Introduction à la théorie des représentations des groupes

Cédric Lecouvey

Université François Rabelais Master II

1 Notion de représentation d'un groupe

1.1 Introduction

La théorie des représentations des groupes permet l'étude des groupes abstraits en représentant leurs éléments par des matrices inversibles. On dispose alors des méthodes de l'algèbre linéaire qui rendent souvent l'étude de ces groupes plus facile et permettent d'en obtenir de nouvelles propriétés. L'idée est de faire agir un groupe G sur un espace vectoriel V de telle sorte que l'action de chaque élément soit compatible avec la structure d'espace vectoriel, c'est à dire soit un élément de $GL(V)$ le groupe des automorphismes linéaires de V et plus seulement une bijection de V sur V.

Ce concept émerge à la fin du 19-ième siècle et l'étude générale des représentations d'un groupe est largement développée par William Burnside et Ferdinand Georg Frobenius au début du 20-ième siècle. Frobenius complète notamment l'étude des représentations du groupe symétrique que nous allons détailler dans la suite. Nous nous limiterons par ailleurs aux groupes finis. Pour un historique très complet sur le développement de la théorie des représentations des groupes, le lecteur peut consulter avec profit [5].

La théorie des représentations a permis de remarquables avancées tout d'abord en théorie des groupes proprement dit. Elle joue notamment un rôle fondamental dans le théorème de classification des groupes simples finis (classification achevée au début des années 80) et tout spécialement dans la preuve du théorème de Feit-Thomson (1963) selon lequel tout groupe simple fini non abélien est de cardinal pair.

Si la théorie des représentations des groupes sur les corps de caractéristique nulle est désormais bien comprise (et nous en exposerons les grandes lignes dans les paragraphes qui suivent), elle demeure encore largement mystérieuse et considérablement plus difficile dans le cas où les corps considérés sont de caractéristique positive. Il reste beaucoup à comprendre dans ce domaine tout spécialement dans le cas des groupes symétriques.

La théorie des représentations des groupes généraux (pas nécessairement finis) et des algèbres possède également de nombreuses applications en physique des particules. Selon le modèle de Wigner (1939) chaque état d'une particule correspond notamment à une représentation du groupe de Poincaré (un groupe de transformations de l'espace compatible avec la théorie de la relativité restreinte).

Dans la suite, k est un corps de caractéristique nulle et les espaces vectoriels considérés le sont sur k. Le plus souvent, on prendra $k = \mathbb{C}$ ou un corps algébriquement clos. Pour tout k-espace vectoriel de dimension finie, on note $GL(V)$ le groupe des automorphismes linéaires de V, c'est-à-dire le groupes des applications linéaires $u : V \to V$ bijectives. Si $\dim_k(V) = n$, on peut identifier

$GL(V)$ au groupe des matrices careés inversibles de taille n à coefficients dans k. On désignera par G un groupe fini.

1.2 Représentations d'un groupe

Définition 1.1 *Une* représentation *du groupe G sur l'espace vectoriel V de dimension finie est un morphisme $\rho : G \to GL(V)$ de G vers le groupe des automorphismes de V. On dit alors que* $\dim_k(V)$ *est le* degré *de la représentation.*

On peut également interpréter cette définition en termes matriciels en considérant $V = k^n$. Une représentation de degré n équivaut à la donnée, pour chaque $g \in G$, d'une matrice inversible R_g, la famille des matrices $(R_g)_{g\in G}$ vérifiant les égalités $R_{gg'} = R_g R_{g'}$ pour tout $g, g' \in G$. Dans ce cas l'application ρ est définie par $\rho(g) = R_g$.

Lorsque le morphisme ρ est injectif, on dit que la représentation est *fidèle*. Dans ce cas, $\rho(G)$ est isomorphe à G et on a réalisé G comme un groupe de matrices.

Exemple 1.2

1. *Considérons $G = S_n$ le groupe symétrique d'ordre n. Pour tout $\sigma \in S_n$, on pose $\rho(\sigma) = M_\sigma$ où M_σ est la matrice de permutation associée à σ, c'est à dire la matrice de l'application linéaire qui envoie la base standard $(e_1, \dots, e_n)$ de $\mathbb{C}^n$ sur $(e_{\sigma(1)}, \dots, e_{\sigma(n)})$. On vérifie facilement que ρ définit une représentation fidèle de S_n sur $\mathbb{C}^n$.*
2. *Pour tout groupe G, le morphisme $\rho : G \to k$ qui envoie tout élément de G sur 1 est une représentation de degré 1 dite représentation* triviale.
3. *Si G est un sous-groupe de $GL_n(\mathbb{C})$ le groupe des matrices inversibles carrées d'ordre n, l'application $\rho : G \to \mathbb{C}$ définie par $\rho(M) = \det(M)$ est une représentation de G. Dans le cas particulier où G est le groupe des matrices de permutation défini dans 1, $\det(M_\sigma) = \varepsilon(\sigma)$ où ε est la signature de la permutation σ. Cela revient à dire que la signature $\varepsilon : S_n \to \mathbb{C}$ est une représentation de degré 1.*
4. *Si $G = \mathbb{Z}/m\mathbb{Z}$, pour définir une représentation de degré n, il suffit de préciser $\alpha = \rho(\bar{1}) \in GL_n(\mathbb{C})$ de telle sorte que $\alpha^m = I_n$ la matrice identité. Par exemple pour $n = 1$, toute racine de l'unité de la forme $\alpha = \exp(2i\pi/k)$ avec k un diviseur de n convient.*

Si $\rho : G \to GL(V)$ est une représentation de G, elle définit une action de G sur V. Il suffit en effet de poser $g \cdot v = \rho(g)(v)$ pour tout $g \in G$ et $v \in V$. Par rapport à une action quelconque de G sur V, l'action définie à partir d'une représentation est linéaire, c'est à dire que l'on a en plus

$$g \cdot (\lambda v + \mu v') = \lambda g \cdot v + \mu g \cdot v' \tag{1}$$

pour tout $g \in G$, $v, v' \in V$ et $\lambda, \mu \in k$. Réciproquement une action de groupe qui vérifie en plus (1) définit une représentation ρ en posant $\rho(g)v = g \cdot v$ pour tout $v \in V$ et $g \in G$ comme précédemment. Dans cette perspective, une représentation du groupe G sur le k-espace vectoriel V n'est rien d'autre qu'une action de G sur V *compatible avec sa structure linéaire.*

A l'inverse, si G agit sur l'ensemble fini $E = \{e_1, \dots, e_n\}$, il existe une représentation associée. Il suffit de considérer l'espace vectoriel $V_E := \oplus_{i=1}^n k e_i$ et de définir pour tout g, $\rho(g) \in GL(V_E)$ comme l'application linéaire envoyant la base E sur la base $\{g \cdot e_1, \dots, g \cdot e_n\}$.

1.3 Semisimplicité

Soient (ρ, V) et (ρ', V') deux représentations d'un même groupe fini G. Un *morphisme* (*de représentations*) $f : V \to V'$ est une application linéaire de V dans V' qui commute avec l'action du groupe G, autrement dit pour tout $g \in G$, on a $f \circ \rho(g) = \rho'(g) \circ f$ l'égalité ayant lieu dans $L(V, V')$ l'espace vectoriel des applications linéaires de V dans V'. On peut également reformuler cette propriété à l'aide du diagramme commutatif suivant :

$$\begin{array}{ccc} V & \xrightarrow{f} & V' \\ \downarrow \rho(g) & & \rho'(g) \downarrow \\ V & \xrightarrow{f} & V' \end{array}.$$

Lorsque f est bijective, on dit que f est un isomorphisme (de représentations). Dans ce cas, c'est aussi un isomophisme d'espaces vectoriels et on a $\dim_k(V) = \dim_k(V')$. Soit $W \subset V$. On dit que W est une *sous-représentation* de G lorsque W est stable sous l'action de G sur V, c'est à dire si $g \cdot w \in W$ pour tout $g \in G$ et tout $w \in W$. Lorsque la représentation V n'admet aucune sous-représentation propre (c'est à dire autre que $W = \{0\}$ ou $W = V$), on dit que V est *irréductible*.

Exemple 1.3 *Considérons $G = \mathbb{Z}/3\mathbb{Z}$ et ρ, ρ' les deux représentations de $\mathbb{Z}/3\mathbb{Z}$ définies par $\rho(\bar{1}) = j$ et $\rho'(\bar{1}) = j^2$ où $j = \exp\left(\frac{2i\pi}{3}\right)$. Elles sont irréductibles (car de dimension 1) et non isomorphes. En effet si il existe $f \in L(\mathbb{C}, \mathbb{C})$ tel que $f \circ \rho(g) = \rho'(g) \circ f$ pour tout $g \in \mathbb{Z}/3\mathbb{Z}$, on obtient avec $g = \bar{1}$ l'égalité $fj = j^2 f$ (en dimension 1 la composition des applications se réduit à la multiplication). Donc $f = 0$.*

Théorème 1.4 (Maschke) *On suppose que k* est de caractéristique nulle. *Soit (ρ, V) une représentation du groupe G et W une sous-représentation de V. Alors, il existe une sous-représentation W' de V telle que $V = W \oplus W'$.*

Preuve. On supposera que $k = \mathbb{C}$, la preuve dans le cas d'un corps de caractéristique nulle est analogue. Considérons une base de V et notons $(\cdot, \cdot)$ le produit scalaire hermitien usuel sur V relatif à cette base. A priori les applications linéaires $\rho(g)$ avec $g \in G$ ne conservent pas le produit scalaire. Comme G est fini, on peut définir une forme sesquilinéaire définie positive $(\cdot, \cdot)_G$ sur V en posant

$$(v_1, v_2)_G := \sum_{g \in G} (g \cdot v_1, g \cdot v_2).$$

On vérifie immédiatement que $(g \cdot v_1, g \cdot v_2)_G = (v_1, v_2)_G$ pour tout $g \in G$ et $v_1, v_2 \in V$. Il suffit alors de prendre pour W' l'orthogonal de W par rapport à $(\cdot, \cdot)_G$ qui est stable sur l'action de G. On notera que $\rho(g) \in U(V)$ est dans le groupe unitaire de V défini par $(\cdot, \cdot)_G$. ■

Il est clair que la connaissance des représentations W et W' (c'est à dire celle des actions de G sur W et W') équivaut à celle de V. En effet, tout vecteur $v \in V$ se décompose sous la forme $v = w + w'$ avec $w \in W$ et $w' \in W'$. On alors $g(v) = g(w) + g(w')$ puisque l'action de G est linéaire. On dit que la représentation V se décompose en la somme directe de W et de W'. En termes matriciels, une fois choisies des bases de W et W', la matrice de $\rho(g)$ est diagonale par bloc :

$$R_g = \begin{pmatrix} R_g^W & 0 \\ 0 & R_g^{W'} \end{pmatrix}$$

où R_g^W et $R_g^{W'}$ sont les matrices des restrictions de $\rho(g)$ à W et W'. Noter également que la preuve précédente montre que les représentations d'un groupe fini sur $\mathbb{C}$ sont *unitaires* (c'est à dire sont dans le groupe unitaire d'un produit scalaire hermitien).

Corollaire 1.5 *Toute représentation V de dimension finie de G* sur un corps de caractéristique nulle *se décompose sous la forme*

$$V = V_1^{\oplus m_1} \oplus \cdots \oplus V_r^{\oplus m_r}$$

où les V_i sous des représentations irréductibles non isomorphes, chacune d'entre elles apparaissant avec la multiplicité m_i. On dit alors que la théorie des représentations de G sur k est semisimple.

Preuve. On obtient l'existence de la décomposition en raisonnant par récurrence sur la dimension de V en utilisant le théorème précédent. ■

Remarque : Nous verrons dans la suite que cette décomposition est de plus unique à isomorphisme près, c'est à dire au remplacement près des V_i par des représentations irréductibles qui leur sont isomorphes.

Les deux problèmes qui suivent sont fondamentaux en théorie des représentations.

1. Déterminer les représentations irréductibles, leur nombre, leur degré.
2. Décomposer une représentation en une somme de ses représentations irréductibles.

Pour les résoudre, nous allons avoir besoin de la notion de caractère qui fera l'objet du chapitre suivant. Montrons auparavant un lemme essentiel.

Lemme 1.6 (Schur) *Soient V_1 et V_2 deux représentations complexes (i.e. sur $\mathbb{C}$) irréductibles du groupe G et $f : V_1 \to V_2$ un morphisme. Alors*

1. *Soit f est un isomorphisme, soit f est l'application nulle $f := 0$.*
2. *Si $V_1 = V_2$, il existe $\lambda \in \mathbb{C}$ tel que $f = \lambda I_d$.*

Preuve.

1 : Comme $\ker f$ et $\operatorname{Im} f$ sont invariants sous l'action de G et que V_1, V_2 sont des représentations irréductibles, on a $\ker f = \{0\}$ ou V_1 et, $\operatorname{Im} f = \{0\}$ ou V_2.

2 : Comme $\mathbb{C}$ est algébriquement clos, f possède une valeur propre λ. Mais alors $\ker(f - \lambda I_d)$ n'est pas réduit à $\{0\}$. Comme, il est stable sous l'action de G, on a $\ker(f - \lambda I_d) = V_1$ et donc $f = \lambda I_d$. ■

Remarque : L'ensemble des endomorphismes $f : V \to V$ qui commutent avec l'action de G est une sous-algèbre de $End_G(V)$ des endomorphismes linéaires de V. Lorsque k n'est pas algébriquement clos, on obtient d'après le point 1 du lemme, que cette sous-algèbre est un corps gauche (c'est à dire un corps non nécessairement commutatif). Lorsque k est algébriquement clos, ce corps n'est autre que k lui-même, en particulier, il est commutatif.

