$ (!). On pourrait donc tout aussi bien supposer $m \geq 3$. Rappelons aussi qu'il existe des preuves élémentaires du théorème de Dirichlet pour le cas particulier $m = 4$ (voir le cours d'Algèbre I).

Le groupe qui intervient est le groupe multiplicatif $(\mathbf{Z}/m\mathbf{Z})^*$ des éléments inversibles dans l'anneau $\mathbf{Z}/m\mathbf{Z}$ des entiers modulo m. C'est un groupe abélien d'ordre $\varphi(m)$; nous le notons $G(m)$. Il est parfois cyclique : c'est par exemple le cas si n est premier (parce que tout sous–groupe multiplicatif du groupe des éléments inversibles d'un corps est cyclique) ; il est parfois non cyclique, par exemple si $m = m_1 m_2$ avec m_1, m_2 au moins 3 et premiers entre eux (c'est une conséquence du théorème chinois).

Rappelons que la *fonction d'Euler* φ a les propriétés suivantes :

$\varphi(n) = 1, 1, 2, 2, 4, 2, 6, 4, \dots$ si $n = 1, 2, 3, 4, 5, 6, 7, 8, \dots$;
$\varphi(p^b) = p^p - p^{b-1}$ pour p premier et $b \geq 1$;
$\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$ pour $n_1, n_2 \geq 1$ tels que $(n_1, n_2) = 1$;
$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ pour tout $n \geq 1$.

Revenons à l'identité d'Euler. Convenons d'abord qu'une fonction $f : \mathbf{N}_{>0} \longrightarrow \mathbf{C}$ est *multiplicative* si f n'est pas identiquement nulle et si

$$f(n_1 n_2) \; = \; f(n_1) f(n_2) \tag{*}$$

pour toute paire n_1, n_2 d'entiers premiers entre eux. Notons qu'il résulte de la définition que $f(1) = 1$. La fonction f est *complètement multiplicative* si l'identité (*) est satisfaite pour *toute* paire n_1, n_2 d'entiers strictement positifs.

Par exemple, la fonction φ d'Euler est multiplicative. Les caractères modulo m introduits plus bas sont des fonctions complètement multiplicatives.

XIV.3. Proposition. *Soit $f : \mathbf{N}_{>0} \longrightarrow \mathbf{C}$ une fonction multiplicative telle que la série $\sum_{n=1}^{\infty} f(n)$ soit absolument convergente. Alors*

$$\sum_{n=1}^{\infty} f(n) \; = \; \prod_{p \in P} \left(1 + f(p) + f(p^2) + \cdots \right),$$

le produit du membre de droite étant absolument convergent. Si de plus la fonction f est complètement multiplicative, alors

$$\sum_{n=1}^{\infty} f(n) \; = \; \prod_{p \in P} \frac{1}{1 - f(p)}.$$

Esquisse de démonstration. Pour les justifications de convergence, voir la preuve détaillée du § VII.4 de [Chand–68] ou le § VI.3 de [Serre–70].

Soit $x \in \mathbf{R}_+$. Notons $\sum_x' f(n)$ la somme des $f(n)$ sur les entiers dont tous les facteurs premiers satisfont l'inégalité $p \leq x$, et $\sum_x'' f(n)$ la somme des $f(n)$ sur les autres entiers ; posons $S = \sum_{n=1}^{\infty} f(n)$. Alors

$$\sum_x{}' f(n) \; = \; \prod_{p \in \mathbf{P}, p \leq x} \left(1 + f(p) + f(p^2) + \cdots \right).$$

En effet, le produit de droite est un produit fini de séries absolument convergentes ; on peut donc effectuer le produit terme à terme, et on trouve le membre de gauche en réarrangant la somme. Par suite,

$$\left| \prod_{p\in\mathbf{P}, p\le x} \big(1 + f(p) + f(p^2) + \cdots\big) \;-\; S \right| \;\le\; \sum_{x}{}'' |f(n)| \;\le\; \sum_{n>x} |f(n)|.$$

Or $\lim_{x\to\infty} \sum_{n>x} |f(n)| = 0$ par l'hypothèse de convergence absolue. La première identité de la proposition en résulte.

Lorsque la fonction f est complètement multiplicative, on montre d'abord que la série $\sum_{b=1}^{\infty} |f(p^b)|$ est absolument convergente, de sorte que[33] $|f(p)| < 1$ pour tout nombre premier p. Par suite

$$\begin{aligned}\sum_{n=1}^{\infty} f(n) \;&=\; \prod_{p\in P} \big(1 + f(p) + f(p^2) + \cdots\big) \;=\; \prod_{p\in P} \big(1 + f(p) + f(p)^2 + \cdots\big)\\ &=\; \prod_{p\in P} \frac{1}{1 - f(p)},\end{aligned}$$

ce qui achève la démonstration. □

Le cas de la fonction f définie par $f(s) = n^{-s}$, avec $s \in \mathbf{C}$ et $\mathrm{Re}(s) > 1$, fournit l'identité d'Euler XIV.1.

XIV.b. Caractères modulo m et relations d'orthogonalité

Le groupe $G(m)$ possède $\varphi(m)$ caractères (comme tout groupe abélien du même ordre) ; nous notons comme d'habitude χ_1 le caractère unité. A tout caractère $\chi : G(m) \longrightarrow \mathbf{C}^*$, on associe le *caractère modulo m*, qui est l'application $\chi_{\mathbf{Z}} : \mathbf{Z} \longrightarrow \mathbf{C}^*$ définie par

$$\begin{aligned} \chi_{\mathbf{Z}}(a) \;&=\; \chi([a]) &&\text{si}\quad (a,m) = 1 \quad\text{et si}\quad [a] \in G(m) \quad\text{est la classe de } a\\ \chi_{\mathbf{Z}}(a) \;&=\; 0 &&\text{dans les autres cas.}\end{aligned}$$

Ceci posé, on s'empresse d'écrire (abusivement !) χ au lieu de $\chi_{\mathbf{Z}}$. En voici quelques propriétés :

$$\begin{aligned} \chi(n) \;&=\; \chi(n') \qquad \text{si} \quad n \equiv n' \pmod{m} \;;\\ \chi(nn') \;&=\; \chi(n)\chi(n') \qquad \text{pour tout} \quad n, n' \in \mathbf{Z} \;;\\ \chi(n) \;&\neq\; 0 \qquad \text{si} \quad (m,n) = 1 \;;\\ \chi(n) \;&=\; 0 \qquad \text{si} \quad (m,n) > 1.\end{aligned}$$

En particulier, le caractère principal modulo m est l'application $\chi_1 : \mathbf{Z} \longrightarrow \mathbf{C}^*$ définie par $\chi_1(n) = 1$ si $(m,n) = 1$ et $\chi_1(n) = 0$ si $(m,n) > 1$ ou si $n = 0$.

[33] Ce point est d'ailleurs évident dans les cas qui apparaissent ici : $f(n) = n^{-s}$ et plus généralement $f(n) = \chi(n)n^{-s}$.

XIV.4. Proposition. *(i) soit χ un caractère modulo m. Alors*

$$\sum_{n \pmod m} \chi(n) \ = \ \begin{cases} \varphi(m) & si \quad \chi = \chi_1 \\ 0 & si \quad \chi \neq \chi_1. \end{cases}$$

La notation indique que la somme est prise sur un système de représentants dans $\mathbf{Z}$ *du groupe additif* $\mathbf{Z}/m\mathbf{Z}$ *des classes d'entiers modulo m.*

(ii) Soit $n \in \mathbf{Z}$. Alors

$$\sum_{\chi} \chi(n) \ = \ \begin{cases} \varphi(m) & si \quad n \equiv 1 \pmod m \\ 0 & sinon. \end{cases}$$

Démonstration. Ce sont des cas particuliers des théorèmes VII.1 et IX.8.

Il existe des démonstrations plus rapides des relations d'orthogonalité dans le cas des groupes finis *abéliens*, seul cas utilisé ici : voir les paragraphes X.2 et X.3 de [Chand–68] ou le § VI.1 de [Serre–70]. □

XIV.5. Exemple : $m = 4$. Les éléments de $G(4)$ sont représentés par les nombres 1 et 3, premiers à 4. Ce groupe d'ordre 2 possède deux caractères χ_1, χ_2 définis par

$$\chi_1(n) \ = \ \begin{cases} 1 & \text{si } n \text{ est impair} \\ 0 & \text{si } n \text{ est pair} \end{cases} \qquad \text{(le caractère principal)}$$

et

$$\chi_2(n) \ = \ \begin{cases} 1 & \text{si} \quad n \equiv 1 \pmod 4 \\ -1 & \text{si} \quad n \equiv 3 \pmod 4 \\ 0 & \text{si} \quad n \quad \text{est pair} \end{cases}$$

(c'est le caractère noté $(-1)^\epsilon$ à l'exemple I.8). Les relations d'orthogonalité s'écrivent

$$\begin{aligned} \chi_1(1) + \chi_1(3) \ &= \ 2 \qquad & \chi_1(1) + \chi_2(1) \ &= \ 2 \\ \chi_2(1) + \chi_2(3) \ &= \ 0 \qquad & \chi_1(3) + \chi_2(3) \ &= \ 0. \end{aligned}$$

Exercice. Ecrire un tableau analogue à celui de l'exemple précédent pour les cas $m = 3$ et $m = 5$.

XIV.c. Séries et fonctions L de Dirichlet

Une *série de Dirichlet* est (ici) une série de la forme

$$\sum_{n=1}^{\infty} a_n n^{-s}$$

où s est un nombre complexe et où $(a_n)_{n \geq 1}$ est une suite de nombres complexes. On écrit selon l'usage

$$s \ = \ \sigma + it$$

avec $\sigma, t \in \mathbf{R}$. Voici quelques–uns des résultats fondamentaux concernant ces séries.

XIV.6. Résultats sur les séries de Dirichlet. *Soit* $\sum_{n=1}^{\infty} a_n n^{-s}$ *comme ci–dessus.*

(i) Il existe une abscisse de convergence $\sigma_0 \in \mathbf{R} \cup \{-\infty, \infty\}$ *possédant les propriétés suivantes. La série converge en tout point* $s \in \mathbf{C}$ *tel que* $\mathrm{Re}(s) > \sigma_0$ *et diverge en tout point* $s \in \mathbf{C}$ *tel que* $\mathrm{Re}(s) < \sigma_0$*. La série converge uniformément dans tout compact du* demi–plan de convergence $\{s \in \mathbf{C} \mid \mathrm{Re}(s) > \sigma_0\}$ *et y définit une fonction holomorphe, dont les dérivées sont égales aux séries de Dirichlet obtenues en dérivant* $\sum_{n=1}^{\infty} a_n n^{-s}$ *terme à terme.*

(ii) Soit $\overline{\sigma}$ l'abscisse de convergence absolue *de la série* $\sum_{n=1}^{\infty} a_n n^{-s}$*, qui est par définition l'abscisse de convergence de la série* $\sum_{n=1}^{\infty} |a_n| n^{-s}$*. Alors*

$$\sigma_0 \;\leq\; \overline{\sigma} \;\leq\; \sigma_0 + 1.$$

La bande de convergence conditionnelle *et la bande* $\{s \in \mathbf{C} \mid \sigma_0 < \mathrm{Re}(s) < \sigma\}$.

(iii) Si $a_n \in \mathbf{R}_+$ *pour tout* $n \geq 1$ *et si* $\sigma_0 < \infty$*, alors le point* σ_0 *est une singularité de la fonction* f *définie en (i).*

Nous renvoyons à [Chand–68] pour la démonstration. L'assertion (iii) est un théorème de Landau.

Il est instructif de comparer ces résultats avec leurs analogues concernant les séries de puissances, ou "séries de Taylor" (pour lesquelles le "rayon de convergence absolue" coïncide toujours avec le rayon de convergence usuel). Pour une discussion de "séries de Dirichlet" plus générales, dont les séries introduites ici et les séries de puissances sont deux cas particuliers, voir le no VI.2.2 de [Serre–70].

XIV.7. Exemple. La série $\sum_{n=1}^{\infty} (-1)^{n+1} n^{-s}$ converge pour tout nombre réel $\sigma > 0$, puisque c'est alors une série alternée dont les termes décroissent en valeur absolue ; elle diverge pour tout nombre réel $\sigma < 0$. Par suite $\sigma_0 = 0$. Par ailleurs, la série $\sum_{n=1}^{\infty} n^{-s}$ converge si et seulement si $\sigma > 1$, de sorte que $\overline{\sigma} = 1$.

