
REPRÉSENTATIONS LINÉAIRES DE GROUPES FINIS

par

Guy Henniart

La théorie de la transformation de Fourier a une version très simple pour les groupes abéliens finis (§1). Les premières difficultés du cas non abélien se présentent déjà pour les groupes finis. Pour un groupe fini non nécessairement abélien, on considère ses représentations dans des espaces vectoriels complexes de dimension finie. L'étude de ces représentations est maintenant l'une des théories de base de l'algèbre. Nous en exposons les principaux résultats aux §§2 à 5 ; notre référence est « Représentations linéaires des groupes finis », de J.-P. Serre, collection Méthodes chez Hermann. On peut aussi consulter le début du cours à l'X de P. Colmez. Nous déterminons ensuite explicitement tous les caractères des représentations irréductibles de $GL(2)$ sur un corps fini ; nous suivons pour cela C.J. Bushnell et G. Henniart « The local Langlands conjecture for $GL(2)$ », Grundlehren der math. Wiss. 335, Springer-Verlag 2006, Chap. 2.

1. Caractères des groupes abéliens finis

On dispose d'une théorie de la transformation de Fourier pour chaque groupe abélien localement compact. Pour un tel groupe H , on note \widehat{H} l'ensemble des *caractères* de H , c'est-à-dire des homomorphismes de groupes, continus, de H dans le groupe \mathbb{U} des nombres complexes de module 1. La multiplication dans \mathbb{U} fait de \widehat{H} un groupe abélien ; si on le munit de la topologie de la convergence uniforme sur

les parties compactes de H , c'est un groupe abélien localement compact. Les cas classiques sont celui où $H = \mathbb{Z}$, auquel cas \widehat{H} s'identifie à \mathbb{U} , celui où $H = \mathbb{U}$, avec \widehat{H} s'identifiant à \mathbb{Z} , et celui où $H = \mathbb{R}$, \widehat{H} s'identifiant alors à \mathbb{R} également, un accident heureux.

La transformation de Fourier associe alors à une fonction sur H , ayant de bonnes propriétés, une fonction sur \widehat{H} ; en particulier, on obtient un isomorphisme de l'espace des fonctions de carré intégrable sur H sur l'espace des fonctions de carré intégrable sur \widehat{H} . Dans tous les cas, le dual $\widehat{\widehat{H}}$ de \widehat{H} s'identifie canoniquement à H : on le voit dans les exemples ci-dessus, et le cas des groupes abéliens finis est traité plus loin. Ainsi la transformation de Fourier, de H vers \widehat{H} , a une application réciproque qui est encore une transformation de Fourier, de \widehat{H} vers $\widehat{\widehat{H}}$ identifié à H .

Le cas où H est un groupe abélien fini – muni tacitement de la topologie discrète – est particulièrement simple, les difficultés analytiques disparaissant.

Si H est un groupe cyclique de cardinal n , et si on choisit un générateur s de H , alors l'application $\chi \mapsto \chi(s)$ est un isomorphisme de \widehat{H} sur le groupe des racines n -ièmes de l'unité dans \mathbb{C} . Si H est le produit direct d'un nombre fini de sous-groupes H_i , $i \in I$, l'application de \widehat{H} dans le produit des groupes \widehat{H}_i , qui à χ associe $(\chi|_{H_i})_{i \in I}$, est un isomorphisme de groupes.

Écrivant alors un groupe abélien fini H comme produit de groupes cycliques, on prouve aisément les faits suivants :

(1) \widehat{H} est un groupe abélien fini isomorphe à H ;

(2) pour tout élément h de H distinct de l'élément neutre 1_H , il existe un caractère χ de H tel que $\chi(h)$ soit différent de 1, et on a alors $\sum_{\chi \in \widehat{H}} \chi(h) = 0$; bien sûr, on a $\sum_{\chi \in \widehat{H}} \chi(1_H) = |H|$.

Exercice. Vérifier les faits précédents ainsi que les assertions des remarques suivantes.

Remarque 1. Pour h dans H , l'application $e_h : \widehat{H} \rightarrow \mathbb{U}$ qui à χ associe $\chi(h)$ est un homomorphisme de groupes ; on obtient ainsi un homomorphisme de groupes $e_H : H \rightarrow \widehat{\widehat{H}}$, $h \mapsto e_h$, qui est injectif par (2) ci-dessus et surjectif par (1). C'est par cette application qu'on identifie $\widehat{\widehat{H}}$ à H .

La théorie de la transformation de Fourier dans ce cadre peut se résumer très simplement. Notons \mathbb{C}^H l'espace vectoriel des applications de H dans \mathbb{C} , et munissons-le du produit scalaire $\langle f, \varphi \rangle_H = \frac{1}{|H|} \sum_{h \in H} \overline{f(h)} \varphi(h)$. Alors les caractères de H forment une *base orthonormale* de \mathbb{C}^H : cela provient du fait (2) ci-dessus. Pour $f \in \mathbb{C}^H$, si l'on pose $\widehat{f}(\chi) = \langle \chi, f \rangle$ pour $\chi \in \widehat{H}$, on a $f = \sum_{\chi \in \widehat{H}} \widehat{f}(\chi) \chi$ et en particulier $f(1_H) = \sum_{\chi \in \widehat{H}} \widehat{f}(\chi)$. L'application $f \mapsto \widehat{f}$ est un isomorphisme d'espaces vectoriels de \mathbb{C}^H sur $\mathbb{C}^{\widehat{H}}$.

Remarque 2. Comme \widehat{H} est encore un groupe abélien fini, on peut appliquer la transformation de Fourier aux applications de \widehat{H} dans \mathbb{C} . Cela donne un isomorphisme $\varphi \mapsto \widehat{\varphi}$ de $\mathbb{C}^{\widehat{H}}$ sur \mathbb{C}^H , par l'identification de $\widehat{\widehat{H}}$ à H . Pour f dans \mathbb{C}^H , on trouve $\widehat{\widehat{f}}(h) = \frac{1}{|H|} f(h^{-1})$ pour h dans H .