1.4 Exemples

1.4.1 Le cas des groupes abéliens

Observons tout d'abord que pour toute représentation irréductible (V, ρ) d'un groupe G et tout $g \in G$, l'action de g donne une application linéaire bijective de $V \to V$ mais celle-ci n'est en général pas un isomorphisme de représentations car on n'a pas nécessairement $h \cdot (g \cdot v) = g \cdot (h \cdot v)$ pour tout $h \in G$ et tout $v \in V$. C'est néanmoins le cas si $g \in Z(G)$ le centre de G. Dans ce cas, d'après le lemme de Schur $\rho(g) = \lambda I_d$ est un multiple de I_d. Il s'ensuite que g agit sur V en multipliant les vecteurs par une constante dès lors que $g \in Z(G)$.

Dans le cas où G est abelien, $G = Z(G)$ et tous les éléments de g stabilisent toutes les droites de V. Il s'ensuite qu'une représentation irréductible est nécessairement de dimension 1. On a donc la proposition suivante :

Proposition 1.7 *Soit G un groupe abélien fini. Alors ses représentations irréductibles sont de degré* 1.

On rappelle que tout groupe abélien fini G est isomorphe à un produit de groupes cycliques. Plus précisément, on a

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z} \tag{2}$$

et si on impose la condition a_{i+1} divise a_i pour tout $i = 1, \ldots, r-1$, la suite $(a_1, \ldots, a_r)$ est unique. On peut alors choisir un ensemble $(g_1, \ldots, g_r)$ de générateurs où, pour tout $i = 1, \ldots, r$, g_i est d'ordre a_i. Tout élément $g \in G$ s'écrit alors sous la forme $g = g_1^{\alpha_1} \cdots g_r^{\alpha_r}$ où $0 \leq \alpha_i \leq a_i - 1$. Pour obtenir une représentation irréductible de G, il suffit donc de déterminer l'image de chaque g_i par ρ. Comme $g_i^{a_i} = 1$, $\rho(g_i)$ doit être une racine a_i-ième de l'unité. Cela donne $|G|$ représentations irréductibles et on vérifie qu'elles sont non isomorphes en raisonnant comme dans l'Exemple 1.3.
Remarque : Il va de soit qu'une représentation de degré 1 est necessairement irréductible. La proposition précédente montre donc que les représentations irréductibles d'un groupe abélien fini sont exactement ses représentations de degré 1.

1.4.2 Le cas du groupe S_3

Nous avons déjà rencontré la représentation triviale et la représentation ε renvoyant la signature de la permutation. Toutes les deux sont irréductibles de degré 1. Nous avons également défini la représentation de degré 3 sur $V = \mathbb{C}^3$ telle que $\sigma(x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$. On vérifie facilement que le plan P d'équation $x_1 + x_2 + x_3 = 0$ est une sous représentation de V irréductible. On montrera un peu plus loin que les trois représentations irréductibles ainsi obtenues sont les seules représentations irréductibles de G.

1.5 Algèbre de groupe et représentation adjointe

Soit G un groupe fini. On définit l'algèbre $k[G]$ du groupe G sur le corps k comme la k-algèbre de base $\{e_g \mid g \in G\}$ où les vecteurs de la base sont soumis aux relations

$$e_g e_{g'} = e_{gg'} \quad \forall g, g' \in G.$$

Un $k[G]$-module est un k-espace vectoriel V où l'algèbre $k[G]$ agit linéairement. Cela signifie que l'on a une action de $k[G]$ sur V telle que

$$a \cdot (\lambda v_1 + \mu v_2) = \lambda a \cdot v_1 + \mu a \cdot v_2 \quad \forall a \in k[G], \quad \forall v_1, v_2 \in V, \quad \forall \lambda, \mu \in k,$$
$$(aa') \cdot v = a \cdot ((a' \cdot v)) \quad \forall a, a' \in k[G] \text{ et}$$
$$(\lambda a_1 + \mu a_2) \cdot v = \lambda a_1 \cdot v + \mu a_2 \cdot v, \quad \forall v \in V, \quad \forall \lambda, \mu \in k.$$

La donnée d'une représentation du groupe G (vue comme une action linéaire de G sur V) équivaut donc à la donnée d'un $k[G]$-module et les deux termes ont tendance à être employés de façon interchangeable dans la littérature.

On peut ne considérer que l'action linéaire de G sur $k[G]$. La représentation de G ainsi obtenue s'appelle la *représentation adjointe* de G. Elle est de degré $|G|$ et nous allons voir dans la suite qu'elle joue un rôle essentiel.

En tant qu'espace vectoriel, $k[G]$ peut également s'interpréter comme le k-espace des fonctions $f : G \to k$ que nous noterons $\mathcal{F}$. En effet, tout élément $f \in k[G]$ se décompose sous la forme

$$f = \sum_{g \in G} f(g) e_g.$$

Il définit donc bien un élément de $\mathcal{F}$. Attention, $\mathcal{F}$ possède aussi une structure *d'algèbre commutative* pour la multiplication des fonctions mais cette structure *ne coïncide pas* avec celle sur $k[G]$ qui n'est pas commutative lorsque G ne l'est pas.

1.6 Exercices

1. Soient V_1 et V_2 deux représentations de dimension finie d'un même groupe G. Vérifier que $V_1 \oplus V_2$ et $V_1 \otimes V_2$ peuvent également être munies d'une struture de de représentation de G.
2. Soit (ρ, V) une représentation de G. Pour tout $g \in G$, on définit $\rho^*(g) : V^* \to V^*$ par $\rho^*(g) =^t \rho(g^{-1})$. Montrer que (ρ^*, V^*) définit une représentation de G dite *représentation duale*.
3. Donner une représentation matricielle de chacune des représentations irréductibles de S_3 rencontrées dans le paragraphe précédent.
4. Donner toutes les représentations irréductibles de A_3.
5. Donner les représentations irréductibles de $\mathbb{Z}/20\mathbb{Z}$.
6. Soit $G = \{g_1, \ldots, g_n\}$ un groupe fini. On pose $c = \sum_{i=1}^n g_i$.
   (a) Montrer que $cg = gc = c$ pour tout $h \in G$. En déduire que c est dans le centre de l'algèbre $k[G]$.
   (b) Montrer que $c^2 = |G|\, c$.
   (c) Quelle est la matrice de la multiplication par c dans $k[G]$ exprimée sur la base $\{g_1, \ldots, g_n\}$?
7. Considérons l'ensemble des matrices 2×2

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}.$$

   (a) Vérifier que G est un groupe et que $V = \mathbb{C}^2$ est une représentation de G.

(b) Déterminer une sous-représentation de V.

(c) La représentation V se décompose-t-elle en somme de représentations irréductibles ? Peut-on appliquer le théorème de Maschke ? Pourquoi ?

8. Soit V une représentation irréductible du groupe fini G et c l'élément de $\mathbb{C}[G]$ défini comme dans l'exercice 6. Montrer que l'action de c est une homothétie.

2 Théorie des caractères

La *théorie des caractères* a pour objectif de caractériser les représentations irréductibles et de calculer la décomposition d'une représentation quelconque en somme directe de représentations irréductibles.

2.1 Définitions et propriétés basiques

Soit (ρ, V) une représentation du groupe G. On a vu que pour tout $g \in G$, on pouvait considérer $\rho(g)$ comme une matrice en fixant une base de V. On rappelle que $\det(\rho(g))$ et $tr(\rho(g))$ ne dépendent alors que de $\rho(g)$ et pas de la base choisie. On dit qu'une fonction $f : G \to k$ est centrale si elle est invariante sur les classes de conjugaison, c'est à dire si $f(hgh^{-1}) = f(g)$ pour tout $g, h \in G$.

Définition 2.1 *Le caractère de la représentation (ρ, V) est l'application $\chi : G \to k$ définie par $\chi(g) = tr(\rho(g))$ pour tout $g \in G$.*

Proposition 2.2 *Soit (ρ, V) une représentation de degré n et χ son caractère.*

1. $\chi(1) = n$.
2. *Si $k = \mathbb{C}$ alors $\chi(g^{-1}) = \overline{\chi(g)}$ pour tout $g \in G$.*
3. $\chi(hgh^{-1}) = \chi(g)$ *pour tout $g, h \in G$, χ est donc* une fonction centrale.

Preuve. Laissée en exercice. Indication pour le 2, utiliser que les valeurs propres de $\rho(g)$ sont des racines de l'unité puisque G est fini. ■

Proposition 2.3 *Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations de G de caractères χ_1 et χ_2.*

1. *Le caractère de $(\rho_1 + \rho_2, V_1 \oplus V_2)$ vaut $\chi_1 + \chi_2$.*
2. *Le caractère de $(\rho_1 \otimes \rho_2, V_1 \otimes V_2)$ vaut $\chi_1\chi_2$.*

Preuve. Laissée en exercice. ■

2.2 Orthogonalité des caractères

On définit un produit scalaire hermitien sur les fonctions $\mathcal{F}$ de G vers $\mathbb{C}$ en posant

$$(\varphi, \psi) = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\psi(g)} \tag{3}$$

pour φ et ψ deux fonctions de G dans $\mathbb{C}$.

Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentations irréductibles de G. Pour toute application linéaire $f : V_1 \to V_2$, on pose

$$f^0 := \frac{1}{|G|} \sum_{g \in G} \rho_2(g)^{-1} f \rho_1(g). \tag{4}$$

Il s'agit donc également d'une application linéaire de V_1 dans V_2.

Lemme 2.4 *On rappelle que V_1 et V_2 sont irréductibles.*

1. *Si V_1 et V_2 ne sont pas isomorphes, on a $f^0 = 0$,*
2. *Si $V_1 = V_2$ et $\rho_1 = \rho_2$, f^0 est une homothétie de V_1 de rapport $\frac{1}{n_1} tr(f)$ où $n_1 = \dim_{\mathbb{C}}(V_1)$.*

Preuve. On vérifie facilement que pour tout $h \in G$, $\rho_2(h) f^0 = f^0 \rho_1(h)$. Cela signifie que $f^0 : V_1 \to V_2$ est un morphisme de représentations. Il découle alors du théorème 1.4 que $f^0 = 0$ dans le cas 1 et que $f^0 = \lambda I_d$ dans le cas 2. On a par ailleurs $tr(f^0) = tr(f)$ d'après (4). ■

Supposons maintenant que ρ_1 et ρ_2 soient données sous formes matricielles. Autrement dit on fixe une base de V_1 et une base de V_2 et pour tout $g \in G$, $\rho_1(g) = (r^{(1)}_{j_1,i_1}(g))$ et $\rho_2(g) = (r^{(2)}_{i_2,j_2}(g))$ sont des matrices carrées d'ordre $n_1 = \dim_{\mathbb{C}}(V_1)$ et $n_2 = \dim_{\mathbb{C}}(V_2)$. Notons respectivement (x_{i_2,i_1}) et $(x^0_{j_2,j_1})$ les matrices de f et f^0 par rapport à ces bases. Ce sont donc des matrices rectangulaires de taille $n_2 \times n_1$. D'après (4), on a

$$x^0_{i_2,i_1} = \frac{1}{|G|} \sum_{j_1=1}^{n_1} \sum_{j_2=1}^{n_2} \sum_{g \in G} r^{(2)}_{i_2,j_2}(g^{-1}) x_{j_2,j_1} r^{(1)}_{j_1,i_1}(g).$$

En faisant décrire à f toutes les applications linéaires de V_1 dans V_2, on dispose donc pour tout couple (i_1, i_2) d'une forme linéaire

$$\theta_G : \left\{ \begin{array}{l} Mat_{n_2 \times n_1}(\mathbb{C}) \to \mathbb{C} \\ M \mapsto x^0_{i_2,i_1} \end{array} \right.$$

définie par

$$\theta_G(M) = \frac{1}{|G|} \sum_{j_1=1}^{n_1} \sum_{j_2=1}^{n_2} \sum_{g \in G} r^{(2)}_{i_2,j_2}(g^{-1}) x_{j_2,j_1} r^{(1)}_{j_1,i_1}(g) \text{ où } M = (x_{j_2,j_1}). \tag{5}$$

Lorsque V_1 et V_2 ne sont pas isomorphes, θ_G est la forme linéaire nulle d'après le lemme précédent. Ses coefficients matriciels (i.e. ceux de chaque coordonnée x_{j_2,j_1}) sont donc nuls, autrement dit

$$\sum_{g \in G} r^{(2)}_{i_2,j_2}(g^{-1}) r^{(1)}_{j_1,i_1}(g) = 0 \quad \text{pour } 1 \leq i_1, j_1 \leq n_1 \text{ et } 1 \leq i_2, j_2 \leq n_2. \tag{6}$$

Lorsque $V_1 = V_2$ et $\rho_1 = \rho_2$

$$x^0_{i_2,i_1} = \frac{1}{n_1} tr(f) \delta_{i_2,i_1} = \frac{1}{n_1} \sum_{j_1,j_2} x_{j_2,j_1} \delta_{j_2,j_1} \delta_{i_2,i_1} = \theta_G(M) \tag{7}$$

avec $tr(f) = \sum_{j_1,j_2} x_{j_2,j_1} \delta_{j_2,j_1}$. Les deux expressions (5) et (7) donnent deux expressions pour les coefficients matriciels de θ_G. On a donc pour $1 \leq i_1, j_1, i_2, j_2 \leq n_1$

$$\frac{1}{|G|} \sum_{g \in G} r^{(1)}_{i_2,j_2}(g^{-1}) r^{(1)}_{j_1,i_1}(g) = \frac{1}{n_1} \sum_{j_1,j_2} \delta_{j_2,j_1} \delta_{i_2,i_1} = \left\{ \begin{array}{l} 1/n_1 \text{ si } i_1 = i_2, j_1 = j_2, \\ 0 \text{ sinon,} \end{array} \right. \tag{8}$$

en particulier si $i_1 = j_1$ et $i_2 = j_2$

$$\frac{1}{|G|}\sum_{g\in G} r^{(1)}_{i_2,i_2}(g^{-1})r^{(1)}_{i_1,i_1}(g) = \begin{cases} 1/n_1 \text{ si } i_1 = i_2 = j_1 = j_2, \\ 0 \text{ sinon.} \end{cases} \tag{9}$$

Théorème 2.5 (orthonormalité des caractères) *On suppose que $k = \mathbb{C}$.*

1. *Si χ est le caractère d'une représentation irréductible de G, on a $\|\chi\|^2 = (\chi, \chi) = 1$.*
2. *Si χ_1 et χ_2 sont deux caractères de deux représentations irréductibles non isomorphes, alors $(\chi_1, \chi_2) = 0$.*

Preuve. Dans le cas 1 on a par définition du produit scalaire et d'après le point 2 de la Proposition 2.2

$$(\chi, \chi) = \frac{1}{|G|}\sum_{g\in G}\chi(g^{-1})\chi(g) = \frac{1}{|G|}\sum_{g\in G}\sum_{i=1}^{n_1}\sum_{j=1}^{n_1} r^{(1)}_{i,i}(g^{-1})r^{(1)}_{j,j}(g).$$

Mais d'après (9), $\frac{1}{|G|}\sum_{g\in G} r^{(1)}_{i,i}(g^{-1})r^{(1)}_{j,j}(g) = \frac{1}{n_1}\delta_{i,j}$ pour tout $i, j = 1, \ldots, n_1$. Donc $(\chi, \chi) = 1$.

