REPRÉSENTATIONS COMPLEXES DES GROUPES FINIS

JEAN-MARC COUVEIGNES

RÉSUMÉ. On présente les résultats fondamentaux sur les représentations et caractères complexes des groupes finis.

TABLE DES MATIÈRES

Date: 30 novembre 2018.

1. Définitions et premiers exemples

Soit E un espace vectoriel de dimension $m \geqslant 1$ finie sur le corps $\mathbf{C}$ des nombres complexes. On note $\mathrm{End}(E)$ l'ensemble des applications linéaires de E dans E. On note $\mathrm{GL}(E)$ l'ensemble des applications linéaires bijectives de E dans E.

1.1. **Définitions.**

Soit G un groupe fini et

$$\rho : G \to \mathrm{GL}(E)$$

un morphisme de groupe. On lui associe une action de G sur E. Cette action est dite linéaire car elle est compatible avec la structure de $\mathbf{C}$-espace vectoriel sur E. On note souvent ρ_s au lieu de $\rho(s)$. Et pour v dans E on note $\rho_s(v)$ pour $(\rho(s))(v)$. Ou plus simplement $s.v$ ou encore ${}^s v$.

On dit que ρ est une **représentation linéaire** de G, et que E est un **espace de représentation**. La dimension m de E est appelée **degré** de la représentation.

Si B est une base de E on note R_s la matrice de ρ_s dans la base B. On définit ainsi un morphisme de groupes $R : G \to \mathrm{GL}_m(\mathbf{C})$. Le morphisme R définit une représentation sous **forme matricielle**. Pour $1 \leqslant i, j \leqslant m$ on note $r_{i,j}(s)$ le coefficient de R_s en position (i,j). On définit ainsi m^2 applications $r_{i,j}$ de G dans $\mathbf{C}$.

Soient $\rho : G \to \mathrm{GL}(E)$ et $\mu : G \to \mathrm{GL}(F)$ deux représentations linéaires du même groupe G. Une application linéaire $u : E \to F$ est dite **équivariante** si pour tout $s \in G$ on a

$$u \circ \rho_s = \mu_s \circ u.$$

On dit aussi que c'est un morphisme de représentations.

Si u est une bijection on dira que ρ et μ sont deux représentations **équivalentes**.

Si $\rho : G \to \mathrm{GL}(E)$ et $\mu : G \to \mathrm{GL}(F)$ sont deux représentations du même groupe on définit une représentation notée $\rho \oplus \mu$ et appelée **somme directe** des représentations ρ et μ. L'espace de représentation de $\rho \oplus \mu$ est $E \oplus F$. Pour tout $s \in G$ l'endomorphisme $(\rho \oplus \mu)_s$ de $E \oplus F$ associé à s est la somme directe des endomorphismes ρ_s et μ_s ainsi définie :

$$\begin{array}{rcl} (\rho \oplus \mu)_s : & E \oplus F \longrightarrow E \oplus F \\ & (e, f) \longmapsto (\rho_s(e), \mu_s(f)). \end{array}$$

Si B est une base de E et C une base de F alors la réunion de B et C est une base de $E \oplus F$. Soit m la dimension de E et n la dimension de F. Soit $R : G \to \mathrm{GL}_m(\mathbf{C})$ la représentation matricielle associée à ρ et B. Soit $M : G \to \mathrm{GL}_n(\mathbf{C})$ la représentation matricielle associée à μ et C. La représentation matricielle associée à $\rho \oplus \mu$ et $B \cup C$ est notée $R \oplus M : G \to \mathrm{GL}_{m+n}(\mathbf{C})$. La matrice $(R \oplus M)_s$ est la matrice diagonale par blocs $\mathrm{Diag}(R_s, M_s)$.

1.2. **Représentations par permutation.** L'application $\sigma \to P_\sigma$ définit un morphisme

$$P : S_n \to \mathrm{GL}(\mathbf{C}^n)$$

du groupe symmétrique de degré n vers le groupe des automorphismes de l'espace des vecteurs colonnes de dimension n.

Si le groupe fini G agit à gauche transitivement sur un ensemble X de cardinal n on fixe une bijection entre X et $\{1, 2, \dots, n\}$ et l'on en déduit un isomorphisme entre l'ensemble $\mathrm{Sym}(X)$ des bijections de X et le groupe symmétrique $S_n = \mathrm{Sym}(\{1, 2, \dots, n\})$. On peut donc supposer que $X = \{1, 2, \dots, n\}$. On dit que l'on a numéroté les éléments de X. Une telle action de G sur $\{1, 2, \dots, n\}$ est décrite par un morphisme $\alpha : G \to S_n$. La composition $P \circ \alpha : G \to \mathrm{GL}(\mathbf{C}^n)$ est appelée représentation linéaire (matricielle) par permutation.

Une façon plus directe de construire cette représentation linéaire est de considérer un $\mathbf{C}$-espace vectoriel E de dimension n et une base $B = (b_x)_{x \in X}$ de E indexée par X. On définit alors pour tout s dans G l'application linéaire $\rho_s : E \to E$ par $\rho_s(b_x) = b_{s.x}$.

Dans le cas particulier où $X = G$ et G agit sur X par multiplication à gauche on obtient la **représentation régulière** de G. On a alors $E = \mathbf{C}^G$ et l'on note $(e_x)_{x \in G}$ la base canonique. On note $\rho_G : G \to \mathrm{GL}(\mathbf{C}^G)$ la représentation régulière. Pour $s \in G$ on a $\rho_G(s)(e_x) = e_{sx}$.

1.3. **Caractères multiplicatifs des groupes cycliques C_n.** Soit $n \geqslant 1$ un entier. On note C_n le groupe formé des puissances 1, r, $\dots$, r^{n-1} d'un élément r tel que $r^n = 1$. On dit que C_n est décrit par le générateur r et la relation $r^n = 1$. C'est le groupe cyclique d'ordre n. L'application de $(\mathbf{Z}/n\mathbf{Z}, +)$ dans C_n qui associe r^k à $k \bmod n$ est un isomorphisme de groupe entre $(\mathbf{Z}/n\mathbf{Z}, +)$ et $(C_n, \times)$.

Soit w un nombre complexe tel que $w^n = 1$. Il existe un unique entier h dans $[0, n[$ tel que $w = \exp(2i\pi h/n)$. On définit un morphisme de groupe

$$\chi_h : C_n \to \mathbf{C}^* = \mathrm{GL}(\mathbf{C})$$

en posant $\chi_h(r^k) = w^k = \exp(2i\pi hk/n)$.

On obtient ainsi n représentations linéaires de C_n de degré 1. Elles sont deux à deux non-isomorphes. On les appelle les **caractères multiplicatifs** du groupe cyclique C_n.

1.4. **Caractères multiplicatifs d'un groupe fini.** Plus généralement, pour G un groupe fini, on appelle **caractère multiplicatif** de G un morphisme de G dans $\mathbf{C}^*$. Les caractères multiplicatifs sont donc les représentations de degré 1 de G. L'ensemble des caractères multiplicatifs est noté

$$\hat{G} = \mathrm{Hom}(G, \mathbf{C}^*).$$

C'est un groupe commutatif. On le nomme le **groupe dual** de G.

Si G_1 et G_2 sont deux groupes finis et $\chi_1 \in \hat{G}_1$ et $\chi_2 \in \hat{G}_2$ des caractères multiplicatifs de G_1 et G_2 respectivement on définit un caractère multiplicatif χ de $G_1 \times G_2$ en posant

$$\chi(g_1, g_2) = \chi_1(g_1).\chi_2(g_2).$$

L'application $(\chi_1, \chi_2) \mapsto \chi$ est un morphisme de groupes

$$\alpha : \hat{G}_1 \times \hat{G}_2 \to \widehat{G_1 \times G}_2.$$

Si maintenant $\chi : G_1 \times G_2 \to \mathbf{C}^*$ est un caractère multiplicatif de $G_1 \times G_2$, la restriction de χ à

$$G_1 \times \{1_{G_2}\} \subset G_1 \times G_2$$

définit un caractère multiplicatif de G_1. Et la restriction de χ à

$$\{1_{G_1}\} \times G_2 \subset G_1 \times G_2$$

définit un caractère multiplicatif de G_2. L'application $\chi \mapsto (\chi_{|G_1 \times \{1_{G_2}\}}, \chi_{|\{1_{G_1}\} \times G_2\}})$ est un morphisme de groupes

$$\beta : \widehat{G_1 \times G_2} \to \hat{G}_1 \times \hat{G}_2.$$

On vérifie que $\beta \circ \alpha$ est l'identité de $\hat{G}_1 \times \hat{G}_2$ et $\alpha \circ \beta$ est l'identité de $\widehat{G_1 \times G_2}$. Donc le dual d'un produit cartésien est canoniquement isomorphe au produit cartésien des duaux.

Dans le cas d'un groupe cyclique C_n les caractères multiplicatifs sont en bijection avec les racines n-ièmes de l'unité. Et cette bijection est un isomorphisme de groupes.

Comme toute groupe commutatif est produit de groupes cycliques, on en déduit que le groupe dual $\hat{G}$ d'un groupe commutatif G est isomorphe à G. Cet isomorphisme n'est pas canonique en ce sens que l'on ne sait pas en choisir un plutôt qu'un autre dans l'ensemble des isomorphismes entre G et $\hat{G}$.

Considérons maintenant un groupe fini G non-nécessairement commutatif. Si a et b sont dans G on note $[a, b]$ et l'on appelle commutateur de a et b l'élément $aba^{-1}b^{-1}$. Si c est dans G, le conjugué par c du commutateur est le commutateur des conjugués :

$$c^{-1}[a, b]c = [c^{-1}ac, c^{-1}bc].$$

L'ensemble des commutateurs est donc stabilisé par tous les automorphismes intérieurs de G. On note $D(G)$ le sous-groupe engendré par les commutateurs. C'est un groupe distingué de G puisqu'il est engendré par un ensemble stabilisé par les automorphismes intérieurs. On l'appelle le **sous-groupe dérivé** de G. Le quotient $G/D(G)$ est abélien. C'est le plus grand quotient abélien de G. On l'appelle l'**abélianisé** de G et l'on le note $\mathrm{Ab}(G)$.

Soit $\chi : G \to \mathbf{C}^*$ un caractère multiplicatif. Pour tout commutateur $[a, b]$ on a

$$\chi([a, b]) = \chi(aba^{-1}b^{-1}) = \chi(a)\chi(b)\chi(a)^{-1}\chi(b)^{-1} = 1.$$

Donc le noyau de χ contient $D(G)$. Il existe un charactère multiplicatif $\rho : \mathrm{Ab}(G) \to \mathbf{C}^*$ de $\mathrm{Ab}(G)$ tel que χ soit la composition de ρ avec l'application quotient $G \to \mathrm{Ab}(G)$. Autrement dit

$$\hat{G} = \widehat{\mathrm{Ab}(G)}.$$

On obtient ainsi une description assez explicite des représentations linéaires de degré 1 des groupes finis.

1.5. **Rappel sur les isométries du plan réel.** On considère le plan affine réel $\mathbf{A}_2(\mathbf{R}) = \mathbf{R}^2$ muni de la distance usuelle. Une isométrie de $\mathbf{A}_2(\mathbf{R})$ est une application de $\mathbf{A}_2(\mathbf{R})$ dans $\mathbf{A}_2(\mathbf{R})$ qui conserve les distances. Les isométries sont des bijections. Elles forment un groupe pour la loi de composition. On montre que ce groupe est engendré par les réflexions. On note $\mathbf{O}_2(\mathbf{R})$ le groupe des isométries qui fixent l'origine O. Ce groupe est engendré par les réflexions d'axe passant par

O. Il est formé de l'identité, des rotations de centre O et des réflexions d'axe passant par O. Dans la base canonique, la matrice de la rotation de centre O et d'angle θ est

$$T(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

et la matrice de la réflexion d'axe horizontal est

$$M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

On vérifique que $M^2 = \mathrm{Id}$ et $MT(\theta)M = T(-\theta)$.