Notons que

$$\begin{aligned}\sum_{n=1}^{\infty} (-1)^{n+1} n^{-s} \;&=\; \left(\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots\right) \;-\; 2\left(\frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \cdots\right) \\ &=\; \zeta(s) \;-\; 2^{1-s}\zeta(s)\end{aligned}$$

pour $\sigma > 1$. Comme $\sum_{n=1}^{\infty} (-1)^{n+1} n^{-s}$ et $(1 - 2^{1-s})\zeta(s)$ définissent des fonctions holomorphes dans le demi–plan $\sigma > 0$ (noter que le pôle simple de ζ en $s = 1$ est régularisé par le zéro de $1 - 2^{1-2s}$), la relation

$$\sum_{n=1}^{\infty} (-1)^{n+1} n^{-s} \;=\; \left(1 - 2^{1-2s}\right) \zeta(s)$$

est vraie en tout point du demi–plan $\sigma > 0$.

XIV.8. Définition A tout caractère χ du groupe $G(m)$ correspond la *série de Dirichlet*

(*) $$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Il y a $\varphi(m)$ séries de ce type. Chacune d'entre elles converge pour $\sigma > 1$, car $|\chi(n)| \leq 1$ pour tout $n \geq 1$, et définit donc (au moins dans[34] le demi–plan $\sigma > 1$) une *fonction L de Dirichlet*

$$L(s,\chi) \;=\; \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Comme les caractères modulo m sont des fonctions arithmétiques complètement multiplicatives, il résulte de la proposition XIV.3 que

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \;=\; \prod_{p \in P} \frac{1}{1-\chi(p)p^{-s}}$$

pour tout nombre complexe s tel que $\mathrm{Re}(s) > 1$.

Lorsque $m = 1$, la fonction $L(s,\chi_1)$ n'est autre que la fonction $\zeta(s)$ de Riemann. Lorsque $m = 2$, c'est un exercice facile de vérifier que $L(s,\chi_1) = (1-2^{-s})\zeta(s)$.

Stratégie de preuve du théorème de Dirichlet. Rappelons que $\mathbf{P}_a$ désigne l'ensemble des nombres premiers de la progressions arithmétique $(a+mk)_{k\geq 1}$; notons θ_a sa fonction caractéristique. Il s'agit de montrer que la série $\sum_{p\in\mathbf{P}_a} \frac{1}{p}$ ou que le produit infini $\prod_{p\in\mathbf{P}_a}\left(1-\frac{1}{p}\right)^{-1}$ diverge

L'idée d'introduire naïvement une fonction $\sum_{p\in\mathbf{P}_a} \frac{\theta_a(n)}{n^s}$ ne suffit pas, car cette fonction d'admet pas de développement en produit. On peut d'abord noter que θ_a est une combinaison linéaire de caractères modulo m (voir le numéro IX.11), et que par suite $\sum_{p\in\mathbf{P}_a} \frac{\theta_a(n)}{n^s}$ est une combinaison linéaire de fonctions $L(s,\chi)$, dont on vient de voir qu'elles admettent des décompositions en produit. Mais il reste des difficultés ... Une nouvelle idée conduit à montrer que, pour $b \in \mathbf{N}$ bien choisi (voir ci-dessous le § XIV.d), nous avons

$$\sum_{p\in\mathbf{P}_a} \frac{1}{p^s} \;\text{''} \sim \text{''}\; \sum_{\chi\in\widehat{G(m)}} \chi(b)\log L(s,\chi)$$

où $\widehat{G(m)}$ désigne le groupe des caractères modulo m et où " $\sim$ " signifie ici que la différence des deux termes est une fonction holomorphe dans un voisinage de $s = 1$ (en fait dans le demi plan $\mathrm{Re}(s) > \frac{1}{2}$).

Il reste à montrer que, pour $\chi \neq \chi_1$, la fonctio n $\log L(s,\chi)$ est holomorphe au voisinage de $s = 1$ et que, pour s tendant vers 1 par valeurs réelles supérieures, nous avons $\lim_{s\to 1}\log L(s,\chi) = \infty$.

Nous allons donner quelques indications de plus en continuant à suivre [Chand–68] et [Serre–70].

[34]A mettre au clair : y a–t–il des $L(\chi,s)$ entières ? Réfléchir à la dichotomie primitif–non primitif pour χ.

XIV.9. Proposition. *(i) Si χ n'est pas le caractère principal, les abscisses de $L(s,\chi)$ sont respectivement $\sigma_0 = 0$ et $\overline{\sigma} = 1$. En particulier, $L(1,\chi)$ est fini.*

(ii) Pour le caractère principal, les abscisses de $L(\chi_1, s)$ sont $\sigma_0 = \overline{\sigma} = 1$. De plus, $L(s,\chi_1)$ possède un prolongement méromorphe dans $\{s \in \mathbf{C} \mid \sigma > 0\}$ avec un seul pôle, en $s = 1$; ce pôle est simple de résidu $\prod_{p\in\mathbf{P},p|m}\left(1-\frac{1}{p}\right) = \frac{\varphi(m)}{m}$.

(iii) Si $\chi \neq \chi_1$, alors $L(1,\chi) \neq 0$.

Démonstration. (i) Supposons $\chi \neq \chi_1$. Soit x un nombre réel positif. Notons $[x] = qm + r$ le résultat de la division euclidienne de la partie entière de x par q, avec $0 \leq r \leq m-1$. Nous avons

$$\begin{aligned}\sum_{n\leq x}\chi(n) &= \sum_{n=1}^{m}\chi(n) + \sum_{n=m+1}^{2m}\chi(n) + \cdots + \sum_{n=(q-1)m+1}^{qm}\chi(n) + \sum_{n=qm+1}^{qm+r}\chi(n)\\ &= \sum_{n=qm+1}^{qm+r}\chi(n)\end{aligned}$$

par la relation d'orthogonalité, de sorte que

$$\left|\sum_{n\leq x}\chi(n)\right| \leq \sum_{n=qm+1}^{qm+r}|\chi(n)| = r < m.$$

Pour $\sigma \in \mathbf{R}$, $\sigma > 0$, la suite $(n^{-\sigma})_{n\geq 1}$ est décroissante et tend vers 0 ; il en résulte que la série $\sum_{n=1}^{\infty}\chi(n)n^{-\sigma}$ converge. Pour $\sigma \in \mathbf{R}$, $\sigma < 0$, la série $\sum_{n=1}^{\infty}\chi(n)n^{-\sigma}$ diverge. L'abscisse de convergence de $L(s,\chi)$ est donc $\sigma_0 = 0$. L'abscisse de convergence absolue de $L(s,\chi)$, qui est aussi celle de la fonction ζ, est $\overline{\sigma} = 1$.

Notons que $L(s,\chi)$ est une fonction holomorphe dans le demi–plan $\{s \in \mathbf{C} \mid \mathrm{Re}(s) > 0\}$, par le théorème XIV.6.i.

(ii) Lorsque $\chi = \chi_1$, nous avons

$$\begin{aligned}L(s,\chi) &= \prod_{p\in\mathbf{P},p\nmid m}\frac{1}{1-p^{-s}} = \prod_{p}\frac{1}{1-p^{-s}}\prod_{p\in\mathbf{P},p|m}\left(1-p^{-s}\right)\\ &= \zeta(s)\prod_{p\in\mathbf{P},p|m}\left(1-p^{-s}\right).\end{aligned}$$

Des propriétés de ζ, on déduit que la fonction $L(s,\chi_1)$ est méromorphe dans le demi–plan $\mathrm{Re}(s) > 0$. Elle y possède un unique pôle, en $s = 1$, qui est simple et dont le résidu est le produit du résidu de ζ en 1 par la valeur en 1 de $\prod_{p\in\mathbf{P},p|m}(1-p^{-s})$.

(iii) Vu les assertions (i) et (ii), il convient de montrer que le produit des fonctions $L(s,\chi)$ n'est pas une fonction régulière en $s = 1$ (produit sur *tous* les caractères modulo m, y compris le caractère principal).

Pour $\mathrm{Re}(s) > 1$, nous avons $|\chi(p)p^{-s}| \leq |p^{-s}| < 1$, de sorte que nous pouvons *définir*

$$\log\left(1-\frac{\chi(p)}{p^s}\right)^{-1} = \sum_{k=1}^{\infty}\frac{\chi(p^k)}{kp^{ks}}.$$

La fonction $\log L(s,\chi)$ est univoquement définie dans le demi–plan $\mathrm{Re}(s) > 1$ par

$$(\sharp) \qquad \log L(s,\chi) \;=\; \sum_{p,k} \frac{\chi(p^k)}{kp^{ks}},$$

la double somme du membre de droite portant sur tous les nombres premiers et sur tous les entiers de 1 à l'infini ; cette double somme est absolument convergente en tout point du demi–plan $\mathrm{Re}(s) > 1$, et nous avons

$$e^{\log L(s,\chi)} \;=\; L(s,\chi),$$

comme il se doit.

La suite de la preuve utilise les relations d'orthogonalité XIV.4.ii, qui interviennent dans l'étude de $\sum_\chi \log L(s,\chi)$, des manipulations astucieuses de séries, et le résultat d'Euler selon lequel la série $\sum_{p\in\mathbf{P}} \frac{1}{p}$ diverge. Pour les détails, nous renvoyons aux pages 119–120 de [Chand–68] ou au no VI.3.4 de [Serre–70]. □

Voici une illustration de l'affirmation (iii). Soit χ_2 le caractère modulo 4 non principal, comme à l'exemple XIV.5. Alors

$$L(\chi_2,1) \;=\; 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - + \cdots \;=\; \frac{\pi}{4}.$$

????? Exercice (vérifier l'énoncé !!!!!) Soient m, m' des entiers tels que $1 \le m' < m$ et $m'|m$; soit χ' un caractère modulo m'. Notons χ le caractère modulo m défini par

$$\chi(n) \;=\; \begin{cases} \chi'(n \pmod{m'}) & \text{si} \quad (n,m) = 1 \\ \quad 0 & \text{sinon.} \end{cases}$$

Montrer que

$$L(\chi,s) \;=\; L(\chi',s) \prod_{p|\frac{m}{m'}} \left(1 - \frac{\chi(p)}{p^s}\right).$$

Les caractères modulo m qui *ne sont pas* défini comme ci-dessus à partir d'un caractère d'un diviseur de m sont les *caractères primitifs* modulo m.

XIV.d. Fin de l'esquisse de démonstration du théorème de Dirichlet.

Soit χ un caractère modulo m. Considérons la série double

$$R(s,\chi) \;=\; \sum_{p\in\mathbf{P}} \sum_{k=2}^{\infty} \frac{\chi(p^k)}{kp^{ks}}$$

extraite de la série ($\sharp$) ci–dessus. Elle définit une fonction holomorphe dans le demi–plan $\mathrm{Re}(s) > \frac{1}{2}$, et

$$(\sharp\sharp) \qquad \log L(s,\chi) \;=\; \sum_{p\in\mathbf{P}} \chi(p)p^{-s} \;+\; R(s,\chi).$$

Soient a, m deux entiers tels que $m > 0$ et $(a, m) = 1$, comme dans le théorème de Dirichlet. Par le théorème de Bézout, il existe un entier $b \geq 1$ tel que $ab \equiv 1 \pmod{m}$. Il en résulte que, pour un nombre premier p, les congruences $p \equiv a \pmod{m}$ et $pb \equiv 1 \pmod{m}$ sont équivalentes. En multipliant ($\sharp\sharp$) par $\chi(b)$ et en sommant sur tous les caractères modulo m, nous obtenons

$$(\sharp\sharp\sharp) \qquad \sum_{\chi} \chi(b) \log L(s,\chi) \;=\; \sum_{p \in \mathbf{P}} \sum_{\chi} \chi(pb) p^{-s} \;+\; \sum_{\chi} \chi(b) R(s,\chi) \quad \text{lorsque} \quad \mathrm{Re}(s) > 1.$$

Le premier terme du membre de droite se simplifie grâce aux relations d'orthogonalité

$$\sum_{\chi} \chi(pb) \;=\; \begin{cases} \varphi(m) & \text{si} \quad pb \equiv 1 \pmod{m} \\ 0 & \text{sinon} \end{cases}$$

et le second terme définit une fonction

$$R''(s) \;=\; \sum_{\chi} \chi(b) R(s,\chi)$$

qui est régulière dans le demi–plan $\mathrm{Re}(s) > \frac{1}{2}$ (comme les fonctions $R(s,\chi)$). La relation ($\sharp\sharp\sharp$) s'écrit donc

$$\sum_{\chi} \chi(b) \log L(s,\chi) \;=\; \varphi(m) \sum_{p \in \mathbf{P}_a} p^{-s} \;+\; R''(s) \qquad \text{lorsque} \quad \mathrm{Re}(s) > 1.$$

Quand s tend vers 1 par valeurs réelles supérieures, nous avons vu que $L(s,\chi)$ tend vers une limite finie non nulle si $\chi \neq \chi_1$ et vers l'infini si $\chi = \chi_1$ (proposition XIV.9) ; on peut vérifier qu'il en est de même de $\log L(s,\chi)$. Nous avons également vu que $R''(s)$ est régulière au voisinage de $s = 1$ (en fait dans $\mathrm{Re}(s) > \frac{1}{2}$). Il en résulte que

$$\lim_{s \to 1} \sum_{p \in \mathbf{P}_a} p^{-s} \;=\; \infty \qquad \text{(limite par valeurs réelles supérieures),}$$

ou encore que

$$\sum_{p \in \mathbf{P}_a} \frac{1}{p} \;=\; \infty,$$

comme promis. □

XV. Projet – quelques compléments et applications

Le projet initial du cours voulait que le chapitre XIV s'insère dans un échantillon d'applications de la théorie des représentations des groupes finis. Voici quelques titres parmi de nombreux autres possibles.