Dans le cas 2,

$$(\chi_1, \chi_2) = \frac{1}{|G|}\sum_{g\in G}\chi_2(g^{-1})\chi_1(g) = \frac{1}{|G|}\sum_{g\in G}\sum_{i=1}^{n_2}\sum_{j=1}^{n_1} r^{(2)}_{i,i}(g^{-1})r^{(1)}_{j,j}(g).$$

Mais d'après (6), $\sum_{g\in G} r^{(2)}_{i,j}(g^{-1})r^{(1)}_{i,j}(g) = 0$ pour $1 \le i \le n_1$ et $1 \le j \le n_2$. On a donc bien $(\chi_1, \chi_2) = 0$. ■

La théorie des caractères permet de calculer la multiplicité de chaque représentation irréductible apparaissant dans la décomposition d'une représentation quelconque en ses composantes irréductibles.

Corollaire 2.6 *On suppose $k = \mathbb{C}$. Soit (ρ, V) une représentation et*

$$V = V_1^{\oplus m_1} \oplus \cdots \oplus V_r^{\oplus m_r}$$

une décomposition en irréductibles. Notons respectivement χ et $\chi_i, i = 1, \ldots, r$ les caractères de V et ceux des V_i. alors pour tout $i = 1, \ldots, r$, on a

$$m_i = (\chi, \chi_i).$$

En particulier, les multiplicités m_i ne dépendent pas de la décomposition considérée.

Le corollaire suivant nous sera très utile dans le Chapitre 5.

Corollaire 2.7 *Soit ϕ une combinaison linéaire à coefficients entiers de caractères irréductibles de G. Pour que ϕ soit un caractère irréductible, il faut et il suffit que $\langle\phi, \phi\rangle = 1$ et $\phi(1) > 0$.*

Preuve. Posons $\phi = \sum_i a_i\chi_i$ où les χ_i sont les caractères irréductibles et $a_i \in \mathbb{Z}$. Comme $\langle\phi, \phi\rangle = 1$, nous avons $\sum a_i^2 = 1$. Donc tous les a_i sont nuls à l'exception d'un seul pour lequel $a_{i_0} = \pm 1$. Mais comme $\phi(1) > 0$, on a $a_{i_0} = 1$ et $\phi = \chi_{i_0}$. ■

2.3 Décomposition de la représentation régulière

On rappelle que la représentation régulière est celle où $V = \mathbb{C}[G]$ et l'action ρ de G sur V s'obtient par multiplication à gauche. Pour calculer χ le caractère de cette représentation, il suffit d'obtenir la trace de la matrice de $\rho(g), g \in G$ dans la base $\{e_h \mid h \in G\}$. Or $g \cdot e_h = \rho(g)(e_h) = e_{gh}$ pour tout $g, h \in G$. Ainsi

$$\chi(g) = \begin{cases} 0 \text{ si } g \neq 1, \\ |G| \text{ si } g = 1. \end{cases}$$

Proposition 2.8 *La représentation régulière se décompose en*

$$\mathbb{C}[G] = V_1^{\oplus \dim_{\mathbb{C}}(V_1)} \oplus \cdots \oplus V_r^{\oplus \dim_{\mathbb{C}}(V_r)}$$

*où $V_1, \ldots, V_r$ est la liste de toutes les représentations irréducible de G. Ainsi leur nombre est fini et chacune d'entre elles apparaît dans $\mathbb{C}[G]$ avec une multiplicité égale à sa dimension. Si on note $n_1, \ldots, n_r$ le degré de ces représentations irréducibles, on a l'*égalité de Burnside

$$|G| = n_1^2 + \cdots + n_r^2.$$

Preuve. Soit V_i une représentation irréductible et χ_i son caractère. On a

$$(\chi, \chi_i) = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi_i(g)} = \frac{1}{|G|}\chi(1)\chi_i(1) = n_i.$$

L'égalité $|G| = n_1^2 + \cdots + n_r^2$ s'obtient en comparant les dimensions. ■

Exemple 2.9 *On retrouve facilement en utilisant l'égalité de Burnside qu'un groupe abélien d'ordre n possède exactement n représentations irréductibles puisqu'elles sont toutes de degré* 1.

2.4 Fonctions centrales

Nous allons maintenant nous intéresser au nombre de représentations irréductibles. L'idée est d'étudier l'algèbre $\mathcal{A}$ sur $\mathbb{C}$ des fonctions centrales sur G définies comme les fonctions $f : G \to \mathbb{C}$ constantes sur les classes de conjugaisons de G. Notons $C_1, \ldots, C_r$ le nombre de classes de conjugaison de G. Pour tout $i = 1, \ldots, r$, on définit la fonction caractéristique $1_{C_i} : G \to \mathbb{C}$ par

$$1_{C_i}(g) = \begin{cases} 1 \text{ si } g \in C_i, \\ 0 \text{ sinon.} \end{cases}$$

Il s'agit bien sûr d'une fonction centrale.

Lemme 2.10 *Les fonctions indicatrices $1_{C_1}, \ldots, 1_{C_r}$ forment une base linéaire de l'algèbre $\mathcal{A}$.*

Preuve. Laissée en exercice. ■

Pour une fonction $f \in \mathcal{A}$ et une représentation (ρ, V) de G, on définit l'endomorphisme u_f de V par

$$u_f := \sum_{g \in G} f(g)\rho(g) \in End(V). \tag{10}$$

Lemme 2.11 *Supposons que (ρ, V) soit une représentation irréductible de degré n. Alors u_f est une homothétie de rapport*

$$\lambda = \frac{1}{n}\sum_{g\in G} f(g)\chi(g) = \frac{|G|}{n}(f, \overline{\chi})$$

où χ est la caractère de (ρ, V).

Preuve. On vérifie facilement que pour tout $g \in G$, $\rho(g)u_f\rho(g)^{-1} = u_f$, c'est à dire que $\rho(g)u_f = u_f\rho(g)$. D'après le Théorème 1.4, u_f est une homothétie. Pour calculer son rapport λ, on applique la trace à (10). Cela donne

$$n\lambda = \sum_{g\in G} f(g)\chi(g).$$

■

Théorème 2.12 *Le nombre de caractères irréductibles est égal au nombre de classes de conjugaison de G. De plus les caractères irréductibles forment une base orthonormée de l'algèbre des fonctions centrales.*

Preuve. Soient $\chi_1, \ldots, \chi_s$ l'ensemble des caractères irréductibles de G. D'après le Théorème 2.5, $\chi_1, \ldots, \chi_s$ est une famille orthonormée donc en particulier, une famille libre. Il suffit de démontrer que tout élément $f \in \mathcal{A}$ orthogonal à tous les χ_i est nul. Considérons une telle fonction f. Pour toute représentation (ρ, V) de G, on définit

$$v_f := \sum_{g\in G} \overline{f(g)}\rho(g).$$

Puisque f est orthogonal à tous les χ_i, le lemme précédent (que l'on applique à $\overline{f}$) implique que $v_f = 0$ lorsque V est une représentation irréductible. Si V n'est pas irréducible, sa décomposition en irréductibles permet d'écrire pour tout $g \in G$, $\rho(g) = \rho_1(g) + \cdots + \rho_k(g)$ où les ρ_i sont irréductibles. On a alors

$$v_f = \sum_{i=1}^{k}\sum_{g\in G} \overline{f(g)}\rho_i(g) = v_f^{(1)} + \cdots + v_f^{(k)} = 0.$$

Donc v_f est en fait toujours nul. En particulier, si on prend pour V la représentation régulière de G de caractère χ, nous aurons

$$v_f(e_1) = \sum_{g\in G} \overline{f(g)}\rho(g)(e_1) = \sum_{g\in G} \overline{f(g)}e_g = 0.$$

Donc $\overline{f(g)} = 0 = f(g)$ pour tout $g \in G$ comme souhaité. ■

2.5 Degré des représentations irréductibles

Nous avons déjà vu que la somme des carrés des degrés des représentations irréductibles d'un groupe fini G était égale au cardinal de ce groupe (égalité de Burnside). Le paragraphe qui suit est consacré à la preuve du théorème suivant (voir aussi le paragraphe II-1 du livre de Serre [7] ou encore le Chapitre 22 de [4]).

Théorème 2.13 *Soit G un groupe fini de cardinal n et d le degré d'une représentation irréductible de G sur $\mathbb{C}$. Alors d/n.*

On rappelle qu'un nombre complexe α est un *entier algébrique* lorsqu'il est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$. Il est clair que les éléments de $\mathbb{Z}$ sont algébriques ainsi que n'importe quelle racine de l'unité. Attention à ne pas confondre avec la notion d'élément algébrique sur $\mathbb{Q}$ où le polynôme annulant α est juste supposé à coefficients dans $\mathbb{Q}$. Ainsi $\cos(\frac{\pi}{3})$ n'est pas un entier algébrique mais est algébrique sur $\mathbb{Q}$. Noter aussi que α est un entier algébrique ssi $\overline{\alpha}$ l'est. Nous allons devoir démontrer quelques lemmes intermédiaires.

Lemme 2.14 *Soit $\alpha \in \mathbb{Q}$ un entier algébrique, alors $\alpha \in \mathbb{Z}$.*

Preuve. A faire en exercice en posant $\alpha = \frac{p}{q}$ avec p et q deux entiers premiers entre eux. ■

Lemme 2.15 *α est algébrique ssi α est valeur propre d'une matrice (carrée) à coefficients dans $\mathbb{Z}$.*

Preuve. Si α est entier algébrique et $P(\alpha) = 0$ avec $P \in \mathbb{Z}[X]$ unitaire, il suffit de considérer la matrice compagnon

$$M = \begin{pmatrix} 0 & \cdot & \cdot & 0 & -c_0 \\ 1 & & & \cdot & -c_1 \\ & \cdot & & \cdot & \cdot \\ 0 & & \cdot & 0 & \cdot \\ 0 & 0 & & 1 & -c_{n-1} \end{pmatrix}$$

de polynôme caractéristique P. Réciproquement si M est une matrice à coefficients dans $\mathbb{Z}$ dont α est valeur propre, son polynôme caractéristique $\det(XI - M)$ est à coefficients dans $\mathbb{Z}$ et annule α. ■

Lemme 2.16 *L'ensemble des entiers algébriques forme un sous-anneau de $\mathbb{C}$.*

Preuve. Soient α et β deux entiers algébriques, M et N deux matrices à coefficients dans $\mathbb{Z}$ d'ordre m et n telles que α et β soient respectivement des valeurs propres de M et N. Soient u_α et u_β des vecteurs propres pour M et N associés à α et β. Alors $u_a \otimes u_\beta$ est vecteur propre de $M \otimes N$ associé à $\alpha\beta$ mais aussi de $M \otimes I_n + I_m \otimes N$ associé à $\alpha + \beta$. Cela montre que $\alpha\beta$ et $\alpha + \beta$ sont des entiers algébriques d'après le lemme précédent. ■

Une conséquence de ce dernier lemme est que *les valeurs prises par les caractères des représentations des groupes finis sont toujours des entiers algébriques* (ce sont des sommes de racines de l'unité). En particulier, si $\chi(g) \in \mathbb{Q}$, alors $\chi(g) \in \mathbb{Z}$.

Soit C une classe de conjugaison du groupe fini G. On pose

$$\overline{C} = \sum_{g \in C} e_g \in \mathbb{C}[G].$$

Lemme 2.17 *Avec les notations précédentes,*

1. *$\overline{C}$ est dans le centre de $\mathbb{C}[G]$,*
2. *Si V est une représentation irréductible de G (et donc aussi un $\mathbb{C}[G]$-module irréductible) de dimension finie, il existe $\lambda \in \mathbb{Z}$ tel que pour tout $v \in V$, $\overline{C} \cdot v = \lambda v$ (i.e. $\overline{C}$ agit comme une homothétie).*

3. *Le rapport de l'homothétie de l'assertion 2 vaut* $\lambda = |C| \frac{\chi(g)}{\chi(1)}$ *où* χ *est le caractère de la représentation* V *et* g *un élément quelconque de* C.
4. *Le nombre* λ *est un entier algébrique.*

Preuve. Le 1 est facile et le 2 découle du lemme de Schur. Pour le 3, on suppose que l'on a fixé une base de V. Pour tout $g \in G$, soit $M(g)$ la matrice de l'action de g dans cette base. Celle correspondant à $\overline{C}$ vaut alors

$$M = \sum_{g \in C} M(g).$$

En prenant la trace et en utilisant le fait que toute les matrices $M(g), g \in C$ sont conjuguées, on obtient $\lambda\chi(1) = |C|\,\chi(g)$. Pour l'assertion 4, comme λ est valeur propre pour l'action de $\overline{C}$ sur V, c'est aussi une valeur propre pour l'action de $\overline{C}$ sur $\mathbb{C}[G]$. En effet, nous avons vu que chaque représentation irréductible apparait comme composante de la représentation adjointe $\mathbb{C}[G]$. Notons $N(g)$ la matrice de l'action de g sur $\mathbb{C}[G]$ relativement à la base $\{e_g \mid g \in G\}$ et N celle de $\overline{C}$. Nous avons

$$N = \sum_{g \in C} N(g).$$

Or les matrices $N(g)$ sont des matrices de permutation, donc à coefficients dans $\mathbb{Z}$. Ainsi λ est valeur propre de N à coefficients dans $\mathbb{Z}$. Le nombre λ est donc bien entier algébrique. ■

Nous pouvons maintenant terminer la preuve du Théorème 2.13.