Pour $H = \mathbb{Z}/n\mathbb{Z}$, on obtient la transformée de Fourier discrète très largement utilisée en algorithmique.

Remarque 3. Le groupe H agit sur \mathbb{C}^H par translation : $g \cdot f(h) = f(hg)$ pour h, g dans H et f dans \mathbb{C}^H . On a $\widehat{g \cdot f} = e_g \widehat{f}$.

2. Représentations linéaires des groupes finis

Si H est un groupe topologique localement compact non nécessairement abélien, le rôle des caractères de H est joué par les représentations unitaires irréductibles de H dans des espaces de Hilbert complexes. Les classes d'isomorphisme de telles représentations forment un espace topologique \widehat{H} , appelé dual unitaire de H , qui n'est pas un groupe en général. La transformation de Fourier associe à certaines fonctions sur H des fonctions, éventuellement à valeurs vectorielles, sur \widehat{H} . Ici encore, les difficultés d'ordre analytique s'évanouissent quand H est un groupe fini, ce que nous supposons désormais.

Par *représentation* de H , nous entendons ici représentation linéaire de H dans un espace vectoriel complexe de dimension finie : il s'agit donc de couples (ρ, V) , où V est un tel espace vectoriel et ρ un homomorphisme de groupes de H dans le groupe $\text{Aut}_{\mathbb{C}}(V)$ des automorphismes de l'espace vectoriel V ; par abus, on désigne souvent

la représentation par ρ , voire simplement par V . La *dimension*, ou degré, de (ρ, V) est la dimension de V .

Un caractère de H donne une représentation de H dans \mathbb{C} : le caractère constant de valeur 1 (dit caractère trivial) donne ainsi une *représentation* dite *triviale*.

Exemple 1. Soit n un entier strictement positif. Le groupe symétrique S_n agit sur \mathbb{C}^n par permutation de la base canonique : l'élément σ de S_n envoie e_i sur $e_{\sigma(i)}$. On obtient ainsi la *représentation de permutation naturelle* de S_n .

Exemple 2. Considérons l'espace euclidien \mathbb{R}^2 et sa base canonique (e_1, e_2) . Le groupe D_4 des isométries du carré $\{e_1, -e_1, e_2, -e_2\}$ agit sur \mathbb{R}^2 . Prolongeant ces isométries par \mathbb{C} -linéarité, on obtient une représentation de dimension 2 de D_4 .

Exemple 3. Plus généralement, soit D_n le groupe des isométries d'un polygone régulier à n côtés. Ce groupe d'ordre $2n$ est engendré par deux éléments, une rotation r d'angle $2\pi/n$ et une symétrie s , assujetties aux relations $r^n = 1$, $s^2 = 1$ et $srs = r^{-1}$.

On pose $X = \begin{pmatrix} e^{2i\pi/n} & 0 \\ 0 & e^{-2i\pi/n} \end{pmatrix}$ et $Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

L'application ρ_h donnée par $\rho_h(r) = X^h$ et $\rho_h(s) = Y$ se prolonge en un homomorphisme de groupes de D_n dans $\mathrm{GL}_2(\mathbb{C})$ et définit donc une représentation de D_n dans \mathbb{C}^2 .

Si (ρ', V') est une autre représentation de H , un *morphisme* de ρ dans ρ' est une application linéaire φ de V dans V' telle que $\varphi \circ \rho(h)$ et $\rho'(h) \circ \varphi$ soient égaux pour tout h dans H . Si φ est bijective, c'est un isomorphisme de ρ sur ρ' , encore appelé *équivalence* de ρ et ρ' . On note $\mathrm{Hom}_H(\rho, \rho')$ ou $\mathrm{Hom}_H(V, V')$ l'espace vectoriel complexe des morphismes de ρ dans ρ' .

Remarque 1. Soit $\mathbb{C}[H]$ l'algèbre du groupe H , dont nous notons les éléments $\sum_{h \in H} a_h h$. Si (ρ, V) est une représentation de H , V devient un module sur $\mathbb{C}[H]$, pour la loi d'action $(\sum_{h \in H} a_h h)v = \sum_{h \in H} a_h \rho(h)v$, pour $\sum a_h h$ dans $\mathbb{C}[H]$ et v dans V .

De cette façon la catégorie des représentations de H s'identifie à la catégorie des $\mathbb{C}[H]$ -modules qui sont de dimension finie sur \mathbb{C} . Une sous-représentation d'une représentation (ρ, V) de H est la même

chose qu'un sous-module du module V sur $\mathbb{C}[H]$, ce qui correspond à un sous-espace vectoriel stable de V , muni de l'action induite – stable signifie ici stable pour tous les $\rho(h)$, $h \in H$. On définit de façon évidente la somme d'une famille de sous-représentations de V .

Définition. Une représentation (ρ, V) de H est *irréductible* si V est un module simple sur $\mathbb{C}[H]$, autrement dit si V n'est pas nul et que ses seuls sous-espaces vectoriels stables sont $\{0\}$ et V .

Exemple 1 (suite). Pour $n \geq 2$, la représentation de permutation naturelle du groupe symétrique S_n n'est pas irréductible car la droite engendrée par $e_1 + e_2 + \dots + e_n$ est stable. À titre d'exercice, on peut démontrer que le supplémentaire formé des vecteurs dont la somme des coordonnées est nulle porte une sous-représentation irréductible de S_n .

Exemple 2 (suite). La représentation naturelle de D_4 dans \mathbb{C}^2 est irréductible.

Exemple 3 (suite). Si n est pair (respectivement impair) la représentation ρ_h de D_n est irréductible pour $h \neq 0$ et $h \neq n/2$ (respectivement $h \neq 0$) et les représentations V_{n-h} , V_{n+h} et V_h sont isomorphes. Ainsi, si n est pair (respectivement impair), nous obtenons $\frac{n}{2} - 1$ (respectivement $\frac{n-1}{2}$) représentations irréductibles de dimension 2, deux à deux non isomorphes.

