107- Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-ev.

Soient G un groupe fini et V un $\mathbb{C}$-ev.

I] Premières définitions.

• Représentation linéaire : On appelle représentation linéaire de G dans V la donnée d'un morphisme de groupe $\rho : G \to GL(V)$.
Ceci correspond à la donnée d'une action linéaire de G sur V définie par $\forall (g,v) \in G\times V \quad g.v = \rho(g)(v)$.
On appelle dimension de la représentation la dimension de V.

• Exemples : → Rep. triviale : $G \to GL(V)\,;\ g \longmapsto Id_V$.

→ $\mathbb{Z}/2\mathbb{Z} \to \mathbb{C}^* = GL(\mathbb{C})$

$\bar{0} \longmapsto 1$

$\bar{1} \longmapsto -1$

→ Rep. signature : $\rho : \mathfrak{S}_n \to \mathbb{C}^*$, $\sigma \longmapsto \varepsilon(\sigma)$ (où ε est le morphisme signature)

→ Si $G < GL_n(\mathbb{C})$ alors l'action

$$G \times \mathbb{C}[X_1,\dots,X_n] \longrightarrow \mathbb{C}[X_1,\dots,X_n]$$
$$(g, P) \longmapsto P\left(g.\begin{pmatrix}X_1\\ \vdots \\ X_n\end{pmatrix}\right)$$

donne une représentation de G dans $\mathbb{C}[X_1,\dots,X_n]_d$ ($d\in\mathbb{N}$) de dimension $\binom{n+d-1}{n-1}$

• Sous-représentation : Soit $\rho : G \to GL(V)$ une représentation de G.
Si W est un sev de V stable par G, alors $\tilde{\rho} : G \to GL(W)$, $g \longmapsto \rho(g)|_W^W$ est une représentation de G dans W.

• Déf : Une représentation V est dite irréductible si les seules ss-rep. sont V et $\{0\}$

• Exemple : On considère la représentation par permutation $\mathfrak{S}_n \to GL_n(\mathbb{C})$, $\sigma \longmapsto P_\sigma$.
Alors $V_1 = Vect(x_1 + \dots + x_n)$ est une ss-représentation.

• Somme directe : Soient $(\rho_1, V_1), (\rho_2, V_2)$ deux représentations de G.
On définit la représentation somme directe $(\rho_1\oplus\rho_2, V_1\oplus V_2)$ par :
$\forall g\in G,\ \forall (v_1,v_2)\in V_1\times V_2 \quad (\rho_1\oplus\rho_2)(g)(v_1,v_2) = (\rho_1(g)(v_1), \rho_2(g)(v_2))$.

• Exemple : On reprend l'exemple de la représentation par permutation $(\mathfrak{S}_n, \mathbb{C}^n)$. On a $\mathbb{C}^n = V_1 \oplus V_2$.
V_1 est défini ci-dessus et $V_2 = \{x_1 + x_2 + \dots + x_n = 0\}$
= représentation standard.

• $\mathbb{C}[G]$: On appelle $\mathbb{C}[G]$ la $\mathbb{C}$-algèbre engendrée par les $\{e_g\}_{g\in G}$ avec les relations $e_g . e_h = e_{gh}$. $\mathbb{C}[G]$ est l'algèbre du groupe G.

• Remarque : L'ev $\mathbb{C}[G]$ s'identifie naturellement à $\mathbb{C}^G$ par :
$$e_g \longmapsto \left(\delta_g : \begin{array}{l} G \to \mathbb{C} \\ h \longmapsto \begin{cases} 0 & \text{si } h\neq g \\ 1 & \text{si } h = g \end{cases}\end{array}\right)$$

• Produit scalaire : On définit un produit scalaire hermitien sur $\mathbb{C}[G]$ par $\forall f,g\in\mathbb{C}[G]$ $\langle f,g\rangle = \frac{1}{|G|}\sum_{x\in G}\overline{f(x)}\,g(x)$.

• Représentation d'algèbre : Soit A une $\mathbb{C}$-algèbre.
On appelle représentation d'algèbre de A dans V la donnée d'un morphisme de $\mathbb{C}$-algèbre $\tilde{\rho} : A \to End(V)$.

• Remarques : ① Toute représentation linéaire $\rho : G \to GL(V)$ se prolonge de façon unique en une représentation d'algèbre $\hat{\rho} : \mathbb{C}[G] \to End(V)$.
② La définition d'une rep. d'algèbre de $\mathbb{C}[G]$ $\Leftrightarrow$ la définition d'un $\mathbb{C}[G]$-module à gauche.
Ainsi la définition d'une représentation de G correspond à la définition d'un $\mathbb{C}[G]$-module à gauche.