1.6. **Le groupe diédral D_n.** Soit $n \geqslant 2$ un entier. Le groupe D_n est d'ordre $2n$. Il contient un sous-groupe distingué isomorphe à C_n, engendré par r tel que $r^n = 1$. Il contient aussi un sous-groupe d'ordre 2 engendré par s tel que $s^2 = 1$. Les deux groupes $< r >$ et $< s >$ sont complémentaires et $srs = r^{-1}$. Autrement dit D_n est le produit semi-direct de $C_n =< r >$ et $C_2 =< s >$ pour l'action $sr^k s = r^{-k}$. On dit que D_n est donné par les les générateurs r et s et les relations $r^n = 1$, $s^2 = 1$ et $srs = r^{-1}$.

On définit un morphisme $\rho : D_n \to \mathrm{GL}_2(\mathbf{C})$ en posant

$$\rho(r) = T(2\pi/n) = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \text{ et } \rho(s) = M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

On vérifie que $(\rho(r))^n = \mathrm{Id}$, $(\rho(s))^2 = \mathrm{Id}$ et $\rho(s)\rho(r)\rho(s) = \rho(r)^{(-1)}$.

On a bien sûr $\rho(r^k) = \rho(r)^k = T(2\pi k/n)$ et $\rho(r^k s) = \rho(r)^k \rho(s)$. La représentation ρ est une représentation matricielle de degré 2 du groupe diédral D_n.

Posons maintenant

$$P = \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \text{ et } \mu(t) = P^{-1}\rho(t)P$$

pour tout $t \in D_n$. En particulier

$$\mu(r) = \begin{pmatrix} \exp(-2i\pi k/n) & 0 \\ 0 & \exp(2i\pi k/n) \end{pmatrix} \text{ et } \mu(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

On obtient une représentation matricielle $\mu : D_n \to \mathrm{PGL}_2(\mathbf{C})$ équivalente à ρ.

Soit maintenant h un entier. On définit un morphisme $\rho^h : D_n \to \mathrm{GL}_2(\mathbf{C})$ en posant

$$\rho^h(r) = T(2h\pi/n) = \begin{pmatrix} \cos(2\pi h/n) & -\sin(2\pi h/n) \\ \sin(2\pi h/n) & \cos(2\pi h/n) \end{pmatrix} \text{ et } \rho^h(s) = M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

et bien sûr $\rho^h(r^k) = \rho^h(r)^k = T(2\pi hk/n)$ et $\rho^h(r^k s) = \rho^h(r)^k \rho^h(s) = T(2\pi hk/n)M$.

Si $h \neq h' \bmod n$ et $h \neq -h' \bmod n$ alors les représentations (ρ^h) et $(\rho^{h'})$ ne sont pas équivalentes.

1.7. **Sous-représentations.** Soit E un $\mathbf{C}$-espace vectoriel de dimension finie. Soit G un groupe fini et $\rho : G \to \mathrm{GL}(E)$ une représentation linéaire de G. Soit F un sous-espace vectoriel de E stable par tous les ρ_s pour $s \in G$. Alors pour tout s la restriction de ρ_s à F est un isomorphisme de F. On obtient donc une représentation linéaire $\rho^F : G \to \mathrm{GL}(F)$. On dit que c'est une sous-représentation de ρ.

Par exemple, le sous-espace nul $\{0\} \subset E$ est stable. La représentation associée est la sous-représentation nulle.

Autre exemple : si $\rho_G : G \to \mathrm{GL}(\mathbf{C}^G)$ est la représentation régulière alors le sous-espace de dimension 1 engendré par $\sum_{x \in G} e_x$ est clairement stable par G. La sous-représentation correspondante est la **représentation unité**.

Théorème 1. *Soit E un $\mathbf{C}$-espace vectoriel de dimension finie. Soit G un groupe fini et $\rho : G \to \mathrm{GL}(E)$ une représentation linéaire de G. Soit F un sous-espace vectoriel de E stable par G. Il existe un supplémentaire H de F dans E qui est stable par G. La représentation ρ est somme directe de ses sous-représentations ρ^F et ρ^H.*

Soit K un supplémentaire de F dans E. Soit π le projecteur sur F parallèlement à K. On pose

$$\Pi = \frac{1}{\#G} \sum_{s \in G} \rho_s \circ \pi \circ \rho_s^{-1}. \tag{1}$$

On vérifie que

(1) la restriction de Π à F est l'identité,

(2) l'image de Π est F,

(3) Π commute à ρ_s pour tout $s \in G$.

Soit alors H le noyau de Π. C'est un supplémentaire de l'image F de Π et il est stable par tous les ρ_s. □.

1.8. **Représentations irréductibles.** Soit E un $\mathbf{C}$-espace vectoriel de dimension finie. Soit G un groupe fini et $\rho : G \to \mathrm{GL}(E)$ une représentation linéaire de G. On dit que ρ est irréductible si et seulement si E est non-nul et ρ n'admet pas d'autre sous-représentation que la représentation nulle et elle même.

Toute représentation de degré 1 est irréductible.

Soit $n \geqslant 2$. Soit h un entier tel que $2h \neq 0 \bmod n$. La représentation ρ^h du groupe diédral D_n introduite à la section 1.6 est irréductible.

Théorème 2. *Soit E un $\mathbf{C}$-espace vectoriel de dimension finie. Soit G un groupe fini et $\rho : G \to \mathrm{GL}(E)$ une représentation linéaire de G. Il existe des sous-espaces $(E_i)_{1 \leqslant i \leqslant I}$ de E stables par G tels que $E = \oplus_{1 \leqslant i \leqslant I} E_i$ et la restriction de ρ à chaque E_i est une représentation irréductible. Autrement dit ρ est somme directe de représentation irréductibles*

$$\rho = \oplus_{1 \leqslant i \leqslant I} \rho^{E_i}.$$

On raisonne par récurrence sur le degré n de la représentation. Si $n = 0$ alors E est nul et ρ est la représentation nulle. Elle est la somme directe d'aucune représentation.

Supposons $n \geqslant 1$. Si ρ est irréductible le théorème est vérifié. Sinon il existe un sous-espace stable F non-nul et différent de E. Soit H un supplémentaire de F dans E stable par G. Les représentations ρ^F et ρ^H sont de degré $< n$ donc chacune est somme directe de représentations irréductibles. Comme $\rho = \rho^F \oplus \rho^H$, il en va de même pour ρ. □.

1.9. **Produit tensoriel d'espaces vectoriels.** Soit K un corps. Soient E et F deux K-espaces vectoriels. Soit $B = (b_i)_{i\in I}$ une base de E. Soit $C = (c_j)_{j\in J}$ une base de F. L'espace vectoriel $K^{(I\times J)}$ est noté $E \otimes F$. Les vecteurs de sa base canonique sont indexés par le produit cartésien $I \times J$. On les note $(d_{(i,j)})_{(i,j)\in I\times J}$. Il existe une unique application bilinéaire $\varphi : E \times F \to E \otimes F$ telle que $\varphi(b_i, c_j) = d_{(i,j)}$. L'espace vectoriel $E \otimes F$ est appelé **produit tensoriel** de E et de F. Pour $e \in E$ et $f \in F$ on écrit souvent $e \otimes f$ au lieu de $\varphi(e, f)$. En particulier $d_{(i,j)} = b_i \otimes c_j$.

Soit maintenant H un K-espace vectoriel et soit $f : E \times F \to H$ une application bilinéaire. Il existe une unique application linéaire $\tilde{f} : E \otimes F \to H$ telle que $\tilde{f}(b_i \otimes c_j) = f(b_i, c_j)$. Donc il existe une unique application $\tilde{f}$ telle que le diagramme suivant commute

$$\begin{tikzcd} E \times F \arrow[rr, "f"] \arrow[dr, "\varphi"'] & & H \\ & E \otimes F. \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

Théorème 3. *Soit K un corps. Soient E et F deux K-espaces vectoriels. Il existe un espace vectoriel $E \otimes F$ et une application bilinéaire $\varphi : E \times F \to E \otimes F$ telle que la propriété suivante, appelée propriété universelle du couple $(E \otimes F, \varphi)$, soit satisfaite. Pour toute application bilinéaire $f : E \times F \to H$ il existe une unique application $\tilde{f}$ telle que le diagramme suivant commute*

$$\begin{tikzcd} E \times F \arrow[rr, "f"] \arrow[dr, "\varphi"'] & & H \\ & E \otimes F. \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

On note $\varphi(e, f) = e \otimes f$. Si $(b_i)_{i\in I}$ est une base de E et $(c_j)_{j\in J}$ une base de F alors les $b_i \otimes c_j$ forment une base de $E \otimes F$.

La propriété universelle implique l'unicité du produit tensoriel $(E \otimes F, \varphi)$ dans le sens suivant. Si $(E \otimes' F, \varphi')$ satisfait lui aussi la propriété universelle alors il existe un unique isomorphisme $\tilde{\varphi}$ tel que le diagramme suivant commute

$$\begin{tikzcd} & E \otimes F \\ E \times F \arrow[ur, "\varphi"] \arrow[dr, "\varphi'"'] & \\ & E \otimes' F. \arrow[uu, "\tilde{\varphi}"'] \end{tikzcd}$$

Il existe aussi un unique isomorphisme $\widetilde{\varphi'}$ tel que le diagramme suivant commute

$$\begin{tikzcd} & E \otimes F \arrow[dd, "\widetilde{\varphi'}"] \\ E \times F \arrow[ur, "\varphi"] \arrow[dr, "\varphi'"'] & \\ & E \otimes' F. \end{tikzcd}$$

Donc $\tilde{\varphi} \circ \widetilde{\varphi'} \circ \varphi = \varphi$. Donc $\tilde{\varphi} \circ \widetilde{\varphi'}$ fixe tous les éléments de $\operatorname{Im}\varphi$. Comme $\operatorname{Im}\varphi$ engendre $E \otimes F$ on en déduit que $\tilde{\varphi} \circ \widetilde{\varphi'}$ est l'identité de $E \otimes F$. On montre de même que $\widetilde{\varphi'} \circ \tilde{\varphi}$ est l'identité de $E \otimes' F$. On peut alors légitimement écrire $\varphi(e, f) = e \otimes f \in E \otimes F$ pour tout $e \in E$ et tout $f \in F$.

Soient maintenant $u_1 : E_1 \to F_1$ et $u_2 : E_2 \to F_2$ deux applications linéaires. On définit une application bilinéaire de $E_1 \times E_2$ dans $F_1 \otimes F_2$ en associant $u_1(e_1) \otimes u_2(e_2)$ à (e_1, e_2). On déduit de la propriété universelle de $E_1 \otimes E_2$ qu'il existe une application linéaire de $E_1 \otimes E_2$ dans $F_1 \otimes F_2$ qui envoie $e_1 \otimes e_2$ sur $u_1(e_1) \otimes u_2(e_2)$. Cette application est notée $u_1 \otimes u_2$ et appelée **produit tensoriel des applications** u_1 et u_2.

1.10. **Produit tensoriel de représentations.** Soit G un groupe fini. Soient E et F deux $\mathbf{C}$-espaces vectoriels de dimension finie. Soient $\rho : G \to \mathrm{GL}(E)$ et $\mu : G \to \mathrm{GL}(F)$ deux représentations linéaires complexes de G. Pour tout s dans G le produit tensoriel $\rho_s \otimes \mu_s$ est un endomorphisme de $E \otimes F$. L'application $s \mapsto \rho_s \otimes \mu_s$ définit une représentation $G \to \mathrm{GL}(E \otimes F)$ notée $\rho \otimes \mu$ et appelée produit tensoriel des représentations ρ et μ.

Soit $B = (b_i)_{1 \leqslant i \leqslant d}$ une base de E. Soit $C = (c_j)_{1 \leqslant j \leqslant e}$ une base de F. Alors

$$(b_i \otimes c_j)_{1 \leqslant i \leqslant d, 1 \leqslant j \leqslant e}$$

est une base de $E \otimes F$.