XV.a. Groupes d'ordres $p^a q^b$

Le théorème célèbre suivant est dû à Burnside. Pour un groupe G, on définit la *suite dérivée* $(D^k(G))_{k\geq 0}$ par $D^0(G) = G$ et $D^k(G) = D(D^{k-1}(G))$ pour $k \geq 1$ (rappelons que $D(G)$ désigne le groupe des commutateurs de G). Un groupe G est *résoluble* s'il existe un entier k tel que $D`k(G) = \{1\}$.

XV.1. Théorème (Burnside). *Tout groupe fini d'ordre $p^a q^b$, avec p, q premiers et $a, b \geq 0$, est résoluble.*

La démonstration se trouve à de multiples endroits. Voir par exemple l'annexe A6 de [Serre–05] ou le chapitre 31 de [JamLi–01].

XV.b. Un théorème de Frobenius

Soient G un groupe fini et H un sous–groupe qui est *malnormal*, c'est–à–dire un sous–groupe propre tel que $H \cap gHg^{-1} = \{1\}$ pour tout $g \in G \setminus H$. L'intérêt de telles paires vient de ce que, pour l'action de G sur $X = G/H$, un élément G qui n'agit pas comme l'identité sur X possède au plus un point fixe. Notons N le *noyau de Frobenius*, c'est–à–dire la réunion de l'identité et des éléments agissant sans point fixe sur X, ou encore $N = \{1\} \cup \left\{ G \setminus \bigcup_{g\in G} gHg^{-1} \right\}$.

XV.2. Théorème (Frobenius). *Soient G un groupe fini, H un sous–groupe malnormal de G et N comme ci–dessus. ALors N est un sous–groupe normal. De plus $N \cap H = \{1\}$, de sorte que G s'écrit comme produit semi–direct $H \ltimes N$.*

Pour la démonstration, voir par exemple le chapitre 6 et l'appendice A7 de [Serre–05]. La difficulté consiste à montrer que N est un sous–groupe de G ; il est alors évident que c'est un sous–groupe normal.

XV.c. Démonstration de Beno Eckmann de résultats de Hurwitz et Radon

Nous allons exposer le schéma de la preuve de [Eckma–43] d'un résultat plus ancien. D'autres articles de la même lignée sont [LamSm–89] et [Eckma–89].

XV.3. Théorème (Hurwitz–Radon, 1923). *Soit $\mathbf{K}$ l'un des corps $\mathbf{R}$, $\mathbf{C}$. Soit n un entier, $n \geq 1$; posons $n = u2^{4\alpha+\beta}$, avec u impair, $\alpha \geq 0$ et $\beta \in \{0, 1, 2, 3\}$. Il existe une application bilinéaire $\mu : \mathbf{K}^p \times \mathbf{K}^n \longrightarrow \mathbf{K}^n$ telle que*

$$(1) \qquad \sum_{k=1}^{n} \mu_k(x,y)^2 = \Big(\sum_{i=1}^{p} x_i^2\Big)\Big(\sum_{j=1}^{n} y_j^2\Big) \qquad \textit{pour tout} \quad (x,y) \in \mathbf{K}^p \times \mathbf{K}^n$$

si et seulement si $p \leq 8\alpha + 2^\beta$.

Désormais, nous considérons le cas où $\mathbf{K} = \mathbf{R}$. Le cas complexe peut s'en déduire facilement. On écrit donc $\|x\|^2$, $\|y\|^2$ et $\|\mu(x,y)\|^2$ au lieu de $\sum_{i=1}^{p} x_i^2$, $\sum_{j=1}^{n} y_j^2$ et $\sum_{k=1}^{n} \mu_k(x,y)^2$.

En particularisant à $p = n$, on retrouve un résultat plus ancien concernant l'existence de certaines "algèbres" (dans un sens plus général que celui de X.9, car on ne demande pas ici que la multiplication soit associative).

XV.4. Théorème (Hurwitz, 1898). *Pour qu'il existe une "multiplication", c'est–à–dire une application bilinéaire* $\mu : \mathbf{R}^n \times \mathbf{R}^n \longrightarrow \mathbf{R}^n$ *telle que* $\|\mu(x,y)\|^2 = \|x\|^2 \|y\|^2$ *pour tous* $x, y \in \mathbf{R}^n$*, il faut et il suffit que* $n \in \{1, 2, 4, 8\}$.

La suffisance résulte de l'existence de multiplications définies sur $\mathbf{R}$ ($n = 1$), le corps des complexes ($n = 2$), l'algèbre des quaternions de Hamilton ($n = 4$) et l'algèbre dite des octaves de Cayley ($n = 8$).

Revenons à la démonstration du théorème XV.3 (cas $\mathbf{K} = \mathbf{R}$), et supposons qu'il existe une "multiplication" $\mu : \mathbf{R}^p \times \mathbf{R}^n \longrightarrow \mathbf{R}^n$ avec les propriétés indiquées. Pour tout $x \in \mathbf{R}^p$ de norme 1, l'endomorphisme linéaire $A_y : y \longmapsto \mu(x,y)$ de $\mathbf{R}^n$ est orthogonal

Notons $(e_1, \ldots, e_p)$ la base canonique de $\mathbf{R}^p$ et de même $(e_1, \ldots, e_n)$ celle de $\mathbf{R}^n$. Pour $i \in \{1, \ldots, p\}$, écrivons A_i au lieu de A_{e_i} ; c'est une matrice de $\mathcal{O}(n)$. La condition (1) se traduit en termes des A_i par

$$(2) \qquad \begin{aligned} &\text{la matrice } A_i \text{ est orthogonale pour tout } i \in \{1, \ldots, p\} \\ &{}^tA_iA_{i'} + {}^tA_{i'}A_i = 0 \quad \text{pour tous} \quad i, i' \in \{1, \ldots, p\} \quad \text{avec} \quad i \neq i' \end{aligned}$$

(où ${}^tA$ désigne la matrice transposée d'une matrice A).

Quitte à composer μ avec l'application orthogonale A_p^{-1}, nous pouvons supposer que $\mu(e_p, y) = y$ pour tout $y \in \mathbf{R}^n$, c'est–à–dire que $A_p = I$ (l'identité). Vu la condition (2), nous avons ${}^tA_i + A_i = 0$ pour tout $i \in \{1, \ldots, p-1\}$, et (2) est donc équivalent à

$$(3) \qquad \begin{aligned} &A_i^2 = -I \quad \text{pour} \quad i = 1, \ldots, p-1, \\ &A_iA_{i'} + A_{i'}A_i = 0 \quad \text{pour tous} \quad i, i' \in \{1, \ldots, p-1\} \quad \text{avec} \quad i \neq i'. \end{aligned}$$

Vu (3), Eckmann définit un groupe $G_{(p,0)}$ engendré par p générateurs $\epsilon, a_1, \ldots, a_{p-1}$ soumis aux relations

$$(4) \qquad \begin{aligned} &\epsilon^2 = 1, \quad a_i^2 = \epsilon \quad (1 \leq i \leq p-1) \\ &a_ia_{i'} = \epsilon a_{i'}a_i \quad (1 \leq i, i' \leq p-1, i \neq i'). \end{aligned}$$

Les familles $A_1, \ldots, A_{p-1}$ de matrices orthogonales satisfaisant (3) sont en bijection avec les représentations $\pi : G_{(p,0)} \longrightarrow \mathcal{O}(n)$ telles que $\pi(\epsilon) = -I$.

On se convainc facilement que $G_{(1,0)}$ est le groupe d'ordre deux, $G_{(2,0)}$ le groupe cyclique d'ordre 4 et $G_{(3,0)}$ le groupe Q des quaternions.

Revenons au cas général. Tout élément de $G_{(p,0)}$ s'écrit soit sous la forme $a_{i_1}a_{i_2}\cdots a_{i_k}$ soit sous la forme $\epsilon a_{i_1}a_{i_2}\cdots a_{i_k}$, avec $k \geq 0$ et $1 \leq i_1 < i_2 < \cdots < i_k \leq p-1$. Par suite $G_{(p,0)}$ est un groupe fini d'ordre au plus 2^p. Un calcul presqu'immédiat montre que $D(G_{(p,0)}) = \{1, \epsilon\}$. Il en résulte que l'abélianisé de $G_{(p,0)}$ est engendré par $p-1$ éléments d'ordre 2 qui commutent deux à deux, et par suite que $G_{(p,0)}/D(G_{(p,0)}) \approx (\mathbf{Z}/2\mathbf{Z})^{p-1}$; en particulier, $|G| \geq 2^{p-1}$. Voici une méthode pour montrer que $|G| = 2^p$, c'est–à–dire que $G_{(p,0)}$ n'est pas abélien dès que $p \geq 3$.

Considérons d'abord, pour $j = 1, 2$, un groupe G_j donné avec un élément $\epsilon_j \in G_j$ central d'ordre deux. Définissons le *produit modifié* des paires (G_1, ϵ_1) et (G_2, ϵ_2) comme le quotient $G = G_1 \times_2 G_2$ du produit direct $G_1 \times G_2$ par le sous–groupe $\{(1,1), (\epsilon_1, \epsilon_2)\}$, muni de la classe ϵ de la paire $(\epsilon_1, 1)$; notons que ϵ est bien un élément central d'ordre deux dans G. Lorsque G_1 et G_2 sont finis, G est fini d'ordre $\frac{1}{2}|G_1|\,|G_2|$. Par exemple, si $G_0 = \mathbf{Z}/2\mathbf{Z} = \{1, \epsilon\}$, alors $G_0 \times_2 G$ et $G \times_2 G_0$ sont isomorphes à G pour toute paire (G, ϵ). On montre que $G_{(4,0)} \times_2 G_{(p,0)} \approx G_{(p+4,0)}$; il en résulte que $G_{(p,0)}$ est d'ordre 2^p. Le bon cadre pour ces calculs est celui d'une famille à deux paramètres $G_{(p,q)}$, ce qui justifie notre choix de notation pour $G_{(p,0)}$; nous renvoyons à [LamSm–89].

Vu que l'abélianisé de G est d'ordre 2^{p-1}, le groupe G possède 2^{p-1} caractères linéaires. Chacun d'entre eux applique ϵ sur 1 ; pour toute représentation irréductible complexe ρ de G de degré strictement supérieur à 1, nous avons $\rho(\epsilon) = -\,\mathrm{id}$. On montre alors les assertions suivantes.

— Si p est impair, G possède $2^{p-1} + 1$ classes de conjugaison, et donc une unique représentation complexe irréductible ρ de degré strictement supérieur à 1 ; ce degré est $2^{\frac{p-1}{2}}$. La représentation ρ est réelle (voir le théorème XI.11) si et seulement si $p \equiv \pm 1 \pmod 8$.

— Si p est pair, G possède $2^{p-1}+2$ classes de conjugaison, et donc deux représentations complexes irréductibles ρ', ρ'' de degré strictement supérieur à 1; ces deux degrés sont égaux à $2^{\frac{p-2}{2}}$. Les représentations ρ', ρ'' sont réelles si et seulement si l'une d'entre elles l'est, si et seulement si $p \equiv 0 \pmod 8$.

On obtient ensuite les degrés des représentations *réelles* π de G telles que $\pi(\epsilon) = -\,\mathrm{id}$; ce sont

— des multiples de $2^{\frac{p-1}{2}}$ si $p \equiv \pm 1 \pmod 8$,
— des multiples pairs de $2^{\frac{p-1}{2}}$, c'est–à–dire des multiples de $2^{\frac{p+1}{2}}$, si $p \equiv \pm 3 \pmod 8$,
— des multiples de $2^{\frac{p-2}{2}}$ si $p \equiv 0 \pmod 8$,
— des multiples pairs de $2^{\frac{p-2}{2}}$, c'est–à–dire des multiples de $2^{\frac{p}{2}}$, si $p \equiv 2, 4, 6 \pmod 8$.