Soit (ρ, V) une représentation de H , et soit W un sous-espace stable de V . Si p est un projecteur dans V d'image W , alors $q = \frac{1}{|H|} \sum_{h \in H} \rho(h) \circ p \circ \rho(h)^{-1}$ est un projecteur dans V d'image W ; il vérifie $\rho(h) \circ q = q \circ \rho(h)$ pour tout h dans H , et son noyau est un supplémentaire stable de W . Ainsi tout sous-espace stable de V possède un supplémentaire stable. On en déduit que ρ est somme directe de sous-représentations irréductibles.

Remarque 2. Par le même procédé de moyenne, on prouve que si (ρ, V) est une représentation de H , il existe sur V un produit scalaire invariant pour l'action de H ; ce produit scalaire fait de V un espace de Hilbert complexe de dimension finie, et de ρ une représentation unitaire de H dans cet espace.

La propriété première des représentations irréductibles est le « lemme de Schur » :

Théorème. *Si (ρ, V) est une représentation irréductible de H , tout endomorphisme de (ρ, V) est une homothétie.*

Si (ρ, V) est une représentation de H , tout élément z du centre $Z(H)$ de H agit dans V par l'endomorphisme $\rho(z)$ de (ρ, V) ; si ρ est irréductible, on en déduit qu'il existe un caractère ω_ρ de $Z(H)$, appelé le *caractère central* de ρ , tel qu'on ait $\rho(z) = \omega_\rho(z)1_V$ pour z dans $Z(H)$. Si H est abélien, on voit donc que toute représentation irréductible de H est de dimension 1, et que les classes d'isomorphisme de représentations irréductibles de H correspondent exactement aux caractères de H .

Remarque 3. Si (ρ, V) est une représentation irréductible de H , il découle du lemme de Schur que deux produits scalaires sur V invariants par H sont proportionnels. Ainsi l'ensemble des classes d'isomorphisme de représentations irréductibles de H n'est autre que le dual unitaire de H mentionné en introduction à ce paragraphe.

Remarque 4. Si (ρ, V) est une représentation de H qui n'est ni nulle ni irréductible, elle est somme directe de deux sous-représentations non nulles V_1 et V_2 , et l'endomorphisme de ρ qui coïncide avec l'identité sur V_1 et est nul sur V_2 n'est pas une homothétie!

3. Caractères des représentations de groupes finis

Si (ρ, V) est une représentation de H , son *caractère* χ_ρ est la fonction $h \mapsto \text{tr } \rho(h)$ de H dans \mathbb{C} – la terminologie est traditionnelle, même si elle peut prêter à confusion si H est abélien. Deux représentations de H qui sont isomorphes ont le même caractère. Si ρ est somme directe de deux sous-représentations ρ_1 et ρ_2 , on a $\chi_\rho = \chi_{\rho_1} + \chi_{\rho_2}$. Il est clair également que la fonction χ_ρ est constante sur les classes de conjugaison de H ; comme pour h dans H , $\rho(h)$ est d'ordre fini, on obtient aussi $\chi_\rho(h^{-1}) = \overline{\chi_\rho(h)}$. Notons $\mathcal{FC}(H)$ le sous-espace de \mathbb{C}^H formé des fonctions constantes sur les classes

de conjugaison, dites « fonctions de classes ». Munissons \mathbb{C}^H du produit scalaire $\langle f, \varphi \rangle_H = \frac{1}{|H|} \sum_{h \in H} \overline{f(h)} \varphi(h)$. Fixons un ensemble \mathcal{R} de représentations irréductibles de H , un par classe d'isomorphisme.

À l'aide du lemme de Schur, on prouve le résultat fondamental suivant.

Théorème. *La famille $(\chi_\rho)_{\rho \in \mathcal{R}}$ est une base orthonormale du sous-espace $\mathcal{FC}(H)$ de \mathbb{C}^H .*

En particulier, le nombre de classes d'isomorphisme de représentations irréductibles de H est le nombre de classes de conjugaison dans H . Les fonctions χ_ρ , pour ρ irréductible, s'appellent les *caractères irréductibles* de H ; notons que si ω_ρ est le caractère central de ρ , on a $\chi_\rho(zh) = \omega_\rho(z)\chi_\rho(h)$ pour $z \in Z(H)$ et $h \in H$.

Les valeurs des $(\chi_\rho)_{\rho \in \mathcal{R}}$ sont présentées sous forme de tableau carré, appelé *table des caractères*, dont la première colonne indique la liste des χ_ρ et la première ligne la liste des classes de conjugaison : chaque classe est représentée par un de ses éléments g , et on indique en indice le cardinal de la classe. On porte en ligne χ_ρ , colonne g , le coefficient $\chi_\rho(g)$.

Exemple 1 (suite). Le groupe S_3 possède 3 classes de conjugaison : $C_1 = \{1\}$, $C_{(1,2)} = \{(1, 2), (2, 3), (1, 3)\}$, $C_{1,2,3} = \{(1, 2, 3), (1, 3, 2)\}$. Nous connaissons déjà ses représentations irréductibles : le caractère trivial, le caractère signature, et la sous-représentation de dimension 2 de la représentation naturelle. La table de caractères de S_3 s'écrit donc :

	Id ₁	(1, 2) ₃	(1, 2, 3) ₂
χ_1	1	1	1
χ_{sign}	1	-1	1
χ_ρ	2	0	-1

Exemple 2 (suite). On écrit

$$D_4 = \{\text{Id}, r, r^2 = -\text{Id}, r^3 = -r, s, sr, -s, -sr\},$$

où r est la rotation de centre O et d'angle $\pi/2$ et s la symétrie par rapport à une des diagonales et on a $srs = r^{-1}$. Les classes de conjugaison de D_4 sont :

$$\begin{aligned} C_{\text{Id}} &= \{\text{Id}\} & C_r &= \{r, -r = srs\} & C_s &= \{s, -s = rsr^{-1}\} \\ C_{-\text{Id}} &= \{-\text{Id}\} & C_{sr} &= \{sr, -sr\}. \end{aligned}$$

Ainsi, D_4 possède 5 représentations irréductibles, à isomorphisme près : celle de dimension 2 vue précédemment et 4 représentations de dimension 1 données par $\chi(r) = \pm 1$ et $\chi(s) = \pm 1$, ce qui donne la table de caractères suivante :

	$C_{\text{Id}} \quad 1$	$C_r \quad 2$	$C_s \quad 2$	$C_{-\text{Id}} \quad 1$	$C_{sr} \quad 2$
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	-1	1	1	-1
χ_4	1	-1	-1	1	1
χ_5	2	0	0	-2	0

Exemple 3 (suite). Les classes de conjugaison dans $H = D_n$ dépendent de la parité de n : si n est pair, les symétries forment deux classes de conjugaison, et les rotations $\frac{n}{2} + 1$; mais D_n possède alors 4 représentations de dimension 1, ce qui complète la liste des caractères irréductibles. Si n est impair, les symétries forment une seule classe de conjugaison, les rotations $\frac{n+1}{2}$ et D_n a deux représentations de dimension 1.

