COURS REPRÉSENTATIONS

STÉPHANE LAMY

Table des matières

Théorie générale

Principale référence : [CG14, p. 443–505], voir aussi [RW10, p. 45], [Pey04], [Col11], [Ulm12, chapitre 17], [Mal81].

Une *représentation linéaire* d'un groupe G est la donnée d'un morphisme de groupe $\rho\colon G \to \mathrm{GL}(V)$. Autrement dit, c'est une action linéaire $G \times V \to V$ du groupe G sur un espace vectoriel V. On utilise le vocabulaire usuel des actions, par exemple la représentation est dite *fidèle* si ρ est injective. Dans ce cours, on se restreint au cas où G est un groupe fini, et V est un $\mathbb{C}$-espace vectoriel de dimension finie. La dimension de V est souvent appelée le *degré* de la représentation.

Si $\rho\colon G \to \mathrm{GL}(V)$ et $\rho'\colon G \to \mathrm{GL}(V')$ sont deux représentations d'un même groupe, un *morphisme de représentations* (les français disent parfois "opérateur d'entrelacement", je préfère l'anglicisme plus court "G-morphisme") est une application linéaire $\varphi\colon V \to V'$ qui fait commuter le diagramme :

$$\begin{array}{ccc} G \times V & \longrightarrow & V \\ {\scriptstyle \mathrm{Id}\times\varphi}\downarrow & & \downarrow{\scriptstyle \varphi} \\ G \times V' & \longrightarrow & V' \end{array}$$

Cela revient à demander l'égalité

$$\varphi(\rho(g)(v)) = \rho'(g)(\varphi(v)) \text{ pour tout } g \in G, v \in V. \qquad (\dagger)$$

Deux représentations sont dites isomorphes s'il existe un tel φ inversible. On note $\mathrm{Hom}_G(V, V')$ l'espace des G-morphismes de V vers V' (ρ et ρ' sont implicites).

Exemple 1. En posant $\rho(\bar{1}) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\rho'(\bar{1}) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ on définit deux représentations fidèles de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathrm{GL}_2(\mathbb{C})$ qui sont non isomorphes (comparer les ensembles de points fixes).

Si $W \subset V$ est un sous-espace stable par tous les $\rho(g)$, $g \in G$, alors la restriction $\rho_W\colon G \to \mathrm{GL}(W)$ est une représentation, on dit que ρ_W est une *sous-représentation* de ρ.

On dit qu'une représentation est *irréductible*, ou *simple*, si les seuls sous-espaces stables sont $\{0\}$ et V.

Remarque 2. Si G est abélien, les $\rho(G)$ sont simultanément diagonalisables, ainsi toute représentation irréductible de G est de dimension 1.

Lemme 3 (Schur)**.** *Soient $\rho\colon G \to \mathrm{GL}(V)$ et $\rho'\colon G \to \mathrm{GL}(V')$ deux représentations irréductibles et $\varphi\colon V \to V'$ un G-morphisme. Alors :*

(1) *Le morphisme φ est ou bien nul ou bien un isomorphisme ;*

Date: 1er avril 2017.

(2) *Si $V = V'$, φ est une homothétie.*

(3) *Si les représentations V et V' sont isomorphes, alors* $\dim \mathrm{Hom}_G(V, V') = 1$.

Preuve. (1) Le noyau de φ est une sous-représentation de V : si $v \in \mathrm{Ker}\,\varphi$, on a $\rho'(g)(\varphi(v)) = \rho'(g)(0) = 0$, donc par (†), $\rho(g)(v) \in \mathrm{Ker}\,\varphi$.

De façon analogue l'image de φ est une sous-représentation de V' : si $v' = \varphi(v)$ est dans l'image de φ, alors par (†), $\rho'(g)(v') = \varphi(\rho(g)(v))$ est également dans l'image de φ.

Supposons φ non nul. Par irréducibilité des représentations, on en déduit que $\mathrm{Ker}\,\varphi = \{0\}$, et $\mathrm{Im}\,\varphi = V'$, autrement dit φ est un isomorphisme.

(2) Soit $\varphi \in \mathrm{Hom}_G(V, V)$, $\lambda \in \mathbb{C}$ une valeur propre de φ, et V_λ le sous-espace propre associé. Par irréducibilité de ρ, on obtient $V = V_\lambda$, et φ est donc l'homothétie de rapport λ.

(3) Par les deux points précédents, un G morphisme non nul de V vers V' est un isomorphisme, et un G-isomorphisme de V vers V' est uniquement déterminé à précomposition près par une homothétie. □

On dit qu'une représentation est *semi-simple* si toute sous-représentation possède un supplémentaire stable par G.

Rappelons le lemme suivant (où il n'y a pas de groupe en jeu) :

Lemme 4. *Si $f, g \in \mathcal{L}(V)$ sont deux endomorphismes qui commutent, alors le noyau et l'image de l'un sont des sous-espaces stables pour l'autre.*

Théorème 5 (Maschke)**.** *Toute représentation d'un groupe fini G sur un $\mathbb{C}$-espace vectoriel V de dimension finie est semi-simple.*

Preuve. Soit W un sous-espace vectoriel stable, on cherche à trouver un supplémentaire également stable. Pour cela considérons $p\colon V \to V$ un projecteur d'image W, et construisons son moyennisé

$$p' = \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ p \circ \rho(g)^{-1}.$$

On vérifie directement que l'image de p' est W, et que $p'(w) = w$ pour tout $w \in W$, ainsi p' est encore un projecteur d'image W. De plus la moyennisation entraine la propriété supplémentaire qu'il commute avec tous les $\rho(g)$. Le noyau de p' est donc un supplémentaire de W stable par la représentation, par le lemme. □

Le procédé de moyennisation de la preuve est omniprésent dans la théorie, par exemple il permet également de montrer qu'il existe toujours un produit scalaire invariant par une représentation :

Proposition 6. *Soit $\rho\colon G \to \mathrm{GL}(\mathbb{C}^n)$ une représentation d'un groupe fini. Alors il existe un produit scalaire (hermitien) invariant par ρ. En particulier, l'image de ρ est conjugué à sous-groupe de* $\mathrm{U}_n(\mathbb{C})$.

Preuve. On part d'un produit scalaire quelconque $\langle \cdot, \cdot \rangle$ (disons le produit hermitien standard sur $\mathbb{C}^n$), et on moyennise : $\langle v, w \rangle_\rho := \frac{1}{|G|} \sum_g \langle g(v), g(w) \rangle$. □

Une autre application du procédé de moyennisation est de construire des projecteurs sur des sous-espaces intéressants. Voici un exemple important.

Si $\rho\colon G \to \mathrm{GL}(W)$ est une représentation, on appelle *sous-espace des invariants* les points fixes de l'action :

$$W^G = \{w \in W;\ \rho(g)(w) = w \text{ pour tout } g \in G\}.$$

Lemme 7. *Soit $\rho\colon G \to \mathrm{GL}(W)$ une représentation. Alors l'endomorphisme $\pi = \frac{1}{|G|} \sum_{g \in G} \rho(g)$ est un projecteur d'image W^G, de plus c'est un G-morphisme.*

Preuve. On vérifie directement que pour tout $w \in W^G$, $\pi(w) = w$. Par ailleurs, pour $w \in W$ et $h \in G$ on a

$$\rho(h)(\pi(w)) = \frac{1}{|G|} \sum_{g \in G} \rho(hg)(w) = \frac{1}{|G|} \sum_{g' \in G} \rho(g')(w) = \pi(w).$$

Ainsi $\mathrm{Im}\,(\pi) \subset W^G$, et comme de plus $\pi|_{W^G} = \mathrm{Id}|_{W^G}$, on en déduit que $\pi^2 = \pi$ et $\mathrm{Im}\,(\pi) = W^G$. □

A partir de représentations $\rho\colon G \to V$ et $\rho'\colon G \to V'$ on peut en construire d'autres. Un exemple très simple consiste à construire la représentation somme directe $V \oplus V'$, en prenant des matrices diagonales par blocs. En itérant ce procédé m fois avec $V = V'$ on définit une représentation que l'on note $V^m := V \oplus \cdots \oplus V$. Un exemple un peu moins évident consiste à munir l'espace des applications linéaires $\mathrm{Hom}(V, V')$ d'une représentation ρ_{Hom}, en posant

$$\begin{aligned} G \times \mathrm{Hom}(V, V') &\to \mathrm{Hom}(V, V') \\ (\quad g \qquad , \quad \varphi \quad) &\mapsto \rho'(g) \circ \varphi \circ \rho(g^{-1}) \end{aligned}$$

Remarquons que demander que φ soit invariant par cette action revient à demander l'identité (†), autrement dit

$$\mathrm{Hom}_G(V, V') = \mathrm{Hom}(V, V')^G.$$

Remarque 8. Soit V, V', W trois représentations d'un groupe G. Alors

$$\mathrm{Hom}_G(W, V \oplus V') = \mathrm{Hom}_G(W, V) \oplus \mathrm{Hom}_G(W, V').$$

Notons $\mathrm{Irr}(G)$ les classes d'isomorphisme de représentations irréductibles de G. Pour chaque $i \in \mathrm{Irr}(G)$, on fixe un représentant S_i.

Proposition 9. *Soit V une représentation de G. Alors il existe des $m_i \in \mathbb{N}$ uniquement déterminés tel que*

$$V = \bigoplus_{i \in \mathrm{Irr}(G)} S_i^{m_i}.$$

De plus $m_i = \dim \mathrm{Hom}_G(S_i, V)$.

Preuve. L'existence d'une telle décomposition découle du lemme de Maschke, par récurrence sur la dimension. Pour l'unicité, écrivons (en utilisant deux fois la remarque 8) :

$$\mathrm{Hom}_G(S_i, V) = \mathrm{Hom}_G(S_i, \bigoplus_{j \in \mathrm{Irr}(G)} S_j^{m_j}) = \bigoplus_j \mathrm{Hom}_G(S_i, S_j^{m_j}) = \bigoplus_j \bigoplus_{k=1}^{m_j} \mathrm{Hom}_G(S_i, S_j).$$

Par le lemme de Schur, on a $\dim \mathrm{Hom}_G(S_i, S_j) = 1$ si $i = j$, et 0 sinon. Ainsi $m_i = \dim \mathrm{Hom}_G(S_i, V)$ est intrinsèquement défini. □

Le *caractère* d'une représentation $\rho\colon G \to \mathrm{GL}(V)$ est la fonction

$$\chi\colon G \to \mathbb{C}, \quad g \mapsto \mathrm{Tr}\, \rho(g).$$

On note $\mathbb{C}[G]$ l'espace vectoriel des fonctions de G vers $\mathbb{C}$: on verra plus tard qu'on peut le munir d'une structure d'algèbre (produit interne = produit de convolution).

