Représentations linéaires des groupes finis

Thomas Gerber

2020

Table des matières

Introduction

Une représentation d'un groupe G est la donnée d'une action linéaire de G sur un espace vectoriel V. Autrement dit, c'est un morphisme de groupes $G \to \mathrm{GL}(V)$. On peut ainsi "représenter" les éléments de G par des matrices, et utiliser les notions de l'algèbre linéaire (trace, déterminant, valeurs propres) pour étudier G.

Historiquement, c'est Frobenius qui est à l'origine de la théorie à la toute fin du XIXème siècle, puis Schur et Burnside, qui s'intéressent aux cas des groupes finis. En 1911, Burnside démontre son célèbre théorème qui affirme que tout groupe dont l'ordre a au plus deux diviseurs premiers est résoluble, en utilisant la théorie des caractères. Il conjecture aussi que tout groupe d'ordre impair est résoluble, ce qui ne sera démontré qu'en 1963 par Feit et Thompson, dans une preuve de 255 pages dans laquelle la théorie des représentations joue un rôle essentiel. Ce théorème permet d'entrevoir une classification des groupes simples finis, un projet monumental débuté dans les années 1950 et achevé en 2004, et auquel ont participé une centaine d'auteurs, pour plusieurs dizaines de milliers de pages de preuves dans des centaines d'articles différents.

Mais la théorie des représentations ne se limite pas à l'étude des groupes (finis ou infinis). Dès les travaux de Noether en 1929, la théorie des représentations des groupes finis est vue comme un cas particulier de la théorie des représentations des algèbres associatives, elle-même équivalente à la théorie des modules sur ces algèbres. D'autres notions algébriques fondamentales, comme les algèbres de Lie (ou plus généralement de Kac-Moody), les algèbres de Hopf (comme par exemple les groupes quantiques), ou les carquois peuvent être étudiées par leur théorie des représentations. La théorie des catégories permet de généraliser la théorie des représentations linéaires.

Finalement, la théorie des représentations est en interaction avec beaucoup d'autres domaines des mathématiques : la géométrie via l'étude des groupes de Lie et des groupes algébriques, la théorie des nombres via l'étude des formes automorphes et le programme de Langlands, l'analyse harmonique, la topologie via la théorie des nœuds et leurs invariants, ou encore la physique des particules via l'étude des représentations unitaires et le modèle de Wigner.

Dans ce cours, on se étudiera la théorie des représentations des groupes, et on se placera principalement dans le cas suivant :

- Les groupes en question seront finis.
- Les espaces vectoriel de représentation seront de dimension finie.
- Le corps de base sera un corps de caractéristique nulle, typiquement $\mathbb{C}$.

Le cas des groupes infinis (et des autres structures algébriques), des représentations de dimension infinie, et des corps de caractéristique positive (la théorie des représentations modulaires), sont également très intéressants et sont l'objet de cours (et de recherches) indépendants.

Chapitre 1

Représentations de groupes

1.1 Définitions

Soit G un groupe et K un corps commutatif.

Définition 1.1.

(1) Une *représentation linéaire* de G est la donnée d'un K-espace vectoriel V et d'un morphisme de groupes $\rho : G \to \mathrm{GL}(V) = \mathrm{Aut}_K(V)$. Si ρ est injective, la représentation est dite *fidèle*.

(2) Une *représentation matricielle* de G est la donnée d'un entier $n \geq 0$ et d'un morphisme de groupes $\rho : G \to \mathrm{GL}_n(K)$.

On appellera souvent "représentation" seulement ρ ou V, et on oubliera le qualificatif "linéaire". Notons que la définition implique directement $\rho(1) = \mathrm{Id}$ et $\rho(g)^{-1} = \rho(g^{-1})$ pour tout $g \in G$.

Remarque 1.2.

(1) Si $\rho : G \to V$ est une représentation de G et que V est de dimension finie n, alors toute base $B = \{e_1, \ldots, e_n\}$ de V induit une représentation matricielle de G donnée par $\rho' : G \to \mathrm{GL}_n(K), g \mapsto \rho'(g)$, où $\rho'(g)$ est la matrice de $\rho(g)$ dans la base B. L'entier n est appelé *degré* de la représentation.

(2) Réciproquement, toute représentation matricielle $\rho : G \to \mathrm{GL}_n(K)$ induit une représentation $\rho' : G \to \mathrm{GL}(K^n)$, où $\rho'(g)$ est l'automorphisme de K^n déterminé par la matrice $\rho(g)$.

Exemple 1.3.

(1) La *représentation triviale* de G est définie par $1 : G \to \mathrm{GL}(K) = K^\times, g \mapsto 1$.

(2) Supposons G fini. Soit V un K-espace vectoriel de dimension $|G|$, et soit $\{e_g \,;\, g \in G\}$ une base de V. Soit $\rho : G \to \mathrm{GL}(V)$ définie par $\rho(g)(e_h) = e_{gh}$ pour tout $g, h \in G$ (étendue par K-linéarité). L'application ρ est un morphisme de groupes appelé *représentation régulière* de G.

(3) Plus généralement, supposons que G agit sur un ensemble fini X. Soit V un K-espace vectoriel de dimension $|X|$, et soit $\{e_x \,;\, x \in X\}$ une base de V. Soit $\rho : G \to \mathrm{GL}(V)$ définie par $\rho(g)(e_x) = e_{gx}$ pour tout $g \in G$, $x \in X$ (étendue par K-linéarité). L'application ρ est un morphisme de groupes appelé *représentation de permutation* de G.

(4) Soit $G = S_3$, le groupe symétrique agissant sur $\{1, 2, 3\}$. Ce groupe est engendré par les transpositions (12) et (23). L'application

$$\rho : G \to \mathrm{GL}_3(K), \quad (12) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (23) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

définit une représentation matricielle de G, correspondant à la représentation de permutation de S_3.

Définition 1.4.

(1) Soient (V_1, ρ_1), (V_2, ρ_2) deux représentations de G. Un *morphisme* de (V_1, ρ_1) vers (V_2, ρ_2) est une application linéaire $\alpha : V_1 \to V_2$ telle que pour tout $g \in G$, $\rho_2(g)\alpha = \alpha\rho_1(g)$. Si α est un isomorphisme, les représentations (V_1, ρ_1) et (V_2, ρ_2) de G sont dites *équivalentes* ou *isomorphes*.

(2) Deux représentations matricielles ρ_1 et ρ_2 de G de degré n sont dites *équivalentes* ou *isomorphes* s'il existe $\in \mathrm{GL}_n(K)$ telle que pour tout $g \in G$, $\rho_2(g) = Z\rho_1(g)Z^{-1}$.

Remarque 1.5. Deux représentations sont isomorphes si et seulement si les représentations matricielles correspondantes (pour un choix quelconque de base) sont isomorphes.

Définition 1.6. Soit (V, ρ) une représentation de G

(1) Une *sous-représentation* de V est un sous-espace vectoriel $W \subseteq V$ vérifiant $\rho(g)(W) \subseteq W$ pour tout $g \in G$ (dans ce cas, on dit que W est *stable par* G).

(2) La représentation V est dite *irréductible* si $V \neq \{0\}$ et si ses seules sous-représentations sont $\{0\}$ et V.

Exemple 1.7. Supposons G fini et soit V la représentation régulière de G. Le vecteur $x = \sum_{g\in G} e_g$ engendre un sous-espace vectoriel W de dimension 1 de V. On a $\rho(g)(x) = x$ pour tout $g \in G$, et W est donc une sous-représentation de V, isomorphe à la représentation triviale.

1.2 Groupes finis et théorème de Maschke

Théorème 1.8 (Maschke)**.** Soit G un groupe fini et K un corps.

(1) Si $\mathrm{char}(K) \nmid |G|$ (ceci inclut le cas $\mathrm{char}(K) = 0$), alors pour toute représentation V de G et toute sous-représentation W de V, il existe une sous-représentation W' de V telle que $V = W \oplus W'$.

(2) Si $\mathrm{char}(K) \mid |G|$, alors il existe une représentation V de G et une sous-représentation W de V qui n'a pas de supplémentaire stable par G.

Preuve.

(1) Soit W_0 un supplémentaire de W dans V, c'est-à-dire $V = W \oplus W_0$. Soit p le projecteur de V sur W correspondant à cette décomposition, et considérons

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

Puisque p envoie V sur W et que $\rho(g)$ conserve W, on déduit que p' envoie V sur W. De plus, pour tout $w \in W$, on a

$$\begin{aligned} p'(w) &= \frac{1}{|G|} \sum_{g\in G} \rho(g)\ p\ \rho(g)^{-1}(w) \\ &= \frac{1}{|G|} \sum_{g\in G} \rho(g)\ \rho(g)^{-1}(w) \qquad \text{car } \rho(g)^{-1}(w) \in W \end{aligned}$$

$$= \frac{1}{|G|} \sum_{g \in G} w$$
$$= w \qquad \text{car } \mathrm{char}(K) \nmid |G|.$$

Ainsi, p' est un projecteur de V sur W, et en posant $W' = \mathrm{Ker}\, p'$, on a $V = W \oplus W'$. De plus, pour tout $h \in G$ on a

$$\begin{aligned}
\rho(h)\ p'\ \rho(h) &= \frac{1}{|G|} \sum_{g \in G} \rho(h)\ \rho(g)\ p\ \rho(g)^{-1}\ \rho(h)^{-1} \\
&= \frac{1}{|G|} \sum_{g \in G} \rho(hg)\ p\ \rho(gh)^{-1} \\
&= \frac{1}{|G|} \sum_{k \in G} \rho(k)\ p\ \rho(k)^{-1} \\
&= p',
\end{aligned}$$

c'est-à-dire que $\rho(h)$ commute avec p' pour tout $h \in G$. Maintenant, pour $x \in W'$ et $g \in G$, on a $p'(x) = 0$, d'où $p'\rho(g)(x) = \rho(g)p'(x) = 0$, donc $\rho(g)(x) \in W'$, c'est-à-dire que W' est stable par G.

(2) Notons que $|G| \neq 1$, car sinon on ne peut avoir $\mathrm{char}(K) \mid |G|$. Considérons V la représentation régulière de G, et soit

$$\varepsilon : V \to K, \quad \sum_{g \in G} \lambda_g e_g \mapsto \sum_{g \in G} \lambda_g.$$

Posons $W = \mathrm{Ker}(\varepsilon)$. Alors W est une sous-représentation de V. Soit W' une sous-représentation quelconque de V. Nous allons prouver que $W \cap W' \neq \{0\}$. Soit $w = \sum_{g \in G} \lambda_g e_g \in W'$. Si $\varepsilon(w) = 0$, alors l'assertion est triviale. Sinon, soit $s = \sum_{g \in G} e_g$. Alors $\varepsilon(s) = |G|.1 = 0$ car $\mathrm{char}(K) \mid |G|$, donc $s \in W$. Considérons alors l'élément $x = \sum_{h \in G} \rho(h)(w) \in V$. Puisque W' est une sous-représentation, on a $x \in W'$. De plus, on a

$$\begin{aligned}
x &= \sum_{h \in G} \rho(h)(w) \\
&= \sum_{h \in G} \rho(h)(\sum_{g \in G} \lambda_g e_g) \\
&= \sum_{h \in G} \sum_{g \in G} \lambda_g \rho(h)(e_g) \\
&= \sum_{h \in G} \sum_{g \in G} \lambda_g e_{hg} \\
&= \sum_{g \in G} \lambda_g \sum_{h \in G} e_{hg} \\
&= \sum_{g \in G} \lambda_g \sum_{k \in G} e_k \\
&= \varepsilon(w)s,
\end{aligned}$$

et puisque $s \in W$, on a $x \in W$. Donc $x \in W \cap W'$, ce qui conclut la démonstration.

□

Corollaire 1.9. Sous les hypothèses (1) du théorème de Maschke, toute représentation V de G de dimension finie admet une décomposition en somme directe de sous-représentations irréductibles.

Preuve. On raisonne par récurrence sur $\dim(V)$. Si $\dim(V) = 0$, alors V est somme directe vide de représentations irréductibles. Supposons le résultat vrai jusqu'à $\dim(V) = n-1$ où $n \geq 1$ est fixé. Si V est irréductible, il n'y a rien à démontrer. Sinon, V possède une sous-représentation propre W. Par le théorème de Maschke, il existe $W' \leq V$ stable par G tel que $V = W \oplus W'$. Puisqu'on a $\dim(W) \leq n-1$ et $\dim(W') \leq n-1$, on peut appliquer l'hypothèse de récurrence à W et W', et on obtient une décomposition de $V = W \oplus W'$ en somme directe de sous-représentations irréductibles. □

Dans le cas $K = \mathbb{C}$, on a en outre un résultat d'unicité qui découle du lemme suivant.

Lemme 1.10 (Lemme de Schur)**.** Soient V, W deux représentations irréductibles de G et $f : V \to W$ un morphisme de représentations.

(1) Soit f est un isomorphisme, soit $f = 0$.

(2) Supposons K algébriquement clos. Si $V = W$, alors il existe $\lambda \in K$ tel que $f = \lambda \mathrm{Id}$.

Preuve.

(1) Les sous-espaces $\mathrm{Ker}\, f$ et $\mathrm{Im}\, f$ sont stables par G. Mais puisque V et W sont irréductibles, on a $\mathrm{Ker}\, f = \{0\}$ ou V et $\mathrm{Im}\, f = \{0\}$ ou W. Si $\mathrm{Ker}\, f = \{0\}$ alors $V \simeq \mathrm{Im}\, f$. Puisque $V \neq \{0\}$, on a $\mathrm{Im}\, f = W$, donc f est un isomorphisme. Si $\mathrm{Ker}\, f = V$ alors $\mathrm{Im}\, f \simeq V/V \simeq \{0\}$, donc $f = 0$.

(2) Puisque K est algébriquement clos, f possède une valeur propre λ, et $\mathrm{Ker}(f - \lambda \mathrm{Id})$ n'est pas réduit à $\{0\}$. Mais comme il est stable par G, on a $\mathrm{Ker}(f - \lambda \mathrm{Id}) = V$, c'est-à-dire $f = \lambda \mathrm{Id}$.

□

Corollaire 1.11. Supposons $K = \mathbb{C}$. Dans la décomposition obtenue au corollaire 1.9, les sous-représentations irréductibles qui apparaissent sont uniques à isomorphisme près, et les multiplicités correspondantes sont uniques.

Preuve. Pour V et W deux représentations de G, soit $V = \bigoplus V_i$ et $W = \bigoplus W_j$ une décomposition de V et W en somme directe de sous-représentation irréductibles. Soit $f : V \to W$ un isomorphisme de représentations et notons $f_{i,j} : V_i \to W_j$ la composition de f et de la projection $W \to W_j$. Par le lemme de Schur, chaque $f_{i,j}$ est soit un isomorphisme, soit 0. Puisque f est injective, pour tout j il existe und i tel que $f_{i,j} \neq 0$, et donc $f_{i,j}$ est un isomorphisme. Donc pour tout j, il existe un i tel que $V_i \simeq W_j$.
De plus, pour tous i, j tels que $V_i \not\simeq W_j$, on a $f_{i,j} \neq 0$. Ainsi, l'image de $f|_{V_i}$ est contenue $\bigoplus_{W_j \simeq V_i} W_j$. Maintenant, pour une sous-représentation irréductible S fixée, on peut écrire

$$V = \bigoplus_{V_i \simeq S} V_i \oplus \bigoplus_{V_i \not\simeq S} V_i \quad \text{et} \quad W = \bigoplus_{W_j \simeq S} W_j \oplus \bigoplus_{W_j \not\simeq S} W_j.$$

On a donc $f(\bigoplus_{V_i \simeq S} V_i) \subseteq \bigoplus_{W_j \simeq S} W_j$, et par surjectivité de f, on a en fait

$$f(\bigoplus_{V_i \simeq S} V_i) = \bigoplus_{W_j \simeq S} W_j.$$

Ainsi, f induit un isomorphisme entre $\bigoplus_{V_i \simeq S} V_i$ et $\bigoplus_{W_j \simeq S} W_j$, c'est-à-dire que le nombre de V_i isomorphes à S est égal au nombre de W_j isomorphes à S.

On conclut en appliquant ces observations au cas $W = V$ et $f = \mathrm{Id}$.

□

Ceci donne lieu à deux problèmes fondamentaux en théorie des représentations :

— déterminer les représentations irréductibles, leur nombre, leur degré,

— décomposer une représentation en somme directe de représentations irréductibles.

Le cas des groupes abéliens sur $\mathbb{C}$ est particulièrement simple.

Théorème 1.12. Soit G un groupe abélien fini, et prenons $K = \mathbb{C}$. Alors toute représentation irréductible de G est de dimension 1.

Preuve. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation irréductible de G. Soit $g \in G$. Alors pour tout $h \in G$, on a $\rho(g)\rho(h) = \rho(gh) = \rho(hg) = \rho(h)\rho(g)$, c'est-à-dire que $\rho(g) : V \to V$ est un morphisme de représentations. Par le lemme de Schur, on a $\rho(g) = \lambda \mathrm{Id}$ pour un certain $\lambda \in \mathbb{C}$. Ainsi, tout sous-espace de V est stable par $\rho(g)$, et donc par G. Mais comme V est simple, ses seuls sous-espaces stables par G sont $\{0\}$ et V, ce qui implique que $\dim(V) = 1$.

□

1.3 Algèbre de groupe

Définition 1.13. Une *K-algèbre* est un K-espace vectoriel A muni d'une multiplication $A \times A \to A$, $(x, y) \mapsto xy$ qui est K-bilinéaire, c'est-à-dire que pour tous $x, y, z \in A$ et pour tout $\lambda \in K$, on a

(1) $(x + y)z = xz + yz$,

(2) $x(y + z) = xy + xz$,

(3) $(\lambda x)y = \lambda(xy)$.

Exemple 1.14.

(1) L'ensemble des nombres complexes $\mathbb{C}$ est une $\mathbb{R}$-algèbre associative et commutative.

(2) Pour $n \geq 1$, l'ensemble $K^{n\times n}$ des matrices carrées $n \times n$ à coefficients dans K muni du produit matriciel est une K-algèbre associative non commutative.

(3) Pour $n \geq 2$, l'ensemble $A = K^{n\times n}$ des matrices carrées $n \times n$ à coefficients dans K muni du *crochet de Lie* $A \times A \to A$, $(M, N) \mapsto [M, N] = MN - NM$ est une K-algèbre non-associative et non-commutative.

Définition 1.15. Soit G un groupe fini. L'*algèbre de groupe* KG est la K-algèbre associative de base formelle $\{g\,;\, g \in G\}$, et dont la multiplication est donnée par

$$\left(\sum_{g\in G} \lambda_g g\right)\left(\sum_{g\in G} \mu_g g\right) = \sum_{g\in G} \nu_g g \quad \text{où } \nu_g = \sum_{\substack{h,k\in G\\ hk=g}} \lambda_h \mu_k.$$

Comme vu dans l'exemple 1.3, on peut considérer l'action de G sur KG, et voir KG comme la représentation régulière de G, donnée par $\rho(g)(h) = gh$. Dans ce cas, on l'appelle aussi *représentation adjointe* de G.

Exemple 1.16. Soit $G = \mathbb{Z}/2\mathbb{Z} = \langle a\rangle \times \langle b\rangle$ and $H = \mathbb{Z}/4\mathbb{Z} = \langle x\rangle$. L'application $\mathbb{C}H \to \mathbb{C}G$ définie par

$$1 \mapsto 1, \quad x \mapsto \frac{1+i}{2}a + \frac{1-i}{2}b, \quad x^2 \mapsto b, \quad x^3 \mapsto \frac{1-i}{2}a + \frac{1+i}{2}b$$

est un isomorphisme d'anneaux, mais $G \not\simeq H$.

Remarque 1.17. Toute représentation $\rho : G \to \mathrm{GL}(V)$ peut être étendue en un morphisme d'algèbres $\widehat{\rho} : KG \to \mathrm{End}_K(V)$ via la formule

$$\widehat{\rho}(\sum_{g\in G} \lambda_g g) = \sum_{g\in G} \lambda_g \rho(g).$$

Ceci mène à la notion plus générale de *représentation d'algèbre*. Si A est une K-algèbre, une représentation de A est un morphisme de K-algèbres $\widehat{\rho} : A \to \mathrm{End}_K(V)$ où V est un K-espace vectoriel. Ainsi, on a aussi réciproquement que toute représentation $\widehat{\rho} : KG \to \mathrm{End}_K(V)$ de KG détermine une représentation $\rho : G \to \mathrm{GL}(V)$ de G via la formule

$$\rho(g) = \widehat{\rho}|_G(g).$$

Chapitre 2

Modules pour les algèbres de groupes

La théorie des représentations des groupes finis peut être vue comme un cas particulier de la théorie des modules. En effet, nous allons voir que la donnée d'une représentation d'un groupe fini G sur K équivaut à la donnée d'un KG-module.

2.1 Modules

Définition 2.1. Soit R un anneau avec unité 1. Un *R-module à gauche* est un groupe abélien $(M, +)$ muni d'une multiplication externe $R \times M \to M$, $(r, m) \mapsto rm$ vérifiant, pour tous $r, s \in R$, $m, n \in M$,

- $r(m + n) = rm + rn$
- $(r + s)m = rm + sm$,
- $(rs)m = r(sm)$,
- $1m = m$.

On définit de même un R-module à droite en utilisant une multiplication externe $M \times R \to M$.

Dans la suite, on utilisera seulement des modules à gauche.

Exemple 2.2. Le groupe abélien R devient un R-module à gauche en considérant la multiplication à gauche $R \times R \to R$, appelé le *R-module régulier à gauche*, noté ${}_RR$. On construit de façon similaire R_R en utilisant la multiplication à droite.

Remarque 2.3.

(1) Si A est une K-algèbre, alors A est aussi un anneau. La définition 2.1 induit donc en particulier la notion de A-module. De plus, un A-module M est alors un K-espace vectoriel, via la multiplication externe $K \times M \to M, (\lambda, m) \to \lambda m$ définie par $\lambda m = (\lambda 1)m$.

(2) Si R est un corps, on retrouve la définition d'un espace vectoriel.

Définition 2.4.