Les conséquences du théorème précédent sont nombreuses et importantes.

(1) Deux représentations ρ et ρ' de H sont isomorphes exactement quand leurs caractères sont égaux : cela justifie la terminologie de « caractère ». De plus les morphismes de ρ dans ρ' forment un espace vectoriel de dimension $\langle \chi_\rho, \chi_{\rho'} \rangle_H$.

(2) Si une représentation (σ, V) de H est somme directe de sous-représentations irréductibles ρ_i , alors le nombre de ces sous-représentations qui sont isomorphes à un élément donné ρ de \mathcal{R} est $\langle \chi_\rho, \chi_\sigma \rangle_H$. En fait la somme de ces sous-représentations ρ_i est un sous-espace canonique de V appelé *sous-espace isotypique de type* ρ . On a $\chi_\sigma = \sum_{\rho \in \mathcal{R}} \langle \chi_\rho, \chi_\sigma \rangle_H \chi_\rho$, et $\langle \chi_\sigma, \chi_\sigma \rangle_H = \sum_{\rho \in \mathcal{R}} \langle \chi_\rho, \chi_\sigma \rangle_H^2$. En

particulier, la condition $\langle \chi_\sigma, \chi_\sigma \rangle_H = 1$ est une condition nécessaire et suffisante pour que σ soit irréductible. Plus généralement si une fonction f de $\mathcal{FC}(H)$ est combinaison linéaire à coefficients *entiers* de caractères irréductibles de H alors f est un caractère irréductible exactement quand les conditions suivantes sont valides :

- (1) $f(1) \geq 0$
- (2) $\langle f, f \rangle_H = 1$.

Remarques.

(1) Quelques considérations simples de théorie des nombres donnent que la dimension de toute représentation irréductible de H divise $|H|$ et même $|H/Z(H)|$.

(2) L'un des premiers grands succès de la théorie a été le théorème de Burnside selon lequel un groupe fini de cardinal $p^a q^b$, où p et q sont premiers, est résoluble.

L'espace \mathbb{C}^H est l'espace de plusieurs représentations naturelles :

- la représentation régulière droite δ de H , où $\delta(h)f : h' \mapsto f(h'h)$ pour $h \in H$;
- la représentation régulière gauche σ de H , où $\sigma(h)f : h' \mapsto f(h^{-1}h')$ pour $h \in H$;
- la représentation birégulière de $H \times H$, où $(h_1, h_2)f : h' \mapsto f(h_1^{-1}h'h_2)$ pour $(h_1, h_2) \in H \times H$.

Les deux premières ont le même caractère χ , qui vaut $|H|$ en 1_H , et 0 ailleurs ; on a $\langle \chi, \chi_\rho \rangle = \chi_\rho(1) = \dim \rho$ pour $\rho \in \mathcal{R}$, d'où $\chi = \sum_{\rho \in \mathcal{R}} \dim \rho \chi_\rho$, ce qui donne $|H| = \sum_{\rho \in \mathcal{R}} (\dim \rho)^2$ et $\sum_{\rho \in \mathcal{R}} \dim \rho \chi_\rho(h) = 0$ pour $h \neq 1_H$.

Exercices.

- (1) Calculer le caractère de la représentation birégulière.
- (2) Déterminer la table de caractères de S_4 à l'aide des résultats précédents (on peut déterminer le caractère de la représentation irréductible de dimension 2 sans connaître explicitement cette représentation). On obtient le résultat suivant :

	e ₁	$(1\ 2)$ ₆	$(1\ 2)(3, 4)$ ₃	$(1, 2, 3)$ ₈	$(1, 2, 3, 4)$ ₆
χ_1	1	1	1	1	1
χ_2	3	1	-1	0	-1
χ_3	2	0	2	-1	0
χ_4	3	-1	-1	0	1
χ_5	1	-1	1	1	-1

4. Transformation de Fourier

Nous gardons les notations du §3, et notons X l'ensemble des caractères irréductibles de H .

Si f est une fonction sur H , on note \widehat{f} la fonction de X dans \mathbb{C} donnée par $\widehat{f}(\chi) = \langle \chi, f \rangle_H$ pour $\chi \in X$.

On obtient ainsi *toutes* les fonctions sur X , et pour f dans $\mathcal{FC}(H)$, on a la formule d'inversion de Fourier

$$f = \sum_{\chi \in H} \langle \chi, f \rangle_H \chi,$$

donnant en particulier $f(1_H) = \sum_{\chi \in H} \langle \chi, f \rangle_H \cdot \chi(1_H)$.

(Dans le cadre des représentations unitaires d'un groupe localement compact, cette dernière formule est une « formule de Plancherel »).

Dans ce cas non abélien, on ne peut appliquer deux fois la transformation de Fourier, et les produits scalaires $\langle \chi, f \rangle_H$ pour f dans \mathbb{C}^H ne permettent de reconstituer que la projection de f sur $\mathcal{FC}(H)$. Notons cependant que, comme dans le cas abélien, si l'on munit \mathbb{C}^H de l'opération de convolution

$$(f, \varphi) \longmapsto f * \varphi : h \mapsto \sum_{g \in H} f(hg^{-1})\varphi(g)$$

– cette opération correspond à la loi d'algèbre de groupe de $\mathbb{C}[H]$ via l'identification évidente de $\mathbb{C}[H]$ à \mathbb{C}^H –, alors pour χ dans X on a $\widehat{f * \varphi}(\chi) = \widehat{f}(\chi)\widehat{\varphi}(\chi)$. Pour le dire d'une autre façon, si l'on fait agir H sur \mathbb{C}^H par la représentation régulière droite, et sur \mathbb{C}^X par $h \cdot \varphi(\chi) = \chi(h)\varphi(\chi)$ pour $\varphi \in \mathbb{C}^X$, $h \in H$, alors l'application $f \mapsto \widehat{f}$ de \mathbb{C}^H dans \mathbb{C}^X est un morphisme.