On appelle *fonction centrale* une fonction $f\colon G \to \mathbb{C}$ qui est constante sur chaque classe de conjugaison :

$$\forall g, h \in G, \quad f(ghg^{-1}) = f(h).$$

Lemme 10. (1) *Les fonctions centrales forment un sous-espace vectoriel (en fait une sous-algèbre) dont la dimension est le nombre de classes de conjugaison.*

(2) *Les caractères sont des fonctions centrales.*

Preuve. (1) On peut prendre comme base les fonctions indicatrices pour chaque classe de conjugaison.

(2) La trace est un invariant de conjugaison. □

Lemme 11. *Soient V et V' deux représentations complexes d'un groupe fini G, et soient χ et χ' leurs caractères respectifs. Alors le caractère de* $\mathrm{Hom}(V, V')$ *est $\bar{\chi}\chi'$.*

Preuve. Fixons $g \in G$. Soit $e_1, \ldots, e_d$ une base de vecteurs propres pour $\rho(g)$, et $\lambda_1, \ldots, \lambda_d$ les valeurs propres associées (avec éventuelles répétitions) : ce sont des racines de l'unité. De même notons $e'_1, \ldots, e'_{d'}$ et $\lambda'_1, \ldots, \lambda'_{d'}$ les vecteurs et valeurs propres de $\rho'(g)$. Une base de $\mathrm{Hom}(V, V')$ est donnée par les f_{ij} qui envoient e_i sur e'_j, et tous les autres e_k sur 0. Notons ρ_{Hom} la représentation induite par ρ, ρ' sur $\mathrm{Hom}(V, V')$. On a

$$\begin{aligned} \rho_{\mathrm{Hom}}(g)(f_{ij})(e_k) &= \rho'(g) \circ f_{ij} \circ \rho(g)^{-1}(e_k) \\ &= \begin{cases} \overline{\lambda_i}\lambda'_j e'_j & \text{si } i = k \\ 0 & \text{sinon.} \end{cases} \end{aligned}$$

Autrement dit f_{ij} est un vecteur propre de $\rho_{\mathrm{Hom}}(g)$, associé à la valeur propre $\overline{\lambda_i}\lambda'_j$. La valeur du caractère de $\mathrm{Hom}(V,V')$ en g s'en déduit :

$$\chi_{\mathrm{Hom}(V,V')}(g) = \sum_i \sum_j \overline{\lambda_i}\lambda'_j = \sum_i \overline{\lambda_i} \sum_j \lambda'_j = \overline{\chi(g)}\chi'(g). \qquad \square$$

On appelle *produit scalaire hermitien* de deux fonctions $\psi, \psi' \in \mathbb{C}[G]$ le nombre complexe :

$$\langle \psi, \psi' \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\psi(g)}\psi'(g).$$

Proposition 12. *Soient V et V' deux représentations complexes d'un groupe fini G, et soient χ et χ' leurs caractères respectifs. Alors :*

$$\langle \chi, \chi' \rangle = \dim \mathrm{Hom}_G(V, V').$$

En particulier :

(1) *Si V et V' sont irréductibles, alors*

$$\langle \chi, \chi' \rangle = \begin{cases} 1 & \text{si } V \simeq V', \\ 0 & \text{sinon.} \end{cases}$$

Autrement dit les caractères irréductibles forment une famille orthonormée.

(2)

$$V \simeq \bigoplus_{i \in \mathrm{Irr}(G)} S_i^{m_i} \text{ où } m_i = \langle \chi_i, \chi \rangle.$$

En particulier, deux représentations de mêmes caractères sont isomorphes («le caractère caractérise»).

(3)

$$\sum_{i \in \mathrm{Irr}(G)} m_i^2 = \langle \chi, \chi \rangle.$$

(4) *V est irréductible si et seulement si son caractère vérifie $\langle \chi, \chi \rangle = 1$.*

Preuve. On applique le lemme 7 à $W = \mathrm{Hom}(V, V')$, l'espace des morphismes linéaires de V vers V', pour obtenir par moyennisation un projecteur π sur $\mathrm{Hom}(V,V')^G$. On a

$$\begin{aligned} \dim \mathrm{Hom}_G(V,V') &= \dim \mathrm{Hom}(V,V')^G \\ &= \mathrm{Tr}\, \pi \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{\mathrm{Hom}(V,V')}(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\chi'(g) \\ &= \langle \chi, \chi' \rangle. \end{aligned}$$

(1) C'est le lemme de Schur.

(2) Voir proposition 9.

(3) Écrire $\chi = \sum m_i \chi_i$ et développer le produit hermitien $\langle \chi, \chi \rangle$.

(4) $\sum m_i^2 = 1$ ssi tous les m_i sont nuls sauf un égal à 1. $\square$

Les deux exemples suivants sont des constructions importantes de représentations.

Exemple 13 (Représentation par permutation)**.** Soit G un groupe fini agissant sur X un ensemble fini. On note $\mathbb{C}X$ l'espace vectoriel muni de la base canonique e_x indexée par X. On fait agir G sur $\mathbb{C}X$ en posant

$$\rho(g)(e_x) = e_{g \cdot x}.$$

On appelle ρ la *représentation par permutation* (associée à l'action de G sur X). On verra plus loin un moyen de construire des représentations irréductibles à partir de cet exemple.

Exemple 14 (Représentation régulière)**.** Soit G un groupe fini, et considérons l'action de G sur lui-même par translation à gauche (elle est simplement transitive). On appelle *représentation régulière* la représentation par permutation associée.

Théorème 15. *L'ensemble des caractères irréductibles de G est une base orthonormée de l'espace des fonctions centrales.*

En particulier le nombre de représentations irréductibles de G est égal au nombre de classes de conjugaison dans G.

Preuve. On sait déjà que les caractères irréductibles de G forment une famille orthonormée de fonctions centrales. Il reste à voir que cette famille est génératrice, ce qui revient à montrer que l'orthogonal de cette famille est le sous-espace trivial. Soit $f\colon G \to \mathbb{C}$ une fonction centrale orthogonale à tout caractère irréductible ; on veut montrer que f est identiquement nulle. Si $\rho\colon G \to \mathrm{GL}(V)$ est une représentation, on introduit l'endomorphisme suivant :

$$u = \frac{1}{|G|}\sum_{g\in G} f(g)\rho(g) \in \mathrm{End}(V).$$

On vérifie que u commute à tous les $\rho(g)$, autrement dit c'est un endomorphisme de représentations. Si ρ est irréductible, par le lemme de Schur u est une homothétie, dont le rapport est

$$\lambda = \frac{1}{\dim V}\operatorname{Tr} u = \frac{1}{\dim V}\frac{1}{|G|}\sum_{g\in G} f(g)\chi(g) = \frac{\langle \overline{\chi}, f\rangle}{\dim V}.$$

Par hypothèse f est orthogonale à tout caractère irréductible, donc $\lambda = 0$. Comme toute représentation est une somme de représentations irréductibles (Maschke), on obtient que u est toujours l'endomorphisme nul. Ceci s'applique en particulier à la représentation régulière ρ_{reg}, où V est donc l'espace vectoriel engendré par les symboles e_g, $g \in G$. Calculons en particulier $u(e_1)$:

$$0 = u(e_1) = \frac{1}{|G|}\sum_{g\in G} f(g)\rho(g)(e_1) = \frac{1}{|G|}\sum_{g\in G} f(g)e_g$$

ce qui implique $f(g) = 0$ pour tout g, comme attendu. □

La dernière touche théorique consiste à exhiber, via la représentation régulière, une relation sur la somme des carrés des degrés des représentations irréductibles.

Lemme 16. *Soit χ_{reg} le caractère de la représentation régulière d'un groupe fini G. On a :*

(1)
$$\forall g \in G, \quad \chi_{\mathrm{reg}}(g) = \begin{cases} |G| & \text{si } g = 1, \\ 0 & \text{sinon.} \end{cases}$$
En particulier la représentation régulière est fidèle.

(2) *Si χ est le caractère d'une représentation V, on a*
$$\langle \chi, \chi_{\mathrm{reg}}\rangle = \dim V.$$

(3) *En particulier, toutes les représentations irréductibles S_i apparaissent comme sous-représentation de la représentation régulière.*

(4) *On a la relation $|G| = \sum_i (\dim S_i)^2$.*

Preuve. (1) Si $g \neq 1$, on a $\mathrm{Fix}(g) = \emptyset$, donc la matrice de permutation associée n'a que des 0 sur la diagonale.

(2) Ecrire
$$\langle \chi, \chi_{\mathrm{reg}}\rangle = \frac{1}{|G|}\sum_{g\in G} \bar{\chi}(g)\chi_{\mathrm{reg}}(g) = \bar{\chi}(1) = \dim V.$$

(3) Appliquer la proposition 12(2).

(4) Écrire $\chi_{\mathrm{reg}} = \sum(\dim S_i)\chi_i$, et développer l'égalité $|G| = \langle \chi_{\mathrm{reg}}, \chi_{\mathrm{reg}}\rangle$.

□

Corollaire 17. *Un groupe G est abélien ssi tous ses caractères irréductibles sont de degré 1.*

Preuve. Un groupe est abélien ssi toutes ses classes de conjugaison sont ponctuelles, ce qui équivaut par ce qui précède à l'existence d'autant de représentations irréductibles, qui sont de degré 1 par la formule $|G| = \sum_i (\dim V_i)^2$. □

Remarque 18. Le résultat plus précis suivant est mentionné sans preuve dans [RW10] : le degré de tout caractère irréductible de G divise l'ordre de $G/Z(G)$.

1. Développement : Le cube et les représentations de S_4

1.1. Fiche technique.

1.1.1. *Synopsis.* Illustrer sur le cas des rotations préservant un cube comment retrouver les sous-groupes distingués à partir d'une table de caractères.

1.1.2. *Références.* [CG14, F18 p. 490 & F.26–29 p. 493]. Voir aussi [Pey04, p. 230–232].

1.1.3. *Leçons.*

- 101. Groupe opérant sur un ensemble. Exemples et applications
- 103. Exemples et applications des notions de sous-groupe distingué et de groupe quotient
- 104. Groupes finis. Exemples et applications
- 105. Groupe des permutations d'un ensemble fini. Applications
- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications
- 107. Représentations et caractères d'un groupe fini sur un C-espace vectoriel
- 161. Isométries d'un espace affine euclidien de dimension finie. Applications en dimensions 2 et 3
- 183. Utilisation des groupes en géométrie

1.2. **Représentation par permutation.** Pour construire une table de caractère on a besoin d'un procédé de construction de représentations irréductibles. Les représentations par permutations font souvent l'affaire.