(1) Soient M_1, M_2 deux R-modules. Un *morphisme* de R-modules, ou une application *R-linéaire*, est une application $f : M_1 \to M_2$ vérifiant $f(rm + n) = rf(m) + f(n)$ pour tous $r \in R$, $m, n \in M_1$. Si f est bijective, on dit que f est un *isomorphisme* de R-modules.

(2) Un sous-module d'un R-module M est un sous-groupe N de M stable par multiplication externe, c'est-à-dire que pour tout $r \in R$, $n \in N$, on a $rn \in N$. On notera $N \leq M$.

(3) Un module M est dit *simple* si $M \neq \{0\}$ et si ses seuls sous-modules sont $\{0\}$ et M.

Exemple 2.5. Les sous-modules du R-module régulier à gauche (respectivement à droite) sont les idéaux à gauche (respectivement à droite) de R.

On a, comme en algèbre linéaire, une notion de somme directe de modules, de module quotient, de produit tensoriel, ainsi que les mêmes théorèmes d'isomorphisme.

La proposition suivante est fondamentale puisqu'elle permet de remplacer l'étude des représentations d'un groupe fini par l'étude des modules pour l'algèbre de groupe correspondante.
À partir de maintenant, on se restreint au cas où G est fini.

Proposition 2.6. La donnée d'une représentation de G sur K est équivalente à la donnée d'un KG-module.

Preuve. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G sur K. On vérifie alors facilement que V devient un KG-module, c'est-à-dire que pour tous $a, b \in KG$, $v, w \in V$,

— $a(v + w) = av + aw$,

— $(a + b)v = av + bv$,

— $(ab)v = a(bv)$,

— $1v = v$.

Réciproquement, soit V un KG-module. On a déjà vu en Remarque 2.3(1) que V est un K-espace vectoriel. On définit alors $\rho : G \to \mathrm{GL}(V)$ par

$$\rho(g)(v) = gv \quad \forall g \in G, v \in V.$$

On vérifie facilement que ρ est bien définie (c'est-à-dire que $\rho(g) \in \mathrm{GL}(V)$), et que c'est un morphisme de groupes.

□

Remarque 2.7. Ceci donne lieu à un "dictionnaire" entre le langage des modules et celui des représentations :

KG-modules	Représentations de G sur K
morphisme de modules	morphisme de représentations
modules isomorphes	représentations équivalentes
sous-module	sous-représentation
module simple	représentation irréductible
module régulier	représentation régulière

Le lemme de Schur se traduit alors de la façon suivante.

Théorème 2.8 (Lemme de Schur)**.** Soit K un corps, A une K-algèbre de dimension finie, et soient V, W deux A-modules simples.

(1) Si $V \not\simeq W$, alors $\mathrm{Hom}_A(V, W) = \{0\}$.

(2) L'anneau $\mathrm{End}_A(V)$ est un corps (non nécessairement commutatif). De plus, si K est algébriquement clos, alors $\mathrm{End}_A(V) = \{\lambda \mathrm{Id}\,;\, \lambda \in K\} \simeq K$.

2.2 Algèbres semi-simples

Soit K un corps commutatif. Dans cette section, soit $A \neq \{0\}$ une K-algèbre de dimension finie. Tous les A-modules considérés seront supposés de dimension finie (en tant que K-espace vectoriels, voir Remarque 2.3(1)).

Définition 2.9.

(1) Un A-module V est dit *semi-simple* si pour tout sous-module W de V, il existe un sous-module W' de V tel que $V = W \oplus W'$.

(2) L'algèbre A est dite *semi-simple* si le A-module régulier est semi-simple.

Remarque 2.10. Le module trivial $\{0\}$ est semi-simple, mais pas simple.

Lemme 2.11. Soit V un A-module semi-simple et W un sous-module de V. Alors W et V/W sont semi-simples.

Preuve. Écrivons $V = W \oplus W'$, où W' est un sous-module de V. Alors $V/W = (W \oplus W')/W \simeq W'$, donc il suffit de démontrer l'assertion pour les sous-modules. Soit donc U un sous-module de W. Alors U est aussi un sous-module de V, donc il existe un sous-module U' de V tel que $U \oplus U' = V$. On a alors $W = V \cap W = (U \oplus U') \cap W = (U \cap W) \oplus (U' \cap W) = U \oplus (U' \cap W)$. Puisque $U' \cap W$ est un sous-module de W, on conclut que W est semisimple.

□

Théorème 2.12. Soit V un A-module. Les assertions suivantes sont équivalentes.

(1) V est semisimple,

(2) V est somme directe de sous-modules simples,

(3) V est somme de sous-modules simples.

Preuve. (1)⇒(2) se démontre exactement comme le corollaire 1.9. (2)⇒(3) est trivial. Pour démontrer (2)⇒(1), écrivons $V = \sum_i V_i$ avec V_i simple, et soit $W \leq V$. Puisque V est de dimension finie, on peut choisir $U \leq W$ de dimension maximale tel que $U \cap W = \{0\}$. Supposons que $W + U \neq V$. Alors il existe $v \in V$ tel que $v \notin W + U$. On peut écrire $v = \sum_i v_i$ avec $v_i \in V_i$, et il existe i tel que $v_i \notin W + U$, donc $V_i \not\leq W + U$. On a alors $(W + U) \cap V_i = \{0\}$ puisque V_i est simple, ce qui implique $(U + V_i) \cap W = \{0\}$. Mais puisque $U \lneqq U + V_i \leq V$, ceci contredit la maximalité de U.

□

Théorème 2.13. L'algèbre A est semi-simple si et seulement si tout A-module est semi-simple.

Preuve. Si tout A-module est semi-simple, alors en particulier le A-module régulier est semi-simple et A est semi-simple par définition. Réciproquement, supposons A semi-simple, et soit V un A-module. Puisque V est supposé de dimension finie, il existe $v_1, \ldots, v_m$ tels que $V = \sum_{i=1}^{m} Av_i$. Grâce au théorème 2.12, il suffit de montrer que chaque Av_i est semi-simple. Fixons donc $i \in \{1, \ldots, m\}$. L'application $\varphi_i : {}_AA \to Av_i, a \mapsto av_i$ est un morphisme de A-modules surjectif, et on a donc

$$Av_i \simeq {}_AA/\operatorname{Ker}(\varphi_i).$$

On conclut en utilisant le lemme 2.11.

□

On peut énoncer le théorème de Maschke dans le langage des modules.

Théorème 2.14 (Maschke)**.** Soit G un groupe fini et K un corps. Alors KG est semi-simple si et seulement si $\mathrm{char}(K) \nmid |G|$.

On termine avec un théorème de structure pour les algèbres semi-simples de dimension finie.

Lemme 2.15.

(1) Soit V un A-module semi-simple et soit $V = V_1 \oplus \ldots \oplus V_m$ une décomposition de V en somme directe de sous-module simples. Alors pour tout A-module simple S isomorphe à un sous-module ou à un module quotient de V, il existe $i \in \{1, \ldots, m\}$ tel que $S \simeq V_i$.

(2) Si A est semi-simple, alors il n'y a qu'un nombre fini de A-modules simples (à isomorphisme près).

Preuve.

(1) Soit $S' \leq V$ avec $S' \simeq S$. Alors il existe $T \leq V$ tel que $V = T \oplus S'$, et on a alors $S \simeq S' \simeq V/T$. Il suffit donc de prouver l'assertion pour les modules quotients. Soit donc $T \leq V$ tel que $S \simeq V/T$. Puisque S est simple, T est maximal. Soit $i \in \{1, \ldots, m\}$ tel que $V_i \not\leq T$. On a $V = V_i + T$ car T est maximal, et $V_i \cap T = \{0\}$ car V_i est simple. Il suit $V = V_i \oplus T$, et $S \simeq V/T \simeq V_i$.

(2) C'est une conséquence directe de (1) appliqué au A-module ${}_AA$, puisqu'on a vu dans la preuve du théorème 2.13 que tout A-module simple S est isomorphe à un quotient de ${}_AA$ (on a $S \simeq {}_AA/\operatorname{Ker}\varphi$ où φ est la surjection ${}_AA \to S, a \mapsto as$ avec $s \in S \setminus \{0\}$).

□

Théorème 2.16 (Artin-Wedderburn)**.** Soit K un corps algébriquement clos et A une K-algèbre semi-simple de dimension finie. Soient $S_1, \ldots, S_r$ des représentants des classes d'isomorphisme des A-modules simples. Pour tout $i = 1, \ldots, r$, notons $m_i = \dim_K S_i$. On a

$$A \simeq \bigoplus_{i=1}^{r} K^{m_i \times m_i}.$$

Preuve. Puisque A est semi-simple, on peut écrire ${}_AA = V_1 \oplus \ldots \oplus V_t$ où chaque V_i est un A-module simple. Considérons l'algèbre $\mathrm{End}_A({}_AA)$. Elle est isomorphe à l'algèbre des matrices de taille $t \times t$ où le coefficient en position (i, j) est un élément de $\mathrm{Hom}_A(V_i, V_j)$ (munie de la multiplication matricielle usuelle). Mais comme les V_i sont simples, on peut utiliser le lemme de Schur, qui nous assure que $\mathrm{Hom}_A(V_i, V_j) = \{0\}$ si $V_i \not\simeq V_j$, et que $\mathrm{Hom}_A(V_i, V_i) = \mathrm{End}_A(V_i) \simeq K$. Regroupons donc les V_i qui sont isomorphes deux à deux dans la décomposition de ${}_AA$: en posant, pour tout $i = 1, \ldots, r$

$$A_i = \bigoplus_{\substack{i=1,\ldots,t \\ V_i \simeq S_1}} V_i \quad ,$$

on obtient

$${}_AA = A_i \oplus \ldots \oplus A_r \simeq S_1^{\oplus n_1} \oplus \ldots \oplus S_r^{\oplus n_r},$$

où n_j est le nombre de V_i isomorphes à S_j. On obtient donc

$$\begin{aligned} \mathrm{End}_A({}_AA) &\simeq \mathrm{End}_A(S_1^{\oplus n_1}) \oplus \ldots \oplus \mathrm{End}_A(S_r^{\oplus n_r}) \\ &\simeq K^{n_1 \times n_1} \oplus \ldots \oplus K^{n_r \times n_r}. \end{aligned}$$

Maintenant, A est isomorphe (en tant que K-algèbre) à $\mathrm{End}_A({}_AA)^{\mathrm{o}}$, l'algèbre *opposée* à $\mathrm{End}_A({}_AA)$, c'est-à-dire où la multiplication est définie par $a * b = ba$ (exercice). On a donc

$$\begin{aligned} A &\simeq \mathrm{End}_A({}_AA)^{\mathrm{o}} \\ &\simeq \left(K^{n_1\times n_1} \oplus \ldots \oplus K^{n_r\times n_r}\right)^{\mathrm{o}} \\ &\simeq (K^{n_1\times n_1})^{\mathrm{o}} \oplus \ldots \oplus (K^{n_r\times n_r})^{\mathrm{o}} \\ &\simeq K^{n_1\times n_1} \oplus \ldots \oplus K^{n_r\times n_r} \quad \text{(via transposition matricielle)} \end{aligned}$$

Il reste à montrer que $n_i = m_i$ pour tout $i = 1, \ldots, r$. Par construction, l'algèbre $K^{n_i\times n_i}$ agit par zéro sur $S_j^{\oplus n_j}$ si et seulement si $j \neq i$. On a donc un isomorphisme de A-modules $K^{n_i\times n_i} \simeq S_i^{\oplus n_i}$ (puisque les deux sont isomorphes au quotient de ${}_AA$ par les éléments annihilés par $K^{n_i\times n_i}$, voir la construction de la preuve du théorème 2.13). Ainsi, on a

$$n_i^2 = \dim_K K^{n_i\times n_i} = \dim_K S_i^{\oplus n_i} = n_i \dim_K S_i = n_i m_i,$$

ce qui implique $n_i = m_i$.

□

Corollaire 2.17. Avec les notations du théorème précédent, on a

(1) $\dim_K(A) = \sum_{i=1}^r m_i^2$.

(2) $\dim_K(\mathrm{Z}(A)) = r$, où $\mathrm{Z}(A) = \{z \in A \,|\, za = az \ \forall a \in A\}$ est le *centre* de A.

Preuve. Le théorème 2.16 implique directement (1). Puisque $\mathrm{Z}(K^{k\times k}) = \{\lambda I_k \,;\, \lambda \in K\} \simeq K$, on obtient bien (2).

□

Remarque 2.18. Considérons la décomposition ${}_AA = A_i \oplus \ldots \oplus A_r$ dans la preuve du théorème 2.16. On peut donc écrire $1 = e_1 + \ldots + e_r$ avec $e_i \in A_i$ pour tout $i = 1, \ldots, r$. Alors, pour tout $i, j = 1, \ldots, r$, on a (exercice) :

(1) $e_i e_j = \delta_{ij} e_i$,

(2) $A_i = Ae_i = e_iA = e_iAe_i$.

Chapitre 3

Théorie des caractères

À partir de maintenant, on suppose que G est fini et que $K = \mathbb{C}$. Toutes les représentations considérées seront supposées de dimension finie.

3.1 Définitions et premières propriétés

Définition 3.1. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G. Le *caractère* de ρ est la fonction

$$\begin{array}{rccc} \chi_\rho = \chi_V : & G & \longrightarrow & \mathbb{C} \\ & g & \longmapsto & \mathrm{Tr}(\rho(g)). \end{array}$$

Remarque 3.2.

(1) Rappelons que la trace d'un endomorphisme est définie comme la trace de sa matrice dans une base, et qu'elle ne dépend pas de la base choisie. Ainsi, il suffit de choisir une représentation matricielle ρ' associée à ρ (voir la remarque 1.2) pour calculer χ_ρ.

(2) Tout caractère $\chi : G \to \mathbb{C}$ s'étend linéairement en une fonction $\widehat{\chi} : \mathbb{C}G \to \mathbb{C}$.

Proposition 3.3. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G et χ son caractère.

(1) $\chi(1) = \dim_K(V)$.

(2) Pour tout $g \in G$, $\rho(g)$ est diagonalisable avec pour valeur propres des racines n-ième de 1, où n est l'ordre de g.

(3) $\chi(g^{-1}) = \overline{\chi(g)}$ pour tout $g \in G$.

(4) $\chi(hgh^{-1}) = \chi(g)$ pour tous $g, h \in G$.

Définition 3.4. Une application $f : G \to \mathbb{C}$ qui vérifie $f(hgh^{-1}) = f(g)$ pour tous $g, h \in G$ est appelée *fonction centrale*.

Preuve.

(1) $\chi(1) = \mathrm{Tr}(\rho(1)) = \mathrm{Tr}(\mathrm{Id}) = \dim_K(V)$.

(2) Soit $H = \langle g \rangle$. En particulier, H est abélien, donc en combinant le théorème 1.12 et le théorème de Maschke, $\rho|_H$ se décompose en somme directe de représentations de dimension 1. On a donc

une décomposition en somme directe de $\mathbb{C}H$-modules $V = \bigoplus_{i=1}^{d} V_i$ où $\dim V_i = 1$. Dans une base adaptée, la matrice de $\rho(g) = \rho|_H(g)$ est

$$D = \begin{pmatrix} \varepsilon_1 & & & \\ & \varepsilon_2 & & \\ & & \ddots & \\ & & & \varepsilon_d \end{pmatrix}.$$

Puisque $g^n = 1$, on a $D^n = 1$, et donc $\varepsilon_i^n = 1$ pour tout $i = 1, \ldots, d$, c'est-à-dire ε_i est une racine n-ième de l'unité, d'où l'affirmation.

(3) Puisque $\rho(g^{-1}) = \rho(g)^{-1}$, d'après (2), il existe une base dans laquelle la matrice de $\rho(g^{-1})$ est

$$D^{-1} = \begin{pmatrix} \varepsilon_1^{-1} & & & \\ & \varepsilon_2^{-1} & & \\ & & \ddots & \\ & & & \varepsilon_d^{-1} \end{pmatrix},$$

ce qui implique

$$\begin{aligned} \chi(g^{-1}) &= \varepsilon_1^{-1} + \ldots + \varepsilon_d^{-1} \\ &= \overline{\varepsilon_1} + \ldots + \overline{\varepsilon_d} \quad \text{car les } \varepsilon_i \text{ sont des racines de l'unité} \\ &= \overline{\varepsilon_1 + \ldots + \varepsilon_d} \\ &= \overline{\chi(g)}. \end{aligned}$$

(4) Soient $g, h \in G$. On a $\chi(hgh^{-1}) = \mathrm{Tr}(\rho(hgh^{-1})) = \mathrm{Tr}(\rho(h)\rho(g)\rho(h)^{-1}) = \mathrm{Tr}(\rho(g)) = \chi(g)$.

□

3.2 Caractères irréductibles

Définition 3.5. Le caractère d'un $\mathbb{C}G$-module simple est appelé *caractère irréductible*. On note $\mathrm{Irr}(G)$ l'ensemble des caractéres irréductibles.

D'après le lemme 2.15, il n'y a qu'un nombre fini de $\mathbb{C}G$-modules simples à isomorphisme près. L'ensemble des caractères irréductibles est donc fini. Étudions $\mathrm{Irr}(G)$ plus en détail. Pour cela, notons comme au chapitre précédent $S_1, \ldots, S_r$ des représentants des classes d'isomorphisme des $\mathbb{C}G$-modules simples, et pour tout $i = 1 \ldots, r$, notons $\chi_i = \chi_{S_i}$, de sorte que

$$\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_r\}.$$

D'après la remarque 2.18, le module régulier $\mathbb{C}G$ admet la décomposition

$$\mathbb{C}G = \bigoplus_{i=1}^{r} \mathbb{C}Ge_i$$

où les e_i sont des idempotents orthogonaux.

Lemme 3.6. Pour tous $i, j = 1, \ldots, r$, on a $\widehat{\chi_j}(e_i) = \delta_{ij}\chi_j(1)$.

Preuve. Notons $\rho_j : G \to \mathrm{GL}(S_j)$ la représentation de G associée à S_j. Puisque chaque $\mathbb{C}Ge_i$ est isomorphe à une somme directe de copies de S_i, et que les e_i sont orthogonaux, on a $\widehat{\rho_j}(e_i) = 0$ si $i \neq j$. On a donc $\mathrm{Id}_{S_j} = \widehat{\rho_j}(1) = \widehat{\rho_j}(e_1 + \ldots + e_r) = \widehat{\rho_j}(e_1) + \ldots + \widehat{\rho_j}(e_r) = \widehat{\rho_j}(e_j)$. Au final, on a

$$\widehat{\rho_j}(e_i) = \delta_{ij}\mathrm{Id}_{S_j},$$

ce qui implique que $\widehat{\chi_j}(e_i) = \delta_{ij}\dim(S_j) = \delta_{ij}\chi_j(1)$.

□

Le corollaire suivant est immédiat.

Corollaire 3.7. Les caractères χ_i, $i = 1, \ldots, r$ sont deux à deux distincts.

On en déduit une première identité fondamentale.

Théorème 3.8. On a

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |G|.$$

Preuve. On a

$$\begin{aligned} |G| = \dim(\mathbb{C}G) &= \sum_{i=1}^{r} \dim(S_i)^2 && \text{par le corollaire 2.17} \\ &= \sum_{i=1}^{r} \chi_{S_i}(1)^2 && \text{par la proposition 3.3} \\ &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 && \text{par le corollaire 3.7.} \end{aligned}$$

□

Le théorème suivant permet d'exprimer $r = |\mathrm{Irr}(G)|$ de manière élémentaire.

Théorème 3.9. Le nombre de caractères irréductibles de G est égal au nombre de classes de conjugaison de G.

Preuve. Notons $C_1, \ldots, C_s$ les classes de conjugaison de G, pour $i = 1, \ldots, s$, soit $\widehat{C_i} = \sum_{x \in C_i} x \in \mathbb{C}G$. Montrons que $\widehat{C_1}, \ldots, \widehat{C_s}$ est une base de $\mathrm{Z}(\mathbb{C}G)$. Tout d'abord, pour tout $g \in G$ and $i = 1, \ldots, s$, on a

$$g\widehat{C_i} = g\left(\sum_{x \in C_i} x\right) = \left(\sum_{x \in C_i} gxg^{-1}\right) g = \left(\sum_{x \in C_i} x\right) g = \widehat{C_i}g$$

donc $\widehat{C_i} \in \mathrm{Z}(\mathbb{C}G)$. Puisque les $\widehat{C_i}$ sont des sommes d'éléments d'ensembles disjoints, il sont linéairement indépendants. De plus, pour tout élément $z = \sum_{g \in G} \lambda_g g \in \mathrm{Z}(\mathbb{C}G)$, et pour tout $h \in G$, on a $hzh^{-1} = z$, donc $\sum_{g \in G} \lambda_g g = \sum_{g \in G} \lambda_g hgh^{-1}$, et donc $\lambda_g = \lambda_{h^{-1}gh}$, c'est-à-dire que le coefficient λ_g dépend seulement de la classe de conjugaison de g. Donc $z \in \langle \widehat{C_1}, \ldots, \widehat{C_s} \rangle$, c'est-à-dire que les $\widehat{C_i}$ engendrent $\mathrm{Z}(\mathbb{C}G)$. En particulier, on a donc $s = \dim(\mathrm{Z}(\mathbb{C}G))$, et $\dim(\mathrm{Z}(\mathbb{C}G)) = r$ par le corollaire 2.17, ce qui conclut la preuve.

□

Exemple 3.10. Considérons le groupe S_3. Ses classes de conjugaison sont caractérisées par la décomposition en cycles des permutations, c'est-à-dire que S_3 possède les trois classes de conjugaison suivantes

$$\{1\} \qquad \{(12),(23),(13)\} \qquad \{(123),(132)\}.$$

Le théorème 3.9 nous assure donc que S_3 possède trois caractères irréductibles. De plus, d'après le théorème 3.7, la somme des carrés des trois degrés correspondants vaut $|S_3| = 6$. Les degrés des caractères irréductibles valent donc nécessairement 1, 1 et 2. En fait, les représentations correspondantes sont donc celles que l'on connaît déjà (vues en exercice) : la représentation triviale, la signature (toutes les deux de degré 1, clairement non isomorphes), et la représentation irréductible de degré 2 suivante

$$\rho : S_3 \to \mathrm{GL}(\mathbb{C}^2), \quad (12) \mapsto s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (123) \mapsto s_2 = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Corollaire 3.11. Le groupe G est abélien si et seulement si $\chi(1) = 1$ pour tout $\chi \in \mathrm{Irr}(G)$.