Si l'on veut récupérer les fonctions sur H et non plus seulement les fonctions constantes sur les classes de conjugaison, il faut accepter d'utiliser les représentations ρ dans \mathcal{R} et non plus seulement leur caractère. Dans le cas d'un groupe localement compact, le théorème suivant, dû à Burnside, serait un « théorème de Paley-Wiener matriciel ».

Théorème. *L'application $\mathbb{C}[H] \rightarrow \prod_{(\rho, V_\rho) \in \mathcal{R}} \text{End}_{\mathbb{C}}(V_\rho)$ qui à $a = \sum_{h \in H} a_h h$ associe la famille $(\rho(a))_{\rho \in \mathcal{R}}$ où $\rho(a) = \sum_{h \in H} a_h \rho(h)$, est un isomorphisme d'algèbres.*

L'application réciproque est donnée par $(u_\rho) \mapsto \sum_{h \in H} u(h)h$ avec

$$u(h) = \frac{1}{|H|} \sum_{\rho \in \mathcal{R}} \dim \rho \cdot \text{tr}(\rho(h^{-1})u_\rho).$$

On peut décrire en ces termes les sous-espaces isotypiques introduits au § 4. À un caractère irréductible χ de H , on associe l'élément

$$e_\chi = \sum_{h \in H} \frac{\chi(1_H)}{|H|} \chi(h^{-1})h$$

de $\mathbb{C}[H]$; c'est un idempotent indécomposable dans le centre de $\mathbb{C}[H]$, et on a $\sum_{\chi \in X} e_\chi = 1$, et $e_\chi e_{\chi'} = 0$ si χ et χ' sont deux caractères irréductibles distincts. Si (σ, V) est une représentation de H , son sous-espace isotypique de type $\rho \in \mathcal{R}$ est $e_{\chi_\rho} V$.

5. Dualité

Si (σ, V) est une représentation de H , on dispose de la représentation contragrédiente σ^\vee de σ ; c'est la représentation de H sur le dual V^* de V donnée par la formule $\sigma^\vee(h) = {}^t\sigma(h^{-1})$ pour $h \in H$. L'identification de V à son bidual donne un isomorphisme canonique de σ sur $(\sigma^\vee)^\vee$. On a $\chi_{\sigma^\vee}(h) = \chi_\sigma(h^{-1}) = \overline{\chi_\sigma(h)}$ pour $h \in H$. Il s'ensuit que σ^\vee est irréductible si et seulement si σ l'est. On dispose ainsi de la représentation $\sigma \otimes \sigma^\vee$ de $H \times H$ sur le produit tensoriel $V \otimes V^*$; son caractère est donné par $(h, h') \mapsto \chi_\sigma(h)\chi_{\sigma^\vee}(h')$, elle est irréductible.

On peut alors analyser la représentation birégulière de $H \times H$ sur \mathbb{C}^H . Soit ρ dans \mathcal{R} est $\chi = \chi_\rho$. Alors $e_\chi * \mathbb{C}^H$ est à la fois :

- le sous-espace isotypique de type ρ pour la représentation régulière gauche de H ;
- le sous-espace isotypique de type ρ^\vee pour la représentation régulière droite de H ;
- le sous-espace isotypique de type $\rho \otimes \rho^\vee$ pour la représentation régulière.

En fait, ce dernier sous-espace isotypique est irréductible : il est isomorphe à $\rho \otimes \rho^\vee$ comme représentation de $H \times H$. Via l'identification de $\mathbb{C}[H]$ et \mathbb{C}^H , ce n'est qu'une autre façon de voir le théorème de Burnside. Ainsi, comme représentation de $H \times H$, \mathbb{C}^H est isomorphe à $\bigoplus_{\rho \in \mathcal{R}} \rho \otimes \rho^\vee$. Cet énoncé a une généralisation au cas de groupes compacts sous le nom de « Théorème de Peter-Weyl ».

6. Construction de représentations irréductibles : restriction et induction

Pour un groupe fini donné H il est fort intéressant de construire toutes ses représentations irréductibles (à isomorphisme près) ou à tout le moins de déterminer tous ses caractères irréductibles. Noter que pour se donner un caractère irréductible, il suffit de connaître ses valeurs sur les classes de conjugaison et qu'il se peut que H ait beaucoup moins de classes de conjugaison que d'éléments !

En tout cas, on sait qu'il y a autant de caractères irréductibles que de classes de conjugaison ; on essaie donc de construire de plus en plus de caractères irréductibles, en s'arrêtant dès qu'on atteint le bon nombre. Au départ, cependant, on ne connaît guère que les caractères irréductibles de degré 1, les homomorphismes de H dans \mathbb{U} .

Mais on peut essayer une méthode inductive : si H a un sous-groupe sympathique J dont on connaisse les caractères irréductibles, on peut en tirer des caractères irréductibles de H , ou des informations sur ces caractères. C'est le principe de la méthode d'induction-restriction.

On considère un groupe fini H et un sous-groupe J de H . Si (σ, V) est une représentation de H alors $(\sigma|_J, V)$ est une représentation de J appelée restriction de σ à J , et parfois notée $\text{Res}_J^H \sigma$. En sens inverse, si (ρ, W) est une représentation de J , on forme l'espace $\text{Ind}_J^H W$ des fonctions f de H dans W vérifiant $f(jh) = \rho(j)(f(h))$ pour j dans J et h dans H . Sur cet espace de fonctions, H agit par translations à

droite : $hf(h') = f(h'h)$ pour h, h' dans H . On obtient ainsi une représentation de H dite *induite* de ρ et notée $\text{Ind}_J^H \rho$.