Autrement dit, il existe une représentation réelle π de G telle que $\pi(\epsilon) = -\,\mathrm{id}$ de degré $n = m2^s$, avec m un entier strictement positif et $s = s(p) \geq 0$, dans les cas suivants :

— $p \equiv \pm 1 \pmod 8$ et $s = \frac{p-1}{2} \equiv 0, 3 \pmod 4$,
— $p \equiv \pm 3 \pmod 8$ et $s = \frac{p+1}{2} \equiv 2, 4 \pmod 4$,
— $p \equiv 0 \pmod 8$ et $s = \frac{p-2}{2} \equiv 3 \pmod 4$,
— $p \equiv 2, 4, 6 \pmod 8$ et $s = \frac{p}{2} \equiv 1, 2, 3 \pmod 4$.

Pour n donné, n de la forme $u2^s = u2^{4\alpha+\beta}$ avec u impair, $\alpha \geq 0$ et $\beta \in \{0, 1, 2, 3\}$, le plus grand entier p pour lequel il existe une représentation réelle π de G telle que $\pi(\epsilon) = -\,\mathrm{id}$ est donc

— $p = 2s + 1 = 8\alpha + 1$ si $\beta = 0$, c'est–à–dire si $n = u2^{4\alpha}$,
— $p = 2s = 8\alpha + 2$ si $\beta = 1$, c'est–à–dire si $n = u2^{4\alpha+1}$,
— $p = 2s = 8\alpha + 4$ si $\beta = 2$, c'est–à–dire si $n = u2^{4\alpha+2}$,
— $p = 2s + 2 = 8\alpha + 8$ si $\beta = 3$, c'est–à–dire si $n = u2^{4\alpha+3}$,

ou encore

$$p \;=\; 8\alpha + \beta$$

dans tous les cas, comme énoncé au théorème XV.3.

Pour $n \geq 2$, considérons la sphère unité $\mathbf{S}^{n-1}$ de l'espace euclidien $\mathbf{R}^n$. Ecrivons $n = u2^{4\alpha+\beta}$ comme au théorème XV.3, et posons $p = 8\alpha + 2^\beta$. Soit $\mu : \mathbf{R}^p \times \mathbf{R}^n \longrightarrow \mathbf{R}^n$ une application satisfaisant aux conditions de ce théorème, avec de plus $\mu(e_p, y) = y$ pour tout $y \in \mathbf{R}^n$, et soient $A_1, \ldots, A_{p-1}$ comme ci–dessus. Pour tout $y \in \mathbf{S}^{n-1}$, les vecteurs $A_1(y), \ldots, A_{p-1}(y)$ sont orthogonaux à y et peuvent être vus comme des vecteurs tangents à la sphère en y. Ainsi, l'application μ fournit $p-1$ champs de vecteurs tangents à la sphère qui sont orthonormaux (en particulier linéairement indépendants) en tout point, et $p - 1 = 8\alpha + 2^\beta - 1$ est le plus grand entier pour lesquels une telle construction existe.

Notons $\mathrm{env}(\mathbf{S}^{n-1})$ le maximum des entiers k pour lesquels il existe k champs continus de vecteurs tangents à $\mathbf{S}^{n-1}$ linéairement indépendants en tout point ("env" se réfère à "envergure", notre traduction de l'anglais "span"). A priori, $\mathrm{env}(\mathbf{S}^{n-1}) \geq 8\alpha + 2^\beta - 1$. Il est remarquable que $\mathrm{env}(\mathbf{S}^{n-1}) = 8\alpha + 2^\beta - 1$ pour tout n. Dans certains cas particuliers, cette dernière égalité est facile à établir ; par exemple, si n est impair, la caractéristique d'Euler–Poincaré de la sphère est paire, de sorte que tout champ de vecteurs tangents à la sphère s'annule en un point au moins ; autrement dit : $\mathrm{env}(\mathbf{S}^{n-1}) = 0$. Le résultat général est un des succès de la K–théorie [Adams–62].

En particulier, la sphère $\mathbf{S}^{n-1}$ est parallélisable, c'est–à–dire possède $n-1$ champs continus de vecteurs tangents orthogonaux en tout point, si et seulement si $n-1 \in \{1, 3, 7\}$. Voir [BotMi–58, Kerva–58, Milno–58].

Adams–62. J.F. Adams, *Vector fields on spheres*, Annals of Math. **75** (1962), 603–632.

BotMi–58. R. Bott and J. Milnor, *On the parallelizability of the spheres*, Bull. Amer. Math. Soc. **64** (1958), 87–89.

Eckma–44. B. Eckmann, *Gruppen theoretischer Beweis des Satzes von Hurwitz–Radon über die Komposition quadratischer Formen*, Comment. Math. Helvetici **15** (1942/43), 358–366.

Eckma–89. B. Eckmann, *Hurwitz–Radon matrices and periodicity modulo* 8, L'Enseignement Math. **35** (1989), 77–91.

Kerva–58. M. Kervaire, *Non–parallelizability of the n–sphere for n* > 7, Proc. N.A.S. **44** (1958), 280–283.

LamSm–89. T.Y. Lam et T. Smith, *On the Clifford–Littlewood–Eckmanmn groups: a new look at periodicity* (mod 8), Rocky Mountain J. Math. **19** (1989), 749–786.

Milno–58. J. Milnor, *SOme consequences of a theorem of Bott*, Annals of Math. **68** (1958), 444–449.

XV.d. Compléments sur les paires de Gelfand

Soient G un groupe fini, H un sous–groupe de G et X l'espace homogème G/H muni de la G–action à gauche canonique. Notons $\pi : G \longrightarrow GL(\mathbf{C}^X)$ la représentation de permutation correspondante.

Dans la suite, nous identifions d'une part $\mathbf{C}^X$ au sous–espace $[G/H]$ de l'algèbre du groupe $\mathbf{C}[G]$ des fonctions ψ qui sont H–invariantes à droite, c'est–à-dire telles que $\psi(gh) = \psi(g)$ pour tous $g \in G$ et $h \in H$, et d'autre part $\mathbf{C}[H \setminus G/H]$ au sous–espace de $\mathbf{C}[G]$ des fonctions φ qui sont H–bi–invariantes, c'est–à–dire telles que $\varphi(hg) = \varphi(g) = \varphi(gh')$ pour tous $g \in G$ et $h, h' \in H$. Lorsque H est normal dans G, les fonctions de $\mathbf{C}[G/H]$ sont automatiquement bi–H–invariantes et $\mathbf{C}[G/H]$ s'identifie à l'algèbre du groupe quotient G/H. Dans le cas général, des vérifications de routine montrent que

— $\mathbf{C}[H \setminus G/H]$ est une sous–algèbre de l'algèbre de convolution $\mathbf{C}[G]$, avec unité $\frac{1}{|H|}\sum_{h \in H} \delta_h$;

— $\mathbf{C}[G/H]$ est un module à droite sur $\mathbf{C}[H \setminus G/H]$, autrement dit $\psi * \varphi \in \mathbf{C}[G/H]$ pour tous $\psi \in \mathbf{C}[G/H]$ et $\varphi \in \mathbf{C}[H \setminus G/H]$;

— $\big(\pi(g)\psi\big) * \varphi = \pi(g)\big(\psi * \varphi\big)$ pour tous $g \in G$, $\psi \in \mathbf{C}[G/H]$ et $\varphi \in \mathbf{C}[H \setminus G/H]$.

Par suite, la convolution à droite par les fonctions bi–H–invariantes fournit une application linéaire

$$j\ :\ \begin{cases} \mathbf{C}[H\setminus G/H] & \longrightarrow\ \mathcal{L}(\mathbf{C}[G/H])^G \\ \qquad\varphi & \longmapsto\ (\psi\mapsto\psi*\varphi). \end{cases}$$

XV.5. Proposition. *L'application j définie ci–dessus est un isomorphisme de la sous–algèbre $\mathbf{C}[H\setminus G/H]$ des fonctions bi–H–invariantes de l'algèbre de G sur le commutant $\mathcal{L}(\mathbf{C}[G/H])^G=\pi(G)'$ de la représentation π.*

Démonstration. L'application j est injective. En effet, si $j(\varphi)=0$, alors

$$j(\varphi)\Big(\frac{1}{|H|}\sum_{k\in H}\delta_k\Big)\ =\ \Big(\frac{1}{|H|}\sum_{k\in H}\delta_k\Big)*\varphi\ =\ \varphi=0.$$

Pour montrer que j est surjective, considérons $S\in\mathcal{L}(\mathbf{C}[G/H])^G$ et posons

$$\varphi\ =\ S\Big(\frac{1}{|H|}\sum_{k\in H}\delta_k\Big).$$

Par définition, $\varphi\in\mathbf{C}[G/H]$ est H–invariante à droite. De plus

$$\begin{aligned}\varphi(hg)\ &=\ \big(\pi(h^{-1})\varphi\big)(g)\ =\ \left(\pi(h^{-1})S\Big(\frac{1}{|H|}\sum_{k\in H}\delta_k\Big)\right)(g)\\ &=\ \left(S\pi(h^{-1})\Big(\frac{1}{|H|}\sum_{k\in H}\delta_k\Big)\right)(g)\ =\ \left(S\Big(\frac{1}{|H|}\sum_{k\in H}\delta_k\Big)\right)(g)\ =\ \varphi(g)\end{aligned}$$

pour tous $h\in H$ et $g\in G$, de sorte que φ est bi–H–invariante. Enfin, pour toute fonction $\psi\in\mathbf{C}[G/H]$, nous avons

$$\begin{aligned}S(\psi)\ &=\ S\Big(\psi*\frac{1}{|H|}\sum_{k\in H}\delta_k\Big)\ =\ S\left(\sum_{g\in G}\psi(g)\pi(g)\Big(\frac{1}{|H|}\sum_{k\in H}\delta_k\Big)\right)\\ &=\ \sum_{g\in G}\psi(g)\pi(g)S\Big(\frac{1}{|H|}\sum_{k\in H}\delta_k\Big)\ =\ \sum_{g\in G}\psi(g)\pi(g)\varphi=\psi*\varphi.\end{aligned}$$

Donc $S=j(\varphi)$. □

Remarque. Soit G un groupe arbitraire (fini *ou infini*) et H un sous–groupe. Il existe une condition classique qui est suffisante pour qu'on puisse définir un analogue de l'algèbre de convolution $\mathbf{C}[H\setminus G/H]$.

Plus précisément, supposons que (G,H) est une *paire de Hecke*, c'est–à–dire que l'action à gauche de H sur G/H et l'action à droite de H sur $H\setminus G$ ont toutes leurs orbites finies. Soit alors $\mathbf{C}[G,H]$ l'espace des fonctions à valeurs complexes sur G qui sont H–bi–invariantes et dont les projections des supports sur G/H et $H\backslash G$ sont finies. On vérifie que la convolution est bien définie sur $\mathbf{C}[G,H]$ et en fait une algèbre (en général de dimension infinie). Il existe toujours une injection de cette *algèbre de Hecke* dans le commutant de la représentation *quasi–régulière* de G sur $\ell^2(G/H)$, et on peut montrer que cette injection est d'image dense pour la topologie ad hoc (la topologie forte sur l'algèbre des opérateurs bornés sur $\ell^2(G/H)$) ; voir par exemple [Thèse de Robyn Curtis, proposition 1.3.10].

Le lemme suivant est un cas particulier du théorème de réciprocité de Frobenius.

XV.6. Lemme. *Soient G, H, π comme ci–dessus et $\rho : G \longrightarrow GL(W)$ une représentation irréductible de G. On pose*

$$W^H \ = \ \{w \in W \mid \rho(h)w = w \ \ \textit{pour tout} \ \ h \in H\}$$

et on note χ_π, χ_ρ les caractères de π, ρ.

Alors la mutliplicité $\langle \chi_\rho \mid \chi_\pi \rangle$ de ρ dans π est égale à la dimension de W^H.

Démonstration. Notons x_0 le point base de $X = G/H$, c'est–à–dire la classe de 1. Pour tout $x \in X$, choisissons $t_x \in G$ tel que $t_x(x_0) = x$. L'application

$$X \times H \ \longrightarrow \ G, \qquad (x, h) \ \longmapsto \ t_x h$$

est donc une bijection ; en particulier, $|X|\,|H| = |G|$.