Preuve. On a

$$\begin{aligned}
\chi(1) = 1 \text{ pour tout } \chi \in \mathrm{Irr}(G) \quad &\Leftrightarrow \quad \sum_{\mathrm{Irr}(G)} 1 = |G| && \text{par le théorème 3.8} \\
&\Leftrightarrow \quad |\mathrm{Irr}(G)| = |G| \\
&\Leftrightarrow \quad G \text{ a } |G| \text{ classes de conjugaison} && \text{par le théorème 3.9} \\
&\Leftrightarrow \quad \text{chaque classe de conjugaison} \\
&\qquad\quad \text{de } G \text{ a un seul élément} \\
&\Leftrightarrow \quad G \text{ est abélien.}
\end{aligned}$$

□

Théorème 3.12. L'ensemble $\mathrm{Irr}(G)$ est une base de l'espace des fonctions centrales $G \to \mathbb{C}$.

Preuve. On sait déjà d'après la proposition 3.3 que les éléments de $\mathrm{Irr}(G)$ sont des fonctions centrales. Notons $C_1, \ldots, C_s$ l'ensemble des classes de conjugaison de G. L'espace des fonctions centrales de G dans $\mathbb{C}$ a pour base canonique $\varphi_1, \ldots, \varphi_s$, où $\varphi_i : G \to \mathbb{C}$ est définie par $\varphi_i(g) = 1$ si $g \in C_i$ et $\varphi_i(g) = 0$ si $g \notin C_i$. En particulier, sa dimension est s, le nombre de classes de conjugaison de G. Par le théorème 3.9, $s = |\mathrm{Irr}(G)|$, il suffit donc de montrer que $\mathrm{Irr}(G)$ est une famille libre. Soient donc $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ tels que $\sum_{i=1}^{s} \lambda_i \chi_i = 0$. Pour tout $i = 1, \ldots, s$, on obtient $\lambda_i = 0$ en évaluant cette fonction en e_i.

□

Corollaire 3.13.

(1) Soit $\varphi = \sum_{\chi \in \mathrm{Irr}(G)} c_\chi \chi$ une fonction centrale. Alors φ est un caractère si et seulement si $c_\chi \in \mathbb{Z}_{\geq 0}$ pour tout $\chi \in \mathrm{Irr}(G)$.

(2) Soient V, W deux $\mathbb{C}G$-modules. Alors $V \simeq W \Leftrightarrow \chi_V = \chi_W$.

Preuve.

(1) Si φ est un caractère, alors il existe une représentation V de G telle que $\varphi = \chi_V$. D'après le corollaire 1.11, V se décompose de manière unique $V = \bigoplus_{i=1}^r S_i^{\oplus a_i}$ avec $a_i \in \mathbb{Z}_{\geq 0}$. On a alors $\chi_V = \sum_{i=1}^r a_i \chi_i$. Réciproquement, si $c_i \in \mathbb{Z}_{\geq 0}$ pour tout i, alors φ est le caractère de la représentation $\bigoplus_{i=1}^r c_i S_i$.

(2) Si $V \simeq W$, alors $\chi_V = \chi_W$ d'après la remarque 3.2. Réciproquement, supposons que $\chi_V = \chi_W$. Pour tout $i = 1, \ldots, r$, soient $a_i, b_i \in \mathbb{Z}_{\geq 0}$ tels que $V = \bigoplus_{i=1}^r S_i^{\oplus a_i}$ et $W = \bigoplus_{i=1}^r S_i^{\oplus b_i}$, de sorte que $\chi_V = \sum_{i=1}^r a_i \chi_i$ et $\chi_W = \sum_{i=1}^r b_i \chi_i$. Par indépendance linéaire des χ_i, on a $a_i = b_i$ pour tout $i = 1, \ldots, r$, et donc $V \simeq W$.

□

3.3 Table de caractères et relations d'orthogonalité

Définition 3.14. Soient $g_1, \ldots, g_r$ des représentants des classes de conjugaison de G. La matrice

$$(\chi_i(g_j))_{1 \leq i,j \leq r}$$

est appelée *table de caractères* de G.

Exemple 3.15. Comme vu en exemple 3.10, nous connaissons les 3 caractères irréductibles de S_3. La table de caractères de S_3 est

	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Nous allons exprimer e_i en fonction de χ_i, ce qui nous permettra de déduire les premières relations d'orthogonalité. Pour cela, nous avons besoin du lemme suivant. Notons $\chi = \chi_{\mathbb{C}G}$ le caractère de la représentation régulière.

Lemme 3.16. Pour tout $g \in G$, on a

$$\chi(g) = \begin{cases} |G| & \text{si } g = 1 \\ 0 & \text{sinon} \end{cases}$$

Preuve. Choisissons la base G de $\mathbb{C}G$ pour calculer la représentation matricielle R associée au module régulier. Pour tout $g \in G$, on a $R(g) = (\delta_{x,gy})_{x,y \in G}$. On a donc d'une part $R(1) = I_{|G|}$, et d'autre part pour $g \neq 1$, la matrice $R(g)$ n'a que des zéros sur la diagonale, d'où le résultat.

□

Proposition 3.17. Pour tout $i = 1, \ldots, r$, on a

$$e_i = \frac{1}{|G|} \sum_{g \in G} \chi_i(1) \chi_i(g^{-1}) g.$$

Preuve. Fixons $i \in \{1, \ldots, r\}$, et écrivons $e_i = \sum_{h \in G} \lambda_h h$. Par le lemme 3.16, pour tout $g \in G$, on a

$$\widehat{\chi}(e_i g^{-1}) = \widehat{\chi}(\sum_{h \in G} \lambda_h h g^{-1}) = \sum_{h \in G} \lambda_h \chi(h g^{-1}) = \lambda_g |G|.$$

De plus, d'après le théorème 2.16 et la proposition 3.3(1), on a $\mathbb{C}G \simeq \bigoplus_{j=1}^{r} S_j^{\oplus \dim_K(S_j)} = \bigoplus_{j=1}^{r} S_j^{\oplus \chi_j(1)}$, ce qui implique que $\chi = \sum_{j=1}^{r} \chi_j(1)\chi_j$. On a donc

$$\lambda_g |G| = \widehat{\chi}(e_i g^{-1}) = \sum_{j=1}^{r} \chi_j(1)\widehat{\chi_j}(e_i g^{-1}).$$

Maintenant, on a $\widehat{\chi_j}(e_i g^{-1}) = \delta_{ij}\chi_j(g^{-1})$ d'après le lemme 3.6. On obtient donc

$$\lambda_g |G| = \sum_{j=1}^{r} \chi_j(1)\delta_{ij}\chi_j(g^{-1}) = \chi_i(1)\chi_i(g^{-1}),$$

ce qui conclut la preuve.

□

Pour énoncer les premières relations d'orthogonalité, définissons un produit scalaire (c'est-à-dire une forme sesquilinéaire définie positive et hermitienne) sur l'ensemble des fonctions de G dans $\mathbb{C}$ par

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

pour $\varphi, \psi : G \to \mathbb{C}$.

Théorème 3.18 (Premières relations d'orthogonalité)**.** Pour tous $i, j \in \{1, \ldots, r\}$, on a

$$(\chi_i, \chi_j) = \delta_{ij}.$$

Preuve. D'après la remarque 2.18, on a $e_i e_j = \delta_{ij} e_i$. En remplaçant e_i par son expression de la proposition 3.17, et en comparant le coefficient de $1 \in G$ des deux côtés, on obtient

$$\frac{\chi_i(1)\chi_j(1)}{|G|^2} \sum_{g \in G} \chi_i(g)\chi_j(g^{-1}) = \delta_{ij} \frac{\chi_i(1)^2}{|G|}.$$

On conclut en utilisant que $\chi_j(g^{-1}) = \overline{\chi_j(g)}$ comme énoncé en proposition 3.3(3).

□

Remarque 3.19. Autrement dit, d'après les théorèmes 3.12 et 3.18, les caractères irréductibles forment une base orthonormée de l'espace des fonctions centrales.

Corollaire 3.20. Soient χ, ψ deux caractères de G. On a $(\chi, \psi) = (\psi, \chi) \in \mathbb{Z}_{\geq 0}$. De plus, χ est irréductible si et seulement si $(\chi, \chi) = 1$.

Preuve. D'après le corollaire 3.13(1), on peut écrire $\chi = \sum_{i=1}^{r} a_i \chi_i$ et $\psi = \sum_{i=1}^{r} b_i \chi_i$ avec $a_i, b_i \in \mathbb{Z}_{\geq 0}$. On a alors $(\chi, \psi) = (\psi, \chi) = \sum_{i=1}^{r} a_i b_i \in \mathbb{Z}_{\geq 0}$. De plus, $(\chi, \chi) = \sum_{i=1}^{r} a_i^2$, donc $(\chi, \chi) = 1$ si et seulement si $a_i = 1$ pour exactement un i, c'est-à-dire χ est irréductible.

□

Rappelons que l'on a choisi des représentants $g_1, \ldots, g_r$ des classes de conjugaison $C_1, \ldots, C_r$ de G, et notons $X = (\chi_i(g_j))_{1 \leq i,j \leq r}$ la table de caractères de G.

Théorème 3.21 (Deuxièmes relations d'orthogonalité)**.** Pour tous $k, \ell = 1, \ldots, r$, on a

$$\sum_{i=1}^{r} \chi_i(g_k)\chi_i(g_\ell^{-1}) = \begin{cases} |C_G(g_k)| & \text{si } k = \ell, \\ 0 & \text{sinon,} \end{cases}$$

où $C_G(g_k) = \{x \in G \mid xg_k = g_k x\}$ est le centralisateur de g_k dans G.

Preuve. Soit $Y \in \mathbb{C}^{r\times r}$ définie par $Y_{i,j} = \frac{|C_i|}{|G|}\chi_j(g_i^{-1})$. Alors

$$(XY)_{p,q} = \sum_{i=1}^{r} X_{p,i}Y_{i,q} = \sum_{i=1}^{r} \chi_p(g_i)\frac{|C_i|}{|G|}\chi_q(g_i^{-1}) = \delta_{pq}$$

d'après le théorème 3.18, c'est-à-dire que $XY = I_r$. Ceci implique $YX = I_r$, et donc

$$\delta_{pq} = (YX)_{p,q} = \sum_{i=1}^{r} Y_{p,i}X_{i,q} = \sum_{i=1}^{r} \frac{|C_p|}{|G|}\chi_i(g_p^{-1})\chi_i(g_q),$$

donc

$$\sum_{i=1}^{r} \chi_i(g_p^{-1})\chi(g_q) = \begin{cases} \frac{|G|}{|C_p|} & \text{si } p = q, \\ 0 & \text{sinon,} \end{cases}.$$

On conclut en utilisant que $\frac{|G|}{|C_p|} = |C_G(g_p)|$.

□

Exemple 3.22. Prenons $G = S_4$. On connaît déjà deux représentation de degré un de G : la représentation triviale et la signature. On sait d'autre part que les classes de conjugaison de G sont déterminées par la décomposition en cycles. Il y en a donc 5, dont des représentants sont 1, (12), (123), (1234), (12)(34), et leur taille respective est 1, 6, 8, 6, 3. D'après le théorème 3.9, G a donc 5 caractères irréductibles $\chi_i, i = 1, \ldots, 5$. Notons χ_1 la représentation triviale et χ_2 la signature. La seule possibilité pour écrire $|G| = 24$ comme somme de 5 carrés est $24 = 1 + 1 + 2^2 + 3^2 + 3^2$ est de prendre. D'après le théorème 2.16, ceci détermine les degrés de $\chi_i, i = 1, \ldots, 5$, et on peut donc remplir la première colonne de la table de caractères. Construisons une représentation irréductible de degré 3 de G. Pour cela, considérons la représentation naturelle $\rho : G \to \mathrm{GL}_4(\mathbb{C})$ (par les matrices de permutation). Le vecteur $v = (1, 1, 1, 1)^{\mathrm{tr}}$ est un vecteur propre associé à la valeur propre 1 pour la matrice $\rho(g)$ pour tout $g \in G$, et donc $\langle v\rangle$ est une sous-représentation de degré 1 de ρ, isomorphe à la représentation triviale (voir aussi l'exemple 1.7). L'espace quotient $\mathbb{C}^4/\langle v\rangle$ est donc une représentation de degré 3 de G. Soit χ son caractère. On connaît ρ, donc χ explicitement : on vérifie que χ prend les valeurs 3, 1, 0, -1, -1 sur les classes de conjugaison. On a donc

$$(\chi, \chi) = \frac{1}{24}(1.3^2 + 6.1^2 + 8.0^2 + 6.(-1)^2 + 3.(-1)^2 = 1,$$

ce qui prouve que χ est irréductible par le corollaire 3.20. Notons donc $\chi = \chi_4$. En multipliant χ_4 par χ_2, on obtient un nouveau caractère irrédutible χ_5 de degré 3 (c'est le caractère du produit tensoriel des représentations correspondantes, exercice). Il reste à calculer χ_3, le caractère irréductible de dimension 2 de G. Pour cela, il suffit d'utiliser les relations d'orthogonalité. Par example, $|C_G((12))| = 24/6 = 4$, donc $\chi_3((12)) = x$ tel que

$$1^2 + (-1)^2 + 1^2 + (-1)^2 + x^2 = 4,$$

ce qui donne $x = 0$. De même, on trouve les valeurs -1, 0, 2 sur les autres classes de conjugaison. Au final, on obtient

	1	(12)	(123)	(1234)	(12)(34)
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

3.4 Caractères et centre

Soit G un groupe fini. Pour tout caractère χ de G, notons

$$\mathrm{Ker}(\chi) = \{g \in G \mid \chi(g) = \chi(1)\}, \quad \text{le } \textit{noyau} \text{ de } \chi, \text{ et}$$

$$\mathrm{Z}(\chi) = \{g \in G \mid |\chi(g)| = \chi(1)\}, \quad \text{le } \textit{centre} \text{ de } \chi.$$

Proposition 3.23. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de degré d et χ son caractère.

(1) $\mathrm{Ker}(\chi) = \mathrm{Ker}(\rho)$.

(2) $\mathrm{Z}(\chi) = \{g \in G \mid \rho(g) = \varepsilon\mathrm{Id} \text{ pour un certain } \varepsilon \in \mathbb{C}\}$.

(3) $\mathrm{Z}(\chi) \leq G$.

(4) $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi)$ est cyclique.

(5) $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi) \leq \mathrm{Z}(G/\mathrm{Ker}(\chi))$. De plus, si $\chi \in \mathrm{Irr}(G)$, on a $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi) = \mathrm{Z}(G/\mathrm{Ker}(\chi))$.

Preuve.

(1) Soit $g \in \mathrm{Ker}(\rho)$. Alors $\rho(g) = \mathrm{Id}$, et donc $\chi(g) = d$, c'est-à-dire $g \in \mathrm{Ker}(\chi)$. Réciproquement, soit $g \in \mathrm{Ker}(\chi)$. Utilisons le lemme 3.3(2). On a $\chi(g) = \varepsilon_1 + \ldots + \varepsilon_d$ avec ε_i des racines n-èmes de l'unité (n étant l'ordre de g). Puisque $d = \chi(g)$, on a $\varepsilon_i = 1$ pour tout $i = 1, \ldots, d$. Ainsi, dans une certaine base, la matrice de $\rho(g)$ est I_d, donc $\rho(g) = \mathrm{Id}$, c'est-à-dire $g \in \mathrm{Ker}(\rho)$.

(2) Soit $g \in G$ tel que $\rho(g) = \varepsilon\mathrm{Id}$. Alors ε est une racine de l'unité, et $|\chi(g)| = d|\varepsilon| = d$. Réciproquement, soit $g \in \mathrm{Z}(\chi)$, c'est-à-dire $|\chi(g)| = d$. De nouveau, par le lemme 3.3(2), $|\chi(g)| = |\varepsilon_1 + \ldots + \varepsilon_d|$. Par le théorème de Cauchy-Schwarz, on doit avoir $\varepsilon_i = \varepsilon$ pour une racine de l'unité ε, pour tout $i = 1, \ldots, d$.

(3) Soit $\lambda : \mathrm{Z}(\chi) \to \mathbb{C}$ définie par $\rho(g) = \lambda(g)\mathrm{Id}$. Pour $g, h \in \mathrm{Z}(\chi)$, on a $\rho(gh) = \rho(g)\rho(h) = \lambda(g)\lambda(h)\mathrm{Id}$, et donc $\mathrm{Z}(\chi)$ est bien un sous-groupe de G (et λ est un morphisme).

(4) On a $\mathrm{Ker}(\chi) = \mathrm{Ker}(\lambda)$, donc $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi) = \mathrm{Z}(\chi)/\mathrm{Ker}(\lambda) \simeq \mathrm{Im}(\lambda)$. Mais $\mathrm{Im}(\lambda)$ est un sous-groupe multiplicatif fini de $\mathbb{C}^\times$, donc cyclique.

(5) Puisque $\mathrm{Ker}(\chi) = \mathrm{Ker}(\rho)$ d'après (1), on a

$$\mathrm{Z}(\chi)/\mathrm{Ker}(\chi) = \mathrm{Z}(\chi)/\mathrm{Ker}(\rho) \simeq \rho(\mathrm{Z}(\chi)) \underset{(2)}{\leq} \mathrm{Z}(\rho(G)) \simeq \mathrm{Z}(G/\mathrm{Ker}(\rho)) = \mathrm{Z}(G/\mathrm{Ker}(\chi)).$$

De plus, si $\chi \in \mathrm{Irr}(G)$, on a par le théorème d'Artin-Wedderburn $\rho(\mathbb{C}G) = \mathbb{C}^{d\times d}$, et donc $\mathrm{Z}(\rho(G)) = \rho(G) \cap \{\varepsilon I_d \,;\, \varepsilon \in \mathbb{C}^\times\} = \rho(\mathrm{Z}(\chi))$ par (2).

□

Le théorème suivant permet de déterminer le centre d'un groupe à partir de sa table de caractères.

Théorème 3.24. On a

$$\mathrm{Z}(G) = \bigcap_{\chi \in \mathrm{Irr}(G)} \mathrm{Z}(\chi).$$

Preuve. Soit $\chi \in \mathrm{Irr}(G)$. On a $(\mathrm{Z}(G)\,\mathrm{Ker}(\chi))/\mathrm{Ker}(\chi) \leq \mathrm{Z}(G/\mathrm{Ker}(\chi))$, et puisque $\mathrm{Z}(G/\mathrm{Ker}(\chi)) = \mathrm{Z}(\chi)/\mathrm{Ker}(\chi)$ (proposition 3.23(5)), on obtient $\mathrm{Z}(G) \leq \mathrm{Z}(\chi)$. Réciproquement, soit $g \in \mathrm{Z}(\chi)$ pour tout $\chi \in \mathrm{Irr}(G)$. On a

$$|C_G(g)| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\chi(g^{-1}) \quad \text{par le théorème 3.21}$$

$$
\begin{aligned}
&= \sum_{\chi \in \mathrm{Irr}(G)} |\chi(g)|^2 && \text{par la proposition 3.3(4)} \\
&= \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 && \text{car } g \in \mathrm{Z}(\chi) \\
&= |G| && \text{par le théorème 3.8,}
\end{aligned}
$$

donc $g \in \mathrm{Z}(G)$.

□

Chapitre 4

Le théorème de Burnside

Le théorème de Burnside, qui affirme que tout groupe dont l'ordre a au plus deux diviseurs premiers est résoluble, joua un rôle fondateur dans la classification des groupes simples finis. Pour le démontrer, on a besoin de quelques résultats élémentaires de théorie des nombres, qui font l'objet des deux sections suivantes.

4.1 Intégralité

Définition 4.1. Un nombre complexe $c \in \mathbb{C}$ est appelé *entier algébrique* s'il existe un polynôme $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$ unitaire tel quel $f(c) = 0$.

La proposition suivante justifie la terminologie "entier algébrique".

Proposition 4.2. Soit $c \in \mathbb{Q}$. Alors c est un entier algébrique si et seulement si $c \in \mathbb{Z}$.

Preuve. Si $c \in \mathbb{Z}$, alors il suffit de prendre $f = X - c$. Réciproquement, soit $c \in \mathbb{Q}$ et écrivons $c = r/s$ avec $r, s \in \mathbb{Z}$, $s \neq 0$ et $\gcd(r, s) = 1$. Soit $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$ avec $n \geq 1$ tel que $f(c) = 0$, c'est-à-dire

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \ldots + a_1\left(\frac{r}{s}\right) + a_0 = 0.$$

Cela implique

$$r^n = -s(a_{n-1}r^{n-1} + \ldots + a_1rs^{n-2} + a_0s^{n-1}),$$

et donc $s|r^n$, ce qui donne $s = \pm 1$ car $\gcd(r, s) = 1$, et donc $c = \pm r \in \mathbb{Z}$.

□

Lemme 4.3. Soient $c_1, \ldots, c_\ell \in \mathbb{C}$ des entiers algébriques. Alors $\mathbb{Z}[c_1, \ldots, c_\ell] \subset \mathbb{C}$ est un groupe abélien de type fini (c'est-à-dire engendré par une partie finie).

Preuve. Pour tout $i = 1, \ldots, \ell$, soient $n_i \in \mathbb{Z}_{\geq 1}$ et $f_i \in \mathbb{Z}[X] \setminus \{0\}$ tel que $\deg(f_i) = n_i - 1$ et $c_i^{n_i} = f_i(c_i)$. Soit

$$M = \left\{c_1^{k_1} \ldots c_\ell^{k_\ell} \,;\, 0 \leq k_i \leq n_i - 1, i = 1, \ldots, \ell\right\} \subset \mathbb{Z}[c_1, \ldots, c_\ell],$$

donc $\langle M \rangle \leq \mathbb{Z}[c_1, \ldots, c_\ell]$. Réciproquement, pour tout $i = 1, \ldots, \ell$ et $m_i \in \mathbb{Z}_{\geq 0}$, on a $c_i^{m_i} \in \langle 1, c_i, \ldots, c_i^{n_i} \rangle \leq \langle M \rangle$. Donc pour tous $m_1, \ldots, m_\ell \in \mathbb{Z}_{\geq 0}$, on a $c_1^{m_1} \ldots c_\ell^{m_\ell} \in \langle M \rangle$, et donc

$$\mathbb{Z}[c_1, \ldots, c_\ell] \leq \langle M \rangle.$$

□

Lemme 4.4. Soit $S \subset \mathbb{C}$ un sous-anneau tel que $\mathbb{Z} \subset S$. Si S est de type fini en tant que groupe abélien, alors pour tout $c \in C$, c est un entier algébrique.