Preuve du théorème 2.13. D'après le lemme précédent, pour toute classe de conjugaison C dans G, $|C| \frac{\chi(g)}{\chi(1)}$ est un entier algébrique. Par ailleurs $\chi(g)$ et donc aussi $\overline{\chi(g)}$ est un entier algébrique. Ainsi $|C| \frac{\chi(g)\overline{\chi(g)}}{\chi(1)}$ est un entier algébrique pour toute classe C. Cela implique, puisque les entiers algébriques forment un anneau, que

$$\sum_{C \text{ classe de conjugaison}} |C| \frac{\chi(g)\overline{\chi(g)}}{\chi(1)} = \frac{G}{\dim V}(\chi, \chi)_G$$

est un entier algébrique. Mais comme V est irréducible, $(\chi, \chi)_G = 1$ et $\frac{G}{\dim V} \in \mathbb{Q}$ est un entier algébrique. On a donc $\frac{G}{\dim V} \in \mathbb{Z}$. ■

2.6 Exercices

1. Montrer que S_3 possède 3 représentations irréductibles. Donner sa table des caractères.
2. Trouver tous les caractères irréductibles du groupe cyclique C_4 et exprimer le caractère de la représentation régulière comme combinaison linéaires de ces caractères.
3. Montrer que les seuls caractères irréductibles de G non nuls qui soient des homomorphismes de groupes sont les caractères linéaires.
4. Soit ε une représentation de G de dimension 1 telle que $\varepsilon(G) = \{-1, +1\}$. Montrer que $\sum_{g \in G} \varepsilon(g) = 0$.
5. Déterminer à isomorphisme près toutes les représentations du groupe quaternionique Q_8. On rappelle qu'il s'agit du groupe engendré par deux générateurs a et b et par les relations

$$a^4 = 1, \quad a^2 = b^2, \quad b^{-1}ab = a^{-1}.$$

Donner la table des caractères de Q_8.

6. Donner la table des caractères sur groupe dihédral D_8 engendré par les générateurs a et b soumis aux relations $a^4 = 1, b^2 = 1$ et $b^{-1}ab = a^{-1}$. Comparer avec la table de Q_8.
7. Soit π une représentation de G de caractère χ. Montrer que $g \in \ker \pi$ ssi $\chi(g) = \chi(1)$.
8. Soit $g \in G$ tel que pour toute représentation irréductible π, on ait $g \in \ker \pi$. Montrer que $g = 1$.
9. Soit N un sous groupe distingué de G et $p : G \to G/N$ la projection canonique. Soit $\tilde{\pi}$ une représentation de G/N. Montrer que $\pi = \tilde{\pi} \circ p$ est une représentation de G de même degré que $\tilde{\pi}$. Si $\tilde{\pi}$ est irréducible, π est-elle irréductible. Que se passe-t-il dans le cas où $N = D(G)$ est le sous-groupe dérivé de G (i.e. le sous groupe de G engendré par les éléments du type $xyx^{-1}y^{-1}$ avec $x, y \in G$).
10. Soit (π, V) une représentation de G et χ son caractère. On sait que $(\pi \otimes \pi, V \otimes V)$, le carré tensoriel de V est aussi une représentation de G.
    (a) On note $SymV$ le sous-espace de $V \otimes V$ enjendré par les tenseurs symétriques (i.e. de la forme $u \otimes v + v \otimes u$ avec $u, v \in V$). De même soit $\wedge^2 V$ le sous-espace des tenseurs antisymétriques. Montrer que $V \otimes V = SymV \oplus \wedge^2 V$.
    (b) Montrer que $SymV$ et $\wedge^2 V$ sont des sous représentations de $V \otimes V$ dont on notera χ_s et χ_a les caractères.
    (c) Soit $g \in G$. Justifier que $\pi(g)$ est diagonalisable. En utilisant une base de vecteurs propres pour $\pi(g)$ établir que
    $$\chi_s(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2)) \text{ et } \chi_a(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2)).$$
11. Soit G un groupe d'ordre 12. Quels sont les dégrés possibles des représentations irréductibles de G ?
12. Montrer que si $x \in G$ est différent de 1, il y a au moins un caractère irréductible χ de G tel que $\chi(x) \neq \chi(1)$.
13. Soit G un groupe fini et $\rho : G \to GL(V)$ une représentation de G sur le $\mathbb{C}$-espace vectoriel V de dimension n. On note χ le caractère associé.
    Montrer que $\delta : g \to \det(\rho(g))$ est une représentation irréducible de G.
    (a) Prouver que $G/\ker \delta$ est abélien.
    (b) Supposons qu'il existe $g \in G$ tel que $\delta(g) = -1$. Montrer que G possède un sous-groupe normal d'indice 2.
    (c) Montrer que lorsque G n'a pas de sous groupe d'indice 2, ses éléments d'ordre 2 vérifient $\chi(g) \equiv \chi(1) \bmod 4$.
14. Supposons que χ est un caractère du groupe fini G tel que χ ne prennent que des valeurs entières et paires. Peut-on en conclure qu'il existe un caractère ϕ tel que $\chi = 2\phi$?
15. Soit G un groupe fini et $\chi_1, \ldots, \chi_k$ ses caractères irréductibles complexes. On note $C_1, \ldots, C_k$ les classes de conjugaisons de G. Soit $A = (a_{i,j})$ la matrice $k \times k$ telle que
    $$a_{i,j} = \frac{\sqrt{|C_i|}}{\sqrt{|G|}}\chi_j(g_i).$$
    où g_j est un représentant de C_j.

(a) Justifier que A et $\overline{{}^tA}$ sont des matrices unitaires.

(b) En déduire les relations

$$\sum_{j=1}^{k} \chi_j(g_{i_1})\overline{\chi_j(g_{i_2})} = \frac{|G|}{|C_{i_1}|}\delta_{i_1,i_2} \quad \text{pour } 1 \leq i_1, i_2 \leq k.$$

3 Dual d'un groupe fini

3.1 Définition du groupe dual

Soit G un groupe fini noté multiplicativement. On note $\widehat{G}$ l'ensemble des morphismes $f : G \to \mathbb{C}^*$. On voit donc que $\widehat{G} \subset \mathcal{A}$ l'algèbre des fonctions centrales sur G. En effet, pour tout $f \in \widehat{G}$, on a

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

On vérifie en fait que $\widehat{G}$ coincide avec l'ensemble des caractères des représentations de degré 1de G. En effet si ρ est une telle représentation de caractère χ, on a pour tout $g \in G$, $\rho(g) = \chi(g)$ puisque $\rho(g) \in \mathbb{C}$. Le produit tensoriel de deux représentations de degré 1 restant de degré 1, la Proposition 2.3 montre que $\widehat{G}$ est en fait un *groupe abélien*, on l'appelle le *groupe dual* de G.

Si G est de cardinal n, le théorème de Lagrange implique que $f \in \widehat{G}$ est en fait à valeur dans $\mathbb{U}_n$ le groupe des racines n-ièmes de l'unité. En effet, pour tout $g \in G$

$$1 = f(1) = f(g^n) = f(g)^n.$$

Il s'ensuit que $\widehat{G}$ est fini.

3.2 Cas des groupes abéliens

Supposons que G est un groupe abélien fini de cardinal n. Dans ce cas, on sait d'après la Proposition 1.7 que les représentations de degré 1 de G sont les représentations irréductibles. D'après le Théorème 2.12, nous avons exactement n représentations irréducibles (n classes de conjugaison puisque G est abélien). Puisque $\widehat{G}$ coincide avec l'ensemble des caractères des représentations de degré 1 de G, on en déduit que $|G| = \left|\widehat{G}\right|$. En fait, on a la proposition plus forte ci-dessous :

Proposition 3.1 *Les groupes abéliens G et $\widehat{G}$ sont isomorphes.*

Preuve. Avec les notations de (2), nous avons

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

où a_{i+1} divise a_i pour tout $i = 1, \ldots, r-1$. Soit $(g_1, \ldots, g_r)$ un ensemble de générateurs où, pour tout $i = 1, \ldots, r$, g_i est d'ordre a_i. Tout élément $g \in G$ s'écrit sous la forme $g = g_1^{\alpha_1} \cdots g_r^{\alpha_r}$ où $0 \leq \alpha_i \leq a_i - 1$. Chaque représentation ρ de dimension 1 de G est déterminée par l'image des g_i par ρ. Comme $g_i^{a_i} = 1$, $\rho(g_i)$ doit être une racine a_i-ième de l'unité disons α_i. On vérifie alors facilement que l'application

$$\theta : \widehat{G} \to \mathbb{U}_{a_1} \times \cdots \times \mathbb{U}_{a_r}$$

qui à ρ associe $(\alpha_1, \ldots, \alpha_r)$ est un isomorphisme de groupes abéliens. Par ailleurs, on a $\mathbb{U}_{a_1} \times \cdots \times \mathbb{U}_{a_r} \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z}$ ce qui montre que G et $\widehat{G}$ sont isomorphes. ■

Remarque : attention ce résultat est faux avec des groupes non abéliens puisque $\widehat{G}$ est toujours abélien !

Proposition 3.2 *Les éléments de $\widehat{G}$ forment une base orthonormée de $\mathcal{F}$ l'algèbre des fonctions de G dans $\mathbb{C}$ (qui ici coïncide avec $\mathcal{A}$).*

Preuve. Cela découle du fait que ces caractères irréductibles de G forment une base de $\mathcal{A}$ d'après le Théorème 2.12. Or $\mathcal{F} = \mathcal{A}$ puisque G est abélien. De plus, les caractères irréductibles s'identifient à $\widehat{G}$ dans le cas abélien. ■

3.3 Transformée de Fourier pour un groupe abélien fini

Soit G un groupe abélien fini et $\widehat{G}$ son groupe dual. On note $\mathcal{F}$ (resp. $\widehat{\mathcal{F}}$) le $\mathbb{C}$-ev des fonctions de G (resp.$\widehat{G}$) dans $\mathbb{C}$. Pour tout $f, \chi \in \widehat{G}$, on pose

$$\widehat{f}(\chi) = (f, \chi) = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{\chi(g)}.$$

D'après la proposition, $\widehat{G}$ est une base orthonormée de $\mathcal{F}$, on a donc

$$f = \sum_{\chi \in \widehat{G}} (f, \chi)\chi = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi \tag{11}$$

Définition 3.3 *La transformation de Fourier est l'application $\Phi : \mathcal{F} \to \widehat{\mathcal{F}}$ qui à f associe sa transformée de Fourier $\widehat{f}$ définie par :*

$$\widehat{f}(\chi) = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{\chi(g)}.$$

Proposition 3.4 *La transformation de Fourier Φ est un isomorphisme d'espaces vectoriels.*

Preuve. Il s'agit clairement d'une application linéaire. Elle est injective car si $\widehat{f}(\chi) = 0$ pour tout $\chi \in \widehat{G}$, alors $f = 0$ d'après (11). Par ailleurs, chacun des espaces $\widehat{\mathcal{F}}$ et $\mathcal{F}$ a pour dimension n d'après les Propositions 3.1 et 3.2. ■

La transformation de Fourier possède de nombreuses autres propriétés très utiles notamment en arithmétique et même en traitement de l'image. Nous renvoyons le lecteur à [6] pour des développements sur ces questions.

3.4 Sommes de Gauss et réciprocité quadradique

Soit p un nombre premier impair. Pour tout $x \in \mathbb{Z}$, on note $\overline{x}$ la classe de $x \bmod p$. Rappelons que le symbole de Legendre est défini par

$$\left(\frac{x}{p}\right) = \begin{cases} 0 \text{ si } x \in p\mathbb{Z}, \\ 1 \text{ si } \overline{x} \text{ est un carré dans } (\mathbb{Z}/p\mathbb{Z})^*, \\ -1 \text{ sinon.} \end{cases}$$

Proposition 3.5

1. *L'application* $\rho : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$ *telle que* $\rho(\overline{x}) = x^{\frac{p-1}{2}} \bmod p$ *définit une représentation de dimension* 1 *du groupe multiplicatif* $(\mathbb{Z}/p\mathbb{Z})^*$.
2. *On a* $\rho(\overline{x}) = \left(\frac{x}{p}\right)$ *pour tout* $x \in \overline{x}$ *et tout* $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^*$.
3. *Le symbole de Legendre est multiplicatif*

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \ \forall x, y \in \mathbb{Z}.$$

4. *On a l'identité*

$$\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) = 0.$$

5. *Si* $x = x' \bmod p$, *on a* $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$.

Preuve. 1 : L'application est bien définie car $\rho(\overline{x})$ ne dépend pas de $x \in \overline{x}$. Par ailleurs $\rho(\overline{x})^2 = x^{p-1} \bmod p = 1$ donc $\rho(\overline{x}) \in \{\pm 1\}$. Comme $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$, ρ est surjectif. En effet si α est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ (racine primitive modulo p), $\rho(\alpha) = -1$. L'application ρ est clairement un morphisme de groupes multiplicatifs. On a par ailleurs $(\mathbb{Z}/p\mathbb{Z})^*/\ker\rho \simeq \{\pm 1\}$ donc $\ker\rho$ est d'indice 2 dans $(\mathbb{Z}/p\mathbb{Z})^* = \ker\rho \sqcup (\alpha \ker\rho)$.

2 : Si $\overline{x} = \overline{y}^2$ est un carré, on a $\rho(\overline{x}) = y^{p-1} \bmod p = 1$. Sinon on peut écrire puisque $(\mathbb{Z}/p\mathbb{Z})^* = \ker\rho \sqcup (\alpha \ker\rho)$, $\overline{x} = \overline{y}^2\alpha$ et $\rho(\overline{x}) = -1$.

3 : Découle de 1 et 2.

4 : Découle de 1 et de l'exercice 4 du chapitre précédent.