On a un isomorphisme canonique dit de « réciprocity de Frobenius »

$$\text{Hom}_J(\sigma|_J, \rho) \simeq \text{Hom}_H(\sigma, \text{ind}_J^H \rho);$$

si Φ est un morphisme de σ dans $\text{ind}_J^H \rho$, le morphisme correspondant de $\sigma|_J$ dans ρ associe à un vecteur v de V le vecteur $\Phi(v)(1_H)$ de W . (À titre d'exercice, vérifier qu'on a bien ainsi un isomorphisme, et décrire l'isomorphisme réciproque).

Remarques.

(1) Voyant W comme un module sur $\mathbb{C}[J]$, le $\mathbb{C}[H]$ -module $\text{Ind}_J^H W$ s'identifie à $\text{Hom}_{\mathbb{C}[J]}(\mathbb{C}[H], W)$, où $\mathbb{C}[J]$ agit sur $\mathbb{C}[H]$ par multiplications à gauche, et $\mathbb{C}[H]$ sur lui-même par multiplications à droite : à une fonction f dans $\text{Ind}_J^H W$, on associe l'application de $\mathbb{C}[H]$ dans W donnée par $\sum_{h \in H} a_h h \mapsto \sum a_h f(h)$, qui est $\mathbb{C}[J]$ linéaire.

(2) On donne habituellement une autre définition de l'induction : $\text{ind}_J^H \rho$ est l'action de H sur le $\mathbb{C}[H]$ -module $\mathbb{C}[H] \otimes_{\mathbb{C}[J]} W$. Les propriétés du produit tensoriel mènent à une autre « réciprocity de Frobenius » : $\text{Hom}_J(\rho, \sigma|_J) \simeq \text{Hom}_H(\text{ind}_J^H \rho, \sigma)$.

Dans notre cas où H est fini, un exercice permet de montrer que les deux induites sont canoniquement isomorphes, de sorte que les deux « réciprocitys de Frobenius » sont disponibles par $\text{Ind}_J^H \rho$. Dans le cas des représentations de groupes p -adiques, ces deux notions sont distinctes ; voir le texte de C. Blondel dans ce volume.

Si ρ est irréductible, $\text{Ind}_J^H \rho$ ne l'est pas en général, mais souvent on peut analyser $\text{Ind}_J^H \rho$ pour en tirer ses composants irréductibles (cf. § 8). La première chose à faire est de calculer $\text{End}_J(\text{Ind}_J^H \rho)$ ou du moins sa dimension. Plus généralement, soit K un sous-groupe de H et τ une représentation de K . La réciprocity de Frobenius donne un isomorphisme de $\text{Hom}_H(\text{Ind}_J^H \rho, \text{Ind}_K^H \tau)$ sur $\text{Hom}_K((\text{Ind}_J^H \rho)|_K, \tau)$, et il s'agit d'identifier la restriction à K de $\text{Ind}_J^H \rho$. écrivant H comme union disjointe de doubles classes JhK , $(\text{Ind}_J^H \rho)|_K$ apparaît comme la somme directe de sous-espaces Z_h , Z_h étant formé par les fonctions à support dans JhK . L'application qui à $f \in Z_h$ associe la fonction $k \mapsto f(hk)$ sur K donne un isomorphisme de Z_h sur $\text{Ind}_{K \cap h^{-1}Jh}^K(\rho^h)$ où, pour $k \in K \cap h^{-1}Jh$, on a posé $\rho^h(k) = \rho(hkh^{-1})$

(noter que hkh^{-1} appartient à J). Ainsi, $\text{Hom}_H(\text{Ind}_J^H \rho, \text{Ind}_K^h \tau)$ est la somme directe des $\text{Hom}_K(\text{Ind}_{K \cap h^{-1}Jh}^K \rho^h, \tau)$. Utilisant l'autre version de la réciprocity de Frobenius, c'est la somme directe des $\text{Hom}_{K \cap h^{-1}Jh}(\rho^h, \tau|_{K \cap h^{-1}Jh})$.

Il est inutile d'aller plus loin dans le cas général ; cette machinerie est appliquée dans l'exemple du § 8.

(3) On calcule aisément le caractère de $\text{Ind}_J^H \rho$: en $h \in H$ il vaut

$$\frac{1}{|J|} \sum_{\substack{t \in H \\ tht^{-1} \in J}} \chi_\rho(tht^{-1}).$$

Exemple 3 (suite et fin). On considère le sous-groupe C_n de D_n engendré par la rotation r . Il est donc cyclique et ses représentations irréductibles sont les $\chi_h(r) = e^{2i\pi h/n}$ pour $h \in \mathbb{Z}/n\mathbb{Z}$. Les représentations ρ_h décrites précédemment sont équivalentes aux $\text{Ind}_{C_n}^{D_n} \chi_h$.

7. Classes de conjugaison dans $\text{GL}(2, k)$

Il est plus que temps de considérer un groupe un peu compliqué pour déterminer ses caractères irréductibles.

On fixe un corps fini k ; on note q le cardinal de k et G le groupe $\text{GL}(2, k)$. Le cardinal de G est le nombre de bases du k -espace vectoriel k^2 , à savoir $(q^2 - 1)(q^2 - q)$. La classe de similitude d'une matrice A de $M_n(k)$ est déterminée par les facteurs invariants de A ; si $n = 2$, il n'y a que deux facteurs invariants à considérer, le polynôme minimal μ_A et le polynôme caractéristique χ_A , qui vérifient $\mu_A | \chi_A | \mu_A^2$. On n'a donc que deux possibilités : $\mu_A = \chi_A$ ou $\mu_A^2 = \chi_A$, ce dernier cas correspondant aux matrices scalaires. Dans G , il y a $(q - 1)$ matrices scalaires, chacune n'ayant d'autre conjuguée qu'elle-même.