Exemple 19 (Représentation par permutation)**.** Soit G un groupe fini agissant sur X un ensemble fini. On note $\mathbb{C}X$ l'espace vectoriel muni de la base canonique e_x indexée par X. On fait agir G sur $\mathbb{C}X$ en posant

$$\rho(g)(e_x) = e_{g\cdot x}.$$

On appelle ρ la *représentation par permutation* (associée à l'action de G sur X). On remarque que la somme $s = \sum e_x$ est invariante. On note V_X le quotient $\mathbb{C}X/\mathbb{C}s$, qui s'identifie à un sous-espace supplémentaire stable de $\mathbb{C}s$.

Proposition 20. *Soit G agissant sur un ensemble fini X, et V_X le quotient de la représentation par permutation associée (notations de l'exemple).*

(1) *Le caractère χ de la représentation est donné par*

$$\chi(g) = |\operatorname{Fix}(g)| - 1.$$

(2) *Si G agit deux fois transitivement sur X alors V_X est irréductible.*

Preuve. (1) Le caractère de la représentation par permutation avant quotient est $g \mapsto |\operatorname{Fix}(g)|$: un 1 sur la diagonale d'une matrice de permutation correspond à un point fixe. Par ailleurs la représentation triviale sur $\mathbb{C}s$ est de caractère identiquement 1. On conclut par additivité du caractère, en écrivant $\mathbb{C}X = V_X \oplus \mathbb{C}s$ (matriciellement on calcule la trace d'une matrice diagonale par blocs de taille $n-1$ et 1)

(2) Par le point précédent on a

$$\langle \chi, \chi \rangle = \frac{1}{|G|}\sum_g (|\operatorname{Fix}(g)| - 1)^2 = \frac{1}{|G|}\sum_g |\operatorname{Fix}(g)|^2 - 2\frac{1}{|G|}\sum_g |\operatorname{Fix}(g)| + 1$$

Comme l'action est transitive, la formule de Burnside donne

$$1 = \frac{1}{|G|}\sum_g |\operatorname{Fix}(g)|.$$

Le fait que l'action soit doublement transitive se traduit par le fait que l'action diagonale de G sur $X \times X$ admet deux orbites : la diagonale et son complément. La formule de Burnside appliquée à cette action donne donc

$$2 = \frac{1}{|G|}\sum_g |(X \times X)^g| = \frac{1}{|G|}\sum_g |\operatorname{Fix}(g)|^2$$

Finalement $\langle \chi, \chi \rangle = 2 - 2 + 1 = 1$, ce qui donne l'irréducibilité attendue. □

1.3. **La table des caractères de S_4.** On sait que le groupe des isométries directes (= les rotations) de $\mathbb{R}^3$ préservant un cube est isomorphe à S_4 (via l'action sur les 4 grandes diagonales).

Table de caractères :

$\boldsymbol{S_4}$	1 Id	6 $(**)$	8 $(***)$	6 $(****)$	3 $(**)(**)$
$\mathbf{1}$	1	1	1	1	1
ε	1	-1	1	-1	1
perm	3	1	0	-1	-1
$\varepsilon \otimes$ perm	3	-1	0	1	-1
via S_3	2	0	-1	0	2

"perm" est la représentation irréductible de degré 3 obtenue par permutation des 4 diagonales.

"via S_3" est la représentation irréductible de degré 2 obtenue par permutation des 3 paires de faces opposées.

ε est la représentation irréductible de degré 1 obtenue par permutation des 2 tétraèdres inscrits dans le cube : c'est aussi la signature.

On peut remarquer que la représentation $\varepsilon \otimes$ perm correspond à la représentation $S_4 \simeq \mathrm{Isom}^+(\text{cube}) \subset \mathrm{SO}_3(\mathbb{R})$ dont on est parti.

Proposition 21. *Résumé des propriétés d'une table de caractères :*

(1) *Chaque ligne distincte de la représentation triviale a "somme nulle" :*

$$\sum_g \chi(g) = 0.$$

(2) *Deux lignes distinctes sont orthogonales :*

$$\sum_g \overline{\chi(g)}\chi'(g) = 0.$$

(3) *La "norme" d'une ligne correspond au cardinal du groupe (caractérise l'irréducibilité) :*

$$\sum_g \overline{\chi(g)}\chi(g) = |G|.$$

(4) *La somme des carrés des dimensions donne le cardinal du groupe :*

$$\sum_i (\dim S_i)^2 = |G|.$$

(5) *La somme de chaque colonne distincte de la classe du neutre est nulle :*

$$\sum_i (\dim S_i)\chi_i(g) = 0.$$

(6) *Deux colonnes distinctes sont orthogonales :*

$$\sum_i \overline{\chi_i(h)}\chi_i(h') = 0.$$

Preuve. (1) Relation d'orthogonalité entre χ et le caractère de 1.

(2) Relation d'orthogonalité à nouveau.

(3) C'est la formule $\frac{1}{|G|}\sum_g \overline{\chi(g)}\chi(g) = \sum m_i^2$.

(4) Chaque représentation V_i apparaît avec multiplicité $\dim V_i$ dans la représentation régulière, qui est de dimension $|G|$.

(5) La représentation régulière est de caractère nul contre tout $g \neq 1$.

(6) Notons U la matrice de la table de caractères (lignes indicées par les caractères irréductibles, colonnes par les classes de conjugaison), et D la matrice diagonale de même dimension, où les termes diagonaux sont les $\dim S_i$. Il s'agit de réaliser qu'on sait déjà $UDU^* = |G|Id$, et que l'on veut montrer $|G|D^{-1} = U^*U$. Le passage de l'une à l'autre formule est alors facile :

$$UDU^* = |G|Id \quad \Rightarrow \quad \frac{1}{|G|}D = U^{-1}U^{*-1} \quad \Rightarrow \quad |G|D^{-1} = U^*U.$$

NB : on peut aussi établir cette formule d'orthogonalité entre colonne comme découlant d'un changement de base (fonctions caractéristiques en fonction des caractères irréductibles : c'est la transformée de Fourier). Voir [Mal81, 2.4 p. 40]. □

1.4. **Sous-groupes normaux.**

Proposition 22. *Soit G un groupe fini, et $\rho\colon G \to \mathrm{GL}(V)$ une représentation de caractère χ sur un $\mathbb{C}$-espace vectoriel V de dimension d. Alors*

$$\ker \rho = \{g \in G;\ \chi(g) = d\}.$$

Preuve. L'endomorphisme $\rho(g)$ est diagonalisable car d'ordre fini, et ses valeurs propres sont d racines de l'unités. La condition $\chi(g) = d$ implique que ces racines de l'unités sont toutes égales à 1, et donc que $\rho(g)$ est l'identité. □

Proposition 23. *Soit $H \lhd G$ un sous-groupe distingué d'un groupe fini. Alors H est l'intersection de noyaux de représentations irréductibles de G.*

Preuve. Soit $\pi\colon G \to G/H$ le morphisme quotient, et ρ_H la représentation régulière de G/H. Alors comme la représentation ρ_H est fidèle, H est le noyau de la représentation $\rho_H \circ \pi$. En écrivant $\rho_H \circ \pi$ comme une somme directe de représentations irréductibles, on obtient le résultat. □

Exemple 24. En contemplant la table de caractères, on retrouve les sous-groupes distingués (propres) de S_4 : V_4 et A_4.

2. Développement : Structure des groupes abéliens finis

2.1. **Fiche technique.**

2.1.1. *Synopsis.* On propose une preuve de la partie "existence" du théorème de structure des groupes abéliens finis, reposant sur les notions d'exposant d'un groupe, et de dual d'un groupe.

2.1.2. *Références.* [Col11, p. 252].

Certains livres (par exemple [RW10]) déduisent que G et $\hat{G}$ sont isomorphes à partir de la classification des groupes abéliens finis. Ici on a fait le chemin inverse, attention à ne pas utiliser simultanément deux sources incompatibles : typiquement [CG14] est Colmez-compatible, mais [Pey04] ne l'est pas du tout (il ne définit même pas le produit hermitien de la même façon !).

2.1.3. *Leçons.*

- 102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications
- 103. Exemples et applications des notions de sous-groupe distingué et de groupe quotient
- 104. Groupes finis. Exemples et applications
- 107. Représentations et caractères d'un groupe fini sur un C-espace vectoriel
- 108. Exemples de parties génératrices d'un groupe. Applications
- 110. Caractère d'un groupe abélien fini et transformée de Fourier discrète. Applications
- 159. Formes linéaires et dualité en dimension finie. Exemples et applications

2.2. **Théorie des représentations : cas particulier des groupes abéliens.** On commence par rappeler la définition de transformée de Fourier. Soit G un groupe abélien fini, on note $\hat{G}$ son dual défini comme le groupe des morphismes de G vers $\mathbb{C}^*$ (on peut faire la même définition dans le cas non abélien). Ces morphismes sont appelés *caractères linéaires*. Comme $\hat{G}$ correspond aux caractères irréductibles de G, et que les classes de conjugaison de G sont des singletons, la théorie générale dit que dans ce cas G et $\hat{G}$ ont même cardinal.

Les fonctions centrales coïncident maintenant avec l'algèbre $\mathbb{C}[G]$ de toutes les fonctions de G dans $\mathbb{C}$. Pour une telle fonction φ, on a

$$\varphi = \sum_{\chi \in \hat{G}} \langle \chi, \varphi \rangle \chi = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{\varphi}(\chi)\chi,$$

où on a introduit la notation $\hat{\varphi}(\chi) = |G|\langle \chi, \varphi \rangle = \sum \varphi(g)\chi(g)^{-1}$, c'est une fonction de $\hat{G}$ vers $\mathbb{C}$, on l'appelle la transformée de Fourier de φ. En particulier si δ_a est la fonction indicatrice qui vaut 1 en $a \in G$ et 0 ailleurs, on a

$$\hat{\delta}_a(\chi) = |G|\langle \chi, \delta_a \rangle = \chi(a)^{-1}.$$

2.3. **Le théorème de structure.** Le théorème de classification des groupes abéliens finis peut s'énoncer comme suit :

Théorème 25. *Soit G un groupe abélien fini (non trivial). Alors il existe une (unique) suite d'entiers $(a_i)_{i=1}^s$ tels que $a_{i+1} \mid a_i$ pour tout $i = 1, \dots s-1$, $a_s \geqslant 2$, et*

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_s\mathbb{Z}.$$

En particulier a_1 est l'exposant du groupe, et $\prod a_i$ est le cardinal du groupe.

Si G est un groupe fini, rappelons que son exposant est le PPCM des ordres de ses éléments. On aura pris soin de mettre l'énoncé suivant dans le plan :

Lemme 26. *Soit G un groupe abélien fini d'exposant m. Alors il existe $x \in G$ d'ordre m, en particulier pour tout $y \in G$ on a $y^m = 1$.*

Proposition 27. *Soit G un groupe abélien fini. Alors*

(1) *G et $\hat{\hat{G}}$ sont canoniquement isomorphes ;*
(2) *G et $\hat{G}$ ont même exposant.*

Preuve. (1) Il s'agit de voir que le morphisme naturel d'évaluation

$$\begin{aligned} \mathrm{ev} \colon G &\to \quad \hat{\hat{G}} \\ g &\mapsto (\chi \mapsto \chi(g)) \end{aligned}$$

est un isomorphisme. On a déjà remarqué que par la théorie générale, G et $\hat{G}$ (et donc également $\hat{\hat{G}}$) sont de même cardinal, il suffit donc de montrer l'injectivité.