• Représentation régulière : C'est la représentation de G dans $\mathbb{C}[G]$ notée $R(G)$, définie par : $\forall g,h\in G \quad \rho(g)(e_h) = e_g . e_h = e_{gh}$.

• Caractère : On appelle caractère d'une rep. $\rho : G \to GL(V)$ l'application $\chi_\rho : G \to \mathbb{C}$, $g \longmapsto Tr(\rho(g))$.

• Exemples : → Rep. triviale : $\chi_\rho(g) = \dim_{\mathbb{C}}(V)\ \forall g\in G$.

→ Rep. régulière : $\chi_{R(G)}(g) = \begin{cases} 0 & \text{si } g\neq e \\ |G| & \text{si } g = e\end{cases}$

→ $\oplus$: $\chi_{\rho_1\oplus\rho_2} = \chi_{\rho_1} + \chi_{\rho_2}$.

→ Caractères de $\mathbb{Z}/n\mathbb{Z}$: $j\in[0, n-1]$
$$\chi_j : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}^*,\quad \bar{1} \longmapsto (\omega^1)^j \quad \text{où } \omega = e^{\frac{2i\pi}{n}}.$$

• **Remarque**: Pour tout caractère χ sur G et $s \in G$ on a $\chi(s^{-1}) = \overline{\chi(s)}$.

• **Théorème de Molien**: $\forall m \in \mathbb{N}_{>0}$ et $G \leq GL_m(\mathbb{C})$

on a $\displaystyle \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_m - zg)} = \sum_{\ell=0}^{+\infty} \dim_{\mathbb{C}} \left(\mathbb{C}[X_1, \dots, X_m]_\ell^G\right) z^\ell$.

[DEV]

• **G-morphisme**: Soient (V_1, ρ_1) et (V_2, ρ_2) deux représentations de G. On dit qu'une application linéaire $T: V_1 \to V_2$ est un G-morphisme entre ρ_1 et ρ_2 si $\forall g \in G$ le diagramme suivant commute :

$$\begin{array}{ccc} V_1 & \xrightarrow{\rho_1(g)} & V_1 \\ T \downarrow & & \downarrow T \\ V_2 & \xrightarrow{\rho_2(g)} & V_2 \end{array} \qquad T.\rho_1(g) = \rho_2(g).T$$

• **Définition**: (V_1, ρ_1) et (V_2, ρ_2) sont dites isomorphes s'il existe un G-morphisme bijectif entre ρ_1 et ρ_2.

• **Remarque**: Deux représentations isomorphes ont même caractère.

II] Cas des groupes abéliens, Transformée de Fourier: [PEYR].

Dans cette partie G désigne un groupe abélien fini.

• **Remarque**: G fini $\Rightarrow \forall g \in G$ $\rho(g)$ est diagonalisable.

et G commutatif $\Rightarrow \rho(G)$ ss-gpe commutatif de $GL(V)$.

Ainsi il existe une base de diagonalisation commune à tous les $\rho(g)$.

Conséquence : les représentations irréductible de G sont de degré 1.

• **Dual**: Le dual de G, noté $\hat{G}$, est l'ensemble des morphismes $\chi: G \to \mathbb{C}^*$. Ce qui correspond aux caractère des représentations irréductibles de G.

• **Proposition**: $\hat{G}$ est naturellement un groupe abélien fini

• **Proposition**: $\hat{G}$ est une base orthonormale de $\mathbb{C}[G]$.

• **Coefficient de Fourier**: Pour $f \in \mathbb{C}[G]$ on définit pour $\chi \in \hat{G}$, le coefficient de Fourier $c_f(\chi) = \langle f, \chi \rangle$

On définit $c: \mathbb{C}[G] \to \mathbb{C}[\hat{G}]$, $f \mapsto c_f$

• **Transformée de Fourier**: $\mathcal{F}: \mathbb{C}[G] \to \mathbb{C}[\hat{G}]$, $f \mapsto \hat{f}$

où $\hat{f}$ est définie par $\forall \chi \in \hat{G}$ $\hat{f}(\chi) = |G|\, c_f(\overline{\chi}) = \sum_{x \in G} f(x) \chi(x)$.

• **Formule d'inversion**: Pour $f \in \mathbb{C}[G]$ on a la formule d'inversion

$$f = \sum_{\chi \in \hat{G}} c_f(\chi) \chi = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi^{-1}.$$

• **Théorème**: c et $\mathcal{F}$ sont des isomorphismes d'ev.