Soit $R_s = (r_{i,k}(s))_{1 \leqslant i,k \leqslant d}$ la matrice de ρ_s dans la base B. Soit $M_s = (m_{j,l}(s))_{1 \leqslant j,l \leqslant e}$ la matrice de μ_s dans la base C. La matrice P_s de $\rho_s \otimes \mu_s$ dans la base $(b_i \otimes c_j)_{1 \leqslant i \leqslant d, 1 \leqslant j \leqslant e}$ est

$$P_s = (p_{(i,j),(k,l)})_{1 \leqslant i,k \leqslant d, 1 \leqslant j,l \leqslant e} = (r_{i,k}(s) m_{j,l}(s))_{1 \leqslant i,k \leqslant d, 1 \leqslant j,l \leqslant e} \tag{2}$$

notée $R_s \otimes M_s$ et appelée **produit tensoriel** des matrices R_s et M_s.

Par exemple le produit tensoriel des représentations ρ^h et $\rho^{h'}$ du groupe cyclique C_n définies à la section 1.4 n'est autre que la représentation $\rho^{h+h'}$ où la somme $h + h'$ s'entend modulo n.

1.11. **La représentation duale.** Soit G un groupe fini. Soient E et F deux $\mathbf{C}$-espaces vectoriels. Soient $\rho : G \to \mathrm{GL}(E)$ et $\mu : G \to \mathrm{GL}(F)$ deux représentations linéaires complexes de G. On note $\mathrm{Hom}_{\mathbf{C}}(E, F)$ l'ensemble de applications $\mathbf{C}$-linéaire de E dans F. On définit une action de G sur $\mathrm{Hom}_{\mathbf{C}}(E, F)$ en posant, pour $s \in G$ et $f \in \mathrm{Hom}_{\mathbf{C}}(E, F)$

$$\begin{aligned} s.f : \quad & E \longrightarrow F \\ & v \longmapsto \mu_s(f(\rho_{s^{-1}}(v))). \end{aligned}$$

Autrement dit $s.f = \mu_s \circ f \circ (\rho_s)^{-1}$. On a ainsi défini une représentation $G \to \mathrm{GL}(\mathrm{Hom}_{\mathbf{C}}(E, F))$. Dans le cas particulier où F est $\mathbf{C}$ lui-même muni de l'action triviale de G, l'espace $\mathrm{Hom}_{\mathbf{C}}(E, \mathbf{C})$ n'est autre que le dual $\hat{E}$ de E. On pourra noter $\hat{\rho} : G \to \mathrm{GL}(\hat{E})$ la représentation ainsi obtenue. On a $\hat{\rho}_s(f) = f \circ \rho_s^{-1}$. Soit B une base de E. La matrice de $\hat{\rho}(s)$ dans la base duale de B est la transposée de la matrice de $\rho(s^{-1})$ dans la base B.

1.12. **Moyennes et vecteurs invariants.** Soit G un groupe fini. Soit E un $\mathbf{C}$-espace vectoriel de dimension finie. Soit $\rho : G \to \mathrm{GL}(E)$ une représentation linéaire. On note E^G l'ensemble de vecteur fixés par tous les éléments de g

$$E^G = \{m \in E \,|\, \forall s \in G,\ \rho_s(m) = m\}.$$

C'est un sous-espace vectoriel de E. Les vecteurs de E^G sont dits **invariants** par G. On définit l'application $\mathcal{M} : E \to E$ par

$$\mathcal{M}(v) = \frac{1}{\#G} \sum_{s \in G} \rho_s(v).$$

On vérifie que $\mathcal{M} \circ \mathcal{M} = \mathcal{M}$ et que l'image de $\mathcal{M}$ est E^G. Donc $\mathcal{M}$ est un projecteur d'image E^G. On l'appelle l'opérateur de moyenne de la représentation. En particulier la dimension de E^G est la trace de $\mathcal{M}$ donc

$$\dim(E^G) = \mathrm{Tr}(\mathcal{M}) = \frac{1}{\#G} \sum_{s \in G} \mathrm{Tr}(\rho_s). \tag{3}$$

Un cas intéressant concerne la représentation $\mathrm{Hom}_{\mathbf{C}}(E_1, E_2)$ où E_1 et E_2 sont deux espaces de représentation. Il découle de la définition de cette représentation que le sous-espace des invariants par G dans cette représentation n'est autre que le $\mathbf{C}$-espace vectoriel $\mathrm{Hom}_G(E_1, E_2)$ des applications linéaires équivariantes entre E_1 et E_2.

1.13. **Lemme de Schur.** Soient E et F deux $\mathbf{C}$-espaces vectoriels de dimensions finies. Soient $\rho_1 : G \to \mathrm{GL}(E_1)$ et $\rho_2 : G \to \mathrm{GL}(E_2)$ deux représentations irréductibles du même groupe fini G. Soit $u : E_1 \to E_2$ une application équivariante. Le noyau de u est stable par G. Il est donc nul ou égal à E_1. L'image de u est stable par G. Elle est donc nulle ou égale à E_2. On en déduit que si u n'est pas nulle elle définit un isomorphisme entre E_1 et E_2. Supposons donc maintenant que $E_1 = E_2$ et $\rho_1 = \rho_2$. Soit u une application équivariante et soit λ l'une de ses valeurs propres. L'application $u - \lambda\mathrm{Id}$ est équivariante et son noyau n'est pas nul. Elle est donc nulle et $u = \lambda\mathrm{Id}$.

Théorème 4 (Lemme de Schur)**.** *Soit G un groupe fini et soient E_1 et E_2 deux $\mathbf{C}$-espaces vectoriels de dimension finie. Soient $\rho_1 : G \to \mathrm{GL}(E_1)$ et $\rho_2 : G \to \mathrm{GL}(E_2)$ deux représentation irréductibles de G. Si ρ_1 et ρ_2 ne sont pas isomorphes alors $\mathrm{Hom}_G(E_1, E_2) = 0$. Sinon $\mathrm{Hom}_G(E_1, E_2)$ est un $\mathbf{C}$-espace vectoriel de dimension 1. Dans le cas où $E_1 = E_2 = E$ et $\rho_1 = \rho_2 = \rho$ l'espace $\mathrm{Hom}_G(E, E)$ est formé des homothéties de E.*

1.14. **Généralisation.** Soit K un corps et E un espace vectoriel sur K. Soit G un groupe. Un morphisme de groupe $\rho : G \to \mathrm{End}(E)$ définit une **représentation linéaire** de G. Il n'est pas nécessaire que K soit le corps des complexes ni que le groupe G soit fini. Par exemple on peut considérer le K-espace vectoriel K^G des applications de G dans K. Si $\varphi : G \to K$ est une telle fonction et $g \in G$ on définit la fonction $g.\varphi$ par

$$g.\varphi : \qquad \begin{array}{ccc} G & \longrightarrow & \mathbf{C} \\ \\ x & \longmapsto & f(g^{-1}x). \end{array}$$

On obtient ainsi une représentation $\rho : G \to \mathrm{End}(K^G)$. On peut obtenir une sous-représentation de ρ en se restreignant par exemple au sous-espace $K^{(G)}$ des fonctions à support fini. Dans le cas où G est un groupe fini et $K = \mathbf{C}$ on retrouve ainsi la représentation régulière introduite à la section 1.2.

Supposons que G est un groupe topologique, c'est-à-dire un groupe muni d'une topologie telle que les applications produit $G \times G \to G$ et inverse $G \to G$ soient continues. On peut alors obtenir une sous-représentation de ρ en se restreignant par exemple au sous-espace $C(G, K)$ des fonctions continues.

On a vu, par exemple dans le preuve du théorème 1, l'importance des moyennes comme celle de la formule (3) dans l'étude des représentations. Pour développer une théorie des représentations de groupes dans un cadre général on rencontre des difficultés pour former ces moyennes.

Si le groupe est infini on peut essayer de le munir d'une structure d'espace topologique et d'une théorie de l'intégration compatibles avec la loi de groupe. On peut alors remplacer les moyennes par des intégrales, au moins quand le groupe est compact.

Si le corps K n'est pas de caractéristique nulle et même si le groupe est fini, on rencontre des difficultés lorsque la caractéristique du corps divise l'ordre de G. Considérons par exemple le cas où $K = (\mathbf{Z}/2\mathbf{Z}, +, \times)$ est le corps à deux éléments et $G = (C_2, \times) = (\{1, s\}, \times)$ est le groupe cyclique à deux éléments. On pose $E = K^2$. Soit (e_1, e_2) la base canonique de E. Soit $u \in \mathrm{End}(E)$ l'endomorphisme qui envoie e_1 sur e_1 et e_2 sur $e_1 + e_2$. On vérifie que $u \circ u$ est l'identité de E. La matrice de u dans la base canonique est

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}).$$

Soit $\rho : C_2 \to \mathrm{GL}_2(E)$ le morphisme de groupe qui envoie s sur u. C'est une représentation K-linéaire de C_2. Or E n'admet que trois sous-espaces non-triviaux, engendrés respectivement par e_1, e_2 et $e_1 + e_2$. Le sous-espace engendré par e_1 est stable par G. L'espace engendré par e_2 n'est pas stable car $u(e_2) = e_1 + e_2$. L'espace engendré par $e_1 + e_2$ n'est pas stable car $u(e_1 + e_2) = e_2$. Donc le sous-espace engendré par e_1 est stable par G mais n'admet pas de supplémentaire stable. Le théorème 1 ne peut pas se généraliser lorsque la caractéristique de K divise le cardinal de G.

2. Caractères d'un groupe fini

On se donne un groupe fini G. Soit E un $\mathbf{C}$-espace vectoriel de dimension finie et $\rho : G \to \mathrm{GL}(E)$ une représentation de G. On associe à tout élément s de G la trace de ρ_s. On définit ainsi une application

$$\chi_\rho : \quad G \longrightarrow \mathbf{C}$$

$$s \longmapsto \mathrm{Tr}(\rho_s)$$

appelée **caractère** de la représentation ρ. Les **caractères d'un groupe fini** sont les caractères de ses représentations.

Dans le cas particulier d'une représentation $\rho : G \to \mathrm{GL}_1(\mathbf{C}) = \mathbf{C}^*$ de degré 1 la valeur du caractère $\chi_\rho(s)$ s'identifie naturellement à ρ_s. En particulier $\chi_\rho(s_1 s_2) = \chi_\rho(s_1)\chi_\rho(s_2)$. C'est la raison pour laquelle les caractères des représentations de degré 1 sont dits **multiplicatifs**. Il va de soi que les caractères des représentations de degré quelconque n'ont aucune raison d'être multiplicatifs.

2.1. **Premières propriétés.** Si ρ est une représentation de degré n et si 1_G est l'élément neutre de G alors $\rho(1_G)$ est l'identité dans un espace vectoriel de dimension n donc

$$\chi_\rho(1_G) = n.$$

Notons e le cardinal de G. Si s est un élément de G alors $s^e = 1$ d'après le théorème de Lagrange. Donc le polynôme $x^e - 1$ annule l'endomorphisme ρ_s. Comme $x^e - 1 \in \mathbf{C}[x]$ est scindé et sans facteurs carrés on en déduit que ρ_s est diagonalisable. Ainsi $\chi_\rho(s)$ est la somme des valeurs propres de ρ_s en comptant les multiplicités. Ces valeurs propres sont toutes des racines e-ièmes de l'unité. En particulier l'inverse d'une valeur propre est son conjugué. On en déduit que

$$\chi_\rho(s^{-1}) = \overline{\chi_\rho(s)}.$$

On rappelle que si A et B sont deux matrices carrées d'ordre n alors $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$. La trace d'un endomorphisme est la trace de sa matrice dans une base quelconque. Si $s, t \in G$ la trace de $\rho_s \circ \rho_t$ est égale à la trace de $\rho_t \circ \rho_s$. Donc

$$\chi_\rho(st) = \chi_\rho(ts)$$

et

$$\chi_\rho(sts^{-1}) = \chi_\rho(t).$$

Autrement dit un caractère prend la même valeur en tous les éléments d'une même classe de conjugaison dans G. On dit que c'est une **fonction centrale** sur G.

Soient $\rho_1 : G \to \mathrm{End}(E_1)$ et $\rho_2 : G \to \mathrm{End}(E_2)$ deux représentations linéaires.