5 : Découle de 2. ■

Soit θ une racine primitive modulo p (par exemple $\theta = \exp(\frac{2i\pi}{p})$. On définit la somme de Gauss τ par

$$\tau = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\theta^x.$$

Proposition 3.6 *Nous avons* $\tau^2 = p\left(\frac{-1}{p}\right)$.

Preuve. Par définition

$$\tau^2 = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\theta^{x+y} = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left(\frac{xy}{p}\right)\theta^{x+y}$$

où la seconde égalité est une conséquence du point 3 de la proposition précédente. Cela donne

$$\tau^2 = \sum_{u=0}^{p-1} \sum_{x+y=u \bmod p} \left(\frac{xy}{p}\right)\theta^u = \sum_{u=0}^{p-1}\sum_{x=0}^{p-1} \left(\frac{x(u-x)}{p}\right)\theta^u = \sum_{u=0}^{p-1} S(u)\theta^u$$

car

$$\sum_{x+y=u \bmod p} \left(\frac{xy}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x(u-x)}{p}\right)$$

d'après le point 5 de la même proposition. Posons pour tout $u \in \{0, \ldots, p-1\}$

$$S(u) = \sum_{x=0}^{p-1} \left(\frac{x(u-x)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x(u-x)}{p}\right).$$

On a $S(0) = \sum_{x=1}^{p-1} \left(\frac{-1}{p}\right) = (p-1)\left(\frac{-1}{p}\right)$. Pour $u \neq 0$, on note x^{-1} [1] l'unique entier de $\{1, \ldots, p-1\}$ tel que $xx^{-1} = 1 \bmod p$. On a alors

$$S(u) = \sum_{x=1}^{p-1} \left(\frac{-x^2(1-x^{-1}u)}{p}\right)$$

puisque pour tout $x = 1, \ldots p-1$, $-x^2(1-x^{-1}u) = x(u-x) \bmod p$. Comme le symbole de Legendre est multiplicatif,

$$S(u) = \left(\frac{-1}{p}\right) \sum_{x=1}^{p-1} \left(\frac{1-x^{-1}u}{p}\right) = \left(\frac{-1}{p}\right) \sum_{z=0, z\neq 1}^{p-1} \left(\frac{z}{p}\right)$$

où la dernière égalité vient du fait que $\{(1-x^{-1}u) \bmod p \mid x = 1, \ldots p-1\} = \{0, 2, \ldots, p-1\}$ car $u \neq 0$ et $x^{-1} \neq 0$. Finalement

$$S(u) = -\left(\frac{-1}{p}\right)$$

en utilisant le point 4 de la proposition précédente. On a donc

$$\tau^2 = S(0) + \sum_{u=1}^{p-1} S(u)\theta^u = \left(\frac{-1}{p}\right)\left(p - 1 - \sum_{u=1}^{p-1} \theta^u\right) = \left(\frac{-1}{p}\right) p$$

puisque $1 + \sum_{u=1}^{p-1} \theta^u = 0$. ■

Théorème 3.7 *Soient p et q deux nombres premiers impairs disctincts. On a*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Preuve. Notons $E = \mathbb{Z}[\theta]$ le sous-anneau de $\mathbb{C}$ engendré par $\mathbb{Z}$ et θ. En utilisant le morphisme de Frobenius dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, nous avons

$$\tau^q = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \theta^{qx} \bmod qE.$$

En utilisant que le symbole de Legendre est multiplicatif, cela donne

$$\tau^q = \left(\frac{q}{p}\right) \sum_{x=1}^{p-1} \left(\frac{qx}{p}\right) \theta^{qx} \bmod qE$$

1. Il s'agit d'une notation un peut trompeuse car x^{-1} n'est pas ici égal à l'inverse de x dans $\mathbb{Z}$ qui n'est pas un entier en général.

de sorte que nous avons $\tau^q = \left(\frac{q}{p}\right)\tau \bmod qE$ puisque la multiplication par q donne une bijection de $\mathbb{F}_p^*$.

Considérons maintenant le nombre

$$\left(\frac{\left(\frac{-1}{p}\right)p}{q}\right) = \left(\left(\frac{-1}{p}\right)p\right)^{\frac{q-1}{2}} = (\tau^2)^{\frac{q-1}{2}} = \tau^{q-1}.$$

En mulitipliant par τ^2, on trouve la congruence

$$\left(\frac{\left(\frac{-1}{p}\right)p}{q}\right)\tau^2 = \tau^{q+1} = \left(\frac{q}{p}\right)\tau^2 \bmod qE.$$

D'après la proposition précédente, nous savons que $\tau^2 = \left(\frac{-1}{p}\right)p$ donc comme p et q sont premiers entre eux, τ^2 est inversible dans E/qE. En simplifiant par $\tau^2 \bmod qE$, nous obtenons

$$\left(\frac{\left(\frac{-1}{p}\right)p}{q}\right) = \left(\frac{q}{p}\right)$$

puisque l'égalité modulo qE équivaut à l'égalité pour des valeurs dans $\{\pm 1\}$. Finalement, nous avons

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{\left(\frac{-1}{p}\right)p^2}{q}\right) = \left(\frac{\left(\frac{-1}{p}\right)}{q}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

■

3.5 Exercices

1. Etant données f_1 et f_2 dans $\mathcal{F}$ (associé à G fini et abélien noté additivement), on définit le produit de convolution $f_1 * f_2 \in \mathcal{F}$ par

$$f_1 * f_2(g) = \sum_{s \in G} f_1(g-s) f_2(g).$$

   Montrer que $*$ est une opération commutative et associative. Démontrer également que

$$\widehat{f_1 * f_2} = |G|\, \widehat{f_1} \times \widehat{f_2}.$$

2. Montrer que la formule de réciprocité quadratique permet de ramener le calcul du symbole de Legendre $\left(\frac{x}{p}\right)$ à $\left(\frac{-1}{p}\right)$ et $\left(\frac{2}{p}\right)$.
3. Le but de l'exercice est le calcul de $\left(\frac{2}{p}\right)$ lorsque p est un nombre premier impair.
   (a) Montrer que $2.4....(p-1) = 2^{\frac{p-1}{2}}(\frac{p-1}{2}!)$.
   (b) On considère l'ensemble E des nombres pairs entre $\frac{p+1}{2}$ et $p-1$. Montrer que $\prod_{k \in E} k = (-1)^\mu \bmod p$ où μ est le nombre d'entiers impairs entre 1 et $\frac{p-1}{2}$ (on pourra considérer l'ensemble des nombres $-(E-p)$.
   (c) En déduire que $2^{\frac{p-1}{2}}(\frac{p-1}{2}!) = (-1)^\mu(\frac{p-1}{2}!)$ puis que $2^{\frac{p-1}{2}} = (-1)^\mu$.
   (d) Montrer que $\mu = \frac{p-1}{4}$ si $\frac{p-1}{2}$ est pair et $\mu = \frac{p+1}{4}$ si $\frac{p-1}{2}$ est impair. En déduire que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

4 Restriction et induction de représentations

4.1 Définition

Soit H un sous-groupe de G. Toute représentation $\rho : G \to GL(V)$ de caractère χ définit par restriction une représentation $\rho_H : H \to GL(V)$. On la notera $\rho_{\downarrow H}$ ou plus simplement $\rho_\downarrow$ lorsqu'il n'y a pas d'ambiguité. Son caractère n'est autre que la restriction $\chi_\downarrow$ du caractère χ au sous-groupe H. Il faut bien noter que même lorsque ρ est une représentation irréductible, $\rho_\downarrow$ ne l'est pas en général. Déterminer sa décomposition en représentations irréductibles pour H est alors un problème difficile.

Frobenius a eu l'idée de construire la table des caractères de G à partir de la table des caractères de ses sous-groupes H en introduisant une opération duale de la restriction appelée *induction*. Cette fois, il s'agit de construire une représentation de G à partir d'une représentation de H. L'exemple le plus simple d'induction est celle obtenue en faisant agir G sur les classes à gauche de G/H. Rappelons que H étant un sous-groupe de G, les classes à gauche de G/H sont les sous-ensembles de la forme

$$gH = \{gh \mid h \in H\}.$$

Il est clair que toutes ces classes ont pour cardinal $|H|$ et, comme elle forment une partition de G, on a $|G/H| = \frac{|G|}{|H|}$. On se donne un système $\{g_1, \ldots, g_k\}$ de représentants de ces classes, c'est à dire que l'on choisit un élément de G dans chaque classe. Le groupe G agit de façon naturelle sur $G/H = \{g_1H, \ldots, g_kH\}$ en posant pour tout $g \in G$

$$g \cdot g_iH = g_{i'}H$$

où $g_{i'}$ est l'unique éléments de $\{g_1, \ldots, g_k\}$ tel que $g_{i'}^{-1} g g_i \in H$. Pour obtenir une représentation de G, il suffit d'introduire une structure linéaire sur G/H. Soit donc $U = \oplus_{i=1}^k \mathbb{C}u_i$. On définit la représentation π_H de G en décrivant l'image des vecteurs de la base $\{u_1, \ldots, u_k\}$ par $\pi_H(g)$. Posons

$$\pi_H(g)(u_i) = u_{i'}$$

où i' est l'unique indice de $\{1, \ldots, k\}$ tel que $g_{i'}^{-1} g g_i \in H$. Il est clair que la matrice de $\pi_H(g)$ est la matrice de permutation correspondant à la permutation σ_g définite par $\sigma_g(i) = i'$.

Exemple 4.1 *Considérons le sous-groupe $H = \{id, (12)\}$ de S_3. Les classes à gauche sont $u_1 = H$, $u_2 = (13)H$ et $u_3 = (23)H$. On vérifie que la matrice de $\pi_H(123)$ du cycle $(123) = (12)(23)$ dans la base $\{u_1, u_2, u_3\}$ est*

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Plus généralement, soit $\psi : H \to GL(V)$ une représentation de H. On définit la représentation induite $\psi^{\uparrow G}$ (ou plus simplement $\psi^\uparrow$) de la façon suivante. L'espace de la représentation $\psi^\uparrow$ est $U \otimes V$ où U est l'espace vectoriel de dimension $k = |G/H|$ introduit précédemment. Rappelons que si $\{v_1, \ldots, v_r\}$ est une base de V, le produit tensoriel $U \otimes V$ est le $\mathbb{C}$ espace vectoriel de dimension kr et de base $\{u_i \otimes v_i \mid 1 \leq i \leq k, 1 \leq j \leq r\}$. Pour définir $\psi^\uparrow$, il suffit donc de donner les images des vecteurs de la base tensorielle. Posons

$$\psi^\uparrow(g)(u_i \otimes v_j) = u_{\sigma_g(i)} \otimes \psi(g_{\sigma_g(i)}^{-1} g g_i)(v_j).$$

L'expression est bien définie puisque nous avons $g_{\sigma_g(i)}^{-1} g g_i \in H$. On en déduit le calcul du caractère induit $\chi^{\uparrow}$.

Proposition 4.2 *Soit ψ une représentation de H sous-groupe du groupe fini G. Le caractère $\chi^{\uparrow}$ de la représentation induite $\psi^{\uparrow}$ est donné par la formule suivante :*

$$\chi^{\uparrow}(g) = \frac{1}{|H|} \sum_{f \in G \text{ t.q. } f^{-1}gf \in H} \chi(f^{-1}gf) \quad \forall g \in G$$

où χ est le caractère de ψ.

Preuve. La matrice de $\psi^{\uparrow}(g)$ dans la base $\{u_i \otimes u_j\}$ est la matrice de permuation par blocs $M_{\psi^{\uparrow}}(g) = (M_{i,s}(g))_{1 \leq i,s \leq k}$ dont les blocs sont les matrices $r \times r$ données par

$$M_{i,s}(g) = \begin{cases} M_{\psi}(g_i^{-1} g g_j) \text{ si } \sigma_g(s) = i, \\ 0 \text{ sinon.} \end{cases}$$

On a donc

$$\chi^{\uparrow}(g) = tr(M_{\psi^{\uparrow}(g)}) = \sum_{i | \sigma_g(i) = i} tr(M_{\psi}(g_i^{-1} g g_i) = \sum_{i | g_i^{-1} g g_i \in H} \chi(g_i^{-1} g g_i).$$

Puisque χ est invariant sur les classes de conjugaison de H, on aura également

$$\chi^{\uparrow}(g) = \frac{1}{|H|} \sum_{f \in G | f^{-1}gf \in H} \chi(f^{-1}gf).$$

■

Exercice 4.3 *Déterminer la table des caractères obtenus par induction à partir des caractères irréductibles de C_4 à Q_8. Décomposer ces caractères induits en irréductibles.*

Corollaire 4.4 *Supposons que ψ soit la représentation triviale de H de caractère la fonction constante égale à 1. La représentation $\psi^{\uparrow}$ est la* représentation permutationelle *de G sur G/H. Son caractère est donné par la formule*

$$\chi^{\uparrow}(g) = \frac{|G| \, |C_g \cap H|}{|H| \, |C_g|} \quad \forall g \in G.$$

Preuve. D'après la formule précédente, pour obtenir $\chi^{\uparrow}(g)$ il suffit de calculer le cardinal de l'ensemble $E(g) = \{f \in G \mid f^{-1}gf \in H\}$. Pour cela considérons l'application

$$\theta : \begin{cases} E(g) \to H \cap C_g \\ f \longmapsto f^{-1}gf \end{cases}$$

Pour tout $u \in H \cap C_g$, on a $\left|\theta^{-1}(u)\right| = |S_g|$ où S_g est le stabilisateur de g sous l'action par conjugaison. Comme θ est surjective, nous avons $|E(g)| = |S_g| \, |C_g \cap H|$. Cela donne

$$\chi^{\uparrow}(g) = \frac{|S_g| \, |C_g \cap H|}{|H|} = \frac{|G| \, |C_g \cap H|}{|H| \, |C_g|}$$

puisque $|S_g| = \frac{|G|}{|C_g|}$. ■

4.2 Loi de réciprocité de Frobenius

Théorème 4.5 *Soit χ un caractère de H et τ un caractère de G. On a $\langle \chi^{\uparrow}, \tau \rangle = \langle \chi, \tau_{\downarrow} \rangle$.*