• **Convolution**: Si $f_1, f_2 \in \mathbb{C}[G]$, on définit leur produit de convolution $f_1 * f_2$ par : $\forall g \in G$ $(f_1 * f_2)(g) = \sum_{x \in G} f_1(x) f_2(x^{-1}g)$.

• **Théorème**: $\mathcal{F}$ est un isomorphisme d'algèbre entre les algèbres $(\mathbb{C}[G], *)$ et $(\mathbb{C}[\hat{G}], \cdot)$

(on a $\widehat{f * g} = \hat{f} \cdot \hat{g}$ et $f * g = c_f \cdot c_g$ $\forall f, g \in \mathbb{C}[G]$)

• **Transformée de Fourier rapide**: Sur $\mathbb{Z}/N\mathbb{Z}$ avec $N \in 2\mathbb{Z}$, on remarque : si $\hat{f}_g = \{\hat{f}[0], \dots, \hat{f}[N/2 - 1]\}$, $\hat{f}_d = \{\hat{f}[N/2], \dots, \hat{f}[N-1]\}$ et si on définit pour $x \in \mathbb{R}$ et $a = (a_0, \dots, a_{N-1}) \in \mathbb{C}^N$ $\mathcal{Y}_N^x a = \left\{a_j e^{-2i\pi \frac{jx}{N}}\right\}_{j=0,\dots,N-1}$

Alors : $\hat{f}_g = \hat{f}_0 + \mathcal{Y}_{N/2}^{1/2} \hat{f}_1$, $\hat{f}_d = \hat{f}_0 - \mathcal{Y}_{N/2}^{1/2} \hat{f}_1$ avec $\begin{cases} f_0 = \{f[0], f[2], \dots, f[N-2]\} \\ f_1 = \{f[1], f[3], \dots, f[N-1]\} \end{cases}$

• **Application**: On déduit de cette remarque un algorithme de transformée de Fourier rapide (FFT) en $O(N \log N)$, au lieu d'un $O(N^2)$ par la méthode naïve.

• **Application**: (Multiplication rapide de polynômes).

On a les isomorphismes d'espace vectoriel

$$\mathbb{C}^{2N} \simeq \mathbb{C}_{2N-1}[X] \longrightarrow \mathbb{C}^{2N} \simeq \mathbb{C}[\mathbb{Z}/2N\mathbb{Z}]$$

$$(a_0, \dots, a_{2N-1}) = \sum_{n=0}^{2N-1} a_n X^n \longmapsto (P(\omega_{2N}^{-i}))_{i=0,\dots,2N-1} = \mathcal{F}((a_0, \dots, a_{2N-1}))$$

Pour $P, Q \in \mathbb{C}_{N-1}[X]$ on a

$$P \times Q = (a_i)_{0 \leq i \leq 2N-1} * (b_i)_{0 \leq i \leq 2N-1} = \mathcal{F}^{-1}\left(\mathcal{F}((a_i)_i) \cdot \mathcal{F}((b_i)_i)\right)$$

$\Longrightarrow$ algorithme de multiplication dans $\mathbb{C}_N[X]$ en $O(N \log N)$.

III] Cas général, Décomposition.

1) quelques définitions.

• Hom(V_1,V_2) : Si V_1 et V_2 sont deux représentations de G on définit une représentation de G dans Hom$(V_1,V_2)=\mathcal{L}(V_1,V_2)$ par.

Si $g\in G$, $u\in$ Hom(V_1,V_2), alors $\forall v\in V_1$ $(g.u)(v)=g.u(g^{-1}.v)$

On a $\chi_{Hom(V_1,V_2)}=\overline{\chi_{V_1}}\cdot\chi_{V_2}$.

• Fonctions centrales : $f\in\mathbb{C}[G]$ est dite centrale si elle est constante sur les classes de conjugaison de G. L'ensemble des fonctions centrales sur G est un sev de $\mathbb{C}[G]$.
C'est le centre de $(\mathbb{C}[G],\cdot)$ où $\cdot$ est la multiplication définie plus haut.

• Remarque : Les caractères de G sont des fonctions centrales sur G.

2) Décomposition en somme directe d'irréductibles

• Th. de Maschke : Soient V une représentation de G et W une sous-représentation. Alors il existe une sous-représentation W' supplémentaire de W dans V. $V=W\oplus W'$.