Pour tout s de G on a vu que la matrice de $\rho_1(s) \oplus \rho_2(s)$ dans une base bien choisie de $E_1 \oplus E_2$ est $\mathrm{Diag}(R_1(s), R_2(s))$. Donc la trace de $\rho_1(s) \oplus \rho_2(s)$ est la somme des traces de $\rho_1(s)$ et $\rho_2(s)$. Autrement dit

$$\chi_{\rho_1 \oplus \rho_2} = \chi_{\rho_1} \oplus \chi_{\rho_2}.$$

De même la matrice de $\rho_1(s) \otimes \rho_2(s)$ est le produit tensoriel des matrices de $\rho_1(s)$ et de $\rho_2(s)$. En examinant la formule (2) on voit que la trace d'un produit tensoriel de matrices est le produit des traces de ces matrices. Donc

$$\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1} . \chi_{\rho_2}.$$

On a vu aussi que la matrice de $\hat{\rho}(s)$ dans la base duale de B est la transposée de la matrice de $\rho(s^{-1})$ dans la base B. Comme les valeurs propres de $\rho(s)$ sont de module 1, la trace de $\hat{\rho}(s)$ est la conjuguée complexe de la trace de $\rho(s)$. Autrement dit

$$\chi_{\hat{\rho}} = \overline{\chi_\rho}.$$

On voit que l'ensemble des caractères d'un groupe fini est stable par conjugaison, par addition et par multiplication.

2.2. **Orthogonalité des caractères irréductibles.** Considérons maintenant la représentation $\mathrm{Hom}_{\mathbf{C}}(E_1, E_2)$. Soit n_1 la dimension de E_1. Soit n_2 la dimension de E_2. Soit s un élément de G. On choisit une base de E_1 formée de vecteurs propres de $\rho_1(s)$. On note $(\lambda_i)_{1\leqslant i\leqslant n_1}$ les valeurs propres correspondantes. On note $(\varphi_i)_{1\leqslant i\leqslant n_1}$ la base duale. C'est une base du dual $\hat{E}_1$ de E_1. On choisit une base $(b_j)_{1\leqslant j\leqslant n_2}$ de E_2 formée de vecteurs propres de $\rho_2(s)$. On note $(\mu_j)_{1\leqslant j\leqslant n_2}$ les valeurs propres correspondantes.

Pour tout $1 \leqslant i \leqslant n_1$ et $1 \leqslant j \leqslant n_2$ on note $\tau_{i,j}$ l'application élémentaires $m \mapsto \varphi_i(m)b_j$. Les $(\tau_{i,j})_{1\leqslant i\leqslant n_1,\, 1\leqslant j\leqslant n_2}$ forment une base de $\mathrm{Hom}_{\mathbf{C}}(E_1, E_2)$. L'image de $\tau_{i,j}$ par s est

$$(\lambda_i)^{-1}\mu_j\tau_{i,j} = \overline{\lambda_i}\mu_j\tau_{i,j}.$$

Donc la trace de s agissant sur $\mathrm{Hom}_{\mathbf{C}}(E_1, E_2)$ est

$$\sum_{1\leqslant i\leqslant n_1,\, 1\leqslant j\leqslant n_2} \overline{\lambda_i}\mu_j = \overline{\sum_{1\leqslant i\leqslant n_1} \lambda_i}.\sum_{1\leqslant j\leqslant n_2} \mu_j = \overline{\mathrm{Tr}(\rho_1(s))}.\mathrm{Tr}(\rho_2(s)).$$

Donc

$$\chi_{\mathrm{Hom}_{\mathbf{C}}(E_1,E_2)} = \overline{\chi_{\rho_1}}.\chi_{\rho_2}.$$

La formule (3) permet alors d'affirmer que la dimension de l'espace des applications équivariantes entre E_1 et E_2 est

$$\dim_{\mathbf{C}} \mathrm{Hom}_G(E_1, E_2) = \frac{1}{\#G}\sum_{s\in G} \overline{\chi_{\rho_1}(s)}.\chi_{\rho_2}(s). \tag{4}$$

Appliquant le lemme de Schur on prouve alors le théorème suivant dit d'**orthogonalité des caractères irréductibles**.

Théorème 5. *Soit G un groupe fini et soit χ le caractère d'une représentation irréductible. Alors*

$$\frac{1}{\#G}\sum_{s\in G} \overline{\chi(s)}.\chi(s) = 1.$$

Si χ_1 et χ_2 sont les caractères de deux représentations irréductibles non-isomorphes, alors

$$\frac{1}{\#G}\sum_{s\in G} \overline{\chi_1(s)}.\chi_2(s) = 0.$$

Le caractère d'une représentation irréductible est dit **caractère irréductible**. Le théorème 5 affirme que les caractères irréductibles forment une système orthonormé dans l'espace des fonctions centrales muni du produit scalaires

$$(f,g) = \frac{1}{\#G}\sum_{s\in G}\overline{f(s)}g(s). \tag{5}$$

On en déduit que deux caractères irréductibles associés à deux représentations irréductibles non-équivalentes sont différents. Comme les caractères irréductibles forment un système orthonormé de l'espace des fonctions centrales sur G, leur nombre est majoré par la dimension de cet espace. Or cette dimension est égale au nombre de classes de conjugaison de G. Le nombre de classes d'équivalence de représentations irréductibles de G est donc majoré par le nombre de classes de conjugaison de G. On note $\mathrm{Irr}(G)$ l'ensemble des classes d'équivalence de représentations irréductibles de G. Le théorème 2 affirme que toute représentation $\mu : G \to \mathrm{GL}(E_\mu)$ de G est équivalente à $\oplus_{\rho\in\mathrm{Irr}(G)}\rho^{\oplus e_\rho(\mu)}$ où les $e_\rho(\mu)$ sont des entiers naturels. On déduit du théorème 5 que

$$e_\rho(\mu) = (\chi_\rho, \chi_\mu).$$

Autrement dit la décomposition de μ en somme de représentations irréductibles n'est pas nécessairement unique, mais le nombre de fois qu'une représentation irréductible $\rho : G \to \mathrm{GL}(E_\rho)$ apparaît dans une décomposition de μ ne dépend que de ρ et de μ. On appellera ce nombre la **multiplicité** de ρ dans μ et l'on se souviendra qu'il est égal au produit scalaire des caractères χ_ρ et χ_μ. Il est aussi égal à la dimension du $\mathbf{C}$-espace vectoriel $\mathrm{Hom}_G(E_\mu, E_\rho)$ d'après la formule (4).

Théorème 6. *Soit G un groupe fini. Soient E_1 et E_2 deux $\mathbf{C}$-espaces vectoriels de dimensions finies. Soient $\mu_1 : G \to \mathrm{GL}(E_1)$ et $\mu_2 : G \to \mathrm{GL}(E_2)$ deux représentations. Si μ_1 et μ_2 ont le même caractère alors elles sont équivalentes.*

C'est évident puisque pour toute représentation irréductible ρ, la multiplicité de ρ dans μ_1 est $(\rho, \chi_1) = (\rho, \chi_2)$. Donc

$$\mu_1 \simeq \oplus_{\rho\in\mathrm{Irr}(G)}\rho^{\oplus(\rho,\chi_1)} = \oplus_{\rho\in\mathrm{Irr}(G)}\rho^{\oplus(\rho,\chi_2)} \simeq \mu_2.$$

□

Si μ est une représentation de G et $e_\rho(\mu)$ la multiplicité de la représentation irréductible ρ dans μ alors $\mu \simeq \oplus_{\rho\in\mathrm{Irr}(G)}\rho^{\oplus e_\rho(\mu)}$ donc

$$\chi_\mu = \sum_{\rho\in\mathrm{Irr}(G)} e_\rho(\mu)\chi_\rho.$$

Donc

$$(\chi_\mu, \chi_\mu) = \sum_{\rho\in\mathrm{Irr}(G)} e_\rho^2(\mu).$$

Théorème 7. *Le carré scalaire (χ_μ, χ_μ) du caractère d'une représentation μ de G est la somme des carrés des multiplicités dans μ des représentations irréductibles de G. En particulier le carré scalaire (χ_μ, χ_μ) vaut 1 si et seulement si μ est irréductible.*

2.3. **Décomposition de la représentation régulière.** Soit $E = \mathbf{C}^G$ et soit $(e_x)_{x\in G}$ la base canonique de E. On a défini la représentation régulière $\rho_G : G \to \mathrm{GL}(E)$ en posant $\rho_G(s)(e_x) = e_{sx}$. Si $s \neq 1$ alors $\rho_G(s)(e_x)$ est un vecteur de base différent de e_x. Donc la trace de $\rho_G(s)$ est nulle. Appelons $\chi_G : G \to \mathbf{C}$ le caractère de la représentation régulière de G. On a $\chi_G(1_G) = \#G$ et $\chi_G(s) = 0$ si $s \neq 1_G$. Si μ est une représentation irréductible de G, la multiplicité de μ dans la représentation régulière est le produit scalaire

$$(\chi_\mu, \chi_G) = \frac{1}{\#G}.\sum_{s\in G}\overline{\chi_\mu(s)}.\chi_G(s) = \frac{1}{\#G}.\#G.\overline{\chi_\mu(1)} = n_\mu$$

où n_μ est le degré de μ. On en déduit le théorème suivant.

Théorème 8. *Soit G un groupe fini. Soit $\rho_G : g \to \mathrm{GL}(\mathbf{C}^G)$ la représentation régulière. Soit μ une représentation complexe irréductible de G. La multiplicité de μ dans ρ_G est égale à son degré n_μ. Donc*

$$\rho_G = \oplus_{\mu\in\mathrm{Irr}(G)}\mu^{\oplus n_\mu} \quad \textit{et} \quad \#G = \chi_G(1) = \sum_{\mu\in\mathrm{Irr}(G)} n_\mu\chi_\mu(1) = \sum_{\mu\in\mathrm{Irr}(G)} n_\mu^2,$$

et si $s \neq 1$,

$$0 = \chi_G(s) = \sum_{\mu\in\mathrm{Irr}(G)} n_\mu\chi_\mu(s).$$

2.4. **Fonctions centrales et applications équivariantes.** Soit G un groupe fini et $f : G \to \mathbf{C}$ une application à valeurs complexes. Soit E un $\mathbf{C}$-espace vectoriel de dimension finie. Soit

$$\rho : G \to \mathrm{GL}(E)$$

une représentation de G. Soit χ son caractère et n son degré. La fonction f permet de définir un endomorphisme

$$\rho_f = \sum_{s\in G} f(s)\rho_s \in \mathrm{End}(E).$$

Soit $t \in G$. La conjugaison de ρ_f par ρ_t est

$$\rho_{t^{-1}}\rho_f\rho_t = \sum_{s\in G} f(s)\rho_{t^{-1}}\rho_s\rho_t = \sum_{s\in G} f(s)\rho_{t^{-1}st} = \sum_{s\in G} f(tst^{-1})\rho_s.$$

On en déduit que si f est une fonction centrale alors ρ_f est une application équivariante.