Preuve. Ecrivons $s = \langle y_1, \ldots, y_n \rangle$ et soit $c \in S$. Alors pour tout i, on peut écrire $cy_i = \sum_{j=1}^{n} a_{ij} y_j$ avec $a_{ij} \in \mathbb{Z}$. Soit $v = (y_1, \ldots, y_n)^{\mathrm{tr}}$ et $A = (a_{ij})_{0 \leq i,j \leq n}$. Notons que $v \neq 0$ car $\mathbb{Z} \subset S$. On a $Av = cv$, c'est-à-dire que v est un vecteur propre pour A associé à la valeur propre c. L'élément c est donc une racine du polynôme

$$f = \det(XI_n - A),$$

qui est unitaire de degré n.

□

Théorème 4.5. L'ensemble des entiers algébriques forme un sous-anneau de $\mathbb{C}$.

Preuve. Soient c_1, c_2 deux entiers algébriques. Alors d'après le lemme 4.3, $\mathbb{Z}[c_1, c_2]$ est un groupe abélien de type fini. Donc les éléments de $\mathbb{Z}[c_1, c_2]$ sont des entiers algébriques d'après le lemme 4.4. En particulier, $c_1 + c_2$, $c_1 - c_2$ et $c_1 c_2$ sont des entiers algébriques.

□

Corollaire 4.6. Soit χ un caractère de G. Alors pour tout $g \in G$, $\chi(g)$ est un entier algébrique.

Preuve. Soit d le degré de χ. Soit $g \in G$ et n l'ordre de g. D'après la proposition 3.3(2), $\chi(g) = \sum_{i=1}^{d} \varepsilon_i$, où les ε_i sont des racines de l'unité d'ordre n, donc des entiers algébriques puisque racines du polynôme $X^n - 1$.

□

Rappelons qu'on avait noté, pour $i = 1, \ldots, r$, χ_i les caractères irréductibles de G, C_i les classes de conjugaison de G, et g_i un représentant de la classe de conjugaison C_i. Notons $d_i = \chi_i(1)$ le degré de la représentation irréductible correspondante.

Théorème 4.7. Pour tous $i, j = 1, \ldots, r$, l'élément $\frac{|C_j|}{d_i} \chi_i(g_j)$ est un entier algébrique.

Preuve. Soit $\rho_i : G \to GL_{d_i}(\mathbb{C})$ une representation matricielle de caractère χ_i, et $\widehat{\rho_i}$ la représentation de $\mathbb{C}G$ correspondante. Pour $z \in \mathrm{Z}(\mathbb{C}G)$, la matrice $\widehat{\rho_i}(z)$ commute avec $\widehat{\rho_i}(g)$ pour tout $g \in G$. Donc $\rho_i(z)$ est un morphisme de représentations, et puisque ρ_i est irréductible, on peut appliquer le lemme de Schur, qui nous assure que $\widehat{\rho_i}(z) = \lambda I_{d_i}$ pour un certain $\lambda \in \mathbb{C}$. On définit ainsi un morphisme de $\mathbb{C}$-algèbres

$$\begin{array}{rccc} \omega_i : & \mathrm{Z}(\mathbb{C}G) & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \lambda. \end{array}$$

Rappelons (voir la preuve du théorème 3.9) que $\mathrm{Z}(\mathbb{C}G)$ admet pour base $\left\{ \widehat{C_i} \,;\, i = 1, \ldots, r \right\}$. Notons c_{jk}^{ℓ} les *constantes de structure de* $\mathbb{C}G$, c'est-à-dire les nombres vérifiant

$$\widehat{C_j}\widehat{C_k} = \sum_{\ell=1}^{r} c_{jk}^{\ell} \widehat{C_\ell}.$$

Ecrivons $\alpha = \omega_i(\widehat{C_j})$. On a alors

$$\alpha \omega_i(\widehat{C_k}) = \omega_i(\widehat{C_j}) \omega_i(\widehat{C_k})$$

$$\begin{aligned}
&= \omega_i(\widehat{C_j}\widehat{C_k}) \\
&= \omega_i(\sum_{\ell=1}^{r} c_{jk}^{\ell}\widehat{C_\ell}) \\
&= \sum_{\ell=1}^{r} c_{jk}^{\ell}\omega_i(\widehat{C_\ell}),
\end{aligned}$$

c'est-à-dire

$$(\alpha I_r - A)\begin{pmatrix}\omega_i(\widehat{C_1})\\ \vdots \\ \omega_i(\widehat{C_r})\end{pmatrix} = 0$$

où $A = (c_{jk}^{\ell})_{0\leq k,\ell\leq r}$. On a donc $\det(\alpha I_r - A) = 0$ puisque $\omega_i \neq 0$, et donc α est un entier algébrique puisque racine du polynôme unitaire $\det(XI_r - A)$. Finalement,

$$d_i\alpha = d_i\omega_i(\widehat{C_j}) = \mathrm{Tr}(\widehat{\rho_i}(\widehat{C_j})) = \mathrm{Tr}(\widehat{\rho_i}(\sum_{g\in C_j} g)) = \sum_{g\in C_j}\mathrm{Tr}(\rho_i(g)) = \sum_{g\in C_j}\chi_i(g) = |C_j|\chi_i(g_j),$$

donc $\alpha = \frac{|C_j|}{d_i}\chi_i(g_j)$, ce qui conclut la preuve.

□

On en déduit le résultat suivant.

Théorème 4.8. Soit $\chi \in \mathrm{Irr}(G)$. On a $\chi(1) \mid |G|$.

Preuve. D'après le théorème 3.18, on a

$$\begin{aligned}
|G| &= \sum_{g\in G}\chi(g)\,\chi\left(g^{-1}\right) \\
&= \sum_{j=1}^{k}|C_j|\,\chi(g_j)\,\chi\left(g_j^{-1}\right)
\end{aligned}$$

ce qui donne

$$\frac{|G|}{\chi(1)} = \sum_{j=1}^{k}\frac{|C_j|\,\chi(g_j)}{\chi(1)}\chi\left(g_j^{-1}\right).$$

D'après le théorème 4.7, le corollaire 3.13 et le théorème 4.5, on déduit que $\dfrac{|G|}{\chi(1)}$ est un entier algébrique, mais puisqu'on a aussi $\dfrac{|G|}{\chi(1)} \in \mathbb{Q}$, la propositition 4.2 permet de conclure que $\dfrac{|G|}{\chi(1)} \in \mathbb{Z}$.

□

Remarque 4.9. Si $\mathrm{char}(K) \mid |G|$, le théorème 4.8 est faux. Par exemple, en caractéristique 7, le groupe $\mathrm{PSL}_2(7)$, qui est d'ordre $168 = 2^3.3.7$ possède une représentation irréductible de degré 5.

4.2 Élements de théorie de Galois

Soient K et L deux corps (commutatifs). On dit que K est un *sous-corps* de L, ou que L est une *extension* de K, si K est un sous-anneau de L, (c'est-à-dire que K est un anneau pour les mêmes opérations et la même unité que L). Un morphisme d'anneaux $\sigma : K \to L$ est appelé *morphisme de corps*.

Lemme 4.10. Tout morphisme de corps est injectif.

Preuve. Soit $\sigma : K \to L$ un morphisme de corps, et supposons qu'il existe $x \in \mathrm{Ker}(\sigma) \setminus \{0\}$. Alors $0 = \sigma(x) = \sigma(x)\sigma(x^{-1}) = \sigma(1) = 1$, ce qui n'est pas autorisé.

□

Soit $S \subseteq L$. On note $K(S)$ le plus petit sous-corps de L contenant K et S. Explicitement, on a

$$K(S) = \bigcap_{\substack{K' \text{ corps} \\ K \subseteq K' \subseteq L \\ S \subseteq K'}} K'.$$

Si $S = \{s\}$ est un singleton, on note $K(s) = K(S)$.

Définition 4.11. Un élément $\alpha \in L$ est dit *algébrique* sur K s'il existe $f \in K[X] \setminus \{0\}$ tel que $f(\alpha) = 0$.

Remarque 4.12. Les entiers algébriques sont en particulier algébriques sur $\mathbb{Q}$.

Théorème 4.13. Soit $\alpha \in L$ algébrique sur K. Il existe un unique $f \in K[X]$ irréductible tel que

(1) $f \neq 0$,
(2) f est unitaire,
(3) $f(\alpha) = 0$,
(4) f divise h pour tout $h \in K[X]$ tel que $h(\alpha) = 0$.

Cet élément est appelé *polynôme minimal* de α sur K. De plus, on a

$$K(\alpha) \simeq K[X]/(f).$$

Preuve. Exercice.

□

Exemple 4.14. Le nombre $i = \sqrt{-1} \in \mathbb{C}$ est algébrique sur $\mathbb{R}$, de polynôme minimal $X^2 + 1$. On a en fait $\mathbb{C} = \mathbb{R}(i) \simeq \mathbb{R}[X]/(X^2 + 1)$.

Proposition 4.15. Soit α algébrique sur K, soit C un corps algébriquement clos, et $\sigma : K \to C$ un morphisme de corps. Alors il existe un morphisme de corps $\tilde{\sigma} : K(\alpha) \to C$ tel que $\tilde{\sigma}|_K = \sigma$.

Preuve. Soit f le polynôme minimal de α sur K, de sorte que $K(\alpha) \simeq K[X]/(f)$ d'après le théorème 4.13. Soit $K' = \sigma(K)$. Puisque σ est injectif par le lemme 4.10, $\sigma : K \to K'$ est un isomorphisme, qu'on peut étendre en un isomorphisme d'anneaux

$$\begin{array}{rccc} \sigma : & K[X] & \longrightarrow & K'[X] \\ & \sum \lambda_i X^i & \longmapsto & \sum \sigma(\lambda_i) X^i. \end{array}$$

Soit $f' = \sigma(f) \in K'[X]$. Puisque C est algébriquement clos, f' possède une racine α' dans C. Comme f est irréductible et σ est un isomorphisme, f' est irréductible dans $K'[X]$, et donc $K'[X]/(f')$ est un corps. Donc le morphisme d'anneaux surjectif $K'[X]/(f') \to K'(\alpha')$ est aussi injectif (par le lemme 4.10), donc $K'[X]/(f') \simeq K'(\alpha')$. On obtient

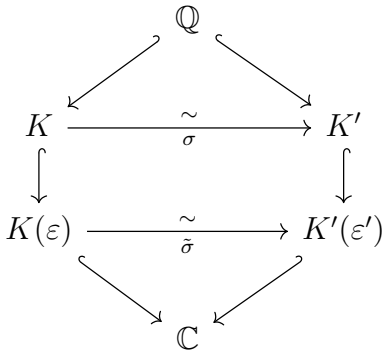
$$\begin{array}{ccc} K[X] & \xrightarrow[\sigma]{\sim} & K'[X] \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ K[X]/(f) & \xrightarrow{\overline{\sigma}} & K'[X]/(f') \end{array}$$

car $\mathrm{Ker}(\pi' \circ \sigma) = \mathrm{Ker}(\pi)$, et $\overline{\sigma}$ est un isomorphisme. Puisque $K[X]/(f) \simeq K(\alpha)$ et $K'[X]/(f') \simeq K'(\alpha') \subseteq C$, on obtient un isomorphisme $\tilde{\sigma} : K(\alpha) \to K'(\alpha')$.

□

Proposition 4.16. Soient $\varepsilon_1, \ldots, \varepsilon_d \in \mathbb{C}$ des racines n-èmes de 1, et soit $\beta = \varepsilon_1 + \ldots + \varepsilon_d$. Soit $f \in \mathbb{Q}[X]$ le polynôme minimal de β sur $\mathbb{Q}$, et soit β' une autre racine de f dans $\mathbb{C}$. Alors $\beta' = \varepsilon_1^k + \ldots + \varepsilon_d^k$ pour un certain $k \in \mathbb{Z}_{\geq 0}$.

Preuve. Notons tous d'abord que puisque les ε_i sont des racines de l'unité, ce sont des entiers algébriques, donc β est un entier algébrique (théorème 4.5). Donc β est algébrique (remarque 4.12), et il a bien un polynôme minimal. Notons $K = \mathbb{Q}(\beta)$, de sorte que $\mathbb{Q}[X]/(f) \simeq K$. De même, en notant $K' = \mathbb{Q}(\beta')$, on a $\mathbb{Q}[X]/(f) \simeq K'$. On a donc un isomorphisme $\sigma : K \to K', \beta \mapsto \beta'$. Soit alors $\varepsilon \in \mathbb{C}$ une racine primitive n-ème de 1. Par la proposition 4.15, on peut prolonger σ en un morphisme de corps $\tilde{\sigma} : K(\varepsilon) \to \mathbb{C}$. Posons $\varepsilon' = \tilde{\sigma}(\varepsilon)$, de sorte que l'image de $\tilde{\sigma}$ est $K'(\varepsilon')$. On a donc les inclusions suivantes.



Comme $\varepsilon^n = 1$, on a $(\varepsilon')^n = \tilde{\sigma}(\varepsilon)^n = \tilde{\sigma}(\varepsilon^n) = \tilde{\sigma}(1) = 1$, donc ε' est une racine n-ème de 1 dans $\mathbb{C}$, c'est-à-dire que $\varepsilon' = \varepsilon^k$ pour un certain $k \in \mathbb{Z}_{\geq 0}$. Ainsi, pour toute racine n-ème de l'unité ε^j, on a $\tilde{\sigma}(\varepsilon^j) = \tilde{\sigma}(\varepsilon)^j = \varepsilon^{jk} = (\varepsilon^j)^k$. En particulier, on a $\tilde{\sigma}(\varepsilon_i) = (\varepsilon_i)^k$ ce qui donne $\beta' = \tilde{\sigma}(\beta) = \tilde{\sigma}(\varepsilon_1 + \ldots + \varepsilon_d) = \tilde{\sigma}(\varepsilon_1) + \ldots + \tilde{\sigma}(\varepsilon_d) = \varepsilon_1^k + \ldots + \varepsilon_d^k$.

□

4.3 Le théorème de Burnside

Soit G un groupe fini.

Théorème 4.17. Soit $\chi \in \mathrm{Irr}(G)$, et soit C une classe de conjugaison de G telle que $\gcd(\chi(1), |C|) = 1$. Alors, pour tout $g \in C$, on a $g \in \mathrm{Z}(\chi)$ ou $\chi(g) = 0$.

Preuve. Notons $d = \chi(1)$. Soit $g \in C$. Comme $\gcd(d, |C|) = 1$, il existe des entiers u et v tels que $ud + v|C| = 1$. Donc $u\chi(g) + v\frac{|C|}{d}\chi(g) = \frac{\chi(g)}{d}$. Notons

$$\alpha = \frac{\chi(g)}{d}.$$

Par le théorème 4.7 et le corollaire 4.6, $\frac{|C|}{d}\chi(g)$ et $\chi(g)$ sont des entiers algébriques, donc α est un entier algébrique en vertu du théorème 4.5. Supposons que $g \notin \mathrm{Z}(\chi)$, et montrons que $\chi(g) = 0$. Tout d'abord, d'après la proposition 3.3(2), $|\chi(g)| = |\sum_{i=1}^{d} \varepsilon_i| \leq \sum_{i=1}^{d} |\varepsilon_i| = d$, puisque les ε_i sont des racines de l'unité. Puisque $g \notin \mathrm{Z}(\chi)$, on a $|\chi(g)| < d$, et donc $|\alpha| < 1$. Comme α est un entier algébrique, il existe $h \in \mathbb{Z}[X]$ unitaire tel que $h(\alpha) = 0$. De plus, α est algébrique sur $\mathbb{Q}$ (remarque 4.12), soit donc $f \in \mathbb{Q}[X]$ son polynôme minimal sur $\mathbb{Q}$. Les racines $\alpha_1, \ldots, \alpha_t$ de f étant aussi des racines de h (puisque f divise h), ce sont des entiers algébriques. De plus, $\alpha = \frac{1}{d}(\varepsilon_1 + \ldots + \varepsilon_d)$, donc d'après la proposition 4.16, on a $\alpha_i = \frac{1}{d}(\varepsilon_1^{k_1} + \ldots + \varepsilon_d^{k_d})$ pour certains $k_i \in \mathbb{Z}_{\geq 0}$. Ainsi, on a aussi $|\alpha_i| \leq 1$, et donc, puisque $|\alpha| < 1$ et que $\alpha = \alpha_i$ pour un certain $i = 1, \ldots, t$,

$$\left|\prod_{i=1}^{t} \alpha_i\right| = \prod_{i=1}^{t} |\alpha_i| < 1.$$

Autrement dit, si a_0 est le terme constant de f, on a $|a_0| < 1$. De plus, puisque $a_0 \in \mathbb{Q}$ et que c'est un entier algébrique (théorème 4.5), la proposition 4.2 nous assure que $a_0 \in \mathbb{Z}$. Donc $a_0 = 0$, et donc $X|f$. Mais puisque f est minimal (et unitaire), on a $f = X$. Donc $\alpha = f(\alpha) = 0$, et donc $\chi(g) = 0$. □

Théorème 4.18. Supposons qu'il existe une classe de conjugaison C de G telle que $|C| = p^a$, avec p un nombre premier et $a \in \mathbb{Z}_{>0}$. Alors G n'est pas un groupe simple non abélien.

Preuve. Supposons que G est simple non abélien et qu'il existe une classe de conjugaison C de G telle que $|C| = p^a$, avec p un nombre premier et $a \in \mathbb{Z}_{>0}$. En particulier, $C \neq \{1\}$. Soit $g \in C$ (en particulier $g \neq 1$) et $\chi \in \mathrm{Irr}(G)$, χ non trivial. D'après la proposition 3.23(1), $\mathrm{Ker}(\chi)$ est un sous-groupe normal de G. Donc, puisque G est simple, $\mathrm{Ker}(\chi) = \{1\}$. Donc $\mathrm{Z}(\chi) = \mathrm{Z}(G)$ d'après la proposition 3.23(5). Puique $\mathrm{Z}(G) \lhd G$ et que G est simple et non abélien, on a $\mathrm{Z}(G) = \{1\}$. Si $p \nmid \chi(1)$ alors par le théorème 4.17, on a $\chi(g) = 0$. Considérons maintenant ψ le caractère de la représentation régulière de G. D'après le théorème d'Artin-Wedderburn (et comme dans la preuve de la proposition 3.17), on a $\psi = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi$. On a

$$\begin{aligned}
0 &= \psi(g) && \text{par le lemme 3.16} \\
&= \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) \\
&= 1 + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ p \nmid \chi(1) \\ \chi \text{ non trivial}}} \chi(1)\chi(g) + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ p | \chi(1)}} \chi(1)\chi(g) \\
&= 1 + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ p | \chi(1)}} \chi(1)\chi(g) && \text{par la discussion précédente}
\end{aligned}$$

D'après le théorème 4.5 et le corollaire 4.6, le nombre rationnel

$$-\frac{1}{p} = \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ p|\chi(1)}} \frac{\chi(1)}{p}\chi(g)$$

est un entier algébrique, donc $-\frac{1}{p} \in \mathbb{Z}$ (par la proposition 4.2), ce qui est une contradiction.

□

Corollaire 4.19 (Théorème $p^a q^b$ de Burnside)**.** Soit G un groupe d'ordre $p^a q^b$ où p, q sont premiers et $a, b \in \mathbb{Z}_{\geq 0}$. Alors G est résoluble.

Preuve. On effectue une récurrence sur $|G|$. Si $|G| = 1$ alors le résultat est trivial. Soit $|G| > 1$, on peut donc supposer $a > 0$, et soit N un sous-groupe normal maximal de G. Si $|N| > 1$, alors N et G/N sont résolubles par hypothèse de récurrence, et donc G est résoluble. Supposons donc $N = \{1\}$, c'est-à-dire que G est simple. Il existe un p-sous groupe de Sylow P de G. C'est un groupe d'ordre p^a, son centre est donc non-trivial. Soit donc $g \in \mathrm{Z}(P) \setminus \{1\}$, de sorte que $P \leq C_G(g)$. On a donc $|P| \mid |C_G(g)|$, et donc, en notant C la classe de conjugaison de g,

$$|C| = [G : C_G(g)] \mid [G : P] = q^b.$$

On peut donc appliquer le théorème 4.18, qui permet de conclure que G est abélien.

□

Chapitre 5

Construction de caractères

On peut naturellement se demander comment trouver des caractères, et comment construire de nouveaux caractères à partirs de caractères donnés. Ce chapitre donne quelques éléments de réponse.

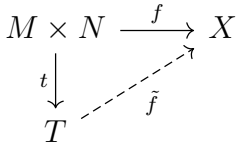
5.1 Produit tensoriel de modules

Soit R un anneau, M un R-module à droite et N un R-module à gauche.

Définition 5.1. Un *produit tensoriel* de M et N est la donnée d'un groupe abélien T et d'une application $t : M \times N \to T$ *R-équilibrée*, c'est-à-dire que pour tous $m, m' \in M, n, n' \in N, r \in R$,

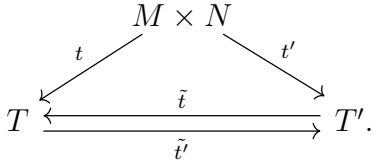
$$\begin{aligned} t(m + m', n) &= t(m, n) + t(m', n) \\ t(m, n + n') &= t(m, n) + t(m, n') \\ t(mr, n) &= t(m, rn) \end{aligned}$$

telle que la propriété universelle suivante est vérifiée : pour tout groupe abélien X et toute application R-équilibrée $f : M \times N \to X$, il existe une unique application $\tilde{f} : T \to X$ telle que le diagramme suivant commute.

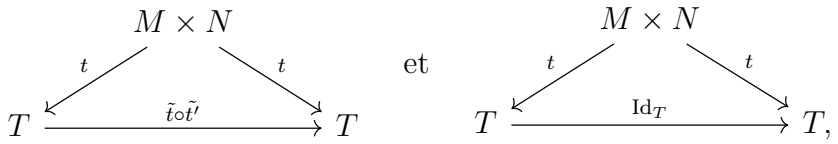


Théorème 5.2. Le produit tensoriel de M et N existe et est unique à isomorphisme près. On le note $M \otimes_R N$, et on note $m \otimes n = t(m, n)$, pour tout $(m, n) \in M \times N$.