Supposons que $a, b \in G$ vérifient $\chi(a) = \chi(b)$ pour tout $\chi \in \hat{G}$, ce qui revient à dire $\langle \chi, \delta_a \rangle = \langle \chi, \delta_b \rangle$ pour tout χ. Cela implique $\delta_a = \delta_b$, et donc $a = b$ comme attendu.

(2) Notons m l'exposant de G. Soit $\chi \in \hat{G}$. Pour tout $g \in G$ on a

$$1 = \chi(g^m) = \chi^m(g).$$

Ainsi l'exposant de $\hat{G}$ divise m. De même l'exposant de $\hat{\hat{G}}$ divise celui de $\hat{G}$, et par la première assertion on en déduit que ces trois exposants sont égaux. □

Preuve de la partie "existence" du théorème. Le résultat est clair pour un groupe G cyclique. On procède maintenant par récurrence sur $|G|$, en supposant de plus G non cyclique. Soit m l'exposant de G, qui est aussi l'exposant de $\hat{G}$ par la proposition. Soit $\chi \in \hat{G}$ d'ordre m. Le morphisme χ est à valeurs dans le groupe U_m des racines $m$ièmes de l'unité (car l'ordre de chaque $g \in G$, et donc aussi chaque $\chi(g)$, est un diviseur de m), de plus ce morphisme est surjectif (sinon χ serait d'ordre un diviseur strict de m). Il existe donc $g \in G$ tel que $\chi(g) = e^{2i\pi/m}$. En particulier g est d'ordre m, et χ est encore surjectif en restriction à $\langle g \rangle$. Soit K le noyau de χ, on a une structure de produit direct $G = \langle g \rangle \times K$ (où K est non trivial puisque G est supposé non cyclique). On conclut en appliquant l'hypothèse de récurrence à K, et en remarquant que l'exposant de K (comme celui de tout sous-groupe) divise celui de G. □

Concernant l'unicité, on peut l'obtenir à partir du résultat suivant, ce qui donne une alternative à l'argument habituel via la décomposition en p-groupes.

Proposition 28. *Soient G, H, G', H' des groupes finis. Si $G \simeq G'$ et $G \times H \simeq G' \times H'$, alors $H \simeq H'$.*

Preuve. Avant de commencer la preuve proprement dite, introduisons les notations suivantes. Étant donnés deux groupes finis G_1, G_2, notons $m(G_1, G_2) \geqslant 1$ le nombre de morphismes de G_1 vers G_2, et $i(G_1, G_2) \geqslant 0$ le nombre de morphismes injectifs. Le théorème de factorisation $G_1/\ker\varphi \simeq \varphi(G_1)$ implique immédiatement que

$$m(G_1, G_2) = \sum_{N \lhd G_1} i(G_1/N, G_2). \qquad (\dagger)$$

Pour tout groupe fini L, on a

$$m(L, G) \cdot m(L, H) = m(L, G \times H) = m(L, G' \times H') = m(L, G') \cdot m(L, H').$$

On en déduit, puisque $m(L, G) = m(L, G') \geqslant 1$, que

$$m(L, H) = m(L, H').$$

Par récurrence sur l'ordre de L, on déduit de (†) que $i(L,H) = i(L,H')$, et en particulier en prenant $L = H$:

$$1 \leqslant i(H,H) = i(H,H').$$

Ainsi il existe un morphisme injectif de H vers H', et ces deux groupes ayant même cardinal, ce morphisme est un isomorphisme. □

Malheureusement je n'ai pas de référence pour cette proposition, à part ce blog internet : blog Mathematical Notes.

Preuve de la partie "unicité" du théorème. Supposons qu'il existe des groupes cycliques $(U_i)_{i=1}^r$ et $(U_i')_{i=1}^s$, avec pour tout i :

$$|U_{i+1}| \text{ divise } |U_i|, \quad |U_{i+1}'| \text{ divise } |U_i'|,$$

et

$$G \simeq U_1 \times \cdots \times U_r \simeq U_1' \times \cdots \times U_s'.$$

On a vu que $U_1 \simeq U_1'$ est un groupe cyclique d'ordre l'exposant de G, et par la proposition 28 on en déduit que

$$U_2 \times \cdots \times U_r \simeq U_2' \times \cdots \times U_s'.$$

On conclut par récurrence sur l'ordre de G. □

Remarque 29. Encore une fois : il est vrai que dans le cas abélien G et $\hat{G}$ sont isomorphes, mais typiquement cela se déduit du théorème de structure que l'on vient de montrer : il ne faut donc pas l'utiliser dans la preuve ! Ici on s'est contenté de renforcer la remarque initiale sur l'égalité des ordres $|G| = |\hat{G}|$ par une égalité des exposants.

3. Développement : Théorème de Molien

3.1. Fiche technique.

3.1.1. *Synopsis.* Une motivation historique pour le développement de la théorie des représentation est l'étude de sous-groupes finis de $GL(V)$, où V est l'espace vectoriel des polynômes en n variables. Comprendre les polynômes laissés fixes par un tel groupe est une question basique, le théorème de Molien permet de calculer les dimensions de tels polynômes invariants, homogènes et d'un degré donné.

3.1.2. *Références.* [CG14, p. 497], [Pey04, p. 219 et 288], [RW10, p. 320], [CLO97, Chapter 7 §2] excellent complément pour le contexte...

3.1.3. *Leçons.*

- 101. Groupe opérant sur un ensemble. Exemples et applications
- 104. Groupes finis. Exemples et applications
- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications
- 107. Représentations et caractères d'un groupe fini sur un C-espace vectoriel
- 142. Algèbre des polynômes à plusieurs indéterminées. Applications
- 151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications

  Possible à défendre : c'est un résultat sur les dimensions des invariants ; illustre le rang d'un projecteur qui vaut sa trace...
- 152. Déterminant. Exemples et applications

  Pas mon préféré sur cette leçon, mais plausible (le déterminant intervient ici via la formule donnant le polynôme caractéristique, qui doit en tout cas être proprement introduite dans cette leçon).
- 154. Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications

  Plausible. Un sous-espace invariant est un exemple particulier de sous-espace stable. Mettre en avant l'argument de la construction du projecteur de Reynolds sur l'espace fixe par le groupe...

- 155. Endomorphismes diagonalisables en dimension finie

  Bon... Illustre certes le fait que quand dans le contexte d'un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$, toutes les matrices en vue sont diagonalisables car annulées par un polynôme scindé à racine simple $X^k - 1$... Un peu ténu, quand même...

3.2. On considère l'action (à gauche) de $\mathrm{GL}_n(\mathbb{C})$ sur l'espace E des formes linéaires en n variables, c'est-à-dire de la forme $a_1X_1 + \cdots + a_nX_n$, en prenant comme base de E les X_i.

On prolonge cette action à l'espace $\mathbb{C}[X_1, \ldots, X_n]$ de tous les polynômes en posant, pour $P = \sum a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$:

$$A \cdot P := \sum a_{i_1 \ldots i_n} (A \cdot X_1)^{i_1} \ldots (A \cdot X_n)^{i_n}.$$

Cette action se restreint à chaque sous-espace $V_d = \mathbb{C}[X_1, \ldots, X_n]_d$ des polynômes homogènes de degré d, on note ρ_d et χ_d les représentation et caractère associés.

Exemple 30 ([CG14, p. 405])**.** Si $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ on a

$$\begin{aligned} A \cdot X_1 &= aX_1 + bX_2, \\ A \cdot X_2 &= cX_1 + dX_2, \\ A \cdot X_1X_2 &= acX_1^2 + (ad + bc)X_1X_2 + bdX_2^2, etc... \end{aligned}$$

Remarque 31. Dans de nombreuses sources (en particulier internet) on trouve des tentatives de définition directe de l'action de $\mathrm{GL}_n(\mathbb{C})$ sur $\mathbb{C}[X_1, \ldots, X_n]$, du style donnée par

$$A \cdot P(X_1, \ldots, X_n) = P((X_1, \ldots, X_n)A^t).$$

Le problème c'est que soit on obtient une action à DROITE, soit on est obligé de mettre un A^{-1} quelque part dans la définition pour récupérer une action à gauche, mais le moindre calcul pratique devient un cauchemard. La définition ci-dessus tirée de Caldero-Germoni semble la plus naturelle, et la plus simple en pratique...

Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$. On s'intéresse à l'anneau $\mathbb{C}[X_1, \ldots, X_n]^G$ des polynômes invariants sous l'action de G, et en particulier au problème de déterminer des générateurs, que l'on peut choisir homogènes. Le théorème de Molien indique dans quels degrés il faut chercher de tels polynômes homogènes générateurs, et permet également d'expliciter les relations entre de tels générateurs.

Théorème 32 ([CG14, F. 40 p. 500])**.** *On a l'égalité entre séries formelles*

$$\frac{1}{|G|} \sum_{A \in G} \frac{1}{\det(I - tA)} = \sum_{d \geqslant 0} \dim \left(V_d^G\right) \, t^d$$

Lemme 33. (1) *Pour tout $A \in G$, de valeurs propres λ_i, on a*

$$\chi_d(A) = \sum_{\substack{(d_i) \in \mathbb{N}^n \\ \sum d_i = d}} \left(\prod_i \lambda_i^{d_i}\right)$$

(2) *Pour tout $A \in G$, on a*

$$\frac{1}{\det(I - tA)} = \sum_{d \geqslant 0} \chi_d(A) t^d.$$

(3) *Pour tout $d \geqslant 0$, on a*

$$\dim V_d^G = \frac{1}{|G|} \sum_{A \in G} \chi_d(A).$$

Preuve. (1) [CG14, F. 38 p. 498] Comme A est d'ordre fini, elle est diagonalisable (elle admet un polynôme annulateur scindé de la forme $X^k - 1$). Notons $\lambda_1, \ldots, \lambda_n$ ses valeurs propres (avec éventuelle répétition), et $D = UAU^{-1} = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ la matrice diagonale semblable à A. L'isomorphisme $P \in V_d \mapsto U \cdot P \in V_d$ est un isomorphisme de G-représentations, entre la

représentation initiale est celle conjuguée par U :

$$\begin{array}{ccc} \mathbb{C}_d[X_1,\dots,X_n] & \xrightarrow{\rho_d} & \mathbb{C}_d[X_1,\dots,X_n] \\ P & & A\cdot P \\ \downarrow{\scriptstyle \cdot U} & & \downarrow{\scriptstyle \cdot U} \\ \mathbb{C}_d[X_1,\dots,X_n] & \xrightarrow{U\rho_d U^{-1}} & \mathbb{C}_d[X_1,\dots,X_n] \\ U\cdot P & & (UAU^{-1})\cdot(U\cdot P) \\ & & = U\cdot(A\cdot P) \end{array}$$