• Corollaire : Toute représentation V de G se décompose en somme directe d'irréductible $V=V_1\oplus\dots\oplus V_k$ (V_i irréd. $i=1,\dots,k$.)

⚠ Il n'y a pas unicité de la décomposition.

• Lemme de Schur : Soient $\rho_V: G\to GL(V)$ et $\rho_W: G\to GL(W)$ deux représentations irréductibles. Soit $f\in\mathcal{L}(V,W)$ un G-morphisme
Alors (i) si ρ_V et ρ_W ne sont pas isomorphes $f\equiv 0$.
(ii) si $f\neq 0$, alors f est un isomorphisme, les représentations sont isomorphes. Si de plus on suppose $V=W$, $\rho_V=\rho_W$ alors f est une homothétie.

3) Propriétés des caractères.

• Relations d'orthogonalité :
→ Si χ est le caractère d'une représentation irréd. $\langle\chi,\chi\rangle=1$.
→ Si χ,χ' sont deux caractères non isomorphes, irréd. $\langle\chi,\chi'\rangle=0$.

• Corollaire : Il n'y a qu'un nombre fini de classe d'isomorphisme de représentation
Pour la suite, soit $(V_i)_{i=1,\dots,p}$ une famille de représentants et $(\chi_i)_{i=1,\dots,p}$ les caractères associés.

• Décomposition canonique : Soit V une représentation de G.
Alors $V\simeq\bigoplus_{i=1}^{p}V_i^{\oplus a_i}$ avec $a_i=\langle\chi_V,\chi_i\rangle$.
De plus $\langle\chi_V,\chi_V\rangle=\sum_{i=1}^{r}a_i^2$.

• Corollaire : Deux représentations sont isomorphes si elles ont même caractère.
De plus une représentation sur V de caractère χ_V est irréd. si et seulement si $\langle\chi_V,\chi_V\rangle=1$.

• Application à la représentation Régulière R :
(i) $\sum_{i=1}^{p}n_i^2=|G|$; (ii) pour $s\neq 1$ $\sum_{i=1}^{p}n_i\chi_i(s)=0$ $\left(\begin{array}{l}\text{avec}\\ n_i=\dim V_i\\ =\langle\chi_R,\chi_i\rangle\end{array}\right)$.

• Théorème : Les χ_i forment une bon de l'esp. des fonctions centrales sur G.

• Corollaire : Nb classe d'isomorphisme de représentation irréd.
= Nb classe de conjugaison de G.

• Corollaire : G commutatif $\Longleftrightarrow$ $\forall i$ $n_i=\dim V_i=1$.

• Corollaire : Si $H\leq G$ commutatif. $\forall i$ $n_i\leq|G/H|$

• Théorème : Le degré d'une rep. irréd. divise $|G|$. [DEV]

4) Table de caractère

• Définition :

(g_i) représentants des classes de conjugaison de G
k_i : ordre de la classe de conjugaison de g_i

	1	k_2 / g_2	$\dots$	k_p / g_p
χ_1	1	1	$\dots$	1
χ_2	n_2	$\chi_2(g_2)$		$\chi_2(g_p)$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
χ_p	n_p	$\chi_p(g_2)$	$\dots$	$\chi_p(g_p)$

• Exemples :

$\boxed{S_3}$

	1 / e	3 / τ	2 / $(1\,2\,3)$
χ_1 triviale	1	1	1
χ_2 signature	1	-1	1
χ_3	2	0	-1

$\boxed{S_4}$ En développement. [DEV]

$\boxed{S_4}$

		1 Id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
triviale	χ_1	1	1	1	1	1
Signature	χ_ε	1	-1	1	-1	1
Standard	χ_s	3	1	0	-1	-1
	χ_ω	3	-1	0	1	-1
	$\chi_{\omega'}$	2	0	-1	0	2

Références:

- "Représentations linéaires de groupes finis" Jean-Pierre Serre.
- "Elements d'analyse et d'algèbre" Pierre Colmez.
- "L'algèbre discrète de la transformée de Fourier" Gabriel Peyré
- "Groupes et symétries" Yvette Kosmann-Schwarzbach.
- "Les groupes finis et leurs représentations complexes" M.P. Malliavin.

Autres idées de développement:

- Lie-Kolchine (Chambert-Loir "Algèbre corporelle")
- Table des caractères de D_n (Serre, Kosmann, Peyré, Colmez).
- Calcul du caractère de la FFT
  Etude des représentations de la FFT } (Hourbaki)

Analogie rep irred / diagon des endom.