Preuve. Commençons par prouver l'uncité. Soient (T, t) et (T', t') deux produits tensoriels de M et N. Il existe alors $\tilde{t}$ et $\tilde{t'}$ qui font commuter le diagramme suivant



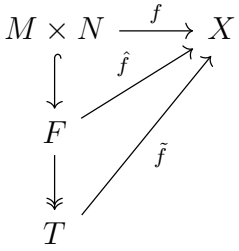
On a donc les deux diagrammes commutatifs suivants



et donc $\tilde{t} \circ \tilde{t'} = \mathrm{Id}_T$ par unicité dans la propriété universelle. De même, $\tilde{t'} \circ \tilde{t} = \mathrm{Id}_{T'}$, et on obtient un isomorphisme canonique $\tilde{t'} : T' \to T$.
Il reste à prouver l'existence. Soit F l'ensemble des combinaisons $\mathbb{Z}$-linéaires formelles d'éléments de $M \times N$ (groupe abélien libre sur $M \times N$), et soit E le sous-module de F engendré par tous les éléments de la forme

$$(mr, n) - (m, rn)$$
$$(m, n + n') - (m, n) - m(n')$$
$$(m + m', n) - (m, n) - (m', n).$$

Posons $T = F/E$ et $t : M \times N \to T, (m, n) \mapsto (m, n) + E$. Alors t est équilibrée par définition de E. De plus, soit $f : M \times N \to X$ une application R-équilibrée. On peut alors définir $\hat{f} : F \to X$ en posant $\hat{f}((m, n)) = f((m, n))$ pour $(m, n) \in M \times N$ et en étendant à F linéairement. Puisque f est équilibrée, on a $\hat{f}(E) = 0$, et donc $\hat{f}$ induit un morphisme de $T = F/E$ dans X en posant $\tilde{f}((m, n) + E) = \hat{f}((m, n))$. En résumé, on a le diagramme commutatif suivant.



On conclut en remarquant que la composition des deux flèches verticales n'est autre que t.

□

Proposition 5.3. Les élément $m \otimes n$, $m \in M$, $n \in N$ engendrent le groupe abélien $M \otimes_R N$, et vérifient

(1) $(m + m') \otimes n = m \otimes n + m' \otimes n$,
(2) $m \otimes (n + n') = m \otimes n + m \otimes n'$,
(3) $mr \otimes n = m \otimes rn$,
(4) $0 \otimes n = 0 = m \otimes 0$,
(5) $(-m) \otimes n = -(m \otimes n) = m \otimes (-n)$.

Preuve. Exercice.

□

5.2 Induction et restriction

Soit G est un groupe fini, et H un sous-groupe de G. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G de caractère χ. Alors la restriction $\rho|_H : H \to \mathrm{GL}(V)$ est une représentation de H. De manière équivalente, le $\mathbb{C}G$-module V est en particulier un $\mathbb{C}H$-module, que l'on notera $\mathrm{Res}^G_H V$. En notant $\mathrm{Res}^G_H \chi$ le caractère de $\mathrm{Res}^G_H V$, on a

$$\chi_{\mathrm{Res}^G_H V} = \chi|_H.$$

Remarque 5.4. Si $\chi \in \mathrm{Irr}(G)$, on n'a pas $\mathrm{Res}^G_H \chi \in \mathrm{Irr}(H)$ en général.

Définition 5.5.

(1) Soit $\varphi = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi$, $a_\chi \in \mathbb{Z}_{\geq 0}$, un caractère de G (voir le corollaire 3.13(1)). Si $a_\chi \neq 0$, on dit que χ est un *constituant irréductible* de φ.

(2) De manière générale, si ψ est un caractère de G tel que $(\varphi, \psi) > 0$, on dit que ψ est un *constituant* de φ.

(3) Soit $\theta \in \mathrm{Irr}(H)$. On note

$$\mathrm{Irr}\,(G|\theta) = \left\{\chi \in \mathrm{Irr}(G) \mid (\mathrm{Res}^G_H \chi, \theta) \neq 0\right\}$$

l'ensemble des caractères irréductibles de G dont la restriction à H admet θ comme constituant irréductible.

On va définir une opération duale appelée induction, qui permet de constuire un caractère de G à partir d'un caractère de H. Pour cela, considérons la structure de $\mathbb{C}H$-module à droite sur $\mathbb{C}G$.

Définition 5.6. Soit V un $\mathbb{C}H$-module de dimension finie d. Le produit tensoriel $\mathbb{C}G \otimes_{\mathbb{C}H} V$ est muni d'une structure de $\mathbb{C}G$-module à gauche via la formule

$$g(x \otimes v) = (gx) \otimes v$$

pour tout $g \in G$, $x \in \mathbb{C}G$, $v \in V$. Ce $\mathbb{C}G$-module est appelé *module induit* de H à G, et noté $\mathrm{Ind}^G_H V$.

On a en fait une description plus explicite des modules induits. Soit V un $\mathbb{C}H$-module. Notons $k = [G : H]$ et soient $g_1, \ldots, g_k \in G$ des représentants de G/H.

Proposition 5.7. On a la décomposition en espaces vectoriels

$$\mathrm{Ind}^G_H V = \bigoplus_{i=1}^{k} g_i \otimes V$$

où $g_i \otimes V = \{g_i \otimes v\,;\, v \in V\} \simeq V$. De plus, $\mathbb{C}G$ permute transivitement les sous-espace $g_i \otimes V$ via la formule

$$g(g_i \otimes v) = g_j \otimes hv$$

pour tout $g \in G$ et $i = 1, \ldots, k$, où $j \in \{1, \ldots, k\}$ et $h \in H$ sont uniquement déterminés par $gg_i = g_j h$.

Preuve. En tant que $\mathbb{C}H$-modules à droite, on a

$$\mathbb{C}G = \mathbb{C}\left(\bigsqcup_{i=1}^{k} g_i H\right) = \bigoplus_{i=1}^{k} \mathbb{C}(g_i H) = \bigoplus_{i=1}^{k} g_i \mathbb{C}H.$$

On a donc

$$\mathrm{Ind}^G_H V = \mathbb{C}G \otimes_{\mathbb{C}H} V = \bigoplus_{i=1}^{k} g_i \mathbb{C}H \otimes_{\mathbb{C}H} V = \bigoplus_{i=1}^{k} g_i \otimes V.$$

et $g_i \otimes V = (g_i \mathbb{C}H) \otimes_{\mathbb{C}H} V \simeq \mathbb{C}H \otimes_{\mathbb{C}H} V \simeq V$. Montrons finalement que G permute les sous-espace $g_i \otimes V$. Pour tout $g \in G$ et $i = 1, \ldots, k$, soient $j \in \{1, \ldots, k\}$ et $h \in H$ tels que $gg_i = g_j h$. On a alors

$$g(g_i \otimes v) = (gg_i) \otimes v = g_j h \otimes v = g_j \otimes hv,$$

et donc on a déjà $g(g_i \otimes V) \subseteq g_j \otimes V$. De même, on a $g^{-1}(g_j \otimes V) \subseteq g_i \otimes V$, ce qui donne $g_j \otimes V = gg^{-1}(g_j \otimes V) = g(g^{-1}(g_j \otimes V)) \subseteq g(g_i \otimes V)$, d'où l'égalité. Cette action est transitive car pour $i, j \in \{1, \ldots, k\}$, $g_j \otimes V = (g_j g_i^{-1}) g_i \otimes V$.

□

Remarque 5.8. En particulier, ceci montre que $\dim_{\mathbb{C}} \operatorname{Ind}_H^G V = [G : H] \dim_{\mathbb{C}} V$.

Exemple 5.9. On a $\mathbb{C}G = \operatorname{Ind}_{\{1\}}^G \mathbb{C}$.

Si V est un $\mathbb{C}H$-module de caractère χ, notons $\operatorname{Ind}_H^G \chi$ le caractère de $\operatorname{Ind}_H^G V$.

Théorème 5.10. Pour tout $g \in G$, on a

$$\operatorname{Ind}_H^G \chi(g) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \chi(x^{-1}gx).$$

Preuve. Soit $g \in G$. On veut calculer la trace de l'action de g sur $\operatorname{Ind}_H^G V$. Considérons la décomposition $\operatorname{Ind}_H^G V = \bigoplus_{i=1}^k g_i \otimes V$ de la proposition 5.7. Puisque g permute les $g_i \otimes V$, si $g_i \otimes V$ n'est pas invariant par g, alors $g(g_i \otimes V) = g_j \otimes V$ (pour un $j \neq i$) et la matrice de l'action de g a un bloc $0 \in \mathbb{C}^{\chi(1) \times \chi(1)}$ à cet endroit :

$$\begin{array}{c} \begin{array}{cccccc} \cdots & g_i \otimes V & \cdots & g_j \otimes V & \cdots & \end{array} \\ \begin{pmatrix} \ddots & & & & & \\ & \boxed{0} & & & & \\ & & \ddots & & & \\ & \boxed{*} & & \ddots & & \\ & & & & \ddots & \end{pmatrix} \begin{array}{c} \vdots \\ g_i \otimes V \\ \vdots \\ g_j \otimes V \\ \vdots \end{array} \end{array}$$

Donc seuls les sous-espaces $g_i \otimes V$ tels que $g(g_i \otimes V) = g_i \otimes V$ contribuent au calcul de $\operatorname{Ind}_H^G \chi(g)$. Ceci est équivalent à $g_i^{-1} g g_i \otimes V = 1 \otimes V$, c'est-à-dire $g_i^{-1} g g_i \in H$. Pour un tel sous-espace $g_i \otimes V$, on a alors, pour tout $v \in V$,

$$g(g_i \otimes v) = g_i(g_i^{-1} g g_i) \otimes v = g_i \otimes (g_i^{-1} g g_i) v,$$

donc la trace de l'action de g sur $g_i \otimes V$ est $\chi(g_i^{-1} g g_i)$. On a donc

$$\operatorname{Ind}_H^G \chi(g) = \sum_{\substack{1 \leq i \leq k \\ g_i^{-1} g g_i \in H}} \chi(g_i^{-1} g g_i).$$

Puisque pour tout $h \in H$, $\chi((g_i h)^{-1} g (g_i h)) = \chi(h^{-1}(g_i^{-1} g g_i) h) = \chi(g_i^{-1} h g_i)$, l'identité précédente se réécrit

$$\operatorname{Ind}_H^G \chi(g) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \chi(x^{-1}gx).$$

□

Exemple 5.11. Soit $G = S_3$ et $H = \{1, (123), (132)\}$. On choisit 1 et (12) comme représentants des classes à gauche. Soit χ le caractère de la représentation triviale de H. On a alors

$$\begin{aligned} &\operatorname{Ind}_H^G \chi(1) = \chi(1) + \chi(1) = 2, \\ &\operatorname{Ind}_H^G \chi((12)) = 0 \text{ (somme vide)}, \\ &\operatorname{Ind}_H^G \chi((123)) = \chi((123)) + \chi((132)) = 2. \end{aligned}$$

Donc, d'après l'exemple 3.15, $\chi = \chi_1 + \chi_2$ où χ_1 est le caractère de la représentation triviale de G et χ_2 est le caractère de la représentation signature de G.

Intéressons-nous au lien entre restriction et induction de représentations. La proposition suivante décrit la propriété universelle d'une représentation induite.

Proposition 5.12. Soit V un $\mathbb{C}H$-module. Alors pour tout $\mathbb{C}G$-module W et pour tout morphisme de $\mathbb{C}H$-modules $f : V \to \mathrm{Res}_H^G W$, il existe un unique morphisme de $\mathbb{C}G$-modules $\tilde{f} : \mathrm{Ind}_H^G V \to W$ tel que le diagramme suivant commute.

$$\begin{array}{ccc} V & \xrightarrow{\quad f \quad} & \mathrm{Res}_H^G W = W \\ {\scriptstyle i}\downarrow & \nearrow_{\tilde{f}} & \\ \mathrm{Ind}_H^G V & & \end{array}$$

où i est le morphisme de $\mathbb{C}H$-modules $i : V \to \mathrm{Ind}_H^G V$, $v \to 1 \otimes V$.

Preuve. Puisque f est un morphisme de $\mathbb{C}H$-modules, l'application

$$\begin{array}{rccc} \overline{f} & : \mathbb{C}G \times V & \longrightarrow & W \\ & (a, v) & \longmapsto & af(v). \end{array}$$

est $\mathbb{C}H$-équilibrée. Par la propriété universelle du produit tensoriel (définition 5.1), on peut donc considérer l'unique application $\tilde{f} : \mathbb{C}G \otimes_{\mathbb{C}H} V \to W, a \otimes v \mapsto af(v)$. Alors $\tilde{f}$ est clairement un morphisme de $\mathbb{C}G$-modules, et $\tilde{f} \circ i = f$ car $(\tilde{f} \circ i)(v) = \tilde{f}(1 \otimes v) = 1f(v) = f(v)$.

□

Corollaire 5.13. Soit V un $\mathbb{C}H$-module et W un $\mathbb{C}G$-module. On a un isomorphisme d'espaces vectoriels

$$\mathrm{Hom}_{\mathbb{C}G}(\mathrm{Ind}_H^G V, W) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}H}(V, \mathrm{Res}_H^G W).$$

Preuve. On considère l'application $\mathrm{Hom}_{\mathbb{C}G}(\mathrm{Ind}_H^G V, W) \to \mathrm{Hom}_{\mathbb{C}H}(V, \mathrm{Res}_H^G W)$, $\varphi \mapsto \varphi \circ i$, où $i : V \to \mathrm{Ind}_H^G V, v \mapsto 1 \otimes v$. Elle est $\mathbb{C}$-linéaire, et elle est surjective et injective par la proposition 5.12.

□

Rappelons que l'on a défini un produit scalaire $(.,.)$ sur l'ensemble des fonctions de G dans $\mathbb{C}$ au chapitre 3 (théorème 3.18).

Lemme 5.14. Soient W_1 et W_2 deux $\mathbb{C}G$-modules, χ_1 et χ_2 leur caractère. On a

$$\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}G}(W_1, W_2) = (\chi_1, \chi_2)\,.$$

Preuve. Exercice.

□

Pour le corollaire suivant, on distingue le produit scalaire $(.,.)$ selon que l'on considère des fonctions sur G ou sur H.

Corollaire 5.15 (Réciprocité de Frobenius)**.** Soit V un $\mathbb{C}H$-module et W un $\mathbb{C}G$-module. On a

$$\left(\mathrm{Ind}_H^G \chi_V, \chi_W\right)_G = \left(\chi_V, \mathrm{Res}_H^G \chi_W\right)_H.$$

Preuve. On a

$$\begin{aligned} \left(\mathrm{Ind}_H^G \chi_V, \chi_W\right)_G &= \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}G}(\mathrm{Ind}_H^G V, W) && \text{par le lemme 5.14} \\ &= \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}H}(V, \mathrm{Res}_H^G W) && \text{par le corollaire 5.13} \\ &= \left(\chi_V, \mathrm{Res}_H^G \chi_W\right)_H && \text{par le lemme 5.14.} \end{aligned}$$

□

5.3 La formule de Mackey

Soit G un groupe fini et $K, H \leq G$. Soit V un $\mathbb{C}H$-module. La formule de Mackey permet de décrire $\mathrm{Res}^G_K \mathrm{Ind}^G_H V$ explicitement, ce qui permet de caractériser quand une représentation induite est irréductible.

Définition 5.16. Pour tout $g \in G$, la *double classe* pour (K, H) de g est l'ensemble

$$KgH = \{kgh\,;\, k \in K, h \in H\} \subseteq G.$$

Proposition 5.17.

(1) Toute double classe pour (K, H) est
   — une union disjointe de classes à droite de K,
   — une union disjointe de classes à gauche de H.

(2) Deux doubles classes pour (K, H) quelconques sont soit disjointes, soit égales. Ainsi, les doubles classes partitionnent G.

(3) L'ensemble des doubles classes pour (K, H) est en bijection avec
   — l'ensemble $K\backslash(G/H)$ des orbites de l'action (à gauche) de K sur G/H, via l'application $KgH \mapsto K(gH)$,
   — l'ensemble $(K\backslash G)/H$ des orbites de l'action (à droite) de H sur $K\backslash G$, via l'application $KgH \mapsto (Kg)H$.

   On note donc $K\backslash G/H$ l'ensemble des doubles classes pour (K, H).

Preuve. Exercice.

□

Exemple 5.18. Prenons $G = S_3$, $K = H = S_2 = \{1, (12)\} \leq S_3$. On a

$$S_2\backslash S_3/S_2 = \{\{1, (12)\}, \{(123), (132), (13), (23)\}\}.$$

Pour la suite, notons, pour $g, x \in G$,

$$^g x = gxg^{-1} \quad \text{et} \quad x^g = g^{-1}xg.$$

Notons de plus $[G/H]$ (respectivement $[K\backslash G]$, respectivement $[K\backslash G/H]$) un ensemble de représentants des classes à gauche de H (respectivement des classes à droite de K, respectivement des doubles classes pour (K, H)).

Proposition 5.19. Soit $g \in G$. La double classe KgH est l'union de $[K : (K \cap {}^g H)]$ classes à gauche de H, et de $[H : K^g \cap H]$ classes à droite de K. On a

$$[G : H] = \sum_{g \in [K\backslash G/H]} [K : (K \cap {}^g H)] \quad \text{et} \quad [G : K] = \sum_{g \in [K\backslash G/H]} [H : K^g \cap H].$$

Preuve. Le sous-groupe K agit sur l'ensemble G/H des classes à gauche de H, voir la proposition 5.17(3). La double classe KgH correspond à l'orbite de gH pour cette action, et est l'union disjointe d'un certain nombre, disons m, de classes à gauche de H par la proposition 5.17(1). Ainsi, m est le cardinal de l'orbite de gH sous l'action de K. Notons que puisque chaque classe à gauche de H est

en bijection avec H, on a $m = |KgH|/|H|$. Maintenant, m est l'indice du stabilisateur de gH dans K, qui est

$$\begin{aligned}\mathrm{Stab}_K(gH) &= \{k \in K \mid kgH = gH\} \\ &= \{k \in K \mid k^g H = H\} \\ &= \{k \in K \mid k^g \in H\} \\ &= K \cap {}^g H.\end{aligned}$$

On a donc $m = [K : K \cap {}^g H]$ comme énoncé. En faisant la somme sur toutes les doubles classes, on obtient le nombre total de classes à gauche pour H, c'est-à-dire $[G : H]$. L'argument est analogue pour les classes à droite de K.

□

Définition 5.20. Soit V un $\mathbb{C}H$-module, et $g \in G$. On note ${}^g V$ le $\mathbb{C}^g H$-module V dont la structure est donnée par la formule

$${}^g h v = hv \quad \text{pour tout } h \in H, v \in V.$$

Le $\mathbb{C}^g H$-module ${}^g V$ est appelé le *conjugué* de V par g.

Lemme 5.21. Pour tout $g \in [G/H]$, on a un isomorphisme de $\mathbb{C}^g H$-modules $g \otimes V \simeq {}^g V$.

Preuve. Rappelons que les espace $g \otimes V$, $g \in [G/H]$, apparaissent dans la décomposition de $\mathrm{Ind}_H^G V$ obtenue à la proposition 5.7. Tout d'abord, chaque $g \otimes V$ est bien un $\mathbb{C}^g H$-module, puisque

$${}^g h(g \otimes v) = (ghg^{-1})(g \otimes v) = (ghg^{-1}g) \otimes v = (gh) \otimes v = g \otimes (hv).$$

L'isomorphisme de $\mathbb{C}^g H$-modules désiré est simplement

$$\begin{array}{ccc} g \otimes V & \longrightarrow & {}^g V \\ g \otimes v & \longmapsto & v. \end{array}$$

□

Théorème 5.22 (Formule de Mackey)**.** On a

$$\mathrm{Res}_K^G \mathrm{Ind}_H^G V \simeq \bigoplus_{g \in [K \backslash G / H]} \mathrm{Ind}_{K \cap {}^g H}^K \left(\mathrm{Res}_{K \cap {}^g H}^{{}^g H} {}^g V \right).$$

Preuve. On a, par la proposition 5.7, $\mathrm{Ind}_H^G V = \bigoplus_{x \in [G/H]} x \otimes V$. Soit KgH une double classe. En regroupant tous les termes tels que $x \in KgH$, c'est-à-dire en considérant

$$\bigoplus_{\substack{x \in [G/H] \\ x \in KgH}} x \otimes V,$$

on obtient un espace stable par K (puisque les termes de cette somme sont permutés par l'action de K). De plus, $\mathrm{Stab}_K(g \otimes V) = \{k \in K \mid kg \in gH\} = K \cap {}^g H$, donc (exercice)

$$\bigoplus_{\substack{x \in [G/H] \\ x \in KgH}} x \otimes V \simeq \mathrm{Ind}_{K \cap {}^g H}^K g \otimes V.$$

D'autre part, d'après le lemme 5.21, on a un isomorphisme de $\mathbb{C}[K \cap {}^gH]$-modules $g \otimes V \simeq \mathrm{Res}^{{}^gH}_{K\cap {}^gH}{}^gV$. En sommant la formule précédente sur tous les $g \in [K\backslash G/H]$, on obtient donc la formule attendue.

□

On peut donc énoncer le critère d'irréductibilité pour une représentation induite. Notons χ le caractère du $\mathbb{C}H$-module V et, pour tout $g \in G$, notons ${}^g\chi$ le caractère de ${}^gV$.

Corollaire 5.23. (Critère d'irréductibilité de Mackey) On suppose que $\chi \in \mathrm{Irr}(H)$. Alors $\mathrm{Ind}_H^G V$ est simple si et seulement si $\left(\mathrm{Res}^{{}^gH}_{H\cap {}^gH}{}^g\chi, \mathrm{Res}^H_{H\cap {}^gH}\chi\right) = 0$ pour tout $g \in G \setminus H$.