Les monômes $\prod x_i^{d_i}$ avec $\sum d_i = d$ forment une base de vecteurs propres pour l'action de D sur V_d, et donc

$$\chi_d(A) = \chi_d(D) = \sum_{\substack{(d_i)\in\mathbb{N}^n \\ \sum d_i = d}} \left(\prod_i \lambda_i^{d_i}\right)$$

(2) [CG14, F. 39 p. 499] Reprenons les notations précédentes, et écrivons le polynôme caractéristique de A :

$$\det(xI - A) = \prod(x - \lambda_i).$$

En posant $x = 1/t$, et en multipliant les deux côtés de l'égalité par t^n, on obtient

$$\det(I - tA) = t^n \det(\tfrac{I}{t} - A) = \prod(1 - \lambda_i t).$$

Comme $(1-\lambda_i t)^{-1} = \sum_{d_i \geqslant 0} \lambda_i^{d_i} t^{d_i}$, en faisant le produit de Cauchy de n telles sommes formelles on obtient (la dernière égalité est le lemme précédent)

$$\frac{1}{\det(I - tA)} = \prod(1 - \lambda_i t)^{-1} = \sum_{d\geqslant 0} \sum_{\substack{(d_i)\in\mathbb{N}^n \\ \sum d_i = d}} \left(\prod_i \lambda_i^{d_i}\right) t^d = \sum_{d\geqslant 0} \chi_d(A) t^d.$$

(3) [CG14, F. 40 p. 500] On sait (et on a écrit dans le plan !) que si G est un sous-groupe fini agissant linéairement sur un espace vectoriel V_d, alors la moyenne des éléments dans $\mathrm{GL}(V_d)$

$$\pi = \frac{1}{|G|} \sum_{A\in G} \rho_d(A)$$

est le projecteur (dit de Reynolds) sur le sous-espace fixe par G. En particulier la dimension du sous-espace fixe est égal au rang de π qui (parce-que c'est un projecteur) est aussi la trace de π, et finalement

$$\dim V_d^G = \operatorname{Tr} \pi = \frac{1}{|G|} \sum_{A\in G} \chi_d(A).$$

□

Preuve du théorème. On conclut en écrivant

$$\begin{aligned} \frac{1}{|G|} \sum_{A\in G} \frac{1}{\det(I - tA)} &= \frac{1}{|G|} \sum_{A\in G} \sum_{d\geqslant 0} \chi_d(A) t^d && \text{(par (2))} \\ &= \sum_{d\geqslant 0} \left(\frac{1}{|G|} \sum_{A\in G} \chi_d(A) \right) t^d && \text{(addition de séries formelles)} \\ &= \sum_{d\geqslant 0} \dim\left(V_d^G\right)\, t^d && \text{(par (3))} \end{aligned}$$

□

Remarques 34.

(1) Savoir calculer la dimension de V_d (choisir $n-1$ séparations parmi $d+n-1$ objets, on obtient $\binom{d+n-1}{n-1}$).

(2) En quoi le terme de gauche du théorème est-il une série formelle ?

(3) Savoir traiter un exemple simple, par exemple $G = \mathbb{Z}/2\mathbb{Z}$. (voir plus bas)

(4) Avoir une idée de l'utilité de la formule de Molien, connaître les cas $G = S_n$ et $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, voir [CLO97].

(5) Un théorème de Noether intéressant à connaître pour culture (voir [CLO97, Theorem 5 p. 331]) : l'algèbre $\mathbb{C}[X_1,\dots,X_n]^G$ est engendrée par des polynômes homogènes de degré au plus $|G|$. Pour trouver des candidats à former un système de générateurs, on peut donc projeter (par π, l'opérateur de Reynolds) des polynômes de degré $\leqslant |G|$.

Exemple 35 ([CG14, F.43 p. 501])**.** On fait agir $G = \{\pm \mathrm{Id}\} \subset \mathrm{GL}_2(\mathbb{C})$ sur $\mathbb{C}[x,y]$, ce que l'on peut aussi voir comme une action de $\mathbb{Z}/2\mathbb{Z}$ via

$$\bar{1} \cdot P(x,y) = P(-x,-y).$$

Comme un monôme $x^a y^b$ est invariant ssi $a+b$ est pair, on déduit que la série de Molien est

$$S(t) = 1 + 3t^2 + 5t^4 + \cdots + (2k+1)t^{2k} + \ldots$$

La formule théorique est (vérifier qu'elles coïncident !)

$$\begin{aligned} S(t) &= \frac{1}{2}\left(\frac{1}{\det\left(\begin{smallmatrix}1-t & 0\\ 0 & 1-t\end{smallmatrix}\right)} + \frac{1}{\det\left(\begin{smallmatrix}1+t & 0\\ 0 & 1+t\end{smallmatrix}\right)}\right) \\ &= \frac{1}{2}\left(\frac{1}{(1-t)^2} + \frac{1}{(1+t)^2}\right) \\ &= \frac{1}{2}\left(\frac{1+t^2+2t+1+t^2-2t}{(1-t^2)^2}\right) \\ &= \frac{1+t^2}{(1-t^2)^2} \end{aligned}$$

On considère maintenant l'algèbre $\mathbb{C}[u,v,w]$, l'élément $a = uv - w^2$, et le morphisme surjectif

$$\pi \colon \mathbb{C}[u,v,w] \to \mathbb{C}[x,y]^G = \mathbb{C}[x^2,y^2] \oplus xy\mathbb{C}[x^2,y^2]$$

défini par $\pi(u) = x^2$, $\pi(v) = y^2$, $\pi(w) = xy$. On veut montrer que $\mathbb{C}[u,v,w]/(a) \to \mathbb{C}[x,y]^G$ est un isomorphisme (d'espaces vectoriels gradués). Pour cela on va montrer que $\mathbb{C}[u,v,w]/(a)$ est une algèbre graduée de série génératrice $S(t)$ (en suivant plus ou moins [CG14, F.37 p. 497]), ce qui donnera l'injectivité degré par degré.

On munit $\mathbb{C}[u,v,w]$ d'une graduation en posant chacune des variables de poids 2. La série $\frac{1}{1-ut^2} = 1 + ut^2 + u^2t^4 + \ldots$ correspond pour $u=1$ à la série de la sous-algèbre $\mathbb{C}[u]$ (avec u de poids 2), et

$$\frac{1}{1-ut^2} \cdot \frac{1}{1-vt^2} \cdot \frac{1}{1-wt^2}$$

correspond pour $u=v=w=1$ à la série de $\mathbb{C}[u,v,w]$, qui s'écrit donc

$$\frac{1}{(1-t^2)^3}.$$

Maintenant considérons le morphisme $\mathbb{C}[u,v,w] \to \mathbb{C}[u,v,w]$, qui envoie $P(u,v,w)$ sur $aP(u,v,w)$ (rappel : $a = uv - w^2$). Cela donne un isomorphisme (d'espaces vectoriels gradués, pas d'algèbre) de $\mathbb{C}[u,v,w]$ vers l'idéal (a), qui augmente la graduation de 4. Donc la série génératrice de (a) est

$$\frac{t^4}{(1-t^2)^3},$$

et celle du quotient est

$$\frac{1}{(1-t^2)^3} - \frac{t^4}{(1-t^2)^3} = \frac{1+t^2}{(1-t^2)^2} = S(t).$$

NB : Il existe d'autres preuves que $(x^2)(y^2) - (xy)^2$ est bien la seule relation entre les générateurs, mais ce n'est jamais complètement trivial (voir [CLO97, Example 4 et 5 p. 340]). L'intérêt est toujours d'illustrer une méthode qui peut s'adapter à des groupes finis plus compliqués.

Si on veut s'entrainer sur un exemple moins "évident", on pourra chercher à retrouver par la méthode des séries de Molien le fait que si G est le groupe cyclique d'ordre 4 engendré par $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$, alors

$$\mathbb{C}[x,y]^G = \mathbb{C}[x^2+y^2, x^3y - xy^3, x^2y^2] \simeq \mathbb{C}[u,v,w]/(u^2w - v^2 - 4w^2).$$

4. Développement : Représentations réelles et groupes d'ordre 8

4.1. **Fiche technique.**

4.1.1. *Synopsis.* On illustre sur le cas de D_4 et $\mathbb{H}_8$ la notion d'indicatrice de Frobenius-Schur, qui permet de repérer qu'une représentation définie a priori sur les complexes est isomorphe à une représentation définie sur les réels.

4.1.2. *Références.* [CG14, p. 477–482]

4.1.3. *Leçons.*

- 103. Exemples et applications des notions de sous-groupe distingué et de groupe quotient
- 104. Groupes finis. Exemples et applications
- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications
- 107. Représentations et caractères d'un groupe fini sur un C-espace vectoriel
- 158. Matrices symétriques réelles, matrices hermitiennes
- 171. Formes quadratiques réelles. Coniques. Exemples et applications

4.2. **Table de caractères.** Table de caractères du groupe quaternionique $\mathbb{H}_8$: il y a cinq classes de conjugaison, qui sont Id, $-\mathrm{Id}$, $\pm I$, $\pm J$ et $\pm K$, où

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

On note ρ_I la représentation irréductible (de degré 1) induite par la représentation par permutation de $\mathbb{H}_8$ agissant sur les deux classes à gauche modulo $\langle I \rangle$. Idem pour ρ_J et ρ_K.

$\mathbb{H}_8$	1 Id	1 $-\mathrm{Id}$	2 $\pm I$	2 $\pm J$	2 $\pm K$	$\frac{1}{\lvert G\rvert}\sum_g \chi(g^2)$
1	1	1	1	1	1	1
ρ_I	1	1	1	-1	-1	1
ρ_J	1	1	-1	1	-1	1
ρ_K	1	1	-1	-1	1	1
via SU_2	2	-2	0	0	0	-1

Si ρ est la représentation (de dimension 3) induite par la représentation par permutation de $\mathbb{H}_8$ agissant sur les classes à gauche modulo $\langle -\mathrm{Id} \rangle$, on calcule via les caractères que $\rho = \rho_I \oplus \rho_J \oplus \rho_K$.

Table de caractères de D_4 : il y a cinq classes de conjugaison, qui sont Id, S_O, S_{diag}, S_{axe}, $R_{\pm\pi/2}$. Le groupe D_4 agit par permutation sur les deux diagonales, sur les deux axes par les milieux de côtés opposés, et sur les deux orientations possibles du plan.