Pour $g, g' \in G$, notons $\delta_{g,g'}$ le symbole de Kronecker qui vaut 1 si $g = g'$ et 0 sinon. Le caractère de π est donné par

$$\chi_\pi(g) \ = \ |\{x \in X \mid gx = x\}| \ = \ \big|\{x \in X \mid t_x^{-1} g t_x \in H\}\big|$$

car $gx = x$ s'écrit aussi $t_x^{-1} g t_x(x_0) = x_0$. On calcule

$$\begin{aligned}
\langle \chi_\rho \mid \chi_\pi \rangle \ &= \ \frac{1}{|G|} \sum_{g \in G} \overline{\chi_\rho(g)} \sum_{x \in X} \sum_{h \in H} \delta_{t_x^{-1} g t_x, h} \\
&= \ \frac{1}{|G|} \sum_{h \in H} \sum_{x \in X} \sum_{g \in G} \overline{\chi_\rho(g)} \delta_{t_x^{-1} g t_x, h} \\
&= \ \frac{1}{|G|} \sum_{h \in H} \sum_{x \in X} \sum_{g' \in G} \overline{\chi_\rho(t_x g' t_x^{-1})} \delta_{g', h} \\
&= \ \frac{1}{|G|} \sum_{h \in H} \sum_{x \in X} \sum_{g' \in G} \overline{\chi_\rho(g')} \delta_{g', h} \\
&= \ \frac{|X|}{|G|} \sum_{h \in H} \sum_{g' \in G} \overline{\chi_\rho(g')} \delta_{g', h} \\
&= \ \frac{|X|}{|G|} \sum_{h \in H} \sum_{h' \in H} \overline{\chi_\rho(h')} \delta_{h', h} \\
&= \ \frac{1}{|H|} \sum_{h \in H} \overline{\chi_\rho(h)} \\
&= \ \langle \chi_\rho \mid 1_H \rangle \,.
\end{aligned}$$

et le lemme en résulte. □

XV.7. Proposition. *Soient G un groupe fini, H un sous–groupe et π la représentation de permutation associée à l'action de G sur H. Les conditions suivantes sont équivalentes :*

(i) *la représentation π est sans multiplicité, c'est–à–dire (G, H) est une paire de Gelfand ;*

(ii) $\dim(W^H) \leq 1$ *pour toute représentation irréductible $\rho : G \longrightarrow GL(W)$ de G ;*

(iii) *la sous–algèbre $\mathbf{C}[H \setminus G/H]$ de $\mathbf{C}[G]$ est commutative.*

Démonstration. L'équivalence de (i) et (ii) est une conséquence immédiate du lemme précédent. L'équivalence de (i) et (iii) est une conséquence de la proposition qui précède et de la proposition VII.14. □

Soient α un automorphisme d'un groupe G et φ une fonction à valeurs complexes sur G. On définit des fonctions φ^α et $\check{\varphi}$ sur G par

$$\varphi^\alpha(g) \;=\; \varphi(\alpha(g)) \qquad \text{et} \qquad \check{\varphi}(g) \;=\; \varphi(g^{-1}).$$

XV.8. Lemme. *Soient G un groupe, α un automorphisme de G et $\varphi, \psi : G \longrightarrow \mathbf{C}$ deux fonctions à support fini. alors*

$$(\varphi * \psi)^\alpha \;=\; \varphi^\alpha * \psi^\alpha \qquad \textit{et} \qquad (\varphi * \psi)\check{} = \check{\psi} * \check{\varphi}.$$

Démonstration : routine. □

XV.9. Proposition. *Soient G un groupe fini et H un sous–groupe. On suppose qu'il existe un automorphisme α de G tel que $\alpha(g) \in Hg^{-1}H$ pour tout $g \in G$.*

Alors (G, H) est une paire de Gelfand

Démonstration. Pour tous $\varphi \in \mathbf{C}[H \setminus G/H]$ et $g \in G$, nous avons par hypothèse $\varphi(\alpha(g)) = \varphi(g^{-1})$, c'est–à–dire $\varphi^\alpha = \check{\varphi}$. Pour $\varphi, \psi \in \mathbf{C}[H \setminus G/H]$, nous avons donc en vertu du lemme précédent

$$(\varphi * \psi)\check{} = \check{\psi} * \check{\varphi} \;=\; \psi^\alpha * \varphi^\alpha \;=\; (\psi * \varphi)^\alpha \;=\; (\psi * \varphi)\check{}$$

et donc aussi $\varphi * \psi = \psi * \varphi$. □

XV.10. Exemples (i) Soit A un groupe abélien fini. Pour tout sous–groupe B de A, la paire (A, B) est de Gelfand. En particulier, la paire $(A, \{1\})$ est de Gelfand (son étude est équivalente à celle de A !).

Néanmoins, tout groupe fini, abélien ou non, fournit canoniquement un exemple de paire de Gelfand, comme nous l'indiquons ci–dessous à l'exemple (iv).

Soit G un groupe fini et N un sous–groupe normal. Pour que la paire (G, N) soit de Gelfand, il faut et il suffit que le quotient G/N soit abélien.

(ii) Soient H un groupe fini, A un groupe abélien fini agissant sur H par automorphismes et $G = A \rtimes H$ le produit semi–direct correspondant. Alors la paire (G, H) est de Gelfand.

En effet, d'une part on vérifie que l'application $\alpha : A \rtimes H \longrightarrow A \rtimes H$ définie par $\alpha(ah) = a^{-1}h$ est un automorphismes de groupe (c'est là que l'hypothèse "A abélien" intervient), et d'autre part nous avons

$$\alpha(ah) \;=\; a^{-1}h \;=\; h(h^{-1}a^{-1})h \;\in\; H(ah)^{-1}H$$

pour tout $ah \in A \rtimes H$.

(iii) En particularisant l'exemple (ii), nous obtenons que la paire

$$(\mathbf{F}_q^k \rtimes \mathrm{Sym}(k), \mathrm{Sym}(k))$$

de l'exercice VII.E18 est une paire de Gelfand pour tout corps fini $\mathbf{F}_q$ et pour tout entier $k \geq 2$.

(iv) Soit H un groupe fini. Notons G le produit direct $H \times H$ et ΔH le sous–groupe diagonal des éléments de la forme (h, h). Ainsi ΔH est un sous–groupe normal de G isomorphe à H, et l'application $G/\Delta H \longrightarrow H$, $(h_1, h_2)\Delta H \longmapsto h_1 h_2^{-1}$ est un isomorphisme. L'action de G sur $G/\Delta H$ s'écrit $(h_1, h_2)\big((x_1, x_2)\Delta H\big) = (h_1 x_1, h_2 x_2)\Delta H$; en identifiant $G/\Delta H$ à H comme ci–dessus, c'est–à–dire en identifiant $(x_1, x_2)\Delta H$ à $x = x_1 x_2^{-1}$, on obtient $(h_1, h_2)x = h_1 x h_2^{-1}$.

La paire $(G, \Delta H)$ est de Gelfand. En effet, si $\alpha : G \longrightarrow G$ est l'automorphisme de la volte[35], défini par $\alpha(h_1, h_2) = (h_2, h_1)$, l'équation

$$(h_2, h_1) \;=\; (h_1, h_1)(h_1^{-1}, h_2^{-1})(h_2, h_2)$$

montre que $\alpha(g) \in (\Delta H) g^{-1} (\Delta H)$ pour tout $g \in G$.

La représentation de permutation π de $G = H \times H$ associée à l'action de G sur $G/\Delta H = H$ est la représentation $\pi : H \times H \longrightarrow GL(\mathbf{C}^H)$ définie par

$$\left(\pi(h_1, h_2)\varphi\right)(x) \;=\; \varphi(h_1^{-1} x h_2)$$

pour tous $h_1, h_2, x \in H$ et $\varphi \in \mathbf{C}^H$. Vu la propriété de définition des paires de Gelfand, cette représentation est sans mulltiplicité.

Par ailleurs, le rang de l'action de H sur $H \times H$ est égal au nombre de classes de conjugaison de H (exercice IX.E3). C'est donc aussi le nombre de représentations irréductibles dont π est somme directe. Il en résulte une démonstration du théorème IX.12.

(v) Pour l'extension, classique, de la notion de paire de Gelfand aux groupes localement compacts, deux des exemples standard sont les paires $(\mathbf{R}^n \rtimes \mathcal{SO}(n), \mathcal{SO}(n))$, pour laquelle l'argument de l'exemple (ii) convient, et $(SL_n(\mathbf{R}), \mathcal{SO}(n))$, pour laquelle on applique la proposition précédente avec $\alpha(g) = ({}^t g)^{-1}$.

XV.11. Exemple. Etant donné une paire de Gelfand (G, H) et la représentation correspondante $\pi : G \longrightarrow GL(\mathbf{C}^X)$, où $X = G/H$, il est en général nettement plus difficile d'identifier les sous–espaces G–invariants irréductibles de $\mathbf{C}^X$ que d'en calculer le nombre (qui est le rang de l'action de G sur X). Voici toutefois une description, pour la paire $(\mathbf{F}_2^k \rtimes \mathrm{Sym}(k), \mathrm{Sym}(k))$ de l'exercice VII.E18.

Identifions comme d'habitude $(\mathbf{F}_2^k \rtimes \mathrm{Sym}(k))/\,\mathrm{Sym}(k)$ à $\mathbf{F}_2^k$. Posons $V = \mathbf{C}^{\mathbf{F}_2^k}$ et $W = \mathbf{C}^{\mathbf{F}_2}$. Nous identifions l'espace V au produit tensoriel $\bigotimes_{j=1}^k W^{(j)}$ de k copies de W. Soit $W = W_0 \oplus W_1$ la décomposition en somme directe de W où W_0 est l'espace des fonctions constantes et W_1 celui des fonctions de somme nulle. Posons

$$V_\epsilon \;=\; \bigoplus_{\substack{\epsilon_1, \dots, \epsilon_k \in \{0,1\} \\ \epsilon_1 + \cdots + \epsilon_k = \epsilon}} W_{\epsilon_1}^{(1)} \otimes \cdots \otimes W_{\epsilon_k}^{(k)} \;, \quad \epsilon = 0, 1, \dots, k \;;$$

autrement dit, V_ϵ est l'espace des sommes de fonctions $\varphi : \mathbf{F}_2^k \longrightarrow \mathbf{C}$ de la forme

$$\varphi(v_1, \dots, v_k) \;=\; f_{\epsilon_1}(v_1) f_{\epsilon_2}(v_2) \cdots f_{\epsilon_k}(v_k) \quad \text{avec} \quad \begin{cases} f_{\epsilon_j} \in W_{\epsilon_j} \quad \text{pour} \quad j = 1, \dots, k \\ \text{et} \quad \epsilon_1 + \cdots + \epsilon_k = \epsilon, \end{cases}$$

[35]Proposition de Christian Kassel pour traduire l'anglais *flip*.

ou encore des sommes de fonctions φ dépendant d'au plus ϵ variables.

Alors les sous–espaces $V_0, \ldots, V_k$ de V sont invariants par π et V est leur somme directe. Ce sont donc les $k+1$ sous–espaces irréductibles de V dont V est la somme directe.

XV.12. Remarque Les paires de Gelfand fournissent un cadre approprié, plus général que celui des groupes (localement compacts) abéliens, dans lequel les outils fondamentaux de "l'analyse harmonique commutative" sont encore vrais : théorie de Fourier "classique", théorème de Plancherel, théorème de Bochner, ... Voir par exemple J. Dieudonné, *éléments d'analyse 6*, Gauthier Villars, 1975.

XV.e. Représentations induites – réciprocité de Frobenius

C'est le procédé le plus efficace de construction de représentations de groupes, finis ou non ! Le résultat principal est le théorème dit de réciprocité de Frobenius.

XV.f. Symétries des molécules et vibrations moléculaires

Voir le chapitre 32 de [JamLi–01] ainsi que

M. Fetizon, H.–P. Gervais et A. Guichardet, *Théorie des groupes et de leurs représentations, application à la spectroscopie moléculaire*, Ellipses, 1987.

XV.g. Quelques applications en probabilités et statistiques

A extraire de [Diaco–88] et

T. Ceccherini–Silberstein, F. Scarabotti et F. Tolli, *Finite Gelfand pairs and their applications to probability and statistics*, Preprint (April 30, 2004).

XV.h. Noyaux reproduisants — Surfaces de Riemann — ???

Noyaux reproduisants : à extraire de

B. Bekka et P. de la Harpe (Appendix in collaboration with Rostislav Grigorchuk), *Irreducibility of unitary group representations and reproducing kernels Hilbert spaces*, Expositiones Math. **21** (2003), 115–149.

Nombre de surfaces de Riemann qui sont des revêtements à n feuilles de $\mathbf{P}^1_{\mathbf{C}}$ ramifiés au dessus de w points ? Parmi les articles de A. Hurwitz : *Über die Anzahl der Riemannschen Flächen mit gegeben Verweigungspunkten,* Math. Ann. 55 (1902) 53–66 ; voir aussi divers articles de A.D. Mednyh (fin des 1970) et [Curti–99, page 73].

Indications supplémentaires et solutions de quelques exercices

Il ne s'agit que de solutions *partielles.*

Exercice V.E5.