Supposons d'abord que ρ est irréductible. Alors ρ_f est une homothétie. La trace de ρ_f est

$$\mathrm{Tr}(\rho_f) = \sum_{s\in G} f(s)\,\mathrm{Tr}(\rho_s) = \sum_{s\in G} f(s)\chi_s = \#G.(\bar{\chi}, f).$$

Donc

$$\rho_f = \frac{\#G}{n}.(\bar{\chi}, f).\mathrm{Id}_E. \tag{6}$$

Théorème 9. *Soit G un groupe fini et soit $f : G \to \mathbf{C}$ une fonction centrale. Soit $\rho : G \to \mathrm{GL}(E)$ une représentation complexe de G. L'endomorphisme $\rho_f = \sum_{s\in G} f(s)\rho_s$ est G-équivariant. Si F est un sous espace de E stable pour l'action de G et si ρ^F est la restriction de ρ à F alors ρ^F_f est la restriction de ρ_f à F. Si ρ est irréductible alors ρ_f est une homothétie de rapport $\frac{\#G}{n}.(\bar{\chi}, f)$.*

Revenons au cas d'une représentation ρ quelconque. Pour toute représentation irréductible μ de G on note $e_\mu(\rho)$ la multiplicité de μ dans ρ. La représentation ρ est équivalente à $\oplus_{\mu\in\mathrm{Irr}(G)}\mu^{\oplus e_\mu(\rho)}$. Donc il existe des sous-espaces vectoriels E_μ de ρ stables par G et tels que

$$E = \oplus_{\mu\in\mathrm{Irr}(G)} E_\mu \tag{7}$$

et la restriction de ρ à E_μ soit équivalente à $\mu^{\oplus e_\mu(\rho)}$. Pour tout μ dans $\mathrm{Irr}(G)$ on note n_μ le degré de μ et

$$p_\mu = \frac{n_\mu}{\#G}.\rho_{\overline{\chi_\mu}}$$

l'endomorphisme de E associé à la fonction centrale $\overline{\chi_\mu}$, corrigé d'un facteur scalaire $n_\mu/\#G$. On déduit du théorème 9 que la retriction de p_μ à E_μ est l'identité de E_μ. De même, si ν est une représentation irréductible de G non-équivalente à μ alors la retriction de p_μ à E_ν est nulle. Autrement dit p_μ est un projecteur d'image E_μ et de noyau $\oplus_{\nu\in\mathrm{Irr}(G),\,\nu\neq\mu}E_\nu$. On en déduit que la décomposition de la formule 7 est unique. Chaque E_μ est caractérisé comme l'image de p_μ. La décomposition de la formule 7 est appelée **décomposition canonique** de ρ.

Théorème 10. *Soit G un groupe fini. Soit E un $\mathbf{C}$-espace vectoriel non-nul de dimension finie. Soit $\rho : G \to \mathrm{GL}(E)$ une représentation de G. Il existe une unique décomposition de E en somme directe*

$$E = \oplus_{\mu\in\mathrm{Irr}(G)} E_\mu$$

telle que chaque E_μ soit stable par G et la restriction de ρ à E_μ soit une somme directe (éventuellement nulle) de représentations de G toutes équivalentes à μ.

2.5. **Base orthonormée de l'espace des fonctions centrales.** On a vu que les caractères irréductibles de G forment un système orthonormé (donc libre) de l'espace des fonctions centrales. On veut montrer que ce système libre est en fait une base de l'espace des fonctions centrales.

La formule (5) définit un produit scalaire sur l'espace des fonctions centrales. Pour montrer que les $(\chi_\mu)_{\mu\in\mathrm{Irr}(G)}$ engendrent l'espace des fonctions centrales il suffit de montrer que toute fonction centrale orthogonale aux $(\chi_\mu)_{\mu\in\mathrm{Irr}(G)}$ est nulle.

Soit donc $f : G \to \mathbf{C}$ une fonction centrale orthogonale à tous les caractères irréductibles. Pour toute représentation $\rho : G \to \mathrm{GL}(E)$ posons $\rho_f = \sum_{s\in G} f(s)\rho_s \in \mathrm{End}(E)$. On déduit du théorème 10 et du théorème 9 que $E = \oplus_{\mu\in\mathrm{Irr}(G)}E_\mu$ et ρ_f s'annulle sur chaque E_μ. Donc ρ_f est nul.

Dans le cas particulier où ρ est la représentation régulière $\rho_G : G \to \mathbf{C}^G$ on obtient

$$0 = \rho_f(e_1) = \sum_{s\in G} f(s)\rho_s(e_1) = \sum_{s\in G} f(s)e_s.$$

Donc $f(s) = 0$ pour tout $s \in G$.

Théorème 11. *Soit G un groupe fini. Les caractères irréductibles complexes forment une base de l'espace des fonctions centrales à valeurs complexes. En particulier le nombre de représentations irréductibles est égal au nombre de classes de conjugaison de G.*

Toute fonction centrale $f : G \to \mathbf{C}$ vérifie

$$f = \sum_{\rho\in\mathrm{Irr}(G)} (\chi_\rho, f)\chi_\rho. \tag{8}$$

Soit $C \subset G$ une classe de conjugaison dans G. Soit $\mathbf{1}_C$ la fonction centrale qui prend la valeur 1 en tous les éléments de C et qui s'annule partout ailleurs. Appliquons la formule (8) à $\mathbf{1}_C$. On calcule

$$(\chi_\rho, \mathbf{1}_C) = \frac{1}{\#G}.\sum_{s \in G} \overline{\chi_\rho(s)}.\mathbf{1}_C(s) = \frac{\#C}{\#G}.\overline{\chi_\rho(C)}$$

où $\chi_\rho(C)$ est la valeur du caractère χ_ρ en tous les éléments de C. Donc

$$\mathbf{1}_C = \frac{\#C}{\#G}.\sum_{\rho \in \mathrm{Irr}(G)} \overline{\chi_\rho(C)}\chi_\rho. \tag{9}$$

Évaluant l'équation (9) en un élément s de C on trouve

$$1 = \frac{\#C}{\#G}.\sum_{\rho \in \mathrm{Irr}(G)} \overline{\chi_\rho(C)}\chi_\rho(C). \tag{10}$$

Évaluant l'équation (9) en un élément s d'une classe de conjugaison C' différente de C on trouve

$$0 = \sum_{\rho \in \mathrm{Irr}(G)} \overline{\chi_\rho(C)}\chi_\rho(C'). \tag{11}$$

Théorème 12. *Soit G un groupe fini et soient s et s' deux éléments de G. Si s et s' ne sont pas conjugués alors*

$$\sum_{\rho \in \mathrm{Irr}(G)} \overline{\chi_\rho(s)}\chi_\rho(s') = 0. \tag{12}$$

Si s et s' appartiennent à la même classe C alors

$$\sum_{\rho \in \mathrm{Irr}(G)} \overline{\chi_\rho(s)}\chi_\rho(s') = \frac{\#G}{\#C}. \tag{13}$$

2.6. **Table des caractères du groupe cyclique.** Soit $n \geqslant 2$ un entier et C_n le groupe cyclique d'ordre n. On a déjà trouvé n représentations irréductibles de degré 1 à la section 1.3. Le nombre de classes de conjugaison de C_n étant n il n'y a pas d'autre représentation irréductible. La valeur de χ_h en (la classe de) r^k est $\exp(2i\pi hk/n)$. Dans le cas $n = 3$ on obtient la table des caractères suivante.

	1	r	r^2
χ_0	1	1	1
χ_1	1	$\exp(2i\pi/3)$	$\exp(4i\pi/3)$
χ_2	1	$\exp(4i\pi/3)$	$\exp(2i\pi/3)$

2.7. **Table des caractères du groupe diédral D_n pour n impair.** Soit $m \geqslant 1$ un entier et soit $n = 2m+1$. Soit D_n le groupe diédral d'ordre $2n$. On a construit à la section 1.6 des représentations de degré 2 irréductibles ρ^h pour $1 \leqslant h \leqslant m$. Elles sont deux à deux non-équivalentes. On note $(\chi_h)_{1\leqslant h\leqslant m}$ les caractères correspondants.

Le groupe dérivé de D_n est le sous-groupe cyclique d'ordre n engendré par r. En effet

$$[s,r] = srs^{-1}r^{-1} = r^{-2}$$

engendre le même groupe que r car l'ordre n de r est impair. L'abélianisé de D_n est donc le quotient D_n/C_n qui est d'ordre 2. Il existe donc deux représentations irréductibles de degré 1. Ce sont les deux caractères multiplicatifs de D_n. La représentation unité ψ_0 d'une part. Et la signature ψ_1 définie par $\psi_1(s) = -1$ et $\psi_1(r) = 1$.

Nous avons trouvé m représentations irréductibles de degré 2 et deux représentations irréductibles de degré 1. Cela fait $m+2$ représentations irréductibles. La somme des carrés des degrés de ces représentations vaut $4m+2 = 2n$ qui est le cardinal du groupe D_n. D'après le théorème 8 il n'existe pas d'autre représentation irréductible.

Les classes de conjugaison de D_n sont donc au nombre de $m+2$ elles aussi. On a la classe de 1, la classe de s, et les classes des r^k pour $1 \leqslant k \leqslant m$.

Dans le cas $m = 3$ on obtient la table des caractères suivante.

	1	r	r^2	r^3	s
ψ_0	1	1	1	1	1
ψ_1	1	1	1	1	-1
χ_1	2	$2\cos(2\pi/7)$	$2\cos(4\pi/7)$	$2\cos(6\pi/7)$	0
χ_2	2	$2\cos(4\pi/7)$	$2\cos(8\pi/7)$	$2\cos(12\pi/7)$	0
χ_3	2	$2\cos(6\pi/7)$	$2\cos(12\pi/7)$	$2\cos(4\pi/7)$	0

3. L'ALGÈBRE DU GROUPE

Soit G un groupe fini. On note $\mathbf{C}[G]$ l'ensemble des combinaisons formelles d'éléments de G à coefficients dans $\mathbf{C}$. Autrement dit

$$\mathbf{C}[G] = \{\sum_{s\in G} a_s.s \,|\, a_s \in \mathbf{C}\}.$$

C'est un $\mathbf{C}$-espace vectoriel isomorphe à $\mathbf{C}^G$. On le munit d'une loi de composition interne (multiplication) notée $\times$ ou . et définie par les propriétés suivantes :

(1) $\times : \mathbf{C}[G] \times \mathbf{C}[G] \to \mathbf{C}[G]$ est une application $\mathbf{C}$-bilinéaire,

(2) pour s et t dans G le produit $s \times t \in \mathbf{C}[G]$ est st.

Autrement dit, la loi $\times$ prolonge par bilinéarité la loi du groupe G. On vérifie que $(\mathbf{C}[G], +, \times)$ est un anneau unitaire. On dit que $\mathbf{C}[G]$ est l'algèbre du groupe G. C'est une $\mathbf{C}$-algèbre associative et unifère. Si G est commutatif alors $\mathbf{C}[G]$ est un anneau commutatif.

Si $A \subset \mathbf{C}$ est un sous-anneau de $\mathbf{C}$ on note $A[G]$ le sous-anneau de $\mathbf{C}[G]$ formé des combinaisons d'éléments de G à coefficients dans A.

Si E est un $\mathbf{C}$ espace vectoriel de dimension finie et $\rho : G \to \mathrm{GL}(E)$ une représentation, on peut munir E d'une structure de $\mathbf{C}[G]$-module à gauche en posant $s.v = \rho_s(v)$ pour $s \in G$ et $v \in E$. Le $\mathbf{C}[G]$-module à gauche ainsi obtenu est de type fini. Réciproquement, si M est un $\mathbf{C}[G]$-module de type fini, alors M est un $\mathbf{C}$-espace vectoriel par restriction des scalaires. Si $(g_i)_{1\leqslant i\leqslant I}$ est une partie génératrice du $\mathbf{C}[G]$-module M alors $(s.g_i)_{1\leqslant i\leqslant I,\, s\in G}$ est une partie génératrice du $\mathbf{C}$-espace vectoriel sous-jacent. Donc ce dernier est de dimension finie. L'application

$$s \mapsto (m \mapsto s.m)$$

est un morphisme de G dans le groupe $\mathrm{GL}(M)$ des automorphismes du $\mathbf{C}$-espace vectoriel M. Elle définit donc une représentation complexe de G.

Il y a donc une correspondance entre les représentations complexes de G de dimension finie et les $\mathbf{C}[G]$-modules de type fini. Soient $\rho : G \to \mathrm{End}(E)$ et $\mu : G \to \mathrm{End}(F)$ deux représentations complexes de G. Soit $u : E \to F$ une application linéaire équivariante. On a $u(s.v) = u(\rho_s(v)) = \mu_s(u(v)) = s.u(v)$. Donc u est un morphisme de $\mathbf{C}[G]$-modules. Réciproquement, un morphisme de $\mathbf{C}[G]$-modules est (par restriction des scalaires) une application $\mathbf{C}$-linéaire, équivariante pour l'action de G. Il est donc équivalent de parler de représentations de G et d'applications équivariantes ou bien de $\mathbf{C}[G]$-modules à gauche et de morphismes de $\mathbf{C}[G]$-modules. Le $\mathbf{C}[G]$-modules à gauche $\mathbf{C}[G]$ n'est autre que la représentation régulière. Le théorème 1 signifie que tout sous-module d'un $\mathbf{C}[G]$-module de type fini est facteur direct.