$\boldsymbol{D_4}$	1 Id	1 S_O	2 S_{diag}	2 S_{axe}	2 $R_{\pm\pi/2}$	$\frac{1}{\lvert G\rvert}\sum_g \chi(g^2)$
1	1	1	1	1	1	1
$perm_{diag}$	1	1	1	-1	-1	1
$perm_{axe}$	1	1	-1	1	-1	1
$perm_{ori}$	1	1	-1	-1	1	1
O_2	2	-2	0	0	0	1

La quantité $\frac{1}{|G|}\sum_g \chi(g^2)$, que l'on a fait apparaître dans les tables ci-dessus, s'appelle l'*indicatrice de Frobenius-Schur*.

4.3. **Représentation induite sur les matrices symétriques.** Si $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ est une représentation de caractère χ, on obtient une représentation ρ_{sym} dans l'espace des formes bilinéaires symétriques, qu'on identifie à l'espace $\mathcal{S}_n$ des matrices symétriques, en composant par

$$\begin{aligned} \mathrm{GL}_n(\mathbb{C}) &\to \mathrm{GL}(\mathcal{S}_n) \\ P &\mapsto (M \mapsto P^{-T} M P^{-1}) \end{aligned}$$

Les exposant -1 peuvent sembler compliqués, mais c'est la seule façon de maintenir la transposée à gauche de l'expression tout en obtenant une action à gauche, donc c'est une définition «naturelle»... Voir la remarque 38 pour plus de détails.

Lemme 36 ([CG14, B.19 p. 461])**.** *Le caractère de la représentation ρ_{sym} est*

$$\Psi\colon g \mapsto \frac{\chi(g^{-1})^2 + \chi(g^{-2})}{2}.$$

Si de plus ρ est irréductible et χ est à valeurs réelles, on a

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

où $\langle 1, \Psi\rangle$ s'interprète comme la dimension de l'espace des formes bilinéaires symétriques G-invariantes.

Preuve. Soit $g \in G$ fixé. Sur $\mathbb{C}^n$, on choisit une base qui diagonalise $\rho(g)$, et on note λ_i les valeurs propres de $\rho(g^{-1})$. Sur $\mathcal{S}_n$, on choisit comme base les $S_{i,j} = E_{i,j} + E_{j,i}$ somme de deux matrices élémentaires, avec $1 \leqslant i \leqslant j \leqslant n$. Alors $S_{i,j}$ est un vecteur propre de ρ_{sym}, de valeur propre $\lambda_i\lambda_j$. La trace de $\rho_{\mathrm{sym}}(g)$ est donc

$$\sum_{1\leqslant i\leqslant j\leqslant n}\lambda_i\lambda_j = \sum_{1\leqslant i\leqslant n}\lambda_i^2 + \sum_{1\leqslant i<j\leqslant n}\lambda_i\lambda_j = \frac{1}{2}\Big(\sum_{1\leqslant i\leqslant n}\lambda_i\Big)^2 + \frac{1}{2}\sum_{1\leqslant i\leqslant n}\lambda_i^2 = \frac{\chi(g^{-1})^2 + \chi(g^{-2})}{2}.$$

Pour la deuxième assertion, on écrit (les g^{-1} deviennent des g via un réindiçage...) :

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

et on remarque que l'hypothèse ρ irréductible et réel implique $1 = \langle\chi, \chi\rangle = \langle\bar{\chi}, \chi\rangle$. □

4.4. **Représentations réalisables sur $\mathbb{R}$.** Soit $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ une représentation de caractère χ. On dit que ρ se réalise sur $\mathbb{R}$ si ρ est isomorphe à une représentation ρ' qui provient d'une représentation $G \to \mathrm{GL}_n(\mathbb{R})$ via l'injection naturelle $\mathrm{GL}_n(\mathbb{R}) \hookrightarrow \mathrm{GL}_n(\mathbb{C})$. Si ρ se réalise sur $\mathbb{R}$ alors χ est à valeurs réelles. Par contre la réciproque est fausse : considérer la représentation de $\mathbb{H}_8$ dans $\mathrm{GL}_2(\mathbb{C})$ via les matrices I, J, K, les traces sont réelles pourtant $\mathbb{H}_8$ n'est pas isomorphe à un sous-groupe de $\mathrm{O}_2(\mathbb{R})$ (les sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$ sont cycliques ou diédraux).

Proposition 37 ([CG14, E.5 p. 478])**.** *Une représentation irréductible $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ est réalisable sur $\mathbb{R}$ si et seulement si $\frac{1}{|G|}\sum_{g\in G}\chi(g^2) = 1$.*

Preuve. On montre en fait que les trois assertions suivantes sont équivalentes :

(1) ρ est réalisable sur $\mathbb{R}$;

(2) Il existe une forme bilinéaire symétrique non nulle sur $\mathbb{C}^n$ invariante par G ;

(3) $\frac{1}{|G|}\sum_{g\in G}\chi(g^2) = 1$.

(1) ⇒ (2) : Un produit scalaire réel invariant (moyennisation) s'étend sur $\mathbb{C}$ en la forme bilinéaire invariante attendue.

(2) ⇒ (1) : Notons β la forme bilinéaire symétrique non nulle G-invariante : β est non dégénérée, car sinon son noyau correspondrait à une sous-représentation propre, en contradiction avec l'irréducibilité de ρ. Par ailleurs par moyennisation du produit standard on sait qu'il existe $\langle\cdot,\cdot\rangle$ un produit hermitien G-invariant (disons anti-linéaire par rapport à la première variable). Il existe alors $\varphi\colon \mathbb{C}^n \to \mathbb{C}^n$ semi-linéaire tel que $\beta(u, v) = \langle\varphi(u), v\rangle$:

$$\langle\varphi(\lambda u), v\rangle = \beta(\lambda u, v) = \lambda\beta(u, v) = \lambda\langle\varphi(u), v\rangle = \langle\bar{\lambda}\varphi(u), v\rangle.$$

L'itérée deuxième φ^2 est linéaire, on vérifie maintenant que sa matrice est hermitienne définie positive :

$$\begin{aligned}\langle\varphi^2(u), v\rangle = \beta(\varphi(u), v) = \beta(v, \varphi(u)) = \langle\varphi(v), \varphi(u)\rangle \\ = \overline{\langle\varphi(u), \varphi(v)\rangle} = \overline{\langle\varphi^2(v), u\rangle} = \langle u, \varphi^2(v)\rangle.\end{aligned}$$

et donc également

$$\langle\varphi^2(u), u\rangle = \langle\varphi(u), \varphi(u)\rangle.$$

Montrons que φ est G-invariante :

$$\langle\rho(g)\varphi(u), v\rangle = \langle\varphi(u), \rho(g)^{-1}v\rangle = \beta(u, \rho(g)^{-1}v) = \beta(\rho(g)u, v) = \langle\varphi(\rho(g)u), v\rangle.$$

Ainsi φ^2 est un G-endomorphisme d'une représentation irréductible, par le lemme de Schur on en déduit que φ^2 est une homothétie (de rapport un réel $\lambda > 0$). Alors φ (vu comme $\mathbb{R}$-endomorphisme de $\mathbb{R}^{2n}$) est annulé par $X^2 - \lambda$ et admet pour valeurs propres $\pm\sqrt{\lambda}$, d'espaces propres associés $V_\pm$. De plus la relation de semi-linéarité $\varphi(iv) = -i\varphi(v)$ implique que $iV_+ = V_-$. En particulier $\dim_{\mathbb{R}} V_+ = \dim_{\mathbb{C}} V$, et le complexifié de V_+ est V : autrement dit V_+ est une réalisation réelle de ρ.

(3) ⇒ (2) : Par le lemme 36 on obtient $\langle 1, \Psi \rangle = 1$, ainsi la multiplicité de la représentation triviale dans la représentation induite par ρ sur les matrices symétriques est 1, autrement dit il existe une forme bilinéaire invariante par ρ (unique à un facteur multiplicatif près).

(2) ⇒ (3) : Une forme bilinéaire (symétrique ou non) invariante s'identifie à un morphisme de représentation de V vers V^* (qui sont deux représentations irréductibles). Par le lemme de Schur 3, l'espace de tels morphismes est de dimension 1. On en déduit que l'espace des formes bilinéaires symétriques invariantes par ρ est ou bien trivial ou bien de dimension 1. On est ici dans le second cas, et par le lemme 36 cela équivaut à $\frac{1}{|G|}\sum \chi(g^2) = 1$. □

Remarque 38. Je développe ici l'identification entre $\mathrm{Hom}(V, V^*)$ et $\mathrm{Bil}(V)$. (Caldero-Germoni semblent dire que pour que ce soit compatible avec les actions de G il faut considérer la représentation de G dans $\mathrm{GL}(V)$ post-composée avec l'involution $M \mapsto M^{-T}$, mais la vérification ci-dessous semble dire que cela marche directement...).

D'abord les identitifications sans action, en termes matriciels (une base de $V \simeq \mathbb{C}^n$ étant choisie, et donc également une base duale pour V^*) :

- V s'identifie à l'espace des vecteurs colonnes ;
- Le dual $V^* = \mathrm{Hom}(V, \mathbb{C})$ s'identifie à l'espace des vecteurs lignes ;
- Les morphismes dans $\mathrm{Hom}(V, V^*)$ sont codés par des matrices carrées M, via
$$x \in V \mapsto x^T M \in V^*.$$
- Les formes bilinéaires dans $\mathrm{Bil}(V)$ sont aussi codées par des matrices M, via
$$(x, y) \in V \times V \mapsto x^T M y \in \mathbb{C}.$$

Maintenant on étudie la compatibilité avec l'action de G. On a quatre représentations à disposition :

- La représentation initiale $\rho \colon G \to \mathrm{GL}(V)$;
- La représentation ρ^* induite sur V^* par précomposition par $\rho(g)^{-1}$:
$$\begin{aligned} \rho^*(g) \colon V^* &\to V^* \\ y^T &\mapsto y^T \rho(g)^{-1} \end{aligned}$$
- La représentation ρ_{Hom} induite sur $\mathrm{Hom}(V, V^*)$ par précomposition par $\rho(g)^{-1}$ et post-composition par $\rho^*(g)$ (en accord avec la définition en bas de page 3) :
$$\begin{aligned} \rho_{\mathrm{Hom}}(g) \colon \mathrm{Hom}(V, V^*) &\to \mathrm{Hom}(V, V^*) \\ (x \mapsto x^T M) &\mapsto (x \mapsto x^T \rho(g)^{-T} M \rho(g)^{-1}) \end{aligned}$$
En effet on connait les trois étapes pour construire le terme de droite :
$$x \in V \mapsto \rho(g)^{-1} x \in V \mapsto x^T \rho(g)^{-T} M \in V^* \mapsto \rho^*(g)(x^T \rho(g)^{-T} M) \in V^*.$$
- La représentation ρ_{Bil} que l'on a défini sur les formes bilinéaires :
$$\begin{aligned} \rho_{\mathrm{Bil}}(g) \colon \mathrm{Bil}(V) &\to \mathrm{Bil}(V) \\ M &\mapsto \rho(g)^{-T} M \rho(g)^{-1} \end{aligned}$$

Ça colle !