Preuve. D'après la Proposition 4.2, nous avons pour tout $g \in G$

$$\chi^{\uparrow}(g) = \frac{1}{|H|} \sum_{f \in G} \chi^*(f^{-1}gf) \text{ avec } \chi^*(h) = \begin{cases} h \text{ si } h \in H, \\ 0 \text{ sinon.} \end{cases}$$

On a donc

$$\langle \chi^{\uparrow}, \tau \rangle = \frac{1}{|G|} \sum_{g \in G} \chi^{\uparrow}(g)\overline{\tau(g)} = \frac{1}{|G|\,|H|} \sum_{g \in G} \sum_{f \in G} \chi^*(f^{-1}gf)\overline{\tau(g)}.$$

En posant $x = f^{-1}gf$, cela donne

$$\langle \chi^{\uparrow}, \tau \rangle = \frac{1}{|G|\,|H|} \sum_{x \in G} \sum_{f \in G} \chi^*(x)\overline{\tau(fxf^{-1})} = \frac{1}{|G|\,|H|} \sum_{x \in G} \sum_{f \in G} \chi^*(x)\overline{\tau(x)} = \frac{1}{|H|} \sum_{x \in F} \chi(x)\overline{\tau(x)} = \langle \chi, \tau_{\downarrow H} \rangle$$

puisque τ est invariant sur les classes de conjugaison de G. ■

Corollaire 4.6 *Supposons que χ soit associé à la représentation irréductible ψ de H et τ à la représentation irréductible ρ de G. Alors, la multiplicité de ρ dans $\psi^{\uparrow G}$ est égale à celle de ψ dans $\rho_{\downarrow H}$.*

4.3 Exercices

1. Déterminer la décomposition en irréductibles de la restriction de la représentation de degré 2 de Q_8 au sous-groupe cyclique C_4 d'ordre 4 engendré par le générateur a (cf Exercice 5).
2. Soit G un groupe fini et H un sous-groupe de G. On note $\psi_1, \ldots, \psi_r$ les caractères irréductibles de H et $\varphi_1, \ldots \varphi_s$ les caractères irréductibles de G.
   (a) Soit $j \in \{1, \ldots, s\}$. Justifier que $\varphi_j^{\downarrow H}$ la restriction de φ_j à H se décompose sous la forme $\varphi_j^{\downarrow H} = \sum_{i=1}^{r} d_{i,j}\psi_i$ où les $d_{i,j}$ sont dans $\mathbb{N}$. Posons $D = (d_{i,j})$ la matrice $r \times s$ associée (dite de décomposition).
   (b) Soit $i \in \{1, \ldots, r\}$. Justifier que $\psi_i^{\uparrow H}$ le caractère induit de H à G se décompose sous la forme $\psi_i^{\uparrow H} = \sum_{j=1}^{s} \delta_{j,i}\varphi_j$ où les $\delta_{i,j}$ sont dans $\mathbb{N}$. On pose $\Delta = (\delta_{j,i})$. Quelle relation lie les matrices D et Δ ?
   (c) Montrer que pour tout $\langle \varphi_j^{\downarrow H}, \varphi_j^{\downarrow H} \rangle_H = \sum_{i=1}^{r} d_{i,j}^2$.
   (d) Etablir que
   $$1 = \langle \varphi_j, \varphi_j \rangle_G = \frac{|H|}{|G|} \sum_{i=1}^{r} d_{i,j}^2 + \frac{1}{|G|} \sum_{g \notin H} |\varphi_j(g)|^2 .$$
   (e) En déduire que pour tout $j \in \{1, \ldots, s\}$, on a $\sum_{i=1}^{r} d_{i,j}^2 \leq [G : H]$ et que l'égalité est réalisée si et seulement si $\varphi_j(g) = 0$ pour tout $g \notin H$.
   (f) Etablir que pour tout $i \in \{1, \ldots, r\}$, on a également $\sum_{j=1}^{s} \delta_{j,i}^2 \leq [G : H]$ et $\sum_{j=1}^{s} d_{i,j}^2 \leq [G : H]$.

3. Soit G un groupe et H un sous groupe abélien de G d'indice k. Montrer $\chi(1) \leq k$ pour tout caractère irréductible χ de G.
4. Soit $G = D_8$ et $H = \langle a^2, b\rangle$. Soit U le sous espace de $\mathbb{C}[H]$ de dimension 1 en genfré par $1 - a^2 + b - a^2b$.
   (a) Vérifier que U est une sous représentation de $\mathbb{C}[H]$ pour H.
   (b) Déterminer une base de $U^{\uparrow G}$.
   (c) Déterminer les caractères de U et de $U^{\uparrow G}$. La représentation $U^{\uparrow G}$ est-elle irréductible ?

5 Caractères des représentations du groupe symétrique

Le but de ce chapitre est de déterminer les caractères irréductibles du groupe symétrique. Les représentations irréductibles du groupe symétrique (et pas seulement leurs caractères) peuvent également être totalement explicitées. Nous renvoyons le lecteur au Chapitre 4 du livre de Fulton et Harris [2] pour une exposition complète.

5.1 Classes de conjugaison

Soit S_n le groupe des permuations de l'ensemble $X_n = \{1, \ldots, n\}$. On note $\sigma = (i_1 i_2 \cdots i_k)$ le cycle de longueur k qui envoie i_a sur i_{a+1} pour tout $1 \leq a < k$, i_k sur i_1 et laisse invariant les entiers de X_n qui ne sont pas dans son support $\{i_1, \ldots, i_k\}$. Il est facile de vérifier que pour tout $\tau \in S_n$, $\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_2)\cdots\tau(i_k))$. On rappelle que toute permutation se décompose en un produit de cycles à supports disjoints. Ces cycles commuttant entre eux, on peut choisir de les écrire par ordre de longueur décroissante. On vérifie alors facilement que les classes de conjugaisons de S_n sont indexées par les partitions de n, c'est à dire par les suites décroissantes $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r)$ d'entiers (notation additive) telles que $\lambda_1 + \cdots + \lambda_r = n$. On note alors $\lambda \vdash n$. Les éléments de la classe C_λ sont ceux dont la décomposition en cycles à supports disjoints fait apparaître r cycles de longueurs $\lambda_1, \ldots, \lambda_r$ (en comptant les cycles de longueur 1). On dit que les éléments de C_λ ont pour type cyclique λ. On peut également choisir d'écrire $\lambda = (1^{m_1} 2^{m_2} \cdots n^{m_n})$ (notation multiplicative) où pour tout i, la partition λ possède m_i parts égales à i.

Exemple 5.1 *Le groupe S_4 possède 5 classes de conjugaison :*

1. $C_{(1^4)} = \{id\}$,
2. $C_{(1^2 2)} = \{(12), (13), (14), (23), (24), (34)\}$,
3. $C_{(2^2 2^2)} = \{(12)(34), (13)(24), (14)(23)\}$,
4. $C_{(13)} = \{(123), (124), (134), (234), (132), (142), (143), (243)\}$,
5. $C_{(4)} = \{1234), (1243), (1324), (1342), (1423), (1432)\}$,

où on n'a pas fait apparaître les cycles de longueur 1.

Proposition 5.2 *Le nombre d'éléments de la classe C_λ avec $\lambda = (1^{m_1} 2^{m_2} \cdots n^{m_n})$ est*

$$|C_\lambda| = \frac{n!}{1^{m_1} m_1! 2^{m_2} m_2! \cdots n^{m_n} m_n!}.$$

Preuve. Considérons la décomposition de $\sigma \in C_\lambda$ en produit de cycles à supports disjoints. On fait agir S_n sur lui-même par conjugaison et on note S_σ le stabilisateur de σ. Un élément τ de S_σ doit permuter les cycles de longueur k de σ. Notons $X(\sigma, k)$ la réunion des supports des cycles de longueur k. En tenant compte du fait qu'il y a k supports différents définissant le même cycle, le nombre de permuations de $X(\sigma, k)$ qui permuttent les cycles de longueur k de σ vaut $m_k! k^{m_k}$. Il s'ensuit que

$$|S_\sigma| = 1^{m_1} m_1! \times 2^{m_2} m_2! \times \cdots \times n^{m_n} m_n!$$

et donc, puisque C_λ est l'orbite de σ, on a bien

$$|C_\lambda| = \frac{n!}{1^{m_1} m_1! \times 2^{m_2} m_2! \times \cdots \times n^{m_n} m_n!}.$$

■

Nous rencontrerons souvent le cardinal du stabilisateur de C_λ dans la suite. Posons $z_\lambda = 1^{m_1} m_1! \times 2^{m_2} m_2! \times \cdots \times n^{m_n} m_n!$.

5.2 Sous-groupes de Young

D'après le Théorème 2.12, le nombre de caractères irréductibles de S_n est égal au nombre $p(n)$ de classes de conjugaison de S_n, autrement dit, nombre $p(n)$ de partitions $\lambda \vdash n$. Pour calculer les caractères de ces représentations irréductibles, l'idée de Frobenius est de commencer par calculer les caractères de certains caractères induits. Pour toute partition λ de n, notons S_λ le sous-groupe de Young défini par

$$S_\lambda := S_{\lambda_1} \times \cdots \times S_{\lambda_k}$$

c'est à dire le sous-groupe de S_n qui laisse invariant chacun des sous-ensembles $\{1, \ldots, \lambda_1\}$ et $\{\lambda_i + 1, \ldots, \lambda_{i+1}\}, i = 1, \ldots, r-1$ de X_n. Il est clair que $|S_\lambda| = \lambda_1! \times \cdots \times \lambda_k!$. Nous allons calculer dans un premiers temps, les caractères des représentations permutationelles de S_n sur l'ensemble des classes S_n/S_λ (cf Corollaire 4.4).

Exercice 5.3 *Donner la liste des* 12 *éléments du sous-groupe* $S_{(3,2)}$ *de* S_5.

Proposition 5.4 *Soit* $\rho = (1^{m_1} \cdots n^{m_n})$ *et* $\lambda = (\lambda_1, \ldots, \lambda_k)$ *deux partitions de* n. *Le nombre de permutations de* $C_\rho \cap S_\lambda$ *est égal à*

$$|C_\rho \cap S_\lambda| = \sum \frac{\lambda_1!}{z_{\rho^{(1)}}} \cdots \frac{\lambda_k!}{z_{\rho^{(k)}}}$$

où la somme porte sur tous les k*-uplets* $(\rho^{(1)}, \ldots, \rho^{(k)})$ *de partitions* $\rho^{(i)} = (1^{m_1^{(i)}} 2^{m_2^{(i)}} \cdots) \vdash \lambda_i$ *tels que* $m_i = \sum_{j=1}^k m_i^{(j)}$ *pour* $1 \leq i \leq n$.

Preuve. Soit $\sigma \in C_\rho \cap S_\lambda$. On peut écrire $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$ où $\sigma_i \in S_{\lambda_i}$. Soit $\rho^{(i)}$ le type cyclique de σ_i. On a $\rho^{(i)} \vdash \lambda_i$ et en notant $\rho^{(i)} = (1^{m_1^{(i)}} 2^{m_2^{(i)}} \cdots) \vdash \lambda_i$, on a $m_i = \sum_{j=1}^k m_i^{(j)}$ pour $1 \leq i \leq n$. D'après la Proposition 5.2, le nombre d'éléments de type cyclique $\rho^{(i)}$ dans S_{λ_i} vaut $\frac{\lambda_i!}{z_{\rho^{(i)}}}$, le résultat s'en déduit facilement. ■

Exercice 5.5 *Déterminer* $\left|C_{(1^3 2)} \cap S_{(3,2)}\right|$ *et* $\left|C_{(14)} \cap S_{(3,2)}\right|$.

5.3 Caractères permutationels

Nous allons maintenant calculer les caractères permutationnels dans le cas du groupe $G = S_n$ et en prenant $H = S_\lambda$ un sous groupe de Young. Notons Σ_λ ce caractère. Nous savons que Σ_λ est constant sur la classe de conjugaison C_ρ. Pour simplifier, nous noterons $\Sigma_\lambda(\rho)$ la valeur prise par Σ_λ sur C_ρ. Rappelons également la notation classique pour les coefficients multinomiaux

$$\binom{p}{p_1, \ldots, p_k} = \frac{p!}{p_1! \cdots p_k!}. \tag{12}$$

Proposition 5.6 *Avec les notations de la Proposition 5.4*

$$\Sigma_\lambda(\rho) = \sum \frac{z_\rho}{z_{\rho^{(1)}} \cdots z_{\rho^{(k)}}} = \sum \binom{m_1}{m_1^{(1)}, \ldots, m_1^{(k)}} \binom{m_2}{m_2^{(1)}, \ldots, m_2^{(k)}} \cdots \binom{m_n}{m_n^{(1)}, \ldots, m_n^{(k)}}$$

où la somme porte sur tous les entiers $m_i^{(j)}$ vérifiant

$$\begin{cases} m_i^{(1)} + \cdots + m_i^{(k)} = m_i \\ m_1^{(j)} + m_2^{(j)} + \cdots + m_n^{(j)} = \lambda_j \end{cases}$$

Preuve. Le résultat s'obtient immédiatement en appliquant le Corollaire 4.4 et la Proposition 5.4. ■

Exemple 5.7

1. *La table suivante donne les valeurs des caractères permutationnels de S_4.*

$\lambda\backslash\rho$	(1^4)	$(1^2 2)$	(2^2)	(13)	(4)
(4)	1	1	1	1	1
$(3,1)$	4	2	0	1	0
$(2,2)$	6	1	2	0	0
$(2,1,1)$	12	2	0	0	0
$(1,1,1,1)$	24	0	0	0	0

2. *Notons que pour $\lambda = (n)$ ($S_\lambda = S_n$), le caractère Σ_λ est celui de la représentation triviale et que pour $\lambda = (1^n)$ ($S_\lambda = \{id\}$), Σ_λ est le caractère de la représentation adjointe. En général, les caractères permutationnels ne coïncident pas avec ceux des représentations irréductibles.*

5.4 Polynômes symétriques

Frobenius remarqua que les caractères permuationnels que nous venons de calculer s'exprimaient naturellement à l'aide des polynômes symétriques. Soient $x_1, \ldots, x_m$ des indéterminées. Un polynôme $P \in \mathbb{C}[x_1, \ldots, x_m]$ en les variables $x_1, \ldots, x_m$ est dit *symétrique* lorsque

$$\sigma P = P(x_{\sigma(1)}, \ldots, x_{\sigma(m)}) = P(x_1, \ldots, x_m) \quad \forall \sigma \in S_m.$$

Il est clair que l'ensemble $\mathbb{C}^{sym}[x_1, \ldots, x_m]$ des polynômes symétriques est un sous-anneau de $\mathbb{C}[x_1, \ldots, x_m]$. Comme on travaille sur le corps $\mathbb{C}$, on peut identifier le polynôme P et la fonction polynomiale associée. On parle donc indifféremment de fonction symétrique ou de polynôme symétrique. Pour tout entier k, notons

$$p_k = x_1^k + \cdots + x_m^k \in \mathbb{C}^{sym}[x_1, \ldots, x_m].$$

Si $\lambda = (\lambda_1, \ldots, \lambda_k)$ est une partition, on pose $p_\lambda = p_{\lambda_1} \cdots p_{\lambda_k}$. Soit $\mathcal{P}_m$ l'ensemble des partitions de longueur au plus égale à m. On vérifie que $\{p_\lambda \mid \lambda \in \mathcal{P}_m\}$ est une base de $\mathbb{C}^{sym}[x_1, \ldots, x_m]$.