Pour toute représentation $\rho : G \to \mathrm{GL}(E)$ on prolonge ρ par linéarité pour définir un morphisme de $\mathbf{C}$-algèbres $\tilde{\rho} : \mathbf{C}[G] \to \mathrm{End}(E)$. Si $a = \sum_{s\in G} a_s.s$ est un élément de $\mathbf{C}[G]$, l'image de a par $\tilde{\rho}$ n'est autre que l'endomorphisme ρ_f défini à la section 2.4 où $f : G \to \mathbf{C}$ est définie par $f(s) = a_s$. Pour tout vecteur v dans E on a

$$a.v = \tilde{\rho}(a)(v) = \sum_{s\in G} a_s \rho_s(v).$$

3.1. **Décomposition de $\mathbf{C}[G]$.** Le produit cartésien des applications $\tilde{\rho}$ lorsque ρ parcourt $\mathrm{Irr}(G)$ définit un morphisme d'algèbres

$$\begin{array}{llll} \mathcal{F} : & \mathbf{C}[G] & \longrightarrow & \oplus_{\rho\in\mathrm{Irr}(G)} \mathrm{End}(E_\rho) \\ & \sum_{s\in G} a_s.s & \longmapsto & \left(\tilde{\rho}(\sum_{s\in G} a_s.s)\right)_{\rho\in\mathrm{Irr}(G)} = \left(\sum_{s\in G} a_s.\rho_s\right)_{\rho\in\mathrm{Irr}(G)} . \end{array}$$

Notons n_ρ le degré de ρ et choisissons une base B_ρ pour chaque E_ρ. Soit B la collection de toutes les bases ainsi choisies. On obtient un morphisme d'algèbres

$$\begin{array}{llllll} \mathcal{F}_B : & \mathbf{C}[G] & \longrightarrow & \oplus_{\rho\in\mathrm{Irr}(G)}\mathcal{M}_{n_\rho}(\mathbf{C}) & \hookrightarrow & \mathcal{M}_{\sum n_\rho}(\mathbf{C}) \\ & s & \longmapsto & (\mathbf{M}(\rho_s, B_\rho))_{\rho\in\mathrm{Irr}(G)} & \longrightarrow & \mathrm{Diag}_{\rho\in\mathrm{Irr}(G)}\,\mathbf{M}(\rho_s, B_\rho) \end{array}$$

où $\mathbf{M}(\rho_s, B_\rho)$ est la matrice de $\rho(s)$ dans la base B_ρ. On note

$$\mathcal{E} = \oplus_{\rho\in\mathrm{Irr}(G)} \mathrm{End}(E_\rho)$$

et l'on définit une forme bilinéaire $\mathbf{T} : \mathcal{E} \times \mathcal{E} \to \mathbf{C}$ en posant

$$\mathbf{T}((u_\rho)_{\rho\in\mathrm{Irr}(G)}, (v_\rho)_{\rho\in\mathrm{Irr}(G)}) = \frac{1}{\#G}. \sum_{\rho\in\mathrm{Irr}(G)} n_\rho . \operatorname{Tr}(u_\rho \circ v_\rho).$$

On vérifie que

$$\mathbf{T}(\mathcal{F}(s), \mathcal{F}(t)) = \frac{1}{\#G}. \sum_{\rho\in\mathrm{Irr}(G)} n_\rho . \operatorname{Tr}(\rho(st)) = \frac{\chi_G(st)}{\#G}$$

où $\chi_G(st)$ est la valeur en st du caractère de la représentation régulière. Donc $\mathbf{T}(\mathcal{F}(s), \mathcal{F}(t))$ vaut 1 si $s = t^{-1}$ et 0 sinon. Cela prouve que les $(\mathcal{F}(s))_{s\in G}$ forment un système libre du $\mathbf{C}$-espace vectoriel $\mathcal{E}$. Comme la dimension de $\mathcal{E}$ est $\#G$ on a trouvé une base de $\mathcal{E}$. Sa base duale est constituée des formes linéaires $* \mapsto \mathbf{T}(\mathcal{F}(s^{-1}), *)$ sur $\mathcal{E}$. On en déduit la **formule d'inversion de Fourier**.

Théorème 13. *L'application*

$$\mathcal{F} : \mathbf{C}[G] \to \mathcal{E} = \oplus_{\rho\in\mathrm{Irr}(G)} \operatorname{End}(E_\rho)$$

est bijective. Soit $a = \sum_{s\in G} a_s.s$ un élément de $\mathbf{C}[G]$. Pour toute représentation irréductible ρ de G notons $u_\rho \in \operatorname{End}(E_\rho)$ l'image de a par $\tilde{\rho} : \mathbf{C}[G] \to \operatorname{End}(E_\rho)$. Autrement dit

$$\mathcal{F}(a) = \mathcal{F}(\sum_{s\in G} a_s.s) = (u_\rho)_{\rho\in\mathrm{Irr}(G)}.$$

Alors

$$a_s = \mathbf{T}(\mathcal{F}(s^{-1}), \mathcal{F}(a)) = \frac{1}{\#G} \sum_{\rho\in\mathrm{Irr}(G)} n_\rho . \operatorname{Tr}(\rho(s^{-1})u_\rho).$$

3.2. **Rappels sur les entiers.** Soit A un anneau commutatif unitaire. On dit qu'un élément x de A est **entier** sur $\mathbf{Z}$ s'il existe des entiers relatifs $(a_i)_{1\leqslant i\leqslant n}$ tels que

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0.$$

Dans le cas $A = \mathbf{C}$ les entiers sont appelés **entiers algébriques**. Les entiers relatifs sont des entiers algébriques.

Théorème 14. *Un nombre rationnel est entier algébrique si et seulement s'il est entier relatif.*

En effet soit r un nombre rationnel. On écrit $r = u/v$ avec v entier naturel positif et u entier relatif tels que le pgcd de u et v est 1. Supposons qu'il existe $n \geqslant 1$ et des $(a_i)_{1\leqslant i\leqslant n}$ tels que $r^n + a_1 r^{n-1} + \cdots + a_{n-1}r + a_n = 0$. Donc $u^n + a_1 v u^{n-1} + \cdots + a_{n-1}v^{n-1}u + a_n v^n = 0$. On en déduit que v divise u^n. Donc $v = 1$. □

Si A est un anneau commutatif unitaire et x un élément de A on note $\mathbf{Z}[x]$ le sous-anneau de A engendré par x. C'est l'image dans A de l'unique morphisme de l'anneau des polynômes $\mathbf{Z}[X]$ dans A qui envoie l'indéterminée X sur $x \in A$.

Théorème 15. *Soit A un anneau commutatif unitaire et x un élément de A. Les trois conditions suivantes sont équivalentes.*

(1) x est entier sur $\mathbf{Z}$,

(2) le sous-anneau $\mathbf{Z}[x]$ est un $\mathbf{Z}$-module de type fini,

(3) il existe un sous-$\mathbf{Z}$-module de type fini de A qui contient $\mathbf{Z}[x]$.

Si *(1)* est vérifiée alors il existe un entier naturel n et des entiers relatifs $(a_i)_{1\leqslant i\leqslant n}$ tels que $x^n = -a_1x^{n-1}-\cdots-a_{n-1}x-a_n$. On en déduit que le $\mathbf{Z}$-module engendré par les x^i pour $0 \leqslant i \leqslant n-1$ contient x^m pour tout $m \geqslant n$. Donc il est égal à $\mathbf{Z}[x]$. Donc *(2)* est vérifiée.

Réciproquement si *(2)* est vérifiée il existe un entier naturel I et des éléments $(g_i)_{1\leqslant i\leqslant I}$ de $\mathbf{Z}[x]$ qui l'engendrent en tant que $\mathbf{Z}$-module. On peut écrire

$$g_i = a_{i,0} + a_{i,1}x + \dots a_{i,d_i}x^{d_i}$$

où les d_i sont des entiers naturels et les $a_{i,j}$ des entiers relatifs. Soit alors n un entier plus grand que tous les d_i. Le $\mathbf{Z}$-module $\mathbf{Z}[x]$ est engendré par les x^j pour $0 \leqslant j \leqslant n-1$. Donc il existe des entiers relatifs $(b_k)_{0\leqslant k\leqslant n-1}$ tels que $x^n = \sum_{0\leqslant k\leqslant n-1} b_kx^k$. Donc x est entier sur $\mathbf{Z}$.

Il est évident que *(2)* implique *(3)*. Réciproquement si *(3)* est vérifiée il existe un $\mathbf{Z}$-module M de type fini qui contient $\mathbf{Z}[x]$. Comme $\mathbf{Z}$ est nœthérien on en déduit que $\mathbf{Z}[x]$ est lui aussi un $\mathbf{Z}$-module de type fini. □

Théorème 16. *Si A est un anneau unitaire commutatif qui est de type fini comme $\mathbf{Z}$-module alors tout élément de A est entier sur $\mathbf{Z}$.*

Cela résulte de l'implication *(3)* implique *(1)* dans le théorème 15. □

Théorème 17. *Soit A un anneau commutatif unitaire. Le sous-ensemble de A formé des éléments entiers sur $\mathbf{Z}$ est un anneau.*

Soit x un élément de A entier sur $\mathbf{Z}$. Le sous-$\mathbf{Z}$-module $\mathbf{Z}[x]$ de A est de type fini. Donc il existe un système fini $(g_i)_{1\leqslant i\leqslant I}$ de générateurs de ce sous-$\mathbf{Z}$-module.

Soit y un autre élément de A entier sur $\mathbf{Z}$. Le sous-$\mathbf{Z}$-module $\mathbf{Z}[y]$ de A est de type fini. Donc il existe un système fini $(h_j)_{1\leqslant j\leqslant J}$ de générateurs de ce sous-$\mathbf{Z}$-module.

Soit maintenant $\mathbf{Z}[x,y]$ le sous-anneau de A engendré par x et y. En tant que $\mathbf{Z}$-sous-module de A il est engendré par les $(x^uy^v)_{u,v\geqslant 0}$. Mais chaque x^uy^v est une combinaison $\mathbf{Z}$-linéaire des $(g_ih_j)_{1\leqslant i\leqslant I,\,1\leqslant j\leqslant J}$. Donc $\mathbf{Z}[x,y]$ est un $\mathbf{Z}$-module de type fini. Donc tous ses éléments sont entiers sur $\mathbf{Z}$. Cela est vrai en particulier de $x-y$ et de xy. Donc l'ensemble de entiers sur $\mathbf{Z}$ est un sous-anneau. □

Notons que si $f : A \to B$ est un morphisme d'anneaux commutatifs unitaires alors l'image par f de l'anneau des entiers sur $\mathbf{Z}$ de A est contenue dans l'anneau des entiers sur $\mathbf{Z}$ de B. En particulier, le conjugué d'un entier algébrique est un entier algébrique.

Soit maintenant G un groupe fini et $\rho : G \to \mathrm{GL}(E)$ une représentation complexe. Pour tout s dans G on a vu que ρ_s est diagonalisable et que ses valeurs propres sont des racines $\#G$-ièmes de l'unité. Ce sont donc des racines du polynôme $x^{\#G}-1$. En particulier ce sont des entiers algébriques. On déduit du théorème 17 que la valeur $\chi(s)$ du caractère de ρ en s est un entier algébrique elle aussi.

3.3. Le centre de $\mathbf{C}[G]$.

Si A est un anneau unitaire on appelle centre de A l'ensemble des a dans A tels que $ax = xa$ pour tout x dans A. Le centre de A est un sous-anneau de A. C'est un anneau unitaire et commutatif.