Si $\mu_A = \chi_A$, l'espace vectoriel k^2 est cyclique pour l'endomorphisme $\varphi_A : X \mapsto AX$, de sorte que le commutant de A dans $M_2(k)$ est l'algèbre $k[A]$ des polynômes en A , isomorphe à $k[X]/(\chi_A)$. Si $\chi_A = X^2 + aX + b$, A est semblable à la matrice compagnon $\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$. On voit donc que si g est un élément non scalaire de G , et P son polynôme caractéristique, son commutant dans G est isomorphe à $(k[X]/P)^\times$; par suite la classe de conjugaison de g a pour cardinal $|G|/|(k[X]/P)^\times|$. On a trois cas possibles :

(i) P est irréductible dans $k[X]$; en ce cas $k[X]/P$ est une extension quadratique de k ; on a $|(k[X]/P)^\times| = q^2 - 1$ et g a $q^2 - q$ conjugués.

(ii) P est produit de deux facteurs linéaires distincts $X - \alpha$ et $X - \beta$ dans $k[X]$. Alors $k[X]/P$ est isomorphe à $k \times k$ et g a $(q+1)q$ conjugués, dont la matrice diagonale $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$.

(iii) $P = (X - \alpha)^2$ pour un élément α de k^\times . Alors $k[X]/P$ est isomorphe à $k[T]/T^2$ et g a $q^2 - 1$ conjugués, dont la matrice $\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$.

Au total on a $q^2 - q$ polynômes caractéristiques possibles, donc G a $q^2 - 1$ classes de conjugaison, et aussi $q^2 - 1$ caractères irréductibles.

8. Les « séries principales »

On note B le sous-groupe des matrices triangulaires supérieures dans G , U son sous-groupe distingué formé des matrices unipotentes. On note T le sous-groupe diagonal de B ; ainsi B est le produit semi-direct de U par T . On a $|U| = q$, $|T| = (q-1)^2$, $|B| = |T||U| = q(q-1)^2$, de sorte que B est d'indice $q+1$ dans G .

Remarquons que T et U sont commutatifs, leurs représentations irréductibles sont de dimension 1. Les caractères irréductibles de T sont les homomorphismes de T dans \mathbb{U} , de la forme $\chi = \chi_1 \otimes \chi_2$: $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mapsto \chi_1(a)\chi_2(b)$, où χ_1 et χ_2 sont des homomorphismes de k^\times dans \mathbb{U} .

On peut voir χ comme une représentation de B triviale sur le sous-groupe distingué U , et former l'induite $\text{Ind}_B^G(\chi)$. Pour décomposer cette induite, il faut écrire G comme réunion disjointe des doubles classes B et BwB où $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. On obtient que $(\text{Ind}_B^G \chi)|_B$ est somme directe de χ et de $\text{Ind}_T^B(\chi^w)$ où $\chi^w = \chi_2 \otimes \chi_1$, (remarquer que $T = B \cap wBw^{-1}$). Si χ' est un autre homomorphisme de T dans \mathbb{U} , on a donc

$$\begin{aligned} \text{Hom}_G(\text{Ind}_B^G \chi, \text{ind}_B^G \chi') &\simeq \text{Hom}_B((\text{Ind}_B^G \chi)|_B, \chi') \\ &= \text{Hom}_B(\chi, \chi') \oplus \text{Hom}_B(\text{Ind}_T^B \chi^w, \chi') \\ &\simeq \text{Hom}_T(\chi, \chi') \oplus \text{Hom}_T(\chi^w, \chi'). \end{aligned}$$

Par suite $\text{End}_G(\text{Ind}_B^G \chi)$ est de dimension 1 si $\chi \neq \chi^w$, de dimension 2 si $\chi = \chi^w$. Ainsi $\text{Ind}_B^G \chi$ est irréductible si $\chi \neq \chi^w$, somme de deux composants irréductibles non isomorphes si $\chi = \chi^w$. De plus $\text{Ind}_B^G \chi$

et $\text{Ind}_B^G \chi'$ ont un composant irréductible en commun si et seulement si $\chi' = \chi$ ou $\chi' = \chi^w$, auxquels cas $\text{Ind}_B^G \chi$ et $\text{Ind}_B^G \chi'$ sont isomorphes.

On a donc obtenu $\frac{(q-1)(q-2)}{2}$ caractères irréductibles de G grâce aux χ vérifiant $\chi^w \neq \chi$, et $2(q-1)$ grâce aux χ tels que $\chi^w = \chi$ soit au total $\frac{(q-1)(q+2)}{2}$ caractères irréductibles. Il nous en manque $\frac{q(q-1)}{2}$.

Remarque. Si χ est l'homomorphisme trivial 1_T de T dans \mathbb{U} , $\text{Ind}_B^G 1_T$ contient un sous-espace de dimension 1 stable par G , formé des fonctions constantes sur G , ce qui donne une sous-représentation de dimension 1 de caractère $1_G : g \mapsto 1$. L'autre composant irréductible de $\text{Ind}_B^G 1_T$, de dimension q , s'appelle la représentation de Steinberg St_G de G . Si $\chi^w = \chi$, c'est-à-dire si $\chi_1 = \chi_2$, alors les deux composants de $\text{Ind}_B^G \chi$ sont isomorphes à $g \mapsto \chi_1 \circ \det(g)$, de dimension 1, et à $g \mapsto \chi_1 \circ \det(g) \text{St}_G(g)$, de dimension q .

9. Les représentations irréductibles cuspidales

Comme $(\text{Ind}_B^G \chi)|_B$ contient χ , certainement $\text{Ind}_B^G \chi$ contient des vecteurs non nuls fixés par U . Inversement soit (σ, V) une représentation de G , et supposons que l'espace V^U des vecteurs fixés par U soit non nul. Comme U est distingué dans B , cet espace est stable par B , et donne une représentation de B triviale sur U , c'est-à-dire une représentation de T ; comme représentation non nulle de T , elle contient une sous-représentation irréductible, forcément donnée par un homomorphisme χ de T dans \mathbb{C}^\times . On a $\text{Hom}_B(\chi, V|_B) \neq 0$ et, par la deuxième version de la réciprocity de Frobenius, $\text{Hom}_G(\text{Ind}_B^G \chi, V) \neq 0$. Par suite si V est irréductible, c'est l'une des représentations irréductibles construites au paragraphe précédent.