Preuve. Soit ψ un caractère de K. Par réciprocité de Frobenius (théorème 5.15), On a

$$\begin{aligned}
\left(\mathrm{Ind}_H^G\chi, \mathrm{Ind}_K^G\psi\right)_G &= \left(\mathrm{Res}_K^G\mathrm{Ind}_H^G\chi, \psi\right)_K && \text{par le théorème 5.15}\\
&= \sum_{g\in[K\backslash G/H]} \left(\mathrm{Ind}^K_{K\cap {}^gH}\left(\mathrm{Res}^{{}^gH}_{K\cap {}^gH}{}^g\chi\right), \psi\right)_K && \text{par le théorème 5.22}\\
&= \sum_{g\in[K\backslash G/H]} \left(\mathrm{Res}^{{}^gH}_{K\cap {}^gH}{}^g\chi, \mathrm{Res}^K_{K\cap {}^gH}\psi\right)_{K\cap {}^gH} && \text{par le théorème 5.15}
\end{aligned}$$

Dans le cas particulier $K = H$ et $\psi = \chi$, ceci donne

$$\begin{aligned}
\left(\mathrm{Ind}_H^G\chi, \mathrm{Ind}_H^G\chi\right)_G &= \sum_{g\in[H\backslash G/H]} \left(\mathrm{Res}^{{}^gH}_{H\cap {}^gH}{}^g\chi, \mathrm{Res}^H_{H\cap {}^gH}\chi\right)_{H\cap {}^gH}\\
&= (\chi,\chi) + \sum_{\substack{g\in[H\backslash G/H]\\ g\notin H}} \left(\mathrm{Res}^{{}^gH}_{H\cap {}^gH}{}^g\chi, \mathrm{Res}^H_{H\cap {}^gH}\chi\right)_{H\cap {}^gH} && \text{car } H\cap {}^gH = H \text{ si } g\in H\\
&= 1 + \sum_{\substack{g\in[H\backslash G/H]\\ g\notin H}} \left(\mathrm{Res}^{{}^gH}_{H\cap {}^gH}{}^g\chi, \mathrm{Res}^H_{H\cap {}^gH}\chi\right)_{H\cap {}^gH} && \text{car } \chi\in\mathrm{Irr}(H) \text{ (corollaire 3.20).}
\end{aligned}$$

On conclut en utilisant de nouveau le corollaire 3.20.

□

5.4 Le théorème de Clifford

La théorie de Clifford étudie les liens entre les représentations d'un groupe et celles de ses sous-groupes normaux. Dans cette section, G est un groupe fini et N un sous-groupe normal de G. On note toujours $[G/N]$ un ensemble de représentants des classes (à gauche) pour N. Rappelons qu'on a définit dans la section précédente le conjugué d'un caractère. Dans le cas où θ est un caractère de N, puisque $N \lhd G$, pour tout $g \in G$, ${}^g\theta$ est aussi un caractère de N.

Lemme 5.24. Soit θ un caractère de N. L'ensemble des conjugués de θ est $\{{}^g\theta\,;\, g \in [G/N]\}$.

Preuve. Il suffit de montrer que deux éléments dans la même classe pour N induisent le même caractère conjugué : pour $g \in [G/N]$, $n \in N$, on a pour tout $h \in N$

$${}^{gn}\theta(h) = \theta((gn)^{-1}h(gn)) = \theta(n^{-1}(g^{-1}hg)n) = \theta(g^{-1}hg) = {}^g\theta.$$

□

Théorème 5.25 (Clifford)**.** Soit $\chi \in \mathrm{Irr}(G)$ et $\theta \in \mathrm{Irr}(N)$ tel que $e := (\mathrm{Res}^G_N\chi, \theta) \neq 0$. Soient $\theta_1, \ldots, \ldots \theta_t$ les caractères conjugués de θ. Alors

$$\mathrm{Res}^G_N\chi = e\sum_{i=1}^{t}\theta_i.$$

Preuve. D'après la formule de Mackey (théorème 5.22), on a

$$\mathrm{Res}^G_N\mathrm{Ind}^G_N\theta = \sum_{g\in[G/N]}\mathrm{Ind}^N_{gN\cap N}\mathrm{Res}^{gN}_{gN\cap N}{}^g\theta = \sum_{g\in[G/N]}{}^g\theta.$$

D'après le lemme 5.24, $\{\theta_1, \ldots, \theta_t\} = \{{}^g\theta\,;\, g \in [G/N]\}$, donc si $\varphi \in \mathrm{Irr}(N) \setminus \{\theta_1, \ldots, \theta_t\}$, on a $\left(\sum_{g\in[G/N]}{}^g\theta, \varphi\right) = 0$, et donc

$$\left(\mathrm{Res}^G_N\mathrm{Ind}^G_N\theta, \varphi\right) = 0.$$

Par réciprocité de Frobenius (théorème 5.15), on a $(\chi, \mathrm{Ind}^G_N\theta) = (\mathrm{Res}^G_N\chi, \theta) > 0$, c'est-à-dire que χ est un constituant de $\mathrm{Ind}^G_N\theta$, donc

$$\left(\mathrm{Res}^G_N\chi, \varphi\right) = 0.$$

Donc tous les constituants irréductibles de $\mathrm{Res}^G_N\chi$ sont parmi les θ_i, c'est-à-dire

$$\mathrm{Res}^G_N\chi = \sum_{i=1}^{t} e_i\theta_i,$$

où $e_i = \left(\mathrm{Res}^G_N\chi, \theta_i\right)$. En fait, on a

$$\begin{aligned} e_i &= \left(\mathrm{Res}^G_N\chi, \theta_i\right) = \left(\mathrm{Res}^G_N\chi, {}^g\theta\right) && \text{pour un } g \in G \\ &= \left({}^g\left(\mathrm{Res}^G_N\chi\right), {}^g\theta\right) && \text{car } \chi \text{ est centrale} \\ &= \left(\mathrm{Res}^G_N\chi, \theta\right) = e. \end{aligned}$$

□

Corollaire 5.26.

(1) Soit $\chi \in \mathrm{Irr}(G)$ et $\theta \in \mathrm{Irr}(N)$ tel que $(\mathrm{Res}^G_N\chi, \theta) \neq 0$. Alors $\theta(1) \mid \chi(1)$.

(2) Soit $\chi \in \mathrm{Irr}(G)$ tel que $(\mathrm{Res}^G_N\chi, \mathrm{Res}^G_N 1) \neq 0$. Alors $N \leq \mathrm{Ker}(\chi)$.

Preuve.

(1) Puisque pour tout $g \in G$, ${}^g\theta(1) = \theta(1)$, on a par le théorème 5.25 $\chi(1) = et\theta(1)$.

(2) Puisque ${}^g\left(\mathrm{Res}^G_N 1\right) = \mathrm{Res}^G_N 1$ pour tout $g \in G$, on a par le théorème 5.25 $\mathrm{Res}^G_N\chi = e\mathrm{Res}^G_N 1$, où $e = (\mathrm{Res}^G_N\chi, \mathrm{Res}^G_N 1) = \chi(1)$. Autrement dit, pour tout $n \in N, \chi(n) = \chi(1)$, c'est-à-dire $n \in \mathrm{Ker}(\chi)$.

□

On s'intéresse maintenant plus précisément aux entiers e et t.

Définition 5.27. Soit $\theta \in \mathrm{Irr}(N)$. L'ensemble

$$I_G(\theta) = \{g \in G \mid {}^g\theta = \theta\}$$

est appelé *groupe d'inertie* de θ dans G.

Les liens entre $\mathrm{Irr}(G)$ et $\mathrm{Irr}(N)$ sont contrôlés par les groupes d'inertie.

Lemme 5.28. Soit $\theta \in \mathrm{Irr}(N)$. On a $N \leq I_G(\theta) \leq G$ et $t = [G : I_G(\theta)]$. En particulier, on a $t \mid [G : N]$.

Preuve. Le groupe G agit sur $\mathrm{Irr}(N)$ par conjugaison : $G \times \mathrm{Irr}(N) \to \mathrm{Irr}(N)$, $(g, \theta) \mapsto {}^g\theta$. L'ensemble $I_G(\theta)$ est le stabilisateur de θ dans G pour cette action, et t est le cardinal de l'orbite de θ. On a donc $I_G(\theta) \leq G$ et $t = [G : I_G(\theta)]$. De plus, puisque θ est une fonction centrale sur N, on a $N \leq I_G(\theta)$.

□

Pour le théorème suivant, fixons $\theta \in \mathrm{Irr}(N)$. Notons $I = I_G(\theta)$ et soit $\psi \in \mathrm{Irr}(I)$ tel que $(\mathrm{Res}^I_N \psi, \theta) \neq 0$. Rappelons qu'on a introduit la notation $\mathrm{Irr}(G|\theta)$ en définition 5.5.

Théorème 5.29. On a

(1) Si $\psi \in \mathrm{Irr}(I|\theta)$, alors $\mathrm{Ind}^G_I \psi \in \mathrm{Irr}(G|\theta)$.

(2) Si $\psi \in \mathrm{Irr}(I|\theta)$, alors en notant $\chi = \mathrm{Ind}^G_I \psi$, on a $(\mathrm{Res}^I_N \psi, \theta) = (\mathrm{Res}^G_N \chi, \theta)$.

(3) L'application $\mathrm{Irr}(I|\theta) \to \mathrm{Irr}(G|\theta)$, $\psi \mapsto \mathrm{Ind}^G_I \psi$ est bijective.

Preuve.

(1) Soit $\psi \in \mathrm{Irr}(I|\theta)$ et $\chi \in \mathrm{Irr}(G)$ un constituant irréductible de $\mathrm{Ind}^G_I \psi$, c'est-à-dire $(\mathrm{Ind}^G_I \psi, \chi) > 0$. Par réciprocité de Frobenius (théorème 5.15), ψ est un constituant irréductible de $\mathrm{Res}^G_I \chi$. Donc, puisque θ est un constituant irréductible de $\mathrm{Res}^I_N \psi$, on a aussi que θ est un constituant irréductible de $\mathrm{Res}^I_N \mathrm{Res}^G_I \chi = \mathrm{Res}^G_N \chi$, c'est-à-dire $\chi \in \mathrm{Irr}(G|\theta)$. Notons $f = (\mathrm{Res}^I_N \psi, \theta)$ et $e = (\mathrm{Res}^G_N \chi, \theta)$. Puisque ψ est un constituant irréductible de $\mathrm{Res}^G_I \chi$, on a $f \leq e$. Maintenant, appliquons le théorème de Clifford 5.25 à χ et ψ. On a $\mathrm{Res}^G_N \chi = e \sum_{i=1}^t \theta_i$, où $\theta_1, \ldots, \theta_t$ sont les conjugués de θ, et $\mathrm{Res}^I_N \psi = f\theta$ puisque θ est invariant par I. On a donc $et\theta(1) = \chi(1) \leq \mathrm{Ind}^G_I \psi(1) = t\psi(1) = tf\theta(1) \leq et\theta(1)$. Ceci force $e = f$ et $\chi(1) = \mathrm{Ind}^G_I \psi(1)$, c'est-à-dire $\chi = \mathrm{Ind}^G_I \psi$.

(2) On a montré en (1) que $e = f$, c'est-à-dire $(\mathrm{Res}^G_N \chi, \theta) = (\mathrm{Res}^I_N \psi, \theta)$.

(3) Injectivité : Soient $\psi_1, \psi_2 \in \mathrm{Irr}(I|\theta)$ tels que $\mathrm{Ind}^G_I \psi_1 = \mathrm{Ind}^G_I \psi_2 = \chi$. En particulier, ψ_1 et ψ_2 sont des constituants irréductibles de $\mathrm{Res}^G_I \chi$. Supposons que $\psi_1 \neq \psi_2$. Alors

$$\begin{aligned}(\mathrm{Res}^G_N \chi, \theta) &= (\mathrm{Res}^I_N \mathrm{Res}^G_I \chi, \theta) \\ &\geq (\mathrm{Res}^I_N(\psi_1 + \psi_2), \theta) \\ &= ((\mathrm{Res}^I_N \psi_1 + \mathrm{Res}^I_N \psi_2), \theta) \\ &> (\mathrm{Res}^I_N \psi_1, \theta).\end{aligned}$$

Ceci contredit (2), donc $\psi_1 = \psi_2$.

Surjectivité : Soit $\chi \in \mathrm{Irr}(G|\theta)$. Puisque $0 < (\mathrm{Res}^G_N \chi, \theta) = (\mathrm{Res}^I_N \mathrm{Res}^G_I \chi, \theta)$, il existe $\psi \in \mathrm{Irr}(I|\theta)$ tel que $(\psi, \mathrm{Res}^G_I \chi) > 0$. Par réciprocité de Frobenius, $(\mathrm{Ind}^G_I \psi, \chi) > 0$, et donc $\chi = \mathrm{Ind}^G_I \psi$ d'après (1).

□

Réciproquement, si θ est un caractère de N, on peut s'intéresser au caractère induit $\mathrm{Ind}^G_N \theta$. En notant $\chi_1, \ldots, \chi_r$ les caractères irréductibles de G, on peut écrire

$$\mathrm{Ind}^G_N \theta = \sum_{i=1}^{s} e_i \chi_i \quad \text{avec } s \leq r \text{ et } e_i \in \mathbb{Z}_{>0}.$$

Notons $I = I_G(\theta)$. D'après le théorème 5.25, on a

$$\mathrm{Res}_N^G \chi_i = e_i \sum_{j=1}^{t} \theta_j,$$

où $\theta_1, \ldots, \theta_t$ sont les conjugués de θ, et où $t = [G : I]$ d'après le lemme 5.28. De plus, on a d'après le théorème 5.29(2)

$$\mathrm{Ind}_N^I \theta = \sum_{i=1}^{s} e_i \psi_i$$

où les $\psi_i \in \mathrm{Irr}(I)$ vérifient $\mathrm{Ind}_I^G \psi_i = \chi_i$. On peut donc déterminer les e_i dans I, et on supposera donc que $I = G$, c'est-à-dire que θ est invariant par G.

Définition 5.30. Soit $\theta \in \mathrm{Irr}(N)$. Le caractère θ est dit *prolongeable* s'il existe $\chi \in \mathrm{Irr}(G)$ tel que $\mathrm{Res}_N^G \chi = \theta$.

Remarque 5.31. Si θ est prolongeable, alors θ est invariant par G.

Exemple 5.32. Soit $G = D_8$ et $N = \mathrm{Z}(G)$. Soit $\theta \in \mathrm{Irr}(N) \setminus \{1\}$. Alors θ est invariant par G mais pas prolongeable : un prolongement de θ serait de degré 1, mais le noyau d'un tel caractère contient N.

Définition 5.33. Soit $\beta : G/N \to \mathrm{GL}(V)$ une représentation de G/N. Alors $\widehat{\beta} : G \to \mathrm{GL}(V)$, $g \mapsto \beta(gN)$ est une représentation de G appelée *inflation* de β à G.

Proposition 5.34. On a $N \leq \mathrm{Ker}(\beta)$. De plus, l'inflation induit une bijection

$$\mathrm{Irr}(G/N) \overset{1:1}{\longleftrightarrow} \{\chi \in \mathrm{Irr}(G) \mid N \leq \mathrm{Ker}(\chi)\}.$$

Preuve. Exercice.

□

Lemme 5.35. Soit ρ la représentation régulière de G/N. Alors $\widehat{\rho} = \mathrm{Ind}_N^G 1$.

Preuve. Soit $g \in G$. D'après le théorème 5.10, le caractère de $\mathrm{Ind}_N^G 1$ vérifie

$$\mathrm{Ind}_N^G 1(g) = \frac{1}{|N|} \sum_{\substack{x \in G \\ x^{-1}gx \in N}} 1 = \begin{cases} |G|/|N| = |G/N| & \text{si } g \in N \\ 0 & \text{si } g \notin N \end{cases}$$

D'après le lemme 3.16, c'est bien le caractère de l'inflation de ρ à G.

□

Le théorème suivant permet d'exprimer les e_i comme certains degrés de caractères irréductibles.

Théorème 5.36. Soit $\theta \in \mathrm{Irr}(N)$ prolongeable, et soit $\chi \in \mathrm{Irr}(G)$ un prolongement de θ. Alors

(1) $\mathrm{Ind}_N^G \theta = \sum_{\beta \in \mathrm{Irr}(G/N)} \beta(1)(\chi\widehat{\beta})$,

(2) $\chi\widehat{\beta} \in \mathrm{Irr}(G)$ pour tout $\beta \in \mathrm{Irr}(G/N)$; et pour tous $\beta, \gamma \in \mathrm{Irr}(G/N)$ on a $\chi\widehat{\beta} = \chi\widehat{\gamma}$ si et seulement si $\beta = \gamma$.

Preuve.

(1) On a

$$\begin{aligned}\mathrm{Ind}_N^G\theta &= \mathrm{Ind}_N^G\mathrm{Res}_N^G\chi = \mathrm{Ind}_N^G((\mathrm{Res}_N^G\chi)(1))\\ &= \chi\mathrm{Ind}_N^G 1 = \chi\widehat{\rho} \quad \text{par le lemme 5.35}\\ &= \chi\sum_{\beta\in\mathrm{Irr}(G/N)}\beta(1)\widehat{\beta} \quad \text{car } \rho \text{ est le caractère régulier de } G/N\\ &= \sum_{\beta\in\mathrm{Irr}(G/N)}\beta(1)(\chi\widehat{\beta}).\end{aligned}$$

(2) On a

$$\begin{aligned}(\mathrm{Ind}_N^G\theta, \mathrm{Ind}_N^G\theta) &= (\theta, \mathrm{Res}_N^G\mathrm{Ind}_N^G\theta) \quad \text{par le théorème 5.15}\\ &= (\theta, [G:N]\theta) \qquad \text{car } \mathrm{Res}_N^G\mathrm{Ind}_N^G\theta = a\theta \text{ pour un entier } a,\\ &\qquad\qquad \text{puisque } \theta \text{ est invariant par } G \text{ (remarque 5.31)}\\ &\qquad\qquad \text{et } a = [G:H] \text{ par la remarque 5.8}\\ &= [G:N](\theta,\theta)\\ &= [G:N] \qquad \text{car } \theta\in\mathrm{Irr}(N).\end{aligned}$$

Donc, d'après (1),

$$[G:N] = (\mathrm{Ind}_N^G\theta, \mathrm{Ind}_N^G\theta) \geq \sum_{\beta\in\mathrm{Irr}(G/N)}\beta(1)^2(\chi\widehat{\beta},\chi\widehat{\beta}) \geq \sum_{\beta\in\mathrm{Irr}(G/N)}\beta(1)^2 = [G:N].$$

On a donc $(\chi\widehat{\beta},\chi\widehat{\beta}) = 1$ pour tout $\beta\in\mathrm{Irr}(G/N)$, c'est-à-dire $\chi\widehat{\beta}\in\mathrm{Irr}(G)$, et $(\chi\widehat{\beta},\chi\widehat{\gamma}) = 0$ pour $\beta\neq\gamma$, c'est-à-dire $\chi\widehat{\beta} = \chi\widehat{\gamma}$ si et seulement si $\beta = \gamma$.

□

Le corollaire suivant est immédiat.

Corollaire 5.37. Soit $\theta\in\mathrm{Irr}(N)$ prolongeable, et soit $\mathrm{Ind}_N^G\theta = \sum_{i=1}^s e_i\chi_i$ avec $e_i > 0$. Alors $e_i = \beta_i(1)$ pour certain $\beta_i\in\mathrm{Irr}(G/N)$. En particulier, $e_i \mid |G/N|$.

Remarque 5.38. La propriété $e_i \mid |G/N|$ est aussi vraie lorsque θ est seulement invariant par G (pas forcément prolongeable). Dans ce cas, e_i est le degré d'un caractère irréductible *projectif* de G/N...

5.5 Produits directs de groupes

Soient G_1 et G_2 sont deux groupes finis. Soit V_1 un $\mathbb{C}G_1$-module et V_2 un $\mathbb{C}G_2$-module. Pour tout $i = 1,2$, l'espace V_i est naturellement un $\mathbb{C}[G_1\times G_2]$-module via la formule : pour tous $g_1\in G_1, g_2\in G_2, v_1\in V_1, v_2\in V_2$,

$$(g_1,g_2)v_i = g_iv_i.$$

Donc (exercice), le produit tensoriel $V_1\otimes_{\mathbb{C}} V_2$ est un $\mathbb{C}[G_1\times G_2]$-module via la formule

$$\begin{aligned}(g_1,g_2)(v_1\otimes v_2) &= (g_1,g_2)v_1\otimes(g_1,g_2)v_2\\ &= g_1v_1\otimes g_2v_2,\end{aligned}$$

Et on a

$$\chi_{V_1\otimes_{\mathbb{C}}V_2} = \chi_{V_1}\chi_{V_2}.$$

Théorème 5.39. Pour $i = 1, 2$, soit $S_1^{(i)}, \dots, S_{r_i}^{(i)}$ une liste de représentants des classes d'isomorphisme des $\mathbb{C}G_i$-modules simples. Alors $S_j^{(1)} \otimes_{\mathbb{C}} S_k^{(2)}$, pour $1 \leq j \leq r_1$ et $1 \leq k \leq r_2$ est une liste de représentants des classes d'isomorphisme des $\mathbb{C}[G_1 \times G_2]$-modules simples. Autrement dit, on a

$$\mathrm{Irr}(G_1 \times G_2) = \left\{ \chi^{(1)}\chi^{(2)} \mid \chi^{(i)} \in \mathrm{Irr}(G_i) \text{ pour } i = 1, 2 \right\}.$$

Preuve. Vérifions tout d'abord que les modules $S_j^{(1)} \otimes_{\mathbb{C}} S_k^{(2)}$ sont simples à l'aide du corollaire 3.20. On a, pour tous $1 \leq j_1, j_2 \leq r_1$ et $1 \leq k_1, k_2 \leq r_2$,

$$\begin{aligned}
\left(\chi_{j_1}^{(1)}\chi_{k_1}^{(2)}, \chi_{j_2}^{(1)}\chi_{k_2}^{(2)}\right) &= \frac{1}{|G_1 \times G_2|} \sum_{(g_1,g_2) \in G_1 \times G_2} \chi_{j_1}^{(1)}\chi_{k_1}^{(2)}(g_1, g_2)\overline{\chi_{j_2}^{(1)}\chi_{k_2}^{(2)}(g_1, g_2)} \\
&= \frac{1}{|G_1|}\frac{1}{|G_2|} \sum_{(g_1,g_2) \in G_1 \times G_2} \chi_{j_1}^{(1)}(g_1)\overline{\chi_{j_2}^{(1)}(g_1)}\chi_{k_1}^{(2)}(g_2)\overline{\chi_{k_2}^{(2)}(g_2)} \\
&= \left(\frac{1}{|G_1|} \sum_{g_1 \in G_1} \chi_{j_1}^{(1)}(g_1)\overline{\chi_{j_2}^{(1)}(g_1)}\right)\left(\frac{1}{|G_2|} \sum_{g_2 \in G_2} \chi_{k_1}^{(2)}(g_2)\overline{\chi_{k_2}^{(2)}(g_2)}\right) \quad \text{(théorème 3.18)} \\
&= \left(\chi_{j_1}^{(1)}, \chi_{j_2}^{(1)}\right)_{G_1} \left(\chi_{k_1}^{(2)}, \chi_{k_2}^{(2)}\right)_{G_2}.
\end{aligned}$$

En particulier, on a bien $\left(\chi^{(1)}\chi^{(2)}, \chi^{(1)}\chi^{(2)}\right) = 1$, et ces caractères sont deux-à-deux distincts. De plus, on a

$$\begin{aligned}
\sum_{\substack{\chi^{(1)} \in \mathrm{Irr}(G_1) \\ \chi^{(2)} \in \mathrm{Irr}(G_2)}} \left(\chi^{(1)}\chi^{(2)}(1)\right)^2 &= \sum_{\substack{\chi^{(1)} \in \mathrm{Irr}(G_1) \\ \chi^{(2)} \in \mathrm{Irr}(G_2)}} \left(\chi^{(1)}(1)\right)^2 \left(\chi^{(2)}(1)\right)^2 \\
&= \left(\sum_{\chi^{(1)} \in \mathrm{Irr}(G_1)} \left(\chi^{(1)}(1)\right)^2\right)\left(\sum_{\chi^{(2)} \in \mathrm{Irr}(G_2)} \left(\chi^{(2)}(1)\right)^2\right) \\
&= |G_1||G_2| \\
&= |G_1 \times G_2|,
\end{aligned}$$

et on conclut grâce au théorème 3.8.