Soit $a = \sum_{s\in G} a_s.s$ un élément de $\mathbf{C}[G]$. Pour tout t dans G on a

$$t^{-1}at = \sum_{s\in G} a_s t^{-1}st = \sum_{s\in G} a_{tst^{-1}}s.$$

Donc a est dans le centre de $\mathbf{C}[G]$ si et seulement si $s \mapsto a_s$ est une application centrale. Donc le centre de $\mathbf{C}[G]$ est un $\mathbf{C}$-espace vectoriel de base $(\underline{C})_{C\in\mathrm{Conj}(G)}$ où $\mathrm{Conj}(G)$ est l'ensemble des classes de conjugaison de G, et pour toute classe de conjugaison C on pose

$$\underline{C} = \sum_{s\in C} s \in \mathbf{C}[G].$$

Plus généralement, si A est un sous-anneau de $\mathbf{C}$ alors le centre de $A[G]$ est un A-module libre de base $(\underline{C})_{C\in\mathrm{Conj}(G)}$. En particulier le centre de $\mathbf{Z}[G]$ est le $\mathbf{Z}$-module libre engendré par les $(\underline{C})_{C\in\mathrm{Conj}(G)}$. On déduit du théorème 16 que tous les éléments de $\mathbf{Z}[G]$ sont entiers sur $\mathbf{Z}$. Si C et D sont deux classes de conjugaison il existe des entiers relatifs $\alpha_{C,D}^E$ tels que

$$\underline{C}.\underline{D} = \sum_{E\in\mathrm{Conj}(G)} \alpha_{C,D}^E.\underline{E}.$$

Les $\alpha_{C,D}^E$ sont appelés **coefficients de structure** du centre de $\mathbf{C}[G]$.

La transformée de Fourier $\mathcal{F}$ est un isomorphisme d'anneaux entre $\mathbf{C}[G]$ et $\mathcal{E} = \oplus_{\rho\in\mathrm{Irr}(G)} \mathrm{End}(E_\rho)$. Elle induit donc un isomorphisme Ω entre le centre de $\mathbf{C}[G]$ et le centre de $\mathcal{E}$.

Or le centre de $\mathcal{E}$ est l'anneau

$$\oplus_{\rho\in\mathrm{Irr}(G)}\mathbf{C}.\mathrm{Id}_{E_\rho} \simeq \mathbf{C}^{\mathrm{Irr}(G)}.$$

Calculons l'image de $\underline{C}$ par Ω. On a

$$\mathcal{F}(\underline{C}) = \left(\sum_{s\in C} \rho_s\right)_{\rho\in\mathrm{Irr}(G)}$$

et chaque composante $\sum_{s\in C} \rho_s$ est une homothétie de l'espace de représentation E_ρ correspondant. Le rapport de cette homothétie est égal à la trace divisée par la dimension n_ρ de E_ρ. Donc

$$\Omega(\underline{C}) = \left(\frac{\#C.\chi_\rho(C)}{n_\rho}\right)_{\rho\in\mathrm{Irr}(G)} \in \mathbf{C}^{\mathrm{Irr}(G)}.$$

Puisque $\underline{C}$ est entier sur $\mathbf{Z}$, son image par le morphisme d'anneaux Ω l'est aussi. Donc les $\frac{\#C.\chi_\rho(C)}{n_\rho}$ sont des entiers algébriques.

Théorème 18. *Soit G un groupe fini, ρ un caractère complexe irréductible de degré n et C une classe de conjugaison de G. Le nombre complexe*

$$\frac{\#C.\chi(C)}{n}$$

est un entier algébrique.

Puisque les valeurs des caractères de G sont des entiers algébriques, pour toute classe C dans $\mathrm{Conj}(G)$, la valeur $\chi(C)$ est un entier algébrique. Le conjugué d'un entier algébrique est un entier algébrique. Donc $\overline{\chi(C)}$ est algébrique. Donc la somme

$$\sum_{C\in \mathrm{Conj}(G)} \frac{\#C.\chi(C).\overline{\chi(C)}}{n} = \sum_{s\in G} \frac{\chi(s).\overline{\chi(s)}}{n}$$

est un entier algébrique. D'après le théorème 5

$$\sum_{s\in G} \frac{\chi(s).\overline{\chi(s)}}{n} = \frac{\#G}{n}.$$

Donc $\frac{\#G}{n}$ est un entier algébrique. C'est donc un entier relatif d'après le théorème 14. On en déduit le théorème d'intégralité suivant.

Théorème 19. *Soit G un groupe fini et soit ρ une représentation complexe irréductible de G. Le degré de ρ divise l'ordre de G.*

4. Exercices

Exercice 1 : Soit $n \geqslant 3$ un entier impair. Soit D_n le groupe diédral d'ordre $2n$. On a construit à la section 1.6 une représentation ρ^h de D_n pour tout entier h.

1. Pour quelles valeurs de h la représentation ρ^h est elle irréductible ?

On reprend les notations de la section 1.6. L'image de s par ρ^h est la matrice M qui a deux espaces propres de dimension 1. L'espace propre associé à la valeur propre 1 est engendré par le premier vecteur de la base canonique. L'espace propre associé à la valeur propre -1 est engendré par le second vecteur de la base canonique. Si ρ^h est reductible alors $\rho^h(r) = T(2h\pi/n)$ doit stabiliser ces deux espaces propres. Donc $\sin(2h\pi/n)$ est nul. Donc n divise $2h$. Donc h est un multiple de n.

Réciproquement, il est évident que si h est un multiple de n alors ρ^h est la somme directe des deux représentations de degré 1 de D_n.

2. Soient h_1 et h_2 deux entiers. Sous quelle condition les représentations ρ^{h_1} et ρ^{h_2} sont elles équivalentes ?

Deux représentations sont équivalentes si et seulement si elles ont le même caractère. Une condition nécessaire et suffisante est donc que $\cos(2\pi k h_1/n) = \cos(2\pi k h_2/n)$ pour tout entier k. C'est équivalent à n divise $h_1 - h_2$ ou $h_1 + h_2$. Autrement dit $h_1 = \pm h_2 \bmod n$.

3. Donnez la décomposition en somme de représentations irréductibles de $\rho^{h_1} \otimes \rho^{h_2}$.

Notons $\chi = \chi_{\rho^{h_1}\otimes\rho^{h_2}}$. On a $\chi = \chi_{\rho^{h_1}}.\chi_{\rho^{h_2}}$ donc

$$\begin{aligned}
\chi(r^k) &= 4\cos(2\pi h_1/n)\cos(2\pi h_2/n) \\
&= 2\cos(2\pi(h_1+h_2)/n) + 2\cos(2\pi(h_1-h_2)/n) \\
&= \chi_{\rho^{h_1+h_2}}(r^k) + \chi_{\rho^{h_1-h_2}}(r^k),
\end{aligned}$$

et

$$\chi(sr^k) = \chi(s) = 0 = \chi_{\rho^{h_1+h_2}}(sr^k) + \chi_{\rho^{h_1-h_2}}(sr^k).$$

Donc $\rho^{h_1} \otimes \rho^{h_2}$ est équivalente à la somme directe de $\rho^{h_1+h_2}$ et $\rho^{h_1-h_2}$. La décomposition en somme d'irréductibles de ces deux représentations a été donnée à la première question.

Exercice 2 : Donnez la table des caractères du groupe diédral D_n d'ordre $2n$ pour tout entier pair $n \geqslant 2$.

On note $n = 2m$ avec $m \geqslant 1$. La représentation ρ^h est réductible si et seulement si $\sin(2h\pi/n)$ est nul. Autrement dit n divise $2h$. Autrement dit h est un multiple de m.

Les représentations ρ^{h_1} et ρ^{h_2} sont équivalentes si et seulement si

$$\cos(2\pi k h_1/n) = \cos(2\pi k h_2/n)$$

pour tout entier k. Autrement dit $h_1 = \pm h_2 \bmod 2m$. Donc il y a $m-1$ représentations irréductibles à équivalence près parmi les ρ^h. Ce sont par exemple les ρ^h pour $1 \leqslant h \leqslant m-1$.

Le groupe dérivé de D_n contient $[s,r] = srs^{-1}r^{-1} = r^{-2}$. Le sous-groupe engendré par r^{-2} est d'ordre m. C'est un sous-groupe distingué isomorphe à C_m. On le note $< r^2 >$. Le quotient $D_n/< r^2 >$ est abélien d'ordre 4 et d'exposant 2. Il est engendré par les classes de r et de s modulo $< r^2 >$. Donc le groupe dérivé $D(D_n)$ de D_n est égal à $< r^2 >$ et l'abélianisé de D_n est

$$\mathrm{Ab}(D_n) = D_n/< r^2 > = < r \bmod D(D_n) > \oplus < s \bmod D(D_n) > .$$

Il y a donc quatre caractères multiplicatifs : le caractère unité ψ_u, la signature ψ_s définie par $\psi_s(r) = 1$ et $\psi_s(s) = -1$, le caractère ψ_r défini par $\psi_r(r) = -1$ et $\psi_r(s) = 1$, et enfin le produit $\psi_r\psi_s$.

La somme des carrés des degrés des représentations irréductibles déjà trouvées vaut $4(m-1) + 4 = 2n = \#D_n$. On a trouvé toutes les représentations irréductibles. Les classes de conjugaisons sont elles aussi au nombre de $m+3$. On trouve d'abord la classe de l'idéntité. Le centre de D_n est $\{1, r^m\}$. On obtient donc une autre classe de cardinal 1. C'est $\{r^m\}$. Pour tout k entre 1 et $m-1$ on trouve la classe de conjugaison $\{r^k, r^{-k}\}$. Le conjugué de $r^k s$ par r^ℓ est $r^{k-2\ell}s$. Il y a donc deux classes de réflexions : la classe de s et celle de rs. On a bien trouvé $m+3$ classes.

Dans le cas $m = 3$ on obtient la table des caractères suivante.

	1	r^3	r, r^{-1}	r^2, r^{-2}	s	rs
ψ_u	1	1	1	1	1	1
ψ_r	1	-1	-1	1	1	-1
ψ_s	1	1	1	1	-1	-1
ψ_{rs}	1	-1	-1	1	-1	1
χ_1	2	$2\cos(6\pi/6) = -2$	$2\cos(2\pi/6) = 1$	$2\cos(4\pi/6) = -1$	0	0
χ_2	2	$2\cos(12\pi/6) = 2$	$2\cos(4\pi/6) = -1$	$2\cos(8\pi/6) = -1$	0	0

Exercice 3 : Soit G un groupe fini et C une classe de conjugaison. Soit

$$D = \{s^{-1} | s \in C\}.$$

1. Montrer que D est une classe de conjugaison.

D'abord D est non-vide car C est non-vide. Soit t un élément de D. Alors $t = s^{-1}$ pour un certain s dans C. Montrons que D est la classe de conjugaison de t.

D'une part si t' est dans D alors $t' = (s')^{-1}$ pour un certain s' dans C. Donc $s' = u^{-1}su$ et $t' = u^{-1}s^{-1}u = u^{-1}tu$ est bien un conjugué de t.

Réciproquement, si t' est conjugué de t alors $t' = u^{-1}tu$ donc $t' = u^{-1}s^{-1}u = (u^{-1}su)^{-1}$ est bien l'inverse d'un élément de C. Donc t' est dans D.

2. Soit χ un caractère de G. Exprimez $\chi(D)$ en fonction de $\chi(C)$.

Soit s un élément de C. On a $\chi(D) = \chi(s^{-1}) = \overline{\chi(s)} = \overline{\chi(C)}$.

Exercice 4 : Soit G un groupe fini. Soit $u : G \to \mathrm{GL}_1(\mathbf{C}) = \mathbf{C}^*$ la représentation unité. Soit E un $\mathbf{C}$-espace vectoriel de dimension finie et soit $\rho : G \to \mathrm{GL}(E)$ un représentation complexe de G. Soit χ le caractère associé à ρ. Soit $E = \oplus_{\mu \in \mathrm{Irr}(G)} E_\mu$ la décomposition canonique de E. On note E_u la composante associée à u dans cette décomposition. On note $e_u(\rho)$ la multiplicité de u dans ρ.