Montrons d'abord une assertion préliminaire ; $\mathbf{T}$ désigne le cercle unité du plan complexe. *Soient d un entier positif et $\omega_1, \ldots, \omega_d \in \mathbf{T}$. Pour tout $\epsilon > 0$, il existe un entier $n \geq 1$ tel que* $\max_{1 \leq j \leq d} |\omega^j - 1| < \epsilon$.

En effet, soit Γ le sous–groupe cyclique de $\mathbf{T}^d = \mathbf{T} \times \cdots \times \mathbf{T}$ (avec d facteurs) engendré par $(\omega_1, \ldots, \omega_d)$. Si Γ est fini d'ordre n, alors $\omega^n = 1$ pour $j = 1, \ldots, d$. Si le groupe cyclique

Γ est infini, il possède un point d'accumulation dans le groupe compact $\mathbf{T}^d$, disons ω, et il en résulte que 1 est aussi un point d'accumulation de Γ.

Soit $a \in M_n(\mathbf{C})$; notons $\lambda_1, \ldots, \lambda_n$ ses valeurs propres, répétées selon leurs multiplicités, et $r = \max\{|\lambda_k|, 1 \leq i \leq n\}$ son rayon spectral. Supposons pour la suite $r > 0$; on ne restreint pas la généralité de l'argument en supposant de plus $\lambda_1, \ldots, \lambda_s$ de module r et $\lambda_{s+1}, \ldots, \lambda_n$ de modules strictement inférieurs. L'assertion précédente montre qu'il existe une suite d'entiers $(k_j)_{j\geq 1}$ strictement croissante telle que $\lim_{j\to\infty}(\lambda_t/\lambda_1)^{k_j} = 1$ pour tout $t \in \{1, \ldots, s\}$; notons que $\lim_{j\to\infty}(\lambda_u/\lambda_1)^{k_j} = 0$ pour tout $t \in \{s+1, \ldots, n\}$. En particulier, $\operatorname{trace}(a^{k_j})$ est proche de $r\lambda_1$ pour j assez grand.

Par suite, si $\operatorname{trace}(a^\ell) = 0$ pour tout ℓ assez grand, alors $r = 0$.

Exercice V.E9.

Notons x et y les coordonnées canoniques de $\mathbf{C}^2$, de sorte que $\xi\begin{pmatrix} x \\ y \end{pmatrix} = x$ et $\eta\begin{pmatrix} x \\ y \end{pmatrix} = y$. Soit n un entier positif. Pour le calcul du caractère χ_n de la représentation π_n, voir le numéro XIII.7. Nous montrons ci–dessous que la représentation π_n de $SL_2(\mathbf{C})$ est irréductible.

Toute application différentiable $\alpha : I \longrightarrow V_n$, où I est un intervalle de $\mathbf{R}$ contenant l'origine, définit un vecteur $\frac{d}{dt}\alpha|_{t=0}$ que nous allons calculer dans trois cas particuliers. (La lectrice savante remarquera que les courbes α sont des groupes à un paramètre évalués sur des vecteurs de V_n et que nous calculons la représentation de l'algèbre de Lie $\mathfrak{sl}_2(\mathbf{C})$ correspondant à π_n.) Choisissons $j \in \{0, 1, \ldots, n\}$; définissons les applications

$$\begin{aligned}
\alpha_{H,j}(t) &= \pi_n\begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix}\xi^{n-j}\eta^j \quad : \quad \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto e^{(-n+2j)t}x^{n-j}y^j \\
\alpha_{X,j}(t) &= \pi_n\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\xi^{n-j}\eta^j \quad : \quad \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto (x-ty)^{n-j}y^j \\
\alpha_{Y,j}(t) &= \pi_n\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}\xi^{n-j}\eta^j \quad : \quad \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto x^{n-j}(-tx+y)^j.
\end{aligned}$$

On calcule

$$\begin{aligned}
&(H) \qquad & \frac{d}{dt}\alpha_{H,j}(t)\big|_{t=0} &= (-n+2j)\xi^{n-j}\eta^j \\
&(X) \qquad & \frac{d}{dt}\alpha_{X,j}(t)\big|_{t=0} &= (-n+j)\xi^{n-j-1}\eta^{j+1} \\
&(Y) \qquad & \frac{d}{dt}\alpha_{Y,j}(t)\big|_{t=0} &= (-n+2j)\xi^{n-j+1}\eta^{j-1}
\end{aligned}$$

(conventions utilisées ici : $\xi^{-1} = \eta^{-1} = 0$).

Soit alors U un sous–espace vectoriel de V_n non réduit à zéro et invariant par π_n. En utilisant la relation (Y), on montre que U contient le vecteur ξ^n. En utilisant la relation (X), on montre ensuite que U contient tous les vecteurs $\xi^{n-j}\eta^j$, de sorte que $U = V_n$. Ceci montre que la représentation π_n est irréductible ; de même, la restriction de π_n au groupe $SL_2(\mathbf{R})$ est irréductible.

Les indices utilisés ci-dessus se réfèrent à la base

$$H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad Y = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

de l'algèbre de Lie $\mathfrak{sl}_2$ des matrices 2–fois—2 à trace nulle.

Le cas de la restriction de π_n au groupe $S\mathcal{U}(2)$ est un peu plus compliqué, mais la même idée fonctionne avec les courbes définies par

$$\begin{aligned}
\alpha_{iH,j}(t) &= \pi_n \begin{pmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{pmatrix} \xi^{n-j}\eta^j \\
\alpha_{X-Y,j}(t) &= \pi_n \begin{pmatrix} \cos(t) & \sin(t) \\ -\sin(t) & \cos(t) \end{pmatrix} \xi^{n-j}\eta^j \\
\alpha_{iX+iY,j}(t) &= \pi_n \begin{pmatrix} \cos(t) & i\sin(t) \\ i\sin(t) & \cos(t) \end{pmatrix} \xi^{n-j}\eta^j.
\end{aligned}$$

En utilisant des combinaisons linéaires appropriées des vecteurs $\frac{d}{dt}\alpha_{*,j}(t)|_{t=0}$, on montre à nouveau que tout sous–espace vectoriel de V_n non réduit à zéro et invariant par $\pi_n(S\mathcal{U}(2))$ est l'espace V_n tout entier.

Les matrices

$$iH = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad X - Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad iX + iY = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

constituent une base de l'algèbre de Lie réelle $\mathfrak{su}(2)$ des matrices complexes 2–fois–2 anti-adjointes à trace nulle.

Pour un exposé élémentaire des groupes de Lie $S\mathcal{U}(2)$, SL_2, de leurs algèbres de Lie, et de leurs représentations de dimension finie, voir [Vinbe89].

Exercice VII.E4.iii.

Le noyau de ϵ_1 est le groupe SG_C. En considérant son action sur les quatre diagonales du cube, on vérifie qu'il est isomorphe au groupe symétrique Sym(4).

Le noyau de ϵ_2 est le groupe G_T correspondant au tétraèdre. En considérant son action sur les quatre sommets de G, on vérifie qu'il est égtalement isomorphe à Sym(4).

Ces deux groupes ne sont pas conjugués dans G_C, car ils sont tous deux normaux, et distincts.

Le noyau de $\epsilon_1\epsilon_2$ est le sous–groupe de G_C des isométries qui ou bien préservent T et l'orientation de $\mathbf{R}^3$, ou bien échangent T avec T' et renversent l'orientation de $\mathbf{R}^3$. C'est le produit direct du sous–groupe $\mathrm{Ker}(\epsilon_1) \cap \mathrm{Ker}(\epsilon_2) = SG_T$ isomorphe à Alt(4) et du groupe $\{\pm \mathrm{id}\}$ à deux éléments ; en particulier, il n'est pas isomorphe à SG_C.

Exercice VII.E5.

Les quatre sous–espaces de W invariants par G_C sont :

(a) le sous–espace W_1 des fonctions constantes,
(b) le sous–espace W_1' des fonctions ψ telles que $\psi(y_1) + \psi(y_2) = 0$ pour toute paire (y_1, y_2) de sommets adjacents [remarque : une telle fonction est nécessairement impaire],
(c) le sous–espace W_3 des fonctions paires de somme nulle,
(d) le sous–espace W_3' des fonctions impaires ψ dont la somme des valeurs est nulle sur les quatre sommets d'un tétraèdre régulier inscrit dans le cube.

L'action du sous–groupe SG_C de G_C sur Y est encore de rang quatre, et ces quatres sous–espaces correspondent donc à des représentations irréductibles de SG_C (les représentations de G_C dans ces espaces sont dont *a fortiori* irréductibles). Avec les notations de la table XI.5, les quatre représentations irréductibles de SG_C sont de caractères χ_1, χ_{sign}, χ_3 et $\chi_{\text{sign}}\chi_3$.

Les valeurs propres de L dans ces sous–espaces sont $\mu_1 = 1$, $\mu_1' = 0$, $\mu_3 = -1/3$, et $\mu_3' = -1/3$. Il en résulte comme en VII.13 que $L^k\psi$ tend exponentiellement vers la valeur moyenne de ψ lorsque k tend vers l'infini.

Exercice VIII.E3.iv.

Soit $\mathbf{K}$ un corps. Notons $B_2(\mathbf{K})$ le groupe des transformations de $\mathbf{K}$ de la forme $x \longmapsto a^2x + b$, avec $a \in \mathbf{K}^*$ et $b \in K$. Il est isomorphe au sous–groupe de $PSL_2(\mathbf{K})$ des classes de matrices de la forme $\begin{bmatrix} a & b' \\ 0 & a^{-1} \end{bmatrix}$, la correspondance étant telle que $b = ab'$. (La notation pour les classes de matrice est celle de l'exercice VIII.4.)

Le calcul

$$\begin{bmatrix} c & d \\ 0 & c^{-1} \end{bmatrix} \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} c^{-1} & -d \\ 0 & c \end{bmatrix} = \begin{bmatrix} a & cd(a^{-1} - a) + c^2b \\ 0 & a^{-1} \end{bmatrix}$$

montre que deux affinités $x \longmapsto a^2x + ab$ et $x \longmapsto {a'}^2x + a'b'$ sont conjuguées dans $B_2(\mathbf{K})$ si et seulement si l'une des quatre situations suivantes est réalisée :

(i) $a^2 = {a'}^2 \neq \pm 1$ ($\frac{q-1}{2} - 1$ classes),
(ii) $a^2 = {a'}^2 = 1$, $b \neq 0 \neq b'$ et $b^{-1}b' \in (\mathbf{F}_q^*)^2$ (une classe),
(iii) $a^2 = {a'}^2 = 1$, $b \neq 0 \neq b'$ et $b^{-1}b' \notin (\mathbf{F}_q^*)^2$ (une classe),
(iv) $a^2 = {a'}^2 = 1$, et $b = b' = 0$ (classe de l'indentité).

En particulier, si $\mathbf{K} = \mathbf{F}_q$ est d'ordre fini impair q, le nombre de classes de conjugaison du groupe $B_2(\mathbf{F}_q)$ est $\frac{q+3}{2}$.

Le commutateur de deux éléments de $B_2(\mathbf{K})$ est dans le groupe des translations de $\mathbf{K}$. Le calcul

$$\begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & -y \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & y \end{bmatrix} = \begin{bmatrix} 1 & (a^2 - a^{-2})y \\ 0 & 1 \end{bmatrix}$$

montre que, si $|\mathbf{K}| > 5$, le groupe dérivé de $B_2(\mathbf{K})$ coïncide avec $\mathrm{Trans}(\mathbf{K})$, donc que l'abélianisé de $B_2(\mathbf{K})$ est isomorphe au groupe $(\mathbf{K}^*)^2$.

Il résulte de ce qui précède que $B_2(\mathbf{K})$ possède $\frac{q-1}{2}$ représentations de degré un et deux représentations irréductibles de degrés n', n'' tels que

$${n'}^2 + {n''}^2 = \frac{(q-1)^2}{2}.$$

Posons $V = \mathbf{C}^{\mathbf{F}_q}$ et notons V_0 l'hyperplan des fonctions de somme nulle. L'action du groupe affine $\mathrm{Aff}(\mathbf{F}_q)$ sur $\mathbf{F}_q$ est de rang deux, et sa restriction au groupe $B_2(\mathbf{F}_q)$ est de rang trois. Par suite, la représentation correspondante $\tilde{\pi}_0$ de $\mathrm{Aff}(\mathbf{F}_q)$ dans V_0 est irréductible et la restriction π_0 de $\tilde{\pi}_0$ au groupe $B_2(\mathbf{F}_q)$ est une somme de deux sous–représentations irréductibles que nous notons π' et π'' (proposition VII.9).

Supposons désormais que q est un nombre premier, $q > 5$, de sorte que $\mathbf{F}_q = \mathbf{Z}/q\mathbf{Z}$. Nous allons montrer que les degrés de π' et π'' sont strictement supérieurs à 1, de sorte que ces degrés sont les nombres n', n'' introduits ci–dessus.