Pour tout $\beta = (\beta_1, \ldots, \beta_m) \in \mathbb{Z}^m$, on pose $x^\beta := x_1^{\beta_1} x_2^{\beta_2} \cdots x_m^{\beta_m}$. On définit également la fonction symétrique monomiale m_λ par

$$m_\lambda = \begin{cases} \sum_{\beta \in O_\lambda} x^\beta \text{ si } \lambda \in \mathcal{P}_m \\ 0 \text{ sinon.} \end{cases}$$

où O_λ est l'orbite de λ sous l'action de S_m. En particulier, $m_{(n)} = p_n$.

Exemple 5.8 $m_{(3,1,1)}(x_1, x_2, x_3) = x_1^3 x_2 x_3 + x_1 x_2^3 x_3 + x_1 x_2^3 x_3$.

On vérifie facilement que $\{m_\lambda \mid \lambda \in \mathcal{P}_m\}$ est une base de $\mathbb{C}^{sym}[x_1, \ldots, x_m]$. Ainsi tout $P \in \mathbb{C}^{sym}[x_1, \ldots, x_m]$ se décompose de façon unique sous la forme

$$P = \sum_{\lambda \in \mathcal{P}_m} a_\lambda m_\lambda.$$

La remarque de Frobenius tient dans la proposition suivante :

Proposition 5.9 *Pour $m \geq k$, le caractère permutationnel $\Sigma_\lambda(\rho)$ est égal au coefficient de $x_1^{\lambda_1} \cdots x_k^{\lambda_k}$ dans p_ρ, autrement dit*

$$p_\rho = \sum_{\lambda \in \mathcal{P}_m, |\lambda| = |\rho|} \Sigma_\lambda(\rho) m_\lambda. \tag{13}$$

Preuve. D'après la formule multinomiale (12), le coefficient de $x_1^{im_i^{(1)}} x_2^{im_i^{(2)}} \cdots x_k^{im_i^{(k)}}$ dans $p_i^{m_i}$ est égal à $\binom{m_i}{m_i^{(1)}, \ldots, m_i^{(k)}}$. En utilisant la Proposition 5.6, on voit donc que le coefficient de $x_1^{\lambda_1} \cdots x_k^{\lambda_k}$ dans p_ρ est égal à $\Sigma_\lambda(\rho)$. ■

Remarque : Noter que le nombre de variables des polynômes symétriques doit juste être supérieur à la longueur des partitions considérées. Comme une partition de n est de longueur maximale n, on peut par exemple prendre $m = n$. En pratique, on travaille avec un nombre de variable suffisament grand et il est même parfois commode de le supposer infini.

5.5 Caractères irréductibles

Nous connaisons maintenant une famille de caractères de S_n indéxées par les partitions de l'entier n. Ces caractères sont linéairement indépendants d'après la proposition précédente (puisque que les polynômes p_ρ et m_λ constituent deux bases de $\mathbb{C}^{sym}[x_1, \ldots, x_m]$). Ainsi les caractères $\Sigma_\lambda, \lambda \vdash n$ forment une base de $\mathbb{Q}$-espace vectoriel des fonctions centrales (donc du $\mathbb{Q}$-espace vectoriel de l'espace engendré par les caractères irréductibles). Il ne reste donc plus qu'à déterminer l'expression des caractères irréductibles sur la base des Σ_λ. Pour toute partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ avec $k \leq m$, posons

$$A_\lambda := \sum_{\sigma \in S_m} \varepsilon(\sigma) x_{\sigma(1)}^{\lambda_1 + m - 1} x_{\sigma(3)}^{\lambda_2 + m - 2} x_{\sigma(3)}^{\lambda_3 + m - 3} \cdots x_{\sigma(m)}^{\lambda_m}$$

où $\lambda_i = 0$ pour $i > k$. On posant $\alpha_i = \lambda_i + m - i$ pour tout $i = 1, \ldots, m$, on voit que A_λ est de le déterminant

$$A_\lambda := \begin{vmatrix} x_1^{\alpha_1} & \cdots & \cdots & x_m^{\alpha_1} \\ \vdots & & & \\ \vdots & & & \\ x_1^{\alpha_m} & \cdots & \cdots & x_m^{\alpha_m} \end{vmatrix}$$

Introduisons également de le déterminant de Vandermonde

$$\Delta := \prod_{1 \leq i < j \leq m} (x_i - x_j) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_m \\ \vdots & & & \\ x_1^{m-1} & \cdots & \cdots & x_m^{m-1} \end{vmatrix}.$$

Noter que les polynômes A_λ et Δ sont des polynômes antisymétriques puisqu'il s'agit de déterminants. En particulier A_λ s'annule pour $x_i = x_j, \forall 1 \leq i < j \leq n$. Il est donc divisible par Δ. Le quotient A_λ/Δ est donc un polynôme symétrique.

Définition 5.10 *On appelle* polynôme de Schur *associé à λ en les variables $x_1, \ldots, x_m$, le polynôme symétrique*

$$s_\lambda(x_1, \ldots, x_m) := \frac{A_\lambda(x_1, \ldots, x_m)}{\Delta(x_1, \ldots, x_m)}.$$

Dans la suite, nous noterons $\leq$ l'odre lexicographique sur $\mathbb{Z}^m$, autrement dit pour β, γ dans $\mathbb{Z}^m$, $\beta < \gamma$ ssi il existe $k \in \{1, \ldots, m\}$ tel que $\beta_i = \gamma_i$ pour $i = 1, \ldots, k-1$ et $\beta_k < \gamma_k$. Il s'agit donc d'un ordre total (deux éléments sont soit égaux, soit comparables).

Proposition 5.11 *Pour toute partition $\lambda \in \mathcal{P}_m$*

$$s_\lambda = m_\lambda + \sum_{\mu \in \mathcal{P}_m, \mu < \lambda, |\lambda| = |\mu|} K_{\lambda,\mu} m_\mu \tag{14}$$

où les coefficients $K_{\lambda,\mu}$ sont des entiers. En particulier, $\{s_\lambda \mid \lambda \in \mathcal{P}_m\}$ est une base de $\mathbb{C}^{sym}[x_1, \ldots, x_m]$ et la matrice de passage de la base $\{s_\lambda \mid \lambda \in \mathcal{P}_m\}$ à la base $\{m_\lambda \mid \lambda \in \mathcal{P}_m\}$ est unitriangulaire une fois les partitions ordonnées suivant l'ordre $\leq$.

Preuve. Comme s_λ est un polynôme symétrique, il suffit de montrer que x^λ apparaît avec un coefficient égal à 1 dans s_λ et que, pour toute partition $\mu \in \mathcal{P}_m$ distincte de λ, x^μ apparaît dans s_λ avec un coefficient non nul seulement si $\mu < \lambda$. Notons $\tau = (m-1, m-2, \ldots, 0) \in \mathbb{Z}^m$. Alors, $A_\lambda = x^{\lambda+\tau} + \sum_{\beta \in \mathbb{N}^m, \beta < \lambda+\tau} a_\beta x^\beta$ avec $a_\beta \in \mathbb{Z}$. De même $\Delta = x^\tau + \sum_{\kappa < \tau} d_\kappa x^\kappa$ avec $d_\kappa \in \mathbb{Z}$. Pour calculer s_λ, il suffit d'effectuer la division euclidienne de A_λ par Δ où ces deux polynômes sont considérés comme des polynômes de $\mathbb{A}[x_1]$ avec $\mathbb{A} := \mathbb{C}[x_2, \ldots, x_m]$. Le principe de la division euclidienne montre alors que $s_\lambda = x^\lambda + \sum_{\beta \in \mathbb{N}^m, \beta < \lambda} u_\beta x^\beta$ avec $u_\beta \in \mathbb{Z}$ ce qui suffit à établir la proposition. ■

Exemple 5.12

$$s_{(3)}(x_1,x_2,x_3)=\frac{\begin{vmatrix} x_1^5 & x_2^5 & x_3^5\\ x_1 & x_2 & x_3\\ 1 & 1 & 1\end{vmatrix}}{\begin{vmatrix} x_1^2 & x_2^2 & x_3^2\\ x_1 & x_2 & x_3\\ 1 & 1 & 1\end{vmatrix}}=\frac{x_1^5x_2-x_1^5x_3-x_1x_2^5+x_1x_3^5+x_2^5x_3-x_2x_3^5}{x_1^2x_2-x_1^2x_3-x_1x_2^2+x_1x_3^2+x_2^2x_3-x_2x_3^2}=$$

$$x_1^3+x_2^3+x_3^3+x_1^2x_2+x_1^2x_3+x_1x_2^2+x_2^2x_3+x_1x_3^2+x_2x_3^2+x_1x_2x_3.$$

Soient $\chi_\lambda(\rho)$ les coefficients du développement

$$p_\rho=\sum_{\lambda\in\mathcal{P}_m,|\lambda|=|\rho|}\chi_\lambda(\rho)s_\lambda$$

dans $\mathbb{C}^{sym}[x_1,\ldots,x_m]$.

Proposition 5.13 *Les coefficients $\chi_\lambda(\rho)$ sont des nombres entiers.*

Preuve. Fixons un entier m. D'après (13), les coefficients de la matrice $P=(\Sigma_\lambda(\rho))_{\lambda,\rho\vdash n}$ sont des entiers. Par ailleurs, la matrice $S=(K_{\lambda,\mu})_{\lambda,\mu\vdash n}$ est unitriangulaire à coefficients entiers. Donc S^{-1} est aussi unitriangulaire à ceofficients entiers. Donc $\Theta=(\chi_\lambda(\rho))_{\lambda,\rho\vdash n}=S^{-1}P$ est à coefficients entiers. ■

Nous pouvons maintenant formuler le théorème central de Frobenius [3].

Théorème 5.14 *Soient λ et ρ deux partitions de n. Le coefficient $\chi_\lambda(\rho)$ est égal à la valeur du caractère irréductible de S_n associé à λ évalué sur la classe C_ρ.*

Exemple 5.15 *Calculons la table des caractères de S_3. On a déjà d'après l'exemple précédent*

$$s_{(3)}(x_1,x_2,x_3)=x_1^3+x_2^3+x_3^3+x_1^2x_2+x_1^2x_3+x_1x_2^2+x_2^3x_3+x_1x_3^2+x_2x_3^2+x_1x_2x_3.$$

On obtient de même

$$s_{(2,1)}(x_1,x_2,x_3)=x_1^2x_3+x_1x_2^2+x_2^3x_3+x_1x_3^2+x_2x_3^2+2x_1x_2x_3,$$
$$s_{(1,1,1)}(x_1,x_2,x_3)=x_1x_2x_3.$$

En termes des fonctions monomiales, on a donc

$$\begin{cases} s_{(3)}=m_{(3)}+m_{(2,1)}+m_{(1,1,1)},\\ s_{(2,1)}=m_{(2,1)}+2m_{(1,1,1)},\\ s_{(1,1,1)}=m_{(1,1,1)}.\end{cases}$$

Par ailleurs,

$$\begin{cases} p_{(3)}=m_{(3)},\\ p_{(2,1)}=m_{(3)}+m_{(2,1)},\\ p_{(1,1,1)}=m_{(3)}+3m_{(2,1)}+6m_{(1,1,1)}.\end{cases}$$

Cela donne

$$\begin{cases} p_{(3)} = s_{(3)} - s_{(2,1)} + s_{(1,1,1)}, \\ p_{(2,1)} = s_{(3)} - s_{(1,1,1)}, \\ p_{(1,1,1)} = s_{(3)} + 2s_{(2,1)} + s_{(1,1,1)}. \end{cases}$$

et donc la table des caractères de S_3 :

	(1^3)	(12)	(3)
(3)	1	1	1
$(2,1)$	2	0	-1
$(1,1,1)$	1	-1	1

La stratégie de Frobenius pour démontrer le Théorème 5.14 est la suivante :

1. Les χ_λ avec $\lambda \vdash n$ (dont on cherche à montrer qu'ils donnent les caractères irréductibles de S_n) sont des combinaisons linéaires à coefficients entiers des caractères permutationnnels Σ_λ, donc des combinaisons à coefficients entiers des caractères irréductibles. Cela découle du fait que les matrices de passages des bases $\{p_\lambda \mid \lambda \vdash n\}, \{m_\lambda \mid \lambda \vdash n\}$ et $\{s_\lambda \mid \lambda \vdash n\}$ sont à coefficients entiers d'après les Propositions 5.9, 5.11 et 5.13.
2. D'après le Corollaire 2.7, pour démontrer que les χ_λ sont les caractères irréductibles, ils suffit de démontrer que
$$\langle \chi_\lambda, \chi_\nu \rangle = \sum_{\rho \vdash n} \frac{\chi_\lambda(\rho)\chi_\nu(\rho)}{z_\rho} = \delta_{\lambda,\mu} \tag{15}$$
pour tout paire (λ, ν) de partitions de n et que $\chi_\lambda(1) > 0$. Noter qu'on utilise ici que les nombres $\chi_\nu(\rho)$ sont des nombres réels (ce sont même des entiers) et que $|C_\rho| = \frac{n!}{z_\rho}$ conformément à la Proposition 5.2.
3. La preuve des relations (15) se ramène à un calcul classique de déterminant du à Cauchy.
4. Enfin, Frobenius montre par un calcul direct que
$$\chi_\lambda(1) = \frac{n! \prod_{1 \le i < j \le n} (\lambda_i - i - \lambda_j + j)}{\prod_{i=1}^n (\lambda_i + n - i)!}$$
expression manifestement positive puisque λ est une partition.