1. Montrez que E_u est un $\mathbf{C}$-espace vectoriel de dimension $e_u(\rho)$.

Pour tout μ la dimension de E_μ est le produit du degré n_μ de μ par la multiplicité $e_\mu(\rho)$. Dans le cas de la représentation unité on trouve $n_u = 1$ donc la dimension de E_u est $e_u(\rho)$.

2. Montrez que $\#G.e_u(\rho) = \sum_{s \in G} \chi(s)$.

La multiplicité $e_u(\rho)$ est le produit scalaire

$$(\chi_u, \chi) = \frac{1}{\#G} \sum_{s \in G} \overline{\chi_u(s)} \chi(s) = \frac{1}{\#G} \sum_{s \in G} \chi(s).$$

Exercice 5 : Soit G un groupe fini. Soit X un ensemble fini. On suppose que G agit sur X. Soit E un $\mathbf{C}$-espace vectoriel de dimension $\#X$ et de base $(e_x)_{x \in X}$. Soit $\rho : G \to \mathrm{End}(E)$ la représentation linéaire définie par $\rho_s(e_x) = e_{s.x}$. C'est la représentation de permutation associée à l'action de G sur X. Soit χ le caractère associé à ρ. Soit $E = \oplus_{\mu \in \mathrm{Irr}(G)} E_\mu$ la décomposition canonique de E. On note E_u la composante associée à u dans cette décomposition. On note $e_u(\rho)$ la multiplicité de u dans ρ.

1. Montrez que E_u est l'ensemble des $\sum_{x \in X} \alpha_x e_x$ où $(\alpha_x)_{x \in X} \in \mathbf{C}^X$ et $\alpha_x = \alpha_{g.x}$ pour tout $x \in X$ et tout $g \in G$.

L'espace E_u est le sous-espace $E^G \subset E$ des vecteurs invariants par G. Tout élément v de E s'écrit $v = \sum_{x \in X} \alpha_x e_x$ pour un $(\alpha_x)_{x \in X} \in \mathbf{C}^X$. Et v est invariant par G si et seulement si pour tout s dans G on a

$$v = s.v = \sum_{x \in X} \alpha_x s.e_x = \sum_{x \in X} \alpha_x e_{sx} = \sum_{x \in X} \alpha_{s^{-1}.x} e_x$$

ce qui revient à demander que $\alpha_{s.x} = \alpha_x$ pour tout $x \in X$ et tout $s \in G$.

2. Montrez que la dimension de E_u est le nombre d'orbites dans X pour l'action de G. Donnez une base de E_u.

Soit $\mathrm{Orb}(X)$ l'ensemble des orbites de X sous l'action de G. Pour chaque orbite $O \in \mathrm{Orb}(X)$ on pose $\underline{O} = \sum_{x \in O} e_x$. Les $(\underline{O})_{O \in \mathrm{Orb}(X)}$ sont linéairement indépendants car ce sont des combinaisons linéaires deux-à-deux disjointes des vecteurs de bases. On a vu à la précédente question qu'un vecteur v de E est dans E_u et et seulement s'il est combinaison linéaire des $(\underline{O})_{O \in \mathrm{Orb}(X)}$. Donc les $(\underline{O})_{O \in \mathrm{Orb}(X)}$ forment une base de E_u et la dimension de E_u est le nombre d'orbites.

3. Montrez que le nombre d'orbites dans X pour l'action de G est $\frac{\sum_{s \in G} \chi(s)}{\# G}$.

Le nombre d'orbites est la dimension de E_u c'est-à-dire la multiplicité $e_u(\rho)$ dans la représentation par permutation ρ. On a calculé cette multiplicité à l'exercice précédent.

4. Pour tout $s \in G$ on note $X_s = \{x \in X | s.x = x\}$ l'ensemble des éléments de X fixés par s. Montrer la formule de Burnside

$$\# \mathrm{Orb}(X) = \frac{\sum_{s \in G} \# X_s}{\# G}.$$

Exercice 6 : Le nombre $\sqrt{\sqrt{2} - 1} + \sqrt{3}$ est il un entier algébrique ?

Exercice 7 : Soit $n \geqslant 2$ un entier. Soit C_n le groupe cyclique d'ordre n.

1. Quel est le centre de l'algèbre $\mathbf{C}[C_n]$?

2. Calculez les coefficients de structure du centre de l'algèbre $\mathbf{C}[C_n]$.

Exercice 8 : Soit $n \geqslant 3$ un entier impair. Soit D_n le groupe diédral d'ordre $2n$. Calculez les coefficients de structure du centre de l'algèbre $\mathbf{C}[D_n]$.

On pose $n = 2m + 1$ avec $m \geqslant 1$.

Les classes de conjugaisons de D_n sont $\{1\}$, $\{s, sr, sr^2, \ldots, sr^{2m}\}$ et $\{r^k, r^{-k}\}$ pour $1 \leqslant k \leqslant m$. On définit les éléments correspondants dans $\mathbf{C}[D_n]$ soit $I = 1$,

$$S = s + sr + sr^2 + \cdots + sr^{2m}$$

et

$$R_k = r^k + r^{-k}$$

pour $1 \leqslant k \leqslant m$.

Il s'agit de calculer la table de multiplication dans cette base. Pour tout entier relatif k non divisible par $2m+1$ on note $\overline{k}$ l'unique entier congru à $\pm k$ dans l'intervale $[1,m]$.

On vérifie que

$$R_kR_l = R_{\overline{k+l}} + R_{\overline{k-l}}$$

si $k \neq l$. Et $R_k^2 = R_{\overline{2k}} + 2I$.

De plus $S.R_k = 2S$ et

$$S^2 = (2m+1)(I + R_1 + R_2 + \cdots + R_m).$$

Exercice 9 : Soit G un groupe fini. Exprimez les coefficients de structure du centre de $\mathbf{C}[G]$ en fonction de la table des caractères de G.

Soient C, D et E trois classes de conjugaison dans G. Le coefficient de structure $\alpha_{C,D}^{E}$ est le coefficients de $\underline{E}$ dans le produit $\underline{C}.\underline{D}$. On utilise la transformée de Fourier $\mathcal{F}$. L'image de $\underline{C}$ par $\mathcal{F}$ est $(u_\rho)_{\rho\in\mathrm{Irr}(G)}$ où $u_\rho \in \mathrm{End}(E_\rho)$ est une homothétie de rapport

$$\mathrm{Tr}(u_\rho)/n_\rho = \#C.\chi_\rho(C)/n_\rho.$$

L'image de $\underline{D}$ par $\mathcal{F}$ est $(v_\rho)_{\rho\in\mathrm{Irr}(G)}$ où $v_\rho \in \mathrm{End}(E_\rho)$ est une homothétie de rapport

$$\mathrm{Tr}(v_\rho)/n_\rho = \#D.\chi_\rho(D)/n_\rho.$$

L'image du produit $\underline{C}.\underline{D}$ est donc $(w_\rho)_{\rho\in\mathrm{Irr}(G)}$ où $w_\rho \in \mathrm{End}(E_\rho)$ est une homothétie de rapport

$$\#C.\#D.\chi_\rho(C).\chi_\rho(D)/n_\rho^2.$$

Soit e un élément de $E \subset G$. Le coefficient $\alpha_{C,D}^{E}$ est le coefficient de e dans $\underline{C}.\underline{D} = \mathcal{F}^{-1}((w_\rho)_{\rho\in\mathrm{Irr}(G)})$. D'après le théorème 13 ce coefficient est

$$\begin{aligned}
\mathbf{T}(\mathcal{F}(e^{-1}),(w_\rho)_{\rho\in\mathrm{Irr}(G)}) &= \frac{1}{\#G}\sum_{\rho\in\mathrm{Irr}(G)} n_\rho\,\mathrm{Tr}(\rho(e^{-1})w_\rho)\\
&= \frac{1}{\#G}\sum_{\rho\in\mathrm{Irr}(G)} \frac{\#C.\#D.\chi_\rho(C).\chi_\rho(D)}{n_\rho}\mathrm{Tr}(\rho(e^{-1}))\\
&= \frac{1}{\#G}\sum_{\rho\in\mathrm{Irr}(G)} \frac{\#C.\#D.\chi_\rho(C).\chi_\rho(D)}{n_\rho}\chi_\rho(e^{-1})\\
&= \frac{\#C.\#D}{\#G}\sum_{\rho\in\mathrm{Irr}(G)} \frac{\chi_\rho(C).\chi_\rho(D).\overline{\chi_\rho(E)}}{n_\rho}.
\end{aligned}$$

Exercice 10 : Soit G un groupe fini. Pour $u = \sum_{s\in G} u_s s$ et $v = \sum_{s\in G} v_s s$ deux éléments de $\mathbf{C}[G]$ on pose

$$< u, v >= \sum_{s\in G} u_{s^{-1}} v_s.$$

1. Montrer que l'application de $\mathbf{C}[G] \times \mathbf{C}[G]$ dans $\mathbf{C}$ qui à (u, v) associe $< u, v >$ est $\mathbf{C}$-bilinéaire.

2. Montrer que pour s et t dans G on a

$$< s, t >= \mathbf{T}(\mathcal{F}(s), \mathcal{F}(t)).$$

3. Montrer que pour u et v dans $\mathbf{C}[G]$ on a

$$< u, v >= \mathbf{T}(\mathcal{F}(u), \mathcal{F}(v)).$$

On dira que la transformée de Fourier est compatible avec les formes bilinéaires $<,>$ et $\mathbf{T}(,)$.

Exercice 11 : Soit $n \geqslant 3$ un entier impair. Soit D_n le groupe diédral d'ordre $2n$. On définit une action de D_n sur $\mathbf{Z}/n\mathbf{Z}$ en posant $rx = x + 1$ et $sx = -x$ pour tout x dans $\mathbf{Z}/n\mathbf{Z}$. On appelle ρ la représentation par permutation associée à cette action.

1. Rappelez la définition de ρ.

2. Calculez le caractère de ρ.

Le caractère χ de ρ compte les points fixes. Pour tout s dans D_n la valeur $\chi(s)$ est le nombre de points de $\mathbf{Z}/n\mathbf{Z}$ fixés par s.

Donc $\chi(1) = n$ et $\chi(r^k) = 0$ si k n'est pas un multiple de n. Et $\chi(sr^k) = 1$.

3. Quelle est la décomposition en somme de représentations irréductibles de ρ ?

On reprend les notations de la section 2.7. On pose en particulier $n = 2m + 1$.

La multiplicité de la représentation unité ψ_0 est le produit scalaire

$$(\psi_0, \chi) = \frac{1.n + (n-1).1.0 + n.1.1}{2n} = 1.$$

La multiplicité de la représentation signature ψ_1 est le produit scalaire

$$(\psi_1, \chi) = \frac{1.n + (n-1).1.0 - n.1.1}{2n} = 0.$$

Soit h un entier entre 1 et m. La multiplicité de la représentation ρ^h est le produit scalaire

$$(\chi^h, \chi) = \frac{2.n + \sum_{1\leqslant k\leqslant m} 2\cos(2\pi hk/n).0 \ - n.0.1}{2n} = 1.$$

Donc $\rho \simeq \chi_0 \oplus_{1\leqslant h\leqslant m} \rho^h$.

RÉFÉRENCES

[1] Jean-Pierre SERRE : *Représentations linéaires des groupes finis*. Hermann, cinquième édition, 1998.

[2] Olivier BRINON : *Cours de Master 1 : modules, espaces quadratiques*. Université de Bordeaux, 2017. https://www.math.u-bordeaux.fr/~obrinon/enseignement/modules/modules.pdf.

[3] Emmanuel KOWALSKI : *An introduction to the representation theory of groups*, volume 155 de *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2014.

[4] Emmanuel KOWALSKI : *Representation theory*. ETH Zürich, 2011. https://people.math.ethz.ch/~kowalski/representation-theory-notes.pdf.

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, BORDEAUX INP, INRIA, CNRS, UMR 5251, F-33400 TALENCE, FRANCE.

E-mail address: Jean-Marc.Couveignes@u-bordeaux.fr