5. Développement : Transformée de Fourier (rapide !) et multiplication de polynômes

5.1. Fiche technique.

5.1.1. *Synopsis.* Les naïfs multiplient les polynômes de degré n en $\mathrm{O}(n^2)$ opérations, les malins utilisent la FFT pour le faire en $\mathrm{O}(n \log n)$ opérations...

5.1.2. *Références.* Je me suis inspiré de notes d'étudiants de l'ENS Rennes, qui suivent le livre introuvable de Dasgupta and co [p. 64–78]. Voir aussi [Pey04, p. 118-119], et Demazure, chapitre 4 «Multiplication de polynômes».

5.1.3. *Leçons.*

- 102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications
- 104. Groupes finis. Exemples et applications ??
- 110. Caractère d'un groupe abélien fini et transformée de Fourier discrète. Applications
- 120. Anneaux Z/nZ. Applications ??
- 144. Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications

5.2. **Background : transformée de Fourier.** On rappelle qu'on note $\mathbb{C}[G]$ l'algèbre des fonctions de G dans $\mathbb{C}$ (centrales ou pas). On peut plonger G dans $\mathbb{C}[G]$, en identifiant $g \in G$ à la fonction δ_g qui vaut 1 en g et 0 ailleurs. Le produit interne sur $\mathbb{C}[G]$ est défini en étendant par linéarité le produit sur G, on obtient le produit de convolution : si $f_1 = \sum_g f_1(g)\delta_g$ et $f_2 = \sum_g f_2(g)\delta_g$,

$$f_1 * f_2 = \sum_{g\in G} \Big(\sum_{h\cdot k = g} f_1(h) f_2(k) \Big) \delta_g = \sum_{g\in G} \Big(\sum_{h\in G} f_1(h) f_2(h^{-1}g) \Big) \delta_g.$$

A noter qu'une fonction est centrale ssi elle est dans le centre de $\mathbb{C}[G]$ pour le produit de convolution ([Pey04, p. 214]). Pour un peu plus de détails voir [Pey04, 4.2 p.16] pour le cas d'un groupe abélien, [CG14, Annexe D p. 472] pour le cas général (eux notent $\mathbb{C}G$).

Diverses définitions de la transformée de Fourier :

(1) [Pey04, p. 212] On peut prolonger une représentation $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ en une application $\tilde{\rho}\colon \mathbb{C}[G] \to \mathrm{End}(\mathbb{C}^n)$, en posant pour tout $f = \sum f(g)\delta_g \in \mathbb{C}[G]$:

$$\tilde{\rho}(f) := \hat{f}(\rho) := \sum_{g\in G} f(g)\rho(g) \in \mathrm{End}(\mathbb{C}^n).$$

On définit alors la transformée de Fourier en appliquant cette construction aux représentations irréductibles de G :

$$\mathcal{F}\colon \mathbb{C}[G] \to \oplus_i \mathrm{End}(V_i)$$
$$f \mapsto (\hat{f}(\rho_i))_{i=1}^p$$

On peut montrer qu'il s'agit d'un isomorphisme d'algèbres. Noter que l'endomorphisme u introduit dans la preuve du théorème 15 correspond à $\tilde{\rho}(f)$: ce n'est pas exactement la transformée de Fourier de f, mais c'est proche.

NB : Peyré note $\tilde{\rho}_i(f)$ au lieu de $\hat{f}(\rho_i)$, il me semble pourtant que ma notation est plus cohérente avec ce qui suit ?

(2) Soit G un groupe abélien. On voudrait définir des $\hat{f}(\chi)$ qui soient à peu de chose près les coefficients de f quand on décompose f dans la base orthogonale des χ. Mais le diable ce cache dans les détails... Discussion de deux conventions possibles :

- Peyré [Pey04] : il définit (p. 3) le produit hermitien comme étant semi-linéaire sur la *deuxième* variable
$$\langle f, g\rangle = \frac{1}{|G|} \sum_{x\in G} f(x)\overline{g(x)}$$
puis il définit $\hat{f}(\chi) = \sum_{x\in G} f(x)\chi(x)$ de façon à obtenir (p. 14–15)
$$f = \frac{1}{|G|} \sum_{\chi\in \hat{G}} \hat{f}(\chi)\chi^{-1}.$$
- [CG14] : eux définissent (p. 455) le produit hermitien comme étant semi-linéaire sur la *première* variable
$$\langle \chi, \chi'\rangle = \frac{1}{|G|} \sum_{g\in G} \overline{\chi(g)}\chi'(g)$$
puis $\hat{f}(\chi) = \langle \chi, f\rangle = \frac{1}{|G|}\sum_g f(g)\bar{\chi}(g)$ de façon à obtenir (p. 470)
$$f = \sum_{\chi\in \hat{G}} \hat{f}(\chi)\chi.$$
[Col11] adopte ces mêmes conventions aussi bien pour le produit hermitien (p. 246) que pour $\hat{f}(\chi)$ (p. 250).

J'adopte la deuxième convention, et définis donc

$$\mathcal{F}\colon \mathbb{C}[G] \to \mathbb{C}[\hat{G}]$$
$$f \mapsto \hat{f}$$

où $\hat{f}$ est défini par $\hat{f}(\chi) := \frac{1}{|G|}\sum_g f(g)\bar{\chi}(g)$.

Proposition 39. *Soit G un groupe fini abélien, et $f_1, f_2 \in \mathbb{C}[G]$. On a*

$$\widehat{f_1 * f_2} = |G|^2 \hat{f}_1 \cdot \hat{f}_2.$$

En particulier l'application $f \mapsto |G|\hat{f}$ est un isomorphisme d'algèbre de $\mathbb{C}[G]$ vers $\mathbb{C}[\hat{G}]$.

Preuve. Pour tout $\chi \in \hat{G}$, on a

$$\begin{aligned}|G|^2 \hat{f}_1(\chi)\cdot\hat{f}_2(\chi) &= \sum_{h\in G} f_1(h)\bar{\chi}(h)\sum_{k\in G} f_2(k)\bar{\chi}(k)\\ &= \sum_{g\in G}\Big(\sum_{h\cdot k=g} f_1(h)f_2(k)\Big)\bar{\chi}(g)\\ &= \widehat{f_1 * f_2}(\chi).\end{aligned}$$

□

(3) [CG14, p. 470]. Soit $G = \mathbb{Z}/n\mathbb{Z}$, alors $\mathbb{C}[G]$ s'identifie à l'espace vectoriel $\mathbb{C}^n$. Il y a deux bases naturelles, indicées par les éléments de $\mathbb{Z}/n\mathbb{Z}$ (que l'on note sans barre, de 0 à $n-1$) : d'une part les fonctions indicatrices δ_i, et d'autre part les caractères linéaires $\chi_j : \bar{a} \in \mathbb{Z}/n\mathbb{Z} \mapsto (\omega^{-j})^a$, où ω est une racine primitive $n$ième de l'unité. Le choix de ω correspond à fixer un isomorphisme entre G et son dual $\hat{G}$. La transformée de Fourier $f \mapsto \hat{f}$ correspond donc au changement de base :

$$\begin{array}{ccc}\mathbb{C}^n & \to & \mathbb{C}^n\\ f = \sum_i f(i)\delta_i & \mapsto & f = \sum_j \hat{f}(j)\chi_j.\end{array}$$

où donc à nouveau

$$\hat{f}(j) = \frac{1}{n}\sum_i f(i)\bar{\chi}_j(i) = \frac{1}{n}\sum_i f(i)(\omega^j)^i.$$

A noter que mon choix de mettre un $-j$ en exposant dans la définition de χ_j se justifie pour simplifier l'expression de $\hat{f}(j)$, mais n'est en rien standard. D'autre part la base des δ_i est orthogonale mais pas orthonormée : chaque δ_i vérifie $\langle\delta_i,\delta_i\rangle = 1/n$, ce qui explique le facteur $1/n$ dans l'expression de $\hat{f}(j)$. Si on écrit l'égalité précédente sous forme matricielle, on pourra reconnaître une matrice déjà rencontrée en septembre dans la feuille de TD d'algèbre linéaire :

$$\begin{pmatrix}\hat{f}(0)\\ \hat{f}(1)\\ \vdots\\ \hat{f}(n-1)\end{pmatrix} = \frac{1}{n}\begin{pmatrix}1 & 1 & \dots & \dots & 1\\ 1 & \omega & \omega^2 & \dots & \omega^{n-1}\\ \vdots & & & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)(n-1)}\end{pmatrix}\begin{pmatrix}f(0)\\ f(1)\\ \vdots\\ f(n-1)\end{pmatrix}$$
$$= \frac{1}{n}A(\omega)\begin{pmatrix}f(0)\\ f(1)\\ \vdots\\ f(n-1)\end{pmatrix}$$

Comme les bases des δ_i et χ_j sont orthogonales, l'inverse de la matrice de passage $A = A(\omega)$ s'obtient à un facteur près comme la matrice adjointe :

$$A\cdot A^* = n\mathrm{Id}.$$

Comme de plus $A^* = A(\omega^{-1})$, on obtient

$$\left(\frac{1}{n}A(\omega)\right)^{-1} = A(\omega^{-1}).$$

5.3. **Exposé du problème.** Soit n un entier (grand, mais fixé une fois pour toute). On veut multiplier deux polynômes de degré au plus $n/2$ de façon algorithmiquement efficace.

Façon «naïve» : Représenter un polynôme via ses coefficients dans la base usuelle $1, X, \dots, X^n$. La multiplication de $P = \sum a_i X^i$ par $Q = \sum b_i X^i$ se fait en $O(n^2)$ opérations (où on rappelle que la notation $O(n^2)$ signifie une fonction de la forme $n^2 B(n)$ avec B bornée) :

$$PQ = \sum_{k=0}^{n} c_k X^k \text{ avec } c_k = \sum_{i=0}^{n/2} a_i b_{k-i}.$$

Façon «maline» : Représenter un polynôme via ses valeurs en $n+1$ points z_i, alors la multiplication se fait en $O(n)$ opérations.

Le problème est ramené à passer de façon efficace de la représentation «naïve» à la «maline», dans les deux sens : «évaluation» puis «interpolation». On va se rendre compte qu'il s'agit essentiellement de la même opération, et que l'on peut le faire rapidement (en $O(n \log n)$ opérations) via la transformée de Fourier rapide (FFT pour «Fast Fourier Transform») en choisissant les z_i des racines de l'unité.