On s'intéresse donc aux représentations irréductibles (σ, V) de G vérifiant $V^U = 0$, qu'on appelle *cuspidales*.

Remarque. Dans le cadre des représentations de groupes p -adiques (voir le texte de C. Blondel dans ce volume), il est plus naturel de considérer l'espace V_U des co-invariants de U dans V , i.e. le plus grand quotient de V sur lequel U agit trivialement, et d'utiliser la première version de la réciprocity de Frobenius. Dans notre cas l'application quotient de V sur V_U donne un isomorphisme de V^U sur V_U .

Nous allons maintenant construire explicitement les caractères irréductibles des représentations cuspidales. Rappelons qu'il en faut $\frac{q^2-q}{2}$.

Soit k'/k une extension quadratique : elles sont toutes isomorphes. Plongeons k' dans $M_2(k)$ comme k -algèbre ; par exemple on peut écrire $k' = k[t]$ où t a pour polynôme minimal $p = X^2 + aX + b$ et envoyer t sur la matrice compagnon de P ; deux tels plongements sont conjugués par un élément de G . Notons T' le groupe k'^{\times} vu comme sous-groupe de G . Enfin, notons Z le centre de G , formé des matrices scalaires, et identifions-le à k^{\times} . Si ω est un homomorphisme de k^{\times} dans \mathbb{U} , et ψ un homomorphisme *non trivial* de U dans \mathbb{U} , on peut former la représentation

$$\omega\psi : zu \longmapsto \omega(z)\psi(u)$$

du groupe ZU , et l'induire à G , pour trouver une représentation $\text{Ind}(\omega\psi)$ de G , de dimension $|G|/|Z||U| = q^2 - 1$. On calcule aisément son caractère :

- sur une matrice scalaire $\alpha 1_2$ il vaut $\omega(\alpha)(q^2 - 1)$
- pour une matrice $\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$, α dans k^{\times} , ses seuls conjugués appartenant à ZU sont ses conjugués par les éléments de B ; comme $\sum_{\alpha \in k^{\times}} \psi(\alpha) = -1$ – car ψ est non trivial – on trouve que le caractère de $\text{Ind}(\omega\psi)$ en $\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$ vaut $-\omega(\alpha)$.
- les autres classes de conjugaison ne rencontrant pas ZU , le caractère de $\text{Ind}(\omega\psi)$ est nul en ces classes. Remarquons que le caractère de $\text{Ind}(\omega\psi)$ ne dépend pas du choix de ψ non trivial.

Considérons maintenant un homomorphisme θ de T' dans \mathbb{U} , et formons l'induite $\text{Ind } \theta$ de T' à G ; c'est une représentation de G de dimension $|G|/|T'| = q^2 - q$. Son caractère vaut $(q^2 - q)\theta(\alpha)$ en une matrice scalaire $\alpha 1_2$, il s'annule en les matrices $\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$ et $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$, $\alpha \neq \beta$, qui n'ont aucun conjugué dans T' . Il suffit donc de déterminer ce caractère en un élément t de $T' - Z$. Remarquons que le groupe T' est cyclique de cardinal $q^2 - 1$ et que Z est un sous-groupe de cardinal $q - 1$, de sorte qu'un élément t de T' appartient à Z si et seulement si $t = t^q$. Si t appartient à $T' - Z$, son polynôme caractéristique P est irréductible dans $k[X]$, et les deux racines de P dans k' sont t et t^q . Ainsi les seuls conjugués de t qui appartiennent à T' sont t et t^q , et on voit que le caractère de $\text{Ind } \theta$ en t vaut $\theta(t) + \theta^q(t)$.

Considérons maintenant la fonction $f_\theta = \chi_1 - \chi_2$ dans $\mathcal{FC}(G)$, où χ_1 est le caractère de $\text{Ind}_{ZU}^G(\theta|_Z \cdot \psi)$ et χ_2 le caractère de $\text{Ind}_{T'}^G(\theta)$. C'est certainement une combinaison linéaire à coefficients entiers de caractères irréductibles de G , et sa valeur en 1 vaut $q - 1$. Les calculs précédents donnent les valeurs de f_θ ; on a $f_\theta = f_{\theta^q}$. Un exercice un peu long mais salutaire donne le résultat principal :

(i) Si $\theta \neq \theta^q$, $\langle f_\theta, f_\theta \rangle_G = 1$.

(ii) Si θ' est un autre homomorphisme de T' dans \mathbb{U} , distinct de θ , θ^q et θ'^q , alors

$$\langle f_\theta, f_{\theta'} \rangle_G = 0.$$

La conséquence majeure est que, si θ est différent de θ^q , alors f_θ est un caractère irréductible de G ; c'est le caractère d'une représentation de dimension $q - 1$, elle n'est donc isomorphe à aucune des représentations irréductibles construites au paragraphe précédent; en particulier, elle est cuspidale.

D'autre part, les caractères f_θ et $f_{\theta'}$ sont égaux si et seulement si θ' est θ ou θ^q . On a donc construit $\frac{q^2 - q}{2}$ caractères distincts de représentations irréductibles cuspidales, ce qui donne exactement les caractères irréductibles manquants.

Remarque. Le groupe G agit par permutation sur la droite projective sur k , qui a $q + 1$ éléments. Pour $q = 2$, on obtient un isomorphisme de G avec S_3 . L'unique caractère cuspidal de G est le caractère signature. Le caractère irréductible de dimension 2 est celui de la représentation de Steinberg. Pour $q = 3$, on obtient un isomorphisme avec S_4 du quotient de G par son centre. Le caractère irréductible de dimension 2 de S_4 correspond à l'unique caractère cuspidal de G dont la restriction au centre est triviale. Le lecteur pourra identifier lequel des caractères dans la table page 9 est le caractère de la représentation de Steinberg de G .

G. HENNIART, CNRS, Laboratoire de Mathématique d'Orsay, UMR 8628,
Bâtiment 425, Faculté des Sciences d'Orsay, Université Paris-Sud 11, F-
91405 Orsay Cedex • *E-mail* : guy.henniart@math.u-psud.fr