□

On obtient le corollaire suivant de manière immédiate.

Corollaire 5.40. La table de caractères de $G_1 \times G_2$ est le produit de Kronecker de la table de caractères de G_1 et de celle de G_2.

Exemple 5.41. Choisissons $G_1 = G_2 = C_2 = \langle x \rangle$, dont la table de caractères est

	1	x
χ_1	1	1
χ_2	1	-1

.

La table de caractères de $G_1 \times G_2 = C_2 \times C_2 = \langle x \rangle \times \langle y \rangle$ est donc

	1	x	y	xy
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	1	-1	-1
χ_4	1	-1	-1	1

.

5.6 Puissances symétriques et extérieures

Soit V un $\mathbb{C}$-espace vectoriel de dimension finie et $n \in \mathbb{Z}_{\geq 1}$.

Définition 5.42. Soit I le sous-espace de $V^{\otimes n}$ engendré par les tenseurs de la forme

$$v_1 \otimes \ldots \otimes v_i \otimes \ldots \otimes v_j \otimes \ldots \otimes v_n - v_1 \otimes \ldots \otimes v_j \otimes \ldots \otimes v_i \otimes \ldots \otimes v_n.$$

La *puissance symétrique* n-ème de V est l'espace $S^n(V) = V^{\otimes n}/I$. Pour tous $v_1, \ldots, v_n \in V$, on note $v_1 \ldots v_n$ l'image de $v_1 \otimes \ldots \otimes v_n$ dans $S^n(V)$.

Remarque 5.43. Par définition, l'ordre dans lequel on prend les vecteurs v_i n'importe pas, on voit donc $v_1 \ldots v_n$ comme un produit commutatif.

Proposition 5.44. Soit $d = \dim V$ et soit $e_1, \ldots, e_d$ une base de V. Alors

$$\{e_{i_1} \ldots e_{i_n} \,;\, 1 \leq i_1 \leq \ldots \leq i_n \leq d\}$$

est une base de $S^n(V)$, et donc $S^n(V) \simeq \mathbb{C}[X_1, \ldots, X_d]_n$, l'espace des polynômes homogènes de degré n en $X_1, \ldots, X_d$.

Preuve. L'ensemble $\{e_{i_1} \otimes \ldots \otimes e_{i_n} \,;\, 1 \leq i_1, \ldots, i_n \leq d\}$ engendre $V^{\otimes n}$, donc par définition de $S^n(V)$, $\{e_{i_1} \ldots e_{i_n} \,;\, i_1 \leq \ldots \leq i_n\}$ engendre $S^n(V)$. Considérons l'application $\varphi : V^{\otimes n} \to \mathbb{C}[X_1, \ldots, X_d]_n$ induite par

$$e_{i_1} \otimes \ldots \otimes e_{i_n} \longmapsto X_{i_1} \ldots X_{i_n}.$$

Clairement, φ est linéaire et surjective. De plus, $I \subseteq \operatorname{Ker} \varphi$ car les indéterminées $X_1, \ldots, X_d$ commutent deux à deux, et donc φ induit une application linéaire $\overline{\varphi} : S^n(V) \to \mathbb{C}[X_1, \ldots, X_d]_n$, $e_{i_1} \ldots e_{i_n} \mapsto X_{i_1} \ldots X_{i_n}$. La famille $\{X_{i_1} \ldots X_{i_n} \,;\, i_1 \leq \ldots \leq i_n\}$ forme une base de $\mathbb{C}[X_1, \ldots, X_d]_n$, elle est en particulier libre. Donc $\{e_{i_1} \ldots e_{i_n} \,;\, i_1 \leq \ldots \leq i_n\}$ est libre. C'est donc une base de $S^n(V)$, et $\overline{\varphi}$ est un isomorphisme.

□

Corollaire 5.45. On a $\dim_{\mathbb{C}} S^n(V) = \binom{n+d-1}{n}$.

Preuve. Choisir un élément de la base $\{X_1^{a_1} \ldots X_d^{a_d} \,;\, a_1 + \ldots + a_d = n\}$ de $\mathbb{C}[X_1, \ldots, X_d]_n$ revient à choisir une configuration de n points alignés séparés par $d-1$ barres. Une telle configuration est entièrement déterminée par la position des n points parmi les $n + d - 1$ positions possibles.

□

Définition 5.46. Soit J le sous-espace de $V^{\otimes n}$ engendré par les tenseurs de la forme

$$v_1 \otimes \ldots \otimes v_i \otimes \ldots \otimes v_j \otimes \ldots \otimes v_n + v_1 \otimes \ldots \otimes v_j \otimes \ldots \otimes v_i \otimes \ldots \otimes v_n.$$

La *puissance extérieure* n-ème de V est l'espace $\Lambda^n(V) = V^{\otimes n}/J$. Pour tous $v_1, \ldots, v_n \in V$, on note $v_1 \wedge \ldots \wedge v_n$ l'image de $v_1 \otimes \ldots \otimes v_n$ dans $\Lambda^n(V)$.

Remarque 5.47. Échanger v_i et v_j dans $v_1 \wedge \ldots \wedge v_n$ revient à changer son signe. En particulier, si $v_i = v_j$, $v_1 \wedge \ldots \wedge v_n = 0$.

Proposition 5.48. Soit $d = \dim V$ et soit $e_1, \ldots, e_d$ une base de V. Alors

$$\{e_{i_1} \wedge \ldots \wedge e_{i_n} \,;\, 1 \leq i_1 < \ldots < i_n \leq d\}$$

est une base de $\Lambda^n(V)$.

Preuve. L'ensemble $\{e_{i_1} \otimes \ldots \otimes e_{i_n} \,;\, 1 \leq i_1, \ldots, i_n \leq d\}$ engendre $V^{\otimes n}$, donc par définition de $\Lambda^n(V)$, la famille $\{e_{i_1} \wedge \ldots \wedge e_{i_n} \,;\, 1 \leq i_1 < \ldots < i_n \leq d\}$ engendre $\Lambda^n(V)$. Pour montrer que cette famille est libre, considérons l'application linéaire $\psi : V^{\otimes n} \to V^{\otimes n}$ induite par

$$e_{i_1} \otimes \ldots \otimes e_{i_n} \longmapsto \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) e_{\sigma(i_1)} \otimes \ldots \otimes e_{\sigma(i_n)}.$$

On vérifie qu'on a $J \subseteq \operatorname{Ker}(\psi)$, de sorte que ψ induit une application $\overline{\psi} : \Lambda^n(V) \to V^{\otimes n}$. Montrons que $\overline{\psi}$ est injective. Soit $w = \sum_{1 \leq i_1 < \ldots < \ldots i_n \leq d} \lambda_{i_1 \ldots i_n} e_{i_1} \wedge \ldots \wedge e_{i_n} \in \operatorname{Ker}(\overline{\psi})$. On a donc

$$\begin{aligned} 0 &= \sum_{1 \leq i_1 < \ldots < \ldots i_n \leq d} \lambda_{i_1 \ldots i_n} \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) e_{\sigma(i_1)} \otimes \ldots \otimes e_{\sigma(i_n)} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \sum_{1 \leq i_1 < \ldots < \ldots i_n \leq d} \lambda_{i_1 \ldots i_n} e_{\sigma(i_1)} \otimes \ldots \otimes e_{\sigma(i_n)} \end{aligned}$$

Puisque la famille $\left\{e_{\sigma(i_1)} \otimes \ldots \otimes e_{\sigma(i_n)} \,;\, 1 \leq i_1 < \ldots < i_n \leq d, \sigma \in S_n\right\}$ est une base de $V^{\otimes n}$, elle est libre et donc $\lambda_{i_1 \ldots i_n} = 0$ pour tout $(i_1, \ldots, i_n)$. Donc ψ est injective, et $\{e_{i_1} \wedge \ldots \wedge e_{i_n} \,;\, 1 \leq i_1 < \ldots < i_n \leq d\}$ est libre dans $\Lambda^n(V)$.

□

Corollaire 5.49. On a $\dim_{\mathbb{C}} \Lambda^n(V) = \binom{d}{n}$. En particulier, $\Lambda^n(V) = 0$ si $n > \dim V$.

Maintenant, soit G un groupe fini et supposons que V est un $\mathbb{C}G$-module. Alors $V^{\otimes n}$ est un $\mathbb{C}G$-module via l'action diagonale

$$g(v_1 \otimes \ldots \otimes v_n) = gv_1 \otimes \ldots \otimes gv_n.$$

Il est clair que les sous-espaces I et J sont stables par l'action de G, donc $S^n(V)$ et $\Lambda^n(V)$ deviennent des $\mathbb{C}G$-modules via l'action

$$\begin{aligned} g(v_1 \ldots v_n) &= gv_1 \ldots gv_n \\ g(v_1 \wedge \ldots \wedge v_n) &= gv_1 \wedge \ldots \wedge gv_n. \end{aligned}$$

Exemple 5.50. Soit $G = C_3 = \langle x \rangle$, et Soit V le $\mathbb{C}G$-module de dimension 2 de base $\{e_1, e_2\}$ tel que $xe_1 = e_2$ et $xe_2 = -e_2 - e_1$ (la représentation correspondante est la somme directe des deux représentations irréductibles non triviales de C_3). Alors $S^2(V)$ a pour base $\{e_1^2, e_1e_2, e_2^2\}$, et on a

$$\begin{aligned} x(e_1^2) &= (xe_1)^2 = e_2^2 \\ x(e_1e_2) &= (xe_1)(xe_2) = e_2(-e_1 - e_2) = -e_1e_2 - e_2^2 \\ x(e_2^2) &= (xe_2)^2 = (-e_1 - e_2)^2 = e_1^2 + 2e_1e_2 + e_2^2, \end{aligned}$$

donc $S^2(V)$ est isomorphe à la représentation régulière. De même, $\Lambda^2(V)$ a pour base $\{e_1 \wedge e_2\}$, et

$$x(e_1 \wedge e_2) = (xe_1) \wedge (xe_2) = e_2 \wedge (-e_1 - e_2) = -e_2 \wedge e_1 = e_1 \wedge e_2,$$

donc $\Lambda^2(V)$ est isomorphe à la représentation triviale.

Dans le cas $n = 2$, on a le résultat suivant.

Théorème 5.51. Soit G un groupe fini et V un $\mathbb{C}G$-module de dimension finie. On a un isomorphisme de $\mathbb{C}G$-modules

$$V \otimes_{\mathbb{C}} V \simeq S^2(V) \oplus \Lambda^2(V).$$

Preuve. Soit $d = \dim V$ et soit $e_1, \dots, e_d$ une base de V. Soit

$$\begin{array}{rccc} \sigma : & V \otimes V & \longrightarrow & V \otimes V \\ & e_i \otimes e_j & \longmapsto & e_j \otimes e_i. \end{array}$$

(étendue par linéarité). Considérons le sous-espace des tenseurs symétriques $\mathrm{Sym}^2(V) = \{w \in V \otimes V \mid \sigma(w) = w\}$ et le sous-espace des tenseurs antisymétriques $\mathrm{ASym}^2(V) = \{w \in V \otimes V \mid \sigma(w) = -w\}$. On a $\mathrm{Sym}^2(V) \cap \mathrm{ASym}^2(V) = \{0\}$. De plus, tout élément de $V \otimes V$ s'écrit comme la somme d'un tenseur symétrique et d'un tenseur antisymétrique :

$$\sum_{1 \leq i,j \leq d} \lambda_{ij} e_i \otimes e_j = \frac{1}{2} \sum_{1 \leq i,j \leq d} \lambda_{ij}(e_i \otimes e_j + e_j \otimes e_i) + \frac{1}{2} \sum_{1 \leq i,j \leq d} \lambda_{ij}(e_i \otimes e_j - e_j \otimes e_i),$$

Donc $V \otimes V = \mathrm{Sym}^2(V) \oplus \mathrm{ASym}^2(V)$. Maintenant, on a $I \leq \mathrm{ASym}^2(V)$ et $J \leq \mathrm{Sym}^2(V)$, et par les corollaires 5.45 et 5.49,

$$\dim I + \dim J = d^2 - \frac{d(d-1)}{2} + d^2 - \frac{(d+1)d}{2} = d^2 = \dim V \otimes V,$$

donc $I = \mathrm{ASym}^2(V)$, $J = \mathrm{Sym}^2(V)$ et $V \otimes V = I \oplus J$. Ceci donne

$$S^2(V) = V \otimes V / I \simeq J = \mathrm{Sym}^2(V)$$

$$\Lambda^2(V) = V \otimes V / J \simeq I \simeq \mathrm{ASym}^2(V)$$

et donc on a l'isomorphisme d'espaces vectoriels

$$\begin{array}{rccc} & V \otimes V & \xrightarrow{\sim} & S^2(V) \oplus \Lambda^2(V) \\ & e_i \otimes e_j & \longmapsto & (e_i e_j, e_i \wedge e_j), \end{array}$$

qui est bien un isomorphisme de $\mathbb{C}G$-modules.

□

Remarque 5.52. Le théorème 5.51 peut être vu comme un particulier de la *dualité de Schur-Weyl*, qui permet de décomposer $V^{\otimes n}$ en somme directe de produits tensoriels de $\mathbb{C}\mathrm{GL}_d(\mathbb{C})$-modules et de $\mathbb{C}S_n$-modules.

Si χ est le caractère de V, notons $S^2\chi$ et $\Lambda^2\chi$ le caractère de $S^2(V)$ et $\Lambda^2(V)$ respectivement.

Théorème 5.53. Soit G un groupe fini et V un $\mathbb{C}G$-module de dimension finie. Pour tout $g \in G$, on a

$$S^2\chi(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2))$$

$$\Lambda^2\chi(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2))$$

Preuve. Soit $g \in G$. D'après la proposition 3.3(2), il existe une base de $\{e_1, \dots, e_d\}$ de V telle que $ge_i = \varepsilon_i e_i$ pour tout $i = 1, \dots, d$, où ε_i est une racine n-ème de 1 et n est l'ordre de g. Une base de $S^2(V)$ est alors donnée par les éléments e_i^2, $1 \leq i \leq d$ et $e_i e_j$, $1 \leq i < j \leq d$ d'après la proposition 5.44. Donc les valeurs propres de g sont ε_i^2, $1 \leq i \leq d$ et $\varepsilon_i \varepsilon_j$, $1 \leq i < j \leq d$, donc

$$S^2\chi(g) = \sum_{1 \leq i \leq d} \varepsilon_i^2 + \sum_{1 \leq i < j \leq d} \varepsilon_i \varepsilon_j$$

$$= \frac{1}{2}\left(\left(\sum_{1\leq i\leq d}\varepsilon_i\right)^2 + \sum_{1\leq i\leq d}\varepsilon_i^2\right)$$
$$= \frac{1}{2}(\chi(g)^2 + \chi(g^2)).$$

De même, une base de $\Lambda^2(V)$ est donnée par les éléments $e_i \wedge e_j$, $1 \leq i < j \leq d$ d'après la proposition 5.48. Donc les valeurs propres de g sont $\varepsilon_i\varepsilon_j$, $1 \leq i < j \leq d$, et

$$\Lambda^2\chi(g) = \sum_{1\leq i<j\leq d}\varepsilon_i\varepsilon_j$$
$$= \frac{1}{2}\left(\left(\sum_{1\leq i\leq d}\varepsilon_i\right)^2 - \sum_{1\leq i\leq d}\varepsilon_i^2\right)$$
$$= \frac{1}{2}(\chi(g)^2 - \chi(g^2)).$$

□

Chapitre 6

Caractères du groupe symétrique

Soit $n \in \mathbb{Z}_{>0}$. Le but de ce chapitre est de déterminer les caractères irréductibles du groupe symétrique S_n : ce sont des résultats de Frobenius. Nous ne le montrerons pas ici, mais on peut en fait construire explicitement les représentations irréductibles correspondantes (modules de Specht).

6.1 Classes de conjugaisons et partitions d'entiers

Nous avons déjà utilisé que les classes de conjugaison de S_n sont déterminées par la décomposition des ses éléments en produits de cycles à support disjoints. Plus précisément, puisque ces cycles commutent deux à deux, on peut choisir des les écrire par ordre de longueur décroissante. Si $\sigma \in S_n$ s'écrit comme le produit de cycles $c_1, \ldots, c_s$ de longueurs respectives $k_1 \geq \ldots \geq k_s$, la suite $(k_1, \ldots, k_s)$ est appelée *type cyclique* de σ.

Définition 6.1. Une *partition* de n est une suite décroissante d'entiers positifs $\lambda = (\lambda_1, \ldots, \lambda_s)$ telle que $\lambda_1 + \ldots + \lambda_s = n$. Si $\lambda = (\lambda_1, \ldots, \lambda_s)$ est une partition de n, l'entier s est appelé la *longueur* de λ, et on notera $|\lambda| = n$ et $\lambda \vdash n$.

Ainsi, le type cyclique d'un élément de S_n est une partition de n, et on a une bijection

$$\begin{array}{ccc} \{\text{partitions de } n\} & \overset{1:1}{\longleftrightarrow} & \{\text{classes de conjugaison de } S_n\} \\ \lambda & \longleftrightarrow & C_\lambda = \left\{ \begin{array}{c} \sigma \in S_n \mid \sigma \text{ est de} \\ \text{type cyclique } \lambda \end{array} \right\} \end{array}$$

Remarque 6.2. Si $\lambda = (\lambda_1, \ldots, \lambda_s)$ est une partition, on notera parfois $\lambda = (n^{m_n} \ldots 2^{m_2} 1^{m_1})$, où $m_k \in \mathbb{Z}_{\geq 0}$ est le nombre de λ_i égaux à k (notation multiplicative).

Exemple 6.3. Les partitions de 4 sont $(1^4), (2\,1^2), (2^2), (3\,1), (4)$, donc le groupe S_4 possède 5 classes de conjugaison, respectivement données par

$$\{1\}, \left\{ \begin{array}{c} (12), (13), (14), \\ (23), (24), (34) \end{array} \right\}, \left\{ \begin{array}{c} (12)(34), \\ (13)(24), \\ (14)(23) \end{array} \right\}, \left\{ \begin{array}{c} (123), (124), (134), (234), \\ (132), (142), (143), (243) \end{array} \right\}, \left\{ \begin{array}{c} (1234), (1243), \\ (1324), (1342), \\ (1423), (1432) \end{array} \right\}.$$

Proposition 6.4. Soit $\lambda = (n^{m_n} \ldots 2^{m_2} 1^{m_1}) \vdash n$. Alors

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

Preuve. Considérons la décomposition en produit de cycles à supports disjoints d'un élément de C_λ. Chacun des m_k cycles peut s'écrire de k manières différentes (déterminées par le choix du premier élément). De plus, l'ordre dans lequel ces cycles sont écrits dans σ n'est pas important. Il y a donc $k^{m_k} m_k!$ manières différentes d'écrire le produit des m_k cycles de longueur k, ce qui donne la formule attendue.

□

Ainsi, en notant

$$z_\lambda = (n^{m_n} m_n!) \dots (2^{m_2} m_2!)(1^{m_1} m_1!),$$

z_λ est le cardinal du centralisateur de σ dans S_n, où σ est une permutation de type cyclique λ.

6.2 Caractères de permutation et polynômes symétriques

D'après le théorème 3.9, le nombre de caractères irréductibles de S_n est égal au nombre de partitions de n. Pour calculer ces caractères irréductibles, l'idée de Frobenius est de commencer par calculer certains caractères induits.

Définition 6.5. Soit $\lambda = (\lambda_1, \dots, \lambda_s) \vdash n$. Le *sous-groupe de Young* est le sous-groupe de S_n qui laisse invariant les sous-ensembles $\{1, \dots, \lambda_1\}$,$\{\lambda_1+1, \dots, \lambda_1+\lambda_2\}$, ... , $\{\lambda_1+\dots+\lambda_{s-1}+1, \dots, \lambda_1+\dots+\lambda_s\}$, de sorte que

$$S_\lambda \simeq S_{\lambda_1} \times \dots \times S_{\lambda_s}.$$

Clairement, $|S_\lambda| = \lambda_1! \dots \lambda_s!$. Dans un premier temps, nous allons calculer les caractères de permutation pour l'action de S_n sur S_n/S_λ, qui est en fait l'induction de S_λ à S_n du caractère trivial (exercice). Notons φ_λ ce caractère, et notons $\varphi_\lambda(\mu)$ sa valeur sur la classe de conjugaison C_μ.