5.4. **Evaluer rapidement un polynôme.** Pour évaluer $P = \sum_{i=0}^{n} a_i X^i$ en un point $z \in \mathbb{C}$, on peut utiliser la méthode d'Horner qui montre que cela se fait en $O(n)$ opérations :

$$a_n \overset{\cdot z + a_{n-1}}{\longrightarrow} a_n z + a_{n-1} \overset{\cdot z + a_{n-2}}{\longrightarrow} a_n z^2 + a_{n-1} z + a_{n-2} z^2 \longrightarrow \dots$$

ce qui revient à écrire $P(z)$ sous la forme

$$P(z) = a_0 + z(a_1 + z(a_2 + \dots + z(a_{n-1} + z a_n))).$$

Donc a priori pour évaluer P en les $n+1$ points z_i il faut $O(n^2)$ opérations. Cependant un choix symétrique des z_i permet de faire mieux. Supposons pour commencer que les points sont groupés par paires de points opposés $\pm z_1, \pm z_2, \dots, \pm z_{(n+1)/2}$ (disons $n+1$ est pair). Alors en regroupant monômes pairs et impairs on écrit P sous la forme

$$P(X) = P_1(X^2) + X P_2(X^2)$$

et l'on remarque que les calculs de $P(\pm z_i)$ se recoupent :

$$P(z_i) = P_1(z_i^2) + z_i P_2(z_i^2)$$
$$P(-z_i) = P_1(z_i^2) - z_i P_2(z_i^2)$$

On a donc ramené (à 2 multiplications et additions près) le problème initial sur un polynôme de degré n (donc avec $n+1$ coefficients) à deux problèmes similaires mais sur des polynômes de degré $(n-1)/2$ (donc avec $(n+1)/2$ coefficients). Si l'on peut poursuivre ce procédé de façon récursive on aura résolu le problème en temps $O(n \log n)$, en effet :

Lemme 40 ([Pey04, Proposition 2.4 p. 68])**.** *Supposons qu'une suite croissante $T(n)$ vérifie une relation de la forme (pour tout entier n pair, et une certaine constante a) :*

$$T(n) = 2T(n/2) + an$$

Alors $T(n) \sim an \log n$, où log *désigne le logarithme en base 2.*

Preuve. En divisant la relation par n et en écrivant $n = 2^x$, c'est-à-dire $x = \log n$, on obtient

$$\frac{T(2^x)}{2^x} = \frac{T(2^{x-1})}{2^{x-1}} + a.$$

Donc en prenant $b = T(1)$, on a $\frac{T(2^x)}{2^x} = ax + b$ pour tout x de la forme $x = \log n$ avec n pair, on en déduit $\frac{T(2^x)}{2^x} \sim ax$. □

L'observation cruciale est alors que si on prend n une puissance de 2, et z_i les racines $n$èmes de l'unité, alors on peut à chaque étape grouper les racines par paires de points opposés, et appliquer récursivement la stratégie ci-dessus. Reste à expliciter l'algorithme en termes d'algèbre linéaire, ce qui permettra de comprendre comment faire le chemin inverse «d'interpolation».

5.5. **L'algorithme.** De façon générale on a

$$\begin{pmatrix} P(z_0) \\ P(z_1) \\ \vdots \\ P(z_n) \end{pmatrix} = \begin{pmatrix} 1 & z_0 & z_0^2 & \dots & z_0^n \\ 1 & z_1 & z_1^2 & \dots & z_1^n \\ \vdots & & & & \vdots \\ 1 & z_n & z_n^2 & \dots & z_n^n \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix}$$

La matrice est une Vandermonde, en particulier inversible si les z_i sont deux à deux distincts. Prenons maintenant $z_n = \omega^n$, où $\omega = e^{2i\pi/n}$. La matrice devient

$$A(\omega) = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^n \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^n & \omega^{2n} & \dots & \omega^{n^2} \end{pmatrix} = \left(w^{ij}\right)_{0 \leqslant i,j \leqslant n}.$$

On reconnait la matrice de la transformée de Fourier. On peut paraphraser l'algorithme expliqué ci-dessus pour évaluer rapidement un polynôme en les racines de l'unité sous la forme matricielle suivante :

Lemme 41 (Fast Fourier Transform)**.** *La multiplication $v \mapsto A(\omega) \cdot v$ d'un vecteur de taille n peut s'effectuer en $O(n \log n)$ opérations.*

Preuve. L'idée est de regrouper les indices pairs et impairs dans le calcul, se ramener à un calcul par blocs de taille $n/2$, et de faire une récurrence sur n (figure 1). A préciser... □

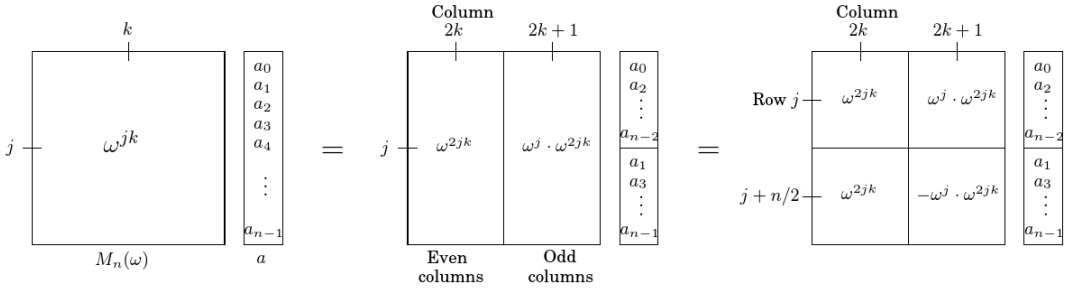

FIGURE 1. (Extrait de Dasgupta & al)

ANNEXE : LEÇONS OÙ L'ON PEUT (DOIT ?) PARLER DE REPRÉSENTATIONS

Disclaimer : liste imparfaite et non exhaustive. Faites appel à votre sens critique !

101. Groupe opérant sur un ensemble. Exemples et applications :

- Développement : Le cube et les représentations de S_4
- Développement : Théorème de Molien

102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications :

- Développement : Structure des groupes abéliens finis
- Développement : Transformée de Fourier (rapide !) et multiplication de polynômes

103. Exemples et applications des notions de sous-groupe distingué et de groupe quotient :

- Développement : Structure des groupes abéliens finis
- Développement : Le cube et les représentations de S_4
- Développement : Représentations réelles et groupes d'ordre 8

104. Groupes finis. Exemples et applications :

- Développement : Structure des groupes abéliens finis
- Développement : Représentations réelles et groupes d'ordre 8
- Développement : Le cube et les représentations de S_4

- Développement : Théorème de Molien

105. Groupe des permutations d'un ensemble fini. Applications :

- Développement : Le cube et les représentations de S_4

106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications :

- Développement : Représentations réelles et groupes d'ordre 8
- Développement : Le cube et les représentations de S_4
- Développement : Théorème de Molien

107. Représentations et caractères d'un groupe fini sur un C-espace vectoriel :

- Développement : Le cube et les représentations de S_4
- Développement : Représentations réelles et groupes d'ordre 8
- Développement : Structure des groupes abéliens finis
- Développement : Théorème de Molien

108. Exemples de parties génératrices d'un groupe. Applications :

- Développement : Structure des groupes abéliens finis

110. Caractère d'un groupe abélien fini et transformée de Fourier discrète. Applications :

- Développement : Structure des groupes abéliens finis
- Développement : Transformée de Fourier (rapide !) et multiplication de polynômes

120. Anneaux Z/nZ. Applications :

- Développement : Transformée de Fourier (rapide !) et multiplication de polynômes ? ?

142. Algèbre des polynômes à plusieurs indéterminées. Applications :

- Développement : Théorème de Molien

144. Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications :

- Développement : Transformée de Fourier (rapide !) et multiplication de polynômes ? ?

150. Exemples d'actions de groupes sur les espaces de matrices :

L'étude de la représentation $\mathrm{Hom}(V, V')$ (action sur des matrices rectangulaires après choix d'une base) induite par deux représentations V, V' est une idée clé de la théorie.

151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications :

- Développement : Théorème de Molien

On peut mentionner les représentations en illustration, par exemple :

- Le fait que la dimension des fonctions centrales correspond au nombre de caractères irréducitbles.
- Le fait qu'on obtienne un projecteur sur l'espace des invariants (et donc sa dimension) par moyennisation.
- Le fait que la multiplicité de S_i dans V correspond à $\dim \mathrm{Hom}_G(S_i, V)$.

152. Déterminant. Exemples et applications :

- Développement : Théorème de Molien

Il y a un lien entre déterminant circulant et transformée de Fourier, voir [Pey04, p. 19].

154. Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications :

- Développement : Théorème de Molien

Le plan peut contenir un paragraphe concernant les représentations.

155. Endomorphismes diagonalisables en dimension finie :

- Développement : Théorème de Molien ? ?

Le plan peut contenir un paragraphe concernant les représentations. (Je ne comprends pas toutes les pistes évoquées par Peyré sur son site web, à creuser...).

158. Matrices symétriques réelles, matrices hermitiennes :

- Développement : Représentations réelles et groupes d'ordre 8

On peut aussi mentionner le produit hermitien sur $\mathbb{C}[G]$ comme exemple de produit hermitien.

159. Formes linéaires et dualité en dimension finie. Exemples et applications :

- Développement : Structure des groupes abéliens finis

Le jury ne semble pas opposé à entendre parler de dualité dans le contexte des groupes (même si l'essentiel de la leçon doit se situer dans le contexte de l'algèbre linéaire).

161. Isométries d'un espace affine euclidien de dimension finie. Applications en dimensions 2 et 3 :

- Développement : Le cube et les représentations de S_4

171. Formes quadratiques réelles. Coniques. Exemples et applications :

- Développement : Représentations réelles et groupes d'ordre 8

Appel du pied explicite dans un des derniers rapports du jury...

183. Utilisation des groupes en géométrie :

- Développement : Le cube et les représentations de S_4

Références

[CG14] P. Caldero et J. Germoni. *Histoires hédonistes de groupes et de géométries, Tome second*. Calvage & Mounet, 2014.

[CLO97] D. A. Cox, J. Little, et D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, second edition, 1997.

[Col11] P. Colmez. *Éléments d'analyse et d'algèbre (2nde éd.)*. École Polytechnique, 2011.

[Mal81] M. Malliavin. *Les groupes finis et leurs représentations complexes*. Masson, 1981.

[Pey04] G. Peyré. *L'algèbre discrète de la transformée de Fourier*. Ellipses, 2004.

[RW10] J.-P. Ramis et A. Warusfel. *Cours de mathématique vol.1 algèbre et géométrie*. De Boeck, 2010.

[Ulm12] F. Ulmer. *Théorie des groupes*. ellipses, 2012.