5.6 Formule de Cauchy

Fixons $m \ge n$ et considérons deux ensembles d'indéterminées $X = \{x_1, \ldots, x_m\}$ et $Y = \{y_1, \ldots, y_m\}$. On rappelle que $\mathbb{Q}[[X, Y]]$ désigne l'algèbre des séries formelles à coefficients dans $\mathbb{Q}$ en les variables $X \cup Y$.

Proposition 5.16 *Dans* $\mathbb{Q}[[X, Y]]$*, on a l'identité suivante*

$$\prod_{1 \le i,j \le m} \frac{1}{1 - x_i y_j} = \sum_{\rho \in \mathcal{P}_m} \frac{1}{z_\rho} p_\rho(X) p_\rho(Y)$$

la somme portant sur toutes les partitions $\rho \in \mathcal{P}_m$ *(de tous les entiers* n*).*

Preuve. Dans $\mathbb{Q}[[a]]$, on a

$$\frac{1}{1-a} = \exp\left(\log \frac{1}{1-a}\right) = \exp\left(\sum_{k\geq 1} \frac{a^k}{k}\right).$$

On en déduit que

$$\prod_{1\leq i,j\leq m} \frac{1}{1-x_i y_j} = \prod_{1\leq i,j\leq m} \exp\left(\sum_{k\geq 1} \frac{x_i^k y_j^k}{k}\right) = \exp\left(\sum \frac{p_k(X)p_k(Y)}{k}\right).$$

En développant l'exponentielle, cela donne bien

$$\prod_{1\leq i,j\leq m} \frac{1}{1-x_i y_j} = \sum_{\rho} \frac{1}{z_\rho} p_\rho(X) p_\rho(Y).$$

■

Exercice 5.17 *Calculer le déterminant de Cauchy*

$$\det \left| \frac{1}{a_i + b_j} \right|_{1\leq i,j\leq m} = \frac{\Delta(a_1,\ldots,a_m)\Delta(b_1,\ldots,b_m)}{\prod_{1\leq i,j\leq n}(a_i+b_j)}.$$

Pour cela retrancher la dernière colonne aux $m-1$ autres, puis la dernière ligne aux $m-1$ autres et en déduire une relation de récurrence. Montrer alors que

$$\det \left| \frac{1}{1-x_i y_j} \right|_{1\leq i,j\leq m} = \frac{\Delta(x_1,\ldots,x_m)\Delta(y_1,\ldots,y_m)}{\prod_{1\leq i,j\leq n}(1-x_i y_j)}. \tag{16}$$

Exercice 5.18 *Soient $C \in M_{k,n}(\mathbb{C})$ et $D \in M_{n,k}(\mathbb{C})$ des matrices. On suppose que $k \leq n$. Etant donnée une partie $I \subset \{1,\ldots,n\}$ à k éléments, on note c_I le déterminant mineur de C pris sur les colonnes de C d'indice dans I et d_I le déterminant mineur de D pris sur les lignes de D d'indice dans I. Démontrer la formule Binet-Cauchy*

$$\det(CD) = \sum_I c_I d_I$$

la somme portant sur tous les sous-ensembles $I \subset \{1,\ldots,n\}$.

L'identité suivante est essentiellement due à Cauchy.

Proposition 5.19 *Dans $\mathbb{Q}[[X,Y]]$*

$$\prod_{1\leq i<j\leq m} \frac{1}{1-x_i y_j} = \sum_{\lambda\in\mathcal{P}_m} s_\lambda(X) s_\lambda(Y),$$

la somme portant sur toutes les partitions λ ayant au plus m parts.

Preuve. La preuve repose sur le calcul (16) classique du déterminant de Cauchy effectuée dans l'exercice précédent. Introduisons la matrice $m \times \infty$ définie par $V(X) = V(x_1, \ldots, x_m) = [x_i^k]_{1 \leq i \leq m, k \geq 0}$. On a alors

$$\left[\frac{1}{1 - x_i y_j}\right]_{1 \leq i,j \leq m} = V(X)V(Y)^{tr}.$$

Ainsi le déterminant de Cauchy apparaît-il comme le déterminant du produit de deux matrices rectangulaires. D'après la formule de Binet-Cauchy, nous obtenons

$$\det \left|\frac{1}{1 - x_i y_j}\right|_{1 \leq i,j \leq m} = \sum_{\lambda} A_\lambda(X) A_\lambda(Y)$$

où

$$A_\lambda(x) = \sum_{\sigma \in S_m} \varepsilon(\sigma) x_{\sigma(1)}^{\lambda_1 + m - 1} x_{\sigma(2)}^{\lambda_2 + m - 2} \cdots x_{\sigma(m)}^{\lambda_m}.$$

Il suffit alors de diviser par le produit $\Delta(X)\Delta(Y)$ pour en déduire la formule annoncée. ■

Corollaire 5.20 *Les fonctions χ_λ et χ_μ sont orthogonales :*

$$\langle \chi_\lambda, \chi_\nu \rangle = \sum_{\rho \vdash n} \frac{\chi_\lambda(\rho)\chi_\nu(\rho)}{z_\rho} = \delta_{\lambda,\mu}.$$

Preuve. D'après la Proposition 5.16, nous avons

$$\prod_{1 \leq i,j \leq m} \frac{1}{1 - x_i y_j} = \sum_{\rho} \frac{1}{z_\rho} p_\rho(X) p_\rho(Y).$$

Mais par définition $p_\rho(X) = \sum_\lambda \chi_\lambda(\rho) s_\lambda(X)$ et de même pour Y. Cela donne

$$\prod_{1 \leq i,j \leq m} \frac{1}{1 - x_i y_j} = \sum_{\lambda,\nu} \left(\sum_{\rho} \frac{\chi_\lambda(\rho)\chi_\nu(\rho)}{z_\rho} \right) s_\lambda(X) s_\nu(Y).$$

En comparant avec le développement obtenu dans la Proposition 5.19, on en déduit les relations d'orthogonalité demandées. ■

Il ne nous reste donc plus qu'à démontrer que les nombre $f_\lambda := \chi_\lambda(1^n)$ sont strictement positifs ce qui va être fait dans le paragraphe suivant par un calcul direct.

5.7 Formule des dimensions

Proposition 5.21 *Soit λ une partition de n. On a*

$$f_\lambda = \chi_\lambda(1) = \frac{n! \prod_{1 \leq i < j \leq n} (\lambda_i - i - \lambda_j + j)}{\prod_{i=1}^n (\lambda_i + n - i)!}.$$

En posant $\alpha_i = \lambda_i + n - i$ pour $i = 1, \ldots, n$, la formule devient

$$f_\lambda = \frac{n! \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)}{\prod_{i=1}^n \alpha_i!}.$$

Preuve. Par définition de f_λ, nous avons

$$p_{(1^n)}(x_1,\dots,x_m)\Delta(x_1,\dots,x_m)=\sum_{\lambda\vdash n} f_\lambda A_\lambda(x_1,\dots,x_m)$$

avec $m\geq n$ fixé. Le premier membre est égal à

$$\sum_{\mu_1+\cdots\mu_m=n}\binom{n}{\mu_1,\cdots,\mu_m}x_1^{\mu_1}\cdots x_m^{\mu_m}\cdot\sum_{\sigma\in S_m}\varepsilon(\sigma)x_1^{\sigma(m)-1}x_2^{\sigma(m-1)-1}\cdots x_m^{\sigma(1)-1}.$$

Le nombre f_λ est alors donné par le coefficient de $x_1^{\lambda_1+m-1}x_2^{\lambda_2+m-2}\cdots x_m^{\lambda_m}$. Il vaut

$$n!\sum_{\sigma\in S_m}\varepsilon(\sigma)\frac{1}{(\lambda_1+m-\sigma(m))!(\lambda_2+m-1-\sigma(m-1))!\cdots(\lambda_m+1-\sigma(1))!}=$$

$$n!\begin{vmatrix} 1/\lambda_1! & 1/(\lambda_1+1)! & \cdots & 1/(\lambda_1+m-1)!\\ 1/(\lambda_2-1)! & 1/\lambda_2! & \cdots & 1/(\lambda_1+m-2)!\\ \vdots & \vdots & \vdots & \vdots\\ 1/(\lambda_m-m+1)! & 1/(\lambda_m-m+2)! & \cdots & 1/\lambda_m! \end{vmatrix}$$

Divisons les colonnes du déterminant par $(m-1)!,(m-2)!,\dots,0!$ et multiplions les lignes par $(\lambda_1+m-1)!,(\lambda_2+m+2)!,\dots,\lambda_m!$. On obtient

$$f_\lambda=\frac{n!(m-1)!(m-2)!\cdots 0!}{(\lambda_1+m-1)!(\lambda_2+m-2)!\cdots\lambda_m!}\begin{vmatrix} \binom{\lambda_1+m-1}{m-1} & \binom{\lambda_1+m-1}{m-2} & \cdots & \binom{\lambda_1+m-1}{0}\\ \binom{\lambda_2+m-2}{m-1} & \binom{\lambda_2+m-2}{m-2} & \cdots & \binom{\lambda_2+m-1}{0}\\ \vdots & \vdots & \vdots & \vdots\\ \binom{\lambda_m}{m-1} & \binom{\lambda_m}{m-2} & \cdots & \binom{\lambda_m}{0} \end{vmatrix}.$$

Maintenant, en tenant compte du fait

$$\binom{x}{p}=\frac{x(x-1)\cdots(x-p+1)}{p!}=x^p/p!+\text{ termes de degré }\leq p-1,$$

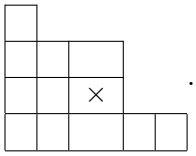
le déterminant se réduit par soustractions de colonnes à

$$f_\lambda=\frac{n!}{(\lambda_1+m-1)!(\lambda_2+m+2)!\cdots\lambda_m!}\begin{vmatrix} (\lambda_1+m-1)^{m-1} & (\lambda_1+m-1)^{m-2} & \cdots & 1\\ (\lambda_2+m-2)^{m-1} & (\lambda_2+m-2)^{m-2} & \cdots & 1\\ \vdots & \vdots & \vdots & \vdots\\ (\lambda_m)^{m-1} & (\lambda_m)^{m-2} & \cdots & 1 \end{vmatrix}$$

et le résultat se déduit en prenant $m=n$. ■

Il n'est pas évident sur l'expression précédente que les f_λ soient des entiers. C'est le cas puisqu'il s'agit de la dimension des représentations irréductibles d'après le Théorème 5.14 que nous venons de terminer de démontrer. Il existe heureusement une façon plus simple de caluler ces dimensions. Il s'agit de la formule des équerres due à Frame, Robinson et Thrall (1954). Pour l'exprimer, il est commode de considérer le diagramme de Young associé à la partition $\lambda=(\lambda_1,\dots,\lambda_m)$. Il s'agit de la superposition alignée sur la gauche de m colonnes contenant respectivement $\lambda_1,\dots,\lambda_m$ boîtes. Chaque boîte de λ est repérée par la paire (i,j) où i est l'indice de la ligne et j celui de la colonne où b apparaît.

Exemple 5.22 *Considérons la partition $\lambda = (5,3,3,1)$. Son diagramme de Young est*

$\lambda =$ 

.

La boîte marquée d'une croix est la boîte $b = (2,3)$.

A chaque boîte $b = (i,j)$ du diagramme de Young de λ correspond une équerre obtenue en considérant toutes les boîtes situées soit sur la ligne i et à la droite de b, soit sur la colonne j et au dessus de b. La longueur $h_{i,j}$ de l'équerre associée à cette boîte est le nombre de boîtes de cette équerre. Dans l'exemple ci-dessus $h_{(2,3)} = 2$. Noter que les longeurs des équerres des boîtes situées dans la première colonne de λ sont les $\alpha_1, \ldots, \alpha_k$ avec $k = \ell(\lambda)$ définies dans la proposition précédente.

Exemple 5.23 *Les longueurs des équerres de $\lambda = (5,3,3,1)$ apparaissent dans les boîtes qui les définissent :*

$\lambda =$
1				
4	2	1		
5	3	2		
8	6	5	2	1

.

Proposition 5.24 *Soit $\lambda \vdash n$. On a*

$$f_\lambda = \frac{n!}{\prod_{b\in\lambda} h(b)}$$

où b décrit toutes les boîtes de la partition λ.

Preuve. La preuve utilise un raisonnement de récurrence sur le nombre de colonnes de λ. Nous renvoyons à [1] pour une eposition complète

■

Exercice 5.25 *Calculer $f_{(5,3,3,1)}$.*

Références

[1] W. Fulton, Young tableaux, with applications to representation theory and geometry. Cambridge University Press (1997).

[2] W. Fulton et J. Harris, Representation theory, gratuate text in mathematics, Springer (1991).

[3] G. Frobenius, Uber dir charaktere der symmetrischen einer gruppe und denen ihrer untergruppen, Akad. d. Wiss. Berlin (1900).

[4] G. James et M. Liebeck, Representation and characters of groups, Cambridge (2001).

[5] T. Y. Lam, Representations of Finite Groups : A Hundred Years, Notices of the Ams (1998).

[6] G. Peyré, L'algèbre discrète de la transformée de Fourier, Ellipse (2004).

[7] J.P. Serre, représentations des groupes finis, Hermann collections méthodes, Paris (1967)