Pour $j \in \{0, 1, \ldots, q-1\}$, notons χ_j le caractère $t \longmapsto \exp(2i\pi jt/q)$ du groupe additif de $\mathbf{F}_q$, identifié au sous–groupe des translations dans $B_2(\mathbf{F}_q)$. Les fonctions $\chi_0, \chi_1, \ldots, \chi_{q-1}$ constituent une base de V, et $\chi_1, \ldots, \chi_{q-1}$ une base de V_0. Soit V' [respectivement V''] le sous–espace de V_0 engendré par les χ_j pour lesquels j est un carré dans $\mathbf{F}_q^*$ [resp. n'est pas un carré dans $\mathbf{F}_q^*$]. Les sous–espaces V' et V'', chacun de diemension $\frac{q-1}{2}$, sont invariants par $B_2(\mathbf{F}_q)$. Il résulte de ce qui précède que les sous–représentations correspondantes π', π'' de π_0 sont irréductibles et que $n' = n'' = \frac{q-1}{2}$.

Nous avons montré que, pour $\mathbf{F}_q = \mathbf{Z}/q\mathbf{Z}$ et $q > 5$, la liste complète (à équivalence près) des représentations complexes irréductibles de $B_2(\mathbf{F}_q)$ est constituée des $\frac{q-1}{2}$ caractères linéaires et des deux représentations π', π'' de degré $\frac{q-1}{2}$ définis ci–dessus. Dans [DaSaV–03, proposition 3.5.3 et théorème 3.5.1)], ce résultat est l'un des ingrédients principaux de la démonstration du théorème que voici : pour q premier, $q > 5$, toute représentation irréductible du groupe $PSL_2(\mathbf{Z}/q\mathbf{Z})$ distincte de la représentation unité a un degré supérieur ou égal à $\frac{q-1}{2}$. (Les exemples XI.5 et XI.4 montrent que l'assertion est également vraie pour $PSL_2(\mathbf{Z}/5\mathbf{Z}) \simeq \mathrm{Alt}(5)$, mais pas pour $PSL_2(\mathbf{Z}/3\mathbf{Z}) \simeq \mathrm{Alt}(4)$.)

A son tour, ce théorème est utile à l'analyse des *graphes de Ramnujan* exposés dans [DaSaV–03].

Exercice VIII.E4.ii&iii.

Vérifions que l'action de $PGL_2(\mathbf{K})$ sur la droite projective $\mathbf{P}^1_{\mathbf{K}}$ d'un corps $\mathbf{K}$ est simplement triplement transitive.

Soient a, b, c trois points de $\mathbf{P}^1_{\mathbf{K}}$ distincts deux à deux. Posons $g_1 = \begin{bmatrix} 0 & 1 \\ 1 & -a \end{bmatrix}$ si $a \neq \infty$ et $g_1 = 1$ si $a = \infty$; alors :

$$g_1(a) = \infty, \quad g_1(b) = b' = \begin{cases} \dfrac{1}{b-a} & \text{si} \quad a \neq \infty \\ b & \text{si} \quad a = \infty \end{cases} \quad \text{et} \quad g_1(c) = c' = \begin{cases} \dfrac{1}{c-a} & \text{si} \quad a \neq \infty \\ c & \text{si} \quad a = \infty \end{cases}$$

(par définition de b' et c'). Posons $g_2 = \begin{bmatrix} 1 & -b' \\ 0 & 1 \end{bmatrix}$; alors :

$$g_2g_1(a) = \infty, \quad g_2g_1(b) = 0, \quad g_2g_1(c) = c'' = \begin{cases} \dfrac{1}{c-a} - \dfrac{1}{b-a} & \text{si} \quad a = \infty \\ c - b & \text{si} \quad a = \infty. \end{cases}$$

Posons $g_3 = \begin{bmatrix} 1 & 0 \\ 0 & c'' \end{bmatrix}$ et $g = g_3g_2g_1$; alors

$$g(a) = \infty, \qquad g(b) = 0, \qquad g(c) = 1.$$

L'action est donc *triplement transitive.*

Soit $h = \begin{bmatrix} u & v \\ x & y \end{bmatrix} \in PGL_2(\mathbf{K})$. Le point ∞ [respectivement le point 0] est fixé par h si et seulement si $x = 0$ [resp. $v = 0$]. Supposons que $x = v = 0$; le point 1 est fixé par h si et seulement si $u = y$, c'est–à–dire si et seulement si $h = \begin{bmatrix} u & 0 \\ 0 & u \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. L'action est donc *simplement* triplement transitive.

Supposons $\mathbf{K} \neq \mathbf{F}_2$; soient a, b, c, d quatre points de $\mathbf{P}^1_{\mathbf{K}}$ distincts deux à deux, et soit g comme plus haut. Si $a \neq \infty$, alors

$$g(d) \;=\; g_3 g_2 \left(\frac{1}{d-a}\right) \;=\; g_3 \left(\frac{1}{d-a} - \frac{1}{b-a}\right) \;=\; \frac{b-d}{(d-a)(b-a)} \, \frac{(c-a)(b-a)}{b-c}$$

ou encore

$$[a, b, c, d] \;=\; \frac{c-a}{c-b} \;:\; \frac{d-a}{d-b}.$$

Si $a = \infty$, on vérifie que la même formule est encore vraie ; le terme de droite se réduit alors à $\frac{d-b}{c-b}$.

Exercice VIII.E5.

Vérifions que l'application naturelle de $PSL_2(\mathbf{F}_3)$ dans le groupe des permutations de $\mathbf{P}^1_{\mathbf{F}_3} = \{\infty, 0, 1, 2\}$ a pour image le groupe alterné Alt(4).

L'élément $\tau = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in PSL_2(\mathbf{F}_3)$ fixe le point ∞ et agit comme le 3–cycle $(0, 1, 2)$ sur les autres points. Soit w, x, y, z une énumération quelconque de $\mathbf{P}^1_{\mathbf{F}_3}$. Comme $PGL_2(\mathbf{F}_3)$ agit triplement transitivement sur $\mathbf{P}^1_{\mathbf{F}_3}$, il existe $g \in PGL_2(\mathbf{F}_3)$ tel que $gw = \infty$, $gx = 0$, $gy = 1$, $gz = 2$. Comme $PSL_2(\mathbf{F}_3)$ est normal dans $PGL_2(\mathbf{F}_3)$, l'élément $g^{-1}\tau g$ est dans $PSL_2(\mathbf{F}_3)$; il fixe le point w et agit comme un 3–cycle sur les autres points.

Ainsi, l'image de $PSL_2(\mathbf{F}_3)$ dans le groupe des permutations de $\{\infty, 0, 1, 2\}$ contient tous les trois cycles, qui engendrent le groupe Alt(4). Comme $PSL_2(\mathbf{F}_3)$ a 12 éléments, cette image coïncide avec Alt(4).

On peut utiliser des arguments du même ordre pour montrer que $PSL_2(\mathbf{F}_2)$ est isomorphe à Sym(3) et que $PSL_2(\mathbf{F}_4)$ est isomorphe à Alt(5).

Exercice VIII.E7.

Dans la suite, (a, b, c, d) désigne un quadrupe de points de $\mathbb{P}^1_{\mathbf{K}}$ distincts deux à deux et $[a, b, c, d] \in \mathbf{K} \setminus \{0, 1\}$ désigne leur birapport.

(i) Soit $t \in \mathbf{K} \setminus \{0, 1\}$. L'élément $\begin{bmatrix} 0 & t \\ 1 & 0 \end{bmatrix}$ de $PGL_2(\mathbf{K})$ applique $\infty, 0, 1, t$ respectivement sur $0, \infty, t, 1$. Par suite, $[0, \infty, t, 1] = [\infty, 0, 1, t] = t$ et, plus généralement,

$$[b, a, d, c] \;=\; [a, b, c, d].$$

De même $\begin{bmatrix} 1 & -t \\ 1 & -1 \end{bmatrix}$ applique $\infty, 0, 1, t$ respectivement sur $1, t, \infty, 0$. Par suite, $[1, t, \infty, 0] = [\infty, 0, 1, t] = t$ et, plus généralement,

$$[c, d, a, b] \;=\; [a, b, c, d].$$

Les deux identités précédentes montrent que nous avons aussi

$$[d, c, b, a] \;=\; [a, b, c, d].$$

Il en résulte que, des 24 valeurs *a priori* du birapport $[a^\sigma, b^\sigma, c^\sigma, d^\sigma]$, il en existe au plus 6 distinctes.

(ii) L'élément $\begin{bmatrix} 1 & 0 \\ 0 & t \end{bmatrix}$ applicque $\infty, 0, t, 1$ respectivement sur $\infty, 0, 1, t^{-1}$. Par suite, $[\infty, 0, t, 1] = [\infty, 0, 1, t^{-1}] = t^{-1}$ et, plus généralement,

$$[a, b, d, c] \; = \; \frac{1}{[a, b, c, d]}.$$

L'élément $\begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}$ applique $\infty, 1, 0, t$ respectivement sur $\infty, 0, 1, 1-t$. Par suite, $[\infty, 1, 0, t] = [\infty, 0, 1, 1-t] = 1-t$ et, plus généralement,

$$[a, c, b, d] \; = \; 1 - [a, b, c, d].$$

(iii) L'action de $\mathrm{Sym}(3) = \mathrm{Sym}(4)/\mathbf{V}$ sur $\mathbf{K} \setminus \{0, 1\}$ se prolonge en une action sur $\mathbf{P}^1_{\mathbf{K}}$ via les transformations

$$\begin{array}{lll} \mathrm{id} \, : \, t \longmapsto t & \rho \, : \, t \longmapsto 1 - \frac{1}{t} & \rho^2 \, : \, t \longmapsto \frac{-1}{t-1} \\ \sigma_1 \, : \, t \longmapsto \frac{1}{t} & \sigma_2 \, : \, t \longmapsto 1 - t & \sigma_3 \, : \, t \longmapsto \frac{t}{t-1} \end{array}$$

satisfaisant les relations

$$(\sigma_1)^2 \; = \; (\sigma_2)^2 \; = \; (\sigma_3)^2 \; = \; \mathrm{id} \qquad \sigma_2 \sigma_1 \; = \; \rho \qquad \rho^3 \; = \; \mathrm{id}\,.$$

Les cas où $\mathbf{K}$ est de caractéristique 2 ou 3, et encore plus le cas où $\mathbf{K}$ est le corps à quatre éléments, sont des cas particuliers.

Pour fixer les idées, supposons désormais que $\mathbf{K} = \mathbf{C}$. Les points fixes sont :

$$\begin{array}{cccccccccc} 1 & \text{et} & -1 & \text{pour} & \sigma_1 & \frac{1}{2} & \text{et} & \infty & \text{pour} & \sigma_2 \\ 0 & \text{et} & 2 & \text{pour} & \sigma_3 & \exp(i\pi/3) & \text{et} & \exp(-i\pi/3) & \text{pour} & \rho \text{ et } \rho^2. \end{array}$$

Pour cette action de $\mathrm{Sym}(3)$ sur la droite projective complexe, il y a deux orbites à trois éléments, $\{\infty, 0, 1\}$ et $\{\frac{1}{2}, 2, -1\}$, ainsi qu'une orbite à deux éléments, $\{\exp(\pm i\pi/3)\}$. Toutes les autres orbites ont six éléments. On peut voir $\mathrm{Sym}(3)$ comme le groupe des automorphismes de $\mathbf{P}^1_{\mathbf{C}}$ qui préservent un "triangle équatorial" dont $\infty, 0, 1$ sont les sommets, $\frac{1}{2}, 2, -1$ les "milieux" des côtés, les "pôles" étant $\exp(\pm i\pi/3)$.

Pour en savoir plus, voir par exemple le § 3 du chapitre 6 dans M. Berger, *Géométrie*, Cedic/F. Nathan, 1977.

Exercice IX.E2.

Le groupe des commutateurs de $H(\mathbf{k})$ coïncide avec le sous–groupe des matrices telles que $x = y = 0$. Par suite, l'homomorphisme

$$\left\{ \begin{array}{ccc} H(\mathbf{k}) & \longrightarrow & \mathbf{k}^2 \\ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} & \longmapsto & (x, y) \end{array} \right.$$

passe au quotient en un isomorphisme de l'abélianisé de $H(\mathbf{K})$ sur $\mathbf{k}^2$. Il en résulte que $H(\mathbf{k})$ possède exactement q^2 représentations de degré 1.

Un calcul élémentaire montre que les matrices $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix}$ sont conjuguées si et seuelement si ou bien $(x, y) = (x', y') \neq (0, 0)$, ou bien $(x, y) = (x', y') = (0, 0)$ et $z = z'$. Le groupe $H(\mathbf{k})$ possède donc $q^2 + q - 1$ classes de conjugaison, et par suite $q - 1$ représentations complexes irréductibles de degrés ≥ 2 ; notons $n_1, \ldots, n_{q-1}$ ces degrés, avec $2 \leq n_2 \leq \cdots \leq n_{q-1}$ (nous nous écartons donc ici de la notation du début du chapitre IX). Alors

$$(*) \qquad \sum_{j=1}^{q-1} n_j^2 \ = \ q^3 - q^2.$$

par le théorème IX.1.

Pour $q = 3$, la seule solution de (*) est $n_1 = n_2 = 3$.

Pour $q = 4$, il vient $n_1^2 + n_2^2 + n_3^2 = 48$, dont la seule solution est $n_1 = n_2 = n_3 = 4$.

Pour $q = 5$, l'équation $n_1^2 + n_2^2 + n_3^2 + n_4^2 = 100$ a plusieurs solutions. Mais certaines ne conviennent pas parce que $n_1 = 1$, c'est le cas de $(1, 1, 7.7)$, et d'autres parce que les n_j ne divisent pas l'ordre du groupe, c'est le cas de $(2, 4, 4, 8)$. La seule solution satisfaisant à la condition pour les n_j de diviser l'ordre du groupe, ici 125, est $(5, 5, 5, 5)$.

En induisant à $H(\mathbf{k})$ des caractères $\chi \neq \chi_1$ du centre (isomorphe à $\mathbf{k}$) vu comme caractères du sous–groupe des matrices caractérisées par $y = 0$, on peut montrer que $H(\mathbf{k})$ possède toujours exactement $q - 1$ représentations complexes irréductibles de degré q.

Exercice XI.E2.

Avec certaines notations comme en III.E1 et d'autres qu'on espère s'expliquant d'elle–mêmes, la table des caractères du groupe diédral D_8 s'écrit

	$\{1\}$	$\{r^2\}$	$\{r, r^3\}$	$\{s, sr^2\}$	$\{sr, sr^3\}$
χ_1	1	1	1	1	1
χ_1'	1	1	1	-1	-1
χ_1''	1	1	-1	1	-1
χ_1'''	1	1	-1	-1	1
χ_2	2	-2	0	0	0

C'est une conséquence immédiate de cette table que le graphe de McKay MK(D_8, π_2), voir XIII.6, est une étoile constituée d'un sommet central π_2 et de quatre sommets périphériques, graphe connu sous le nom de "graphe de Dynkin de type $\tilde{D}_4$".

Pour le groupe Q des quaternions, posons

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \text{et} \quad K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

La table des caractères s'écrit alors

	$\{1\}$	$\{-1\}$	$\{\pm I\}$	$\{\pm J\}$	$\{\pm K\}$
χ_1	1	1	1	1	1
χ_1'	1	1	1	-1	-1
χ_1''	1	1	-1	1	-1
χ_1'''	1	1	-1	-1	1
χ_2	2	-2	0	0	0

et coïncide donc bien avec celle de D_8.

Exercice XI.E7.

Le groupe symétrique Sym(5) possède 7 classes de conjugaison ; le nombre de leurs éléments et des représentants sont indiqués dans la table ci–dessous. Nous connaissons déjà de ce groupe le caractère principal χ_1, la signature χ_{sign}, la représentation irréductible π_4 de degré 4 de l'exemple VII.10 et son caractère noté χ_4, le caractère $\chi_{\text{sign}}\chi_4$, et l'existence de trois autres caractères irréductibles de degrés $5, 5, 6$ (voir XI.6).

Soit π la représentation de permutation associée à l'action de Sym(5) sur l'ensemble des sous–ensembles à deux éléments de $\{1, 2, 3, 4, 5\}$. Cette action étant de rang 3 (exemple VII.10), π est une somme de trois représentation irréductibles : le caractère principal χ_1 et deux représentations que nous notons (provisoirement) π' et π''. Il est facile d'abord de calculer le caractère $\tilde{\chi}$ de $\pi' \oplus \pi''$, comme à l'exemple VII.10, puis de vérifier que $\langle \tilde{\chi} \mid \chi_4 \rangle = 1$. Il en résulte qu'on peut identifier π' à π_4 et que le degré de π'' est 5. Ecrivons désormais π_5 au lieu de π'', et notons χ_5 son caractère. Comme le produit $\chi_{\text{sign}}\chi_5$ est distinct de χ_5, le produit $\chi_1\pi_5$ est une nouvelle représentation irréductible de Sym(5). Ce que nous savons de la table cherchée se présente alors comme suit, où a, b, c, d, e, f sont des valeurs inconnues.

	1	10	20	30	24	20	15
	id	$(1,2)$	$(1,2,3)$	$(1,2,3,4)$	$(1,2,3,4,5)$	$(1,2,3)(3,4)$	$(1,2)(3,4)$
χ_1	1	1	1	1	1	1	1
χ_{sign}	1	-1	1	-1	1	-1	1
χ_4	4	2	1	0	-1	-1	0
$\chi_{\text{sign}}\chi_4$	4	-2	1	0	-1	1	0
χ_5	5	1	-1	-1	0	1	1
$\chi_{\text{sign}}\chi_5$	5	-1	-1	1	0	-1	1
χ_6	6	a	b	c	d	e	f

Pour calculer a, b, c, d, e, f, il suffit par exemple d'écrire que χ_6 est orthogonal à chacun des autres caractères irréductibles, ce qui fournit un système linéaire qu'on résout sans peine :

$$a = b = c = e = 0, \qquad d = 1 \qquad \text{et} \qquad f = -2$$

La restriction au groupe Alt(5) de l'action de Sym(5) sur $\{1, 2, 3, 4, 5\}$ est encore de rang 2, de sorte que la restriction à Alt(5) de la représentation π_4 est encore irréductible ;

il est d'ailleurs facile de vérifier que $\frac{1}{60}\sum_{g\in\mathrm{Alt}(5)}|\chi_4(g)|^2 = 1$. De même, la restriction à Alt(5) de l'action de Sym(5) sur les sous–ensembles à deux éléments de $\{1,2,3,4,5\}$ est encore de rang 3, de sorte que la restriction à Alt(5) de la représentation π_5 est encore irréductible ; on vérifier également que $\frac{1}{60}\sum_{g\in\mathrm{Alt}(5)}|\chi_5(g)|^2 = 1$.

En revanche, le calcul

$$\frac{1}{60}\sum_{g\in\mathrm{Alt}(5)}|\chi_6(g)|^2 \;=\; \frac{1}{60}\left(36+24d^2+15e^2\right) \;=\; 2$$

montre que la restriction à Alt(5) de la représentation irréductible de degré 6 de Sym(5) est somme de deux irréductibles. La table

	1	15	20	12	12
	id	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4,5)$	$(1,3,5,2,4)$
χ_3	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3'	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_6	6	-2	0	1	1

(où les notations sont celles de XI.5) montre que la dernière ligne est la somme des deux précédentes ; ces deux irréductibles sont donc π_3 et π_3'.

Références

AleBe–95. J.L. Alperin et R.B. Bell, *Groups and representations*, Springer, 1995.

Artin–55. E. Artin, *The orders of the linear groups*, Comm. pure and applied math. **8** (1955), 355–366.

Artin–62. E. Artin, *Algèbre géométrique*, Gauthier-Villars, 1962.

ATLAS. J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker et R.A. Wilson, *Atlas of finite groups*, Clarendon Press, 1985.

Bratt–72. O. Bratteli, *Inductive limits of finite dimensional C^*–algebras*, Trans. Amer. Math. Soc. **171** (1972), 195–234.

Chand–68. K. Chandrasekharan, *Introduction to analytic number theory*, Springer, 1968.

Cheva–55. C. Chevalley, *Théorie des groupes de Lie, tome III, théorèmes généraux sur les algèbres de Lie*, Hermann, 1955.

Coxet–73. H.S.M. Coxeter, *Regular polytopes, Third Edition*, Dover, 1973.

CurRe–62. C.W. Curtis et I. Reiner, *Representations theory of finite groups and associative algebras*, Interscience, 1962.

Curti–99. C.W. Curtis, *Pioneers of representation theory: Frobenius, Burnside, Schur, and Brauer*, Amer. Math. Soc., 1999.

DaSaV–03. G. Davidoff, P. Sarnak et A. Valette, *Elementary number theory, group theory, and Ramanujan graphs*, Lodon Math. Soc. Student Texts 55, Cambrdige University Press, 2003.

Diaco–88. P. Diaconis, *Group representations in probability and statistics*, Institute of mathematical Statistics, Hayward, 1988.

Dieud–54. J. Dieudonné, *Les isomorphismes exceptionnels entre les groupes classiques finis*, Canadian J. Math. **6** (1954), 305–315.

DixMo–96. J.D. Dixon et B. Mortimer, *Permutation groups*, Springer, 1996.

Dixon–71. J.D. Dixon, *The structure of linear groups*, North Holland, 1971.
FeKaS–81. B. Fein, W.M. Kantor et M. Schucker, *Relative Brauer groups. II*, J. reine angew. Math. **328** (1981), 39–57.
FoMcK–81. D. Ford et J. McKay, *Representations and Coxeter graphs*, in "The geometric vein, the Coxeter Festschrift", C. Davis, B. Grünbaum, F.A. Sherk Editeurs, Springer (1981), 549–554.
FulHa–91. W. Fulton et J. Harris, *Representation theory, a first course*, Springer, 1991.
GooWa–98. R. Goodman et N.R. Wallach, *Representations and invariants of the classical groups*, Cambridge University Press, 1998.
HaHSV–77. M. Hazewinkel, W. Hesselink, D. Siersma et F.D. Veldkamp, *The ubiquity of Coxeter–Dynkin diagrams (an introduction to the A–D–E problem)*, Nieuw Arch. Wisk. **25** (1977), 257–307.
Humph–96. J.F. Humphreys, *A course in group theory*, Oxford University Press, 1996.
JamLi–01. G. James et M. Liebeck, *Representations and characters of groups, Second Edition*, Cambridge University Press, 2001.
Kiril–74. A. Kirillov, *Eléments de la théorie des représentations*, Mir, 1974.
Klein–56. F. Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, Dover, 1956 [première publication, en allemand, de 1884].
Körne–88. T.W. Körner, *Fourier analysis*, Cambridge University Press.
Lamot–86. K. Lamotke, *Regular solids and isolated singularities*, Vieweg, 1986.
Lang–65. S. Lang, *Algebra*, Addison-Wesley, 1965.
Macke–80. G.W. Mackey, *Harmonic analysis as the exploitation of symmetry – a historical survey*, Bull. Amer. Math. Soc. **3** (1980), 543–698.
McKay–80. J. McKay, *Graphs, singularities, and finite groups*, in "The Santa Cruz conference on finite groups", Proc. Symp. Pure Math. **37** (Amer. Math. Soc. 1980), 183–186.
Neuma–79. P.M. Neumann, *A lemma that is not Burnside!*, Math. Scientist **4** (1979), 133–141.
Rober–83. A. Robert, *Introduction fo the representation theory of compact and locally compact groups*, Cambridge University Press, 1983.
Rotma–95. J.J. Rotman, *An introduction to the theory of groups, Fourth Edition*, Springer, 1995.
Sagan–91. B.E. Sagan, *The symmetric group, representations, combinatorial algorithms, and symmetric functions*, Wadsworth & Brooks, 1991.
Serre–67. J–P. Serre, *Représentations linéaires des groupes finis*, Hermann, 1967.
Serre–70. J–P. Serre, *Cours d'arithmétique*, Presses universitaires de France, 1970.
Serre–72. J–P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Math. **15** (1972), 259–331 [Oeuvres, Volume III, 1–73].
Serre–05. J–P. Serre, *Groupes finis*, Prépublication, arXiv:math.GR/0503154v3, 11 Mar 2005.
Stern–93. S. Sternberg, *Group theory and physics*, Cambridge University Press, 1993.
VLiWi–92. J.H. van Lint et R.M. Wilson, *A course in combinatorics*, Cambridge Univ. Press, 1992.
Vinbe–89. E.B. Vinberg, *Linear representations of groups*, Birkhäuser, 1989.
Weil–40. A. Weil, *L'intégration dans les groupes topologiques et ses applicactions*, Hermann, 1940.
Weyl–52. H. Weyl, *Symmetry*, Princeton University Press, 1952.
Wolf–67. J.A. Wolf, *Spaces of constant curvature*, McGraw–Hill, 1967.

Index des termes

Index des groupes

Index des groupes des polyèdres réguliers

Apparentés.

Pierre de la Harpe, Section de Mathématiques, Université de Genève, C.P. 64, CH–1211 Genève 4, Suisse. Mel : Pierre.delaHarpe@math.unige.ch