Lemme 6.6. Soient $\mu = (n^{m_n} \dots 1^{m_1})$ et $\lambda = (\lambda_1, \dots, \lambda_s)$ deux partitions de n. On a

$$|C_\mu \cap S_\lambda| = \sum \frac{\lambda_1!}{z_{\mu^{(1)}}} \dots \frac{\lambda_s!}{z_{\mu^{(s)}}}$$

où la somme est prise sur tous les s-uplets $(\mu^{(1)}, \dots, \mu^{(s)})$ de partitions $\mu^{(j)} = (n^{m_n^{(j)}} \dots 1^{m_1^{(j)}}) \vdash \lambda_j$ tels que $m_i^{(1)} + \dots + m_i^{(s)} = m_i$.

Preuve. Soit $\sigma \in C_\mu \cap S_\lambda$. On peut écrire $\sigma = \sigma_1 \dots \sigma_s$ avec $\sigma_i \in S_{\lambda_i}$. Soit $\mu^{(i)}$ le type cyclique de σ_i. On a $\mu^{(i)} \vdash \lambda_i$, et on notant $\mu^{(i)} = (n^{m_n^{(i)}} \dots 1^{m_1^{(i)}})$, on a $m_i = \sum_{j=1}^s m_i^{(j)}$ pour $1 \leq i \leq n$. D'après la proposition 6.4, le nombre d'éléments de type cyclique $\mu^{(i)}$ dans S_{λ_i} est égal à $\frac{\lambda_i!}{z_{\mu^{(i)}}}$, d'où le résultat.

□

Pour énoncer le résultat suivant, on utilise la notation classique suivante pour les coefficients multinomiaux

$$\binom{\ell}{\ell_1, \dots, \ell_t} = \frac{\ell!}{\ell_1! \dots \ell_t!}.$$

Proposition 6.7. Avec les notations du lemme 6.6, on a

$$\varphi_\lambda(\mu) = \sum \frac{z_\mu}{z_{\mu^{(1)}} \dots z_{\mu^{(s)}}} = \sum \binom{m_1}{m_1^{(1)}, \dots, m_1^{(s)}} \dots \binom{m_n}{m_n^{(1)}, \dots, m_n^{(s)}}$$

où la somme est prise sur tous les entier $m_i^{(j)}$ tels que

$$m_i^{(1)} + \dots + m_i^{(s)} = m_i$$
$$m_1^{(j)} + 2m_2^{(j)} + \dots + n m_n^{(j)} = \lambda_j.$$

Preuve. Pour toute partition μ de n, on a $\varphi_\lambda(\mu) = \frac{|S_n||C_\mu \cap S_\lambda|}{|S_\lambda||C_\mu|}$ (exercice). On obtient donc la formule attendue en appliquant le lemme 6.6.

□

Exemple 6.8. Prenons $n = 4$. On obtient les caractères de permutation suivants.

λ \ μ	(1^4)	(21^2)	(2^2)	(31)	(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

Remarque 6.9. Notons que $\varphi_{(n)}$ est égal au caractère trivial, et $\varphi_{(1,\dots,1)}$ au caractère régulier.

Soit $\mathbb{C}[X_1, \dots, X_m]$ l'anneau des polynômes en les indéterminées $X_1, \dots, X_m$. Le groupe symétrique S_m agit sur $\mathbb{C}[X_1, \dots, X_m]$ par la formule $S_m \times \mathbb{C}[X_1, \dots, X_m] \to \mathbb{C}[X_1, \dots, X_m]$, $(\sigma, P) \mapsto \sigma P$ où

$$(\sigma P)(X_1, \dots, X_m) = P(X_{\sigma(1)}, \dots, X_{\sigma(m)}).$$

Définition 6.10. Un polynôme $P \in \mathbb{C}[X_1, \dots, X_m]$ est dit *symétrique* (respectivement *anti-symétrique*) lorsque pour tout $\sigma \in S_m$, $\sigma P = P$ (respectivement $\sigma P = \mathrm{sgn}(\sigma)P$). On note $\Lambda(m)$ l'ensemble des polynômes symétriques.

Pour la suite, identifions l'ensemble des partitions de longueur au plus m avec l'ensemble

$$\mathcal{P}_m = \left\{(\lambda_1, \dots, \lambda_m) \in \mathbb{Z}_{\geq 0}^m \mid \lambda_1 \geq \dots \geq \lambda_m\right\}$$

en autorisant certains λ_i à valoir 0. Pour tout $\beta \in \mathbb{Z}^m$, posons $X^\beta = X_1^{\beta_1} \dots X_m^{\beta_m}$. On définit alors la fonction *monomiale*

$$m_\lambda = \sum X^\alpha \in \Lambda(m)$$

où la somme est prise sur toutes les permutations α de $\lambda \in \mathcal{P}_m$.

Exemple 6.11. Prenons $n = 4$, $m = 3$ et $\lambda = (2,1,1)$. On a $m_\lambda = X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2$.

On définit aussi la fonction *somme de puissance*

$$p_k = X_1^k + \dots + X_m^k \in \Lambda(m)$$

et on pose

$$p_\lambda = p_{\lambda_1} \dots p_{\lambda_s}.$$

Pour $\lambda \vdash n$, notons λ' la partition de n définie par $\lambda'_i = |\{j \mid \lambda_j \geq i\}|$, appelée *conjuguée* de λ.

Proposition 6.12. Les ensembles $\{m_\lambda\,;\, \lambda \in \mathcal{P}_m\}$ et $\{p_{\lambda'}\,;\, \lambda \in \mathcal{P}_m\}$ forment deux bases de $\Lambda(m)$.

Preuve. Exercice.

□

Théorème 6.13. Soit $\mu \vdash n$. On a

$$p_\mu = \sum_{\substack{\lambda \in \mathcal{P}_m \\ |\lambda| = |\mu|}} \varphi_\lambda(\mu) m_\mu.$$

Autrement dit, $\varphi_\lambda(\mu)$ est le coefficient de $X_1^{\lambda_1}\dots X_m^{\lambda_m}$ dans la décomposition de p_μ sur la base des fonctions monomiales. En particulier, puisque les partitions de n sont toute de longueur au plus n, il suffit de prendre $m = n$ pour calculer les caractères de permutation de S_n.

Preuve. Le coefficient de $X_1^{im_i^{(1)}}\dots X_m^{im_i^{(m)}}$ dans $p_i^{m_i}$ est donné par le coefficient multinomial $\binom{m_i}{m_i^{(1)},\dots,m_i^{(m)}}$. En utilisant la proposition 6.7, on voit donc que le coefficient de $X_1^{\lambda_1}\dots X_m^{\lambda_m}$ dans p_μ est $\varphi_\lambda(\mu)$.

□

6.3 Caractères irréductibles

Notons

$$\mathrm{Irr}(S_n) = \{\chi_\lambda\,;\,\lambda \vdash n\}\,.$$

On sait que les χ_λ forment une base de l'espace des fonctions centrales sur S_n d'après le théorème 3.12. De plus, le théorème 6.13 et la proposition 6.12 impliquent que les caractères φ_λ sont linéairement indépendants. Ils forment donc une autre base de l'espace des fonctions centrales, et il suffit donc de déterminer l'expression des χ_λ dans la base des φ_λ pour expliciter $\mathrm{Irr}(S_n)$.
Pour ce faire, on introduit les notations suivantes. Pour tout $\lambda \in \mathcal{P}_m$, soit $\alpha_i = \lambda_i + m - i$ et posons

$$A_\lambda = \sum_{\sigma\in S_m} \mathrm{sgn}(\sigma) X_{\sigma(1)}^{\alpha_1} X_{\sigma(2)}^{\alpha_2}\dots X_{\sigma(m)}^{\alpha_m} = \begin{vmatrix} X_1^{\alpha_1} & \dots & X_m^{\alpha_1} \\ \vdots & & \vdots \\ X_1^{\alpha_m} & \dots & X_m^{\alpha_m} \end{vmatrix}.$$

De plus, soit Δ le déterminant de Vandermonde suivant

$$\Delta = \prod_{1\le i<j\le m} (X_i - X_j) = \begin{vmatrix} 1 & \dots & 1 \\ X_1 & \dots & X_m \\ \vdots & & \vdots \\ X_1^{m-1} & \dots & X_m^{m-1} \end{vmatrix}.$$

Lemme 6.14. Le quotient A_λ/Δ est un polynôme symétrique.

Preuve. Les polynômes A_λ et Δ sont tous les deux antisymétriques puisqu'il s'agit de déterminants. En particulier, A_λ s'annule pour $X_i = X_j$, il est donc divisible par Δ, d'où le résultat.

□

Définition 6.15. On appelle *fonction de Schur* le polynôme $s_\lambda = A_\lambda/\Delta$.

Dans la suite, on notera $<$ l'ordre lexicographique sur $\mathbb{Z}^m$.

Théorème 6.16. Pour tout $\lambda \in \mathcal{P}_m$, on a

$$s_\lambda = m_\lambda + \sum_{\substack{\nu\in\mathcal{P}_m \\ \nu<\lambda \\ |\nu|=|\lambda|}} K_{\lambda,\nu} m_\nu,$$

où les $K_{\lambda,\nu}$ sont des entiers.

Preuve. Puisque s_λ un polynôme symétrique d'après le lemme 6.14, il suffit de montrer que le coefficient de X^λ dans s_λ est 1, et que pour tout $\nu \neq \lambda$, le coefficient de X^ν dans s_λ est non nul seulement si $\nu < \lambda$. Notons $\tau = (m-1, m-2, \ldots, 0) \in \mathbb{Z}^m$. Alors $A_\lambda = X^{\lambda+\tau} + \sum_{\substack{\beta \in \mathbb{Z}^m_{\geq 0} \\ \beta < \lambda+\tau}} a_\beta X^\beta$ avec $a_\beta \in \mathbb{Z}$. De même, $\Delta = X^\tau + \sum_{\kappa<\tau} d_\kappa X^\tau$ avec $d_\kappa \in \mathbb{Z}$. Pour calculer s_λ, il suffit d'effectuer la division euclidienne de A_λ par Δ dans l'anneau $\mathbb{A}[X_1]$ où $\mathbb{A} = \mathbb{C}[X_2, \ldots, X_m]$. Le principe de la division euclidienne montre que $s_\lambda = X^\lambda + \sum_{\substack{\beta \in \mathbb{Z}^m_{\geq 0} \\ \beta < \lambda}} u_\beta X^\beta$ avec $u_\beta \in \mathbb{Z}$, d'où le résultat.

□

Exemple 6.17. Prenons $m = 3$ et $\lambda = (3)$. On a

$$\begin{aligned} s_{(3)} &= \frac{\begin{vmatrix} X_1^5 & X_2^5 & X_3^5 \\ X_1 & X_2 & X_3 \\ 1 & 1 & 1 \end{vmatrix}}{\begin{vmatrix} X_1^2 & X_2^2 & X_3^2 \\ X_1 & X_2 & X_3 \\ 1 & 1 & 1 \end{vmatrix}} = \frac{X_1^5X_2 - X_1^5X_3 - X_1X_2^5 + X_1X_3^5 + X_2^5X_3 - X_2X_3^5}{X_1^2X_2 - X_1^2X_3 - X_1X_2^2 + X_1X_3^2 + X_2^2X_3 - X_2X_3^2} \\ &= (X_1^3 + X_2^3 + X_3^3) + (X_1^2X_2 + X_1X_2^2 + X_1^2X_3 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2) + (X_1X_2X_3) \\ &= m_{(3)} + m_{(2,1)} + m_{(1,1,1)}, \end{aligned}$$

de sorte que $K_{(3),\nu} = 1$ pour $\nu = (2,1), (1,1,1)$.

Le théorème 6.16 implique directement le corollaire suivant.

Corollaire 6.18. L'ensemble $\{s_\lambda \,;\, \lambda \in \mathcal{P}_m\}$ forme une base de $\Lambda(m)$, et la matrice de passage entre la base des fonctions monomiales et celle des fonctions de Schur est unitriangulaire relativement à l'ordre lexicographique.

On peut donc exprimer les fonctions sommes de puissance dans la base des fonctions de Schur

$$p_\mu = \sum_{\substack{\lambda \in \mathcal{P}_m \\ |\lambda| = |\mu|}} \theta_\lambda(\mu) s_\lambda,$$

avec $\theta_\lambda(\mu) \in \mathbb{C}$.

Proposition 6.19. Pour tout $\lambda, \mu \in \mathcal{P}_m$, on a $\theta_\lambda(\mu) \in \mathbb{Z}$.

Preuve. D'après la proposition 6.7, les coefficients de la matrice $Q = (\varphi_\lambda(\mu))_{\lambda,\mu}$ sont des entiers. De plus, la matrice $S = (K_{\lambda,\nu})_{\lambda,\nu}$ est unitriangulaire à coefficients entiers. Donc S^{-1} est aussi unitriangulaire à coefficients entiers. En posant $R = (\theta_\lambda(\mu))_{\mu,\lambda}$, on a $R = S^{-1}Q$ et donc R est à coefficients entiers.

□

On peut donc énoncer le théorème central de ce chapitre, dont la preuve sera donnée dans la section suivante.

Théorème 6.20 (Frobenius)**.** Soient $\lambda, \mu \vdash n$. On a $\chi_\lambda(\mu) = \theta_\lambda(\mu)$.

Exemple 6.21. Prenons $n = 3$. On a déjà calculé la fonction de Schur pour $\lambda = (3)$ dans l'exemple 6.17 : on a

$$s_{(3)} = X_1^3 + X_2^3 + X_3^3 + X_1^2X_2 + X_1^2X_3 + X_2^2X_3 + X_1X_2^2 + X_1X_3^2 + X_2X_3^2 + X_1X_2X_3.$$

De même, on obtient

$$s_{(2,1)} = X_1^2X_2 + X_1X_2^2 + X_1^2X_3 + X_1X_3^2 + X_2^2X_3 + X_3X_2^2 + 2X_1X_2X_3 \quad \text{et}$$
$$s_{(1,1,1)} = X_1X_2X_3.$$

On a donc

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

D'autre part, on a

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

Au final, cela donne

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

d'où la table de caractères

	(1^3)	(21)	(3)
(3)	1	1	1
$(2,1)$	2	0	-1
$(1,1,1)$	1	-1	1

,

que l'on peut comparer avec l'exemple 3.15.

6.4 Démonstration du théorème de Frobenius

L'idée de la preuve du théorème 6.20 est la suivante.

(1) D'après les théorèmes 6.13, 6.16, et la proposition 6.19, les fonctions θ_λ sont des combinaisons linéaires à coefficients entiers des caractères de permutations φ_λ. Ce sont donc des combinaisons linéaires à coefficients entiers des caractères irréductibles.

(2) On montre (corollaire 6.23) que les fonctions θ_λ vérifient les relations d'orthogonalité

$$(\theta_\lambda, \theta_\kappa) = \delta_{\lambda,\kappa}.$$

(3) On montre que $\theta_\lambda((1^n)) > 0$ en en donnant une formule explicite (théorème 6.24).

(4) On conclut en utilisant les corollaires 3.13 et 3.20, qui nous assurent que les θ_λ sont bien des caractères, et qu'ils sont irréductibles.

Pour montrer (2), on commence par énoncer le résultat classique suivant. On considère des indéterminées $X_i, Y_i, i = 1, \ldots, m$, et on note $X = (X_1, \ldots, X_m)$ (respectivement $Y = Y_1, \ldots, Y_m$).

Théorème 6.22 (Formule de Cauchy)**.** On a

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

Preuve. On a

$$\begin{aligned}
\frac{\Delta(X)\Delta(Y)}{\prod_{1\leq i,j\leq m}(1-X_iY_j)} &= \det\left(\frac{1}{1-X_iY_j}\right)_{1\leq i,j\leq m} && \text{car il s'agit d'un déterminant de Cauchy (exercice)}\\
&= \det\left(\sum_{k\geq 0}(X_iY_j)^k\right)_{1\leq i,j\leq m}\\
&= \det\left(\left((X_i^k)_{\substack{1\leq i\leq m\\ k\geq 0}}\right)\left((Y_i^k)_{\substack{1\leq i\leq m\\ k\geq 0}}\right)^{\mathrm{tr}}\right)\\
&= \sum_{\lambda\in\mathcal{P}_m}A_\lambda(X)A_\lambda(Y) && \text{par la formule de Binet-Cauchy (exercice).}
\end{aligned}$$

Par définition des fonctions de Schur (définition 6.15), on obtient la formule annoncée en divisant par $\Delta(X)\Delta(Y)$.

□

Corollaire 6.23. On a

$$(\theta_\lambda,\theta_\kappa)=\sum_{\mu\vdash n}\frac{\theta_\lambda(\mu)\theta_\kappa(\mu)}{z_\mu}=\delta_{\lambda,\kappa}.$$

Preuve. On a

$$\begin{aligned}
\sum_{\lambda\in\mathcal{P}_m}s_\lambda(X)s_\lambda(Y) &= \prod_{1\leq i,j\leq m}\frac{1}{1-X_iY_j} && \text{par le théorème 6.22}\\
&= \prod_{1\leq i,j\leq m}\exp\left(\log\frac{1}{1-X_iY_j}\right)\\
&= \prod_{1\leq i,j\leq m}\exp\left(\sum_{k\geq 1}\frac{X_i^kY_j^k}{k}\right)\\
&= \exp\left(\sum_{k\geq 1}\frac{p_k(X)p_k(Y)}{k}\right)\\
&= \sum_{\mu\vdash n}\frac{1}{z_\mu}p_\mu(X)p_\mu(Y)\\
&= \sum_{\lambda,\kappa\vdash n}\left(\sum_{\mu\vdash n}\frac{\theta_\lambda(\mu)\theta_\kappa(\mu)}{z_\mu}\right)s_\lambda(X)s_\kappa(Y) && \text{par définition de } \theta_\lambda(\mu) \text{ et } \theta_\nu(\mu),
\end{aligned}$$

d'où le résultat.

□

Il reste donc à prouver (3). Notons $f_\lambda=\theta_\lambda((1^n))$.

Théorème 6.24. Pour toute partition $\lambda=(\lambda_1,\ldots,\lambda_n)$ de n (en autorisant $\lambda_i=0$), on a

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

Preuve. Par définition, on a

$$p_{(1^n)}(X)\Delta(X) = \sum_{\lambda\vdash n} f_\lambda A_\lambda(X)$$

où $X = (X_1, \dots, X_m)$ pour $m \geq n$ fixé. Le membre de gauche est égal à

$$\sum_{\beta_1+\dots+\beta_m=n} \binom{n}{\beta_1, \dots, \beta_m} X_1^{\beta_1} \dots X_m^{\beta_m} \sum_{\sigma\in S_m} \operatorname{sgn}(\sigma) X_1^{\sigma(m)-1} \dots X_m^{\sigma(1)-1},$$

et puisque le nombre f_λ est le coefficient de $X_1^{\lambda_1+m-1} X_2^{\lambda_2+m-2} \dots X_m^{\lambda_m}$ dans cette expression, on a

$$\begin{aligned} f_\lambda &= n! \sum_{\sigma\in S_m} \operatorname{sgn}(\sigma) \frac{1}{(\lambda_1+m-\sigma(m))!(\lambda_2+m-1-\sigma(m-1))!\dots(\lambda_m+1-\sigma(1))!} \\ &= n! \begin{vmatrix} 1/\lambda_1! & 1/(\lambda_1+1)! & \dots & 1/(\lambda_1+m-1)! \\ 1/(\lambda_2-1)! & 1/\lambda_2! & \dots & 1/(\lambda_2+m-2)! \\ \vdots & \vdots & \ddots & \vdots \\ 1/(\lambda_m-m+1)! & 1/(\lambda_m-m+2)! & \dots & 1/\lambda_m! \end{vmatrix} \end{aligned}$$

En divisant les colonnes par $(m-1)!, (m-2)!, \dots, 0!$ et en multipliant les lignes par $(\lambda_1+m-1)!, (\lambda_2+m-2)!, \dots, \lambda_m!$, on obtient

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

Maintenant, puisque

$$\binom{x}{\ell} = \frac{x(x-1)\dots(x-\ell+1)}{\ell!} = x^\ell/\ell! + R(x)$$

où $R(x) \in \mathbb{C}[x]$ est de degré au plus $\ell-1$, on se ramène par soustraction de colonnes à

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

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

□

Ceci conclut la preuve du théorème 6.20. En particulier, on voit que les f_λ sont les degrés des caractères irréductibles, ce sont donc des entiers, ce qui n'est pas évident avec la formule du théorème 6.24).

Il existe une formule plus simple pour calculer ces degrés.

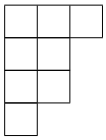
Définition 6.25. Soit $\lambda = (\lambda_1, \dots, \lambda_s)$ une partition. Le *diagramme de Young* de λ est

$$[\lambda] = \{(i,j)\,;\, 1 \leq i \leq s, 1 \leq j \leq \lambda_i\}\,.$$

On représente $[\lambda]$ par la superposition de s lignes contenant respectivement $\lambda_1, \dots, \lambda_s$ boîtes.

Exemple 6.26. Prenons $\lambda = (3,2,2,1)$ On a

$$[\lambda] = \{(1,1),(1,2),(1,3),(2,1),(2,2),(3,1),(3,2),(4,1)\} =$$



Pour $b = (i_0, j_0) \in [\lambda]$, on note $h(b)$ la longueur de l'équerre contenant b, c'est-à-dire

$$h(b) = |\{(i,j) \in [\lambda] \mid (i = i_0 \text{ et } j > j_0) \text{ ou } (j = j_0 \text{ et } i > i_0)\}|\,.$$

Exemple 6.27. Ecrivons les longueurs des équerres dans chaque boîte de $[\lambda]$ de l'exemple 6.26 :

6	4	1
4	2	
3	1	
1		

.

Le résultat suivant est énoncé sans démonstration.

Théorème 6.28 (Formule des équerres)**.** Soit $\lambda \vdash n$. On a

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

Exemple 6.29. Reprenons l'exemple 6.27. On a $f_\lambda = 8!/6.4.1.4.2.3.1.1 = 70$.

En fait, la combinatoire des diagrammes de Young permet de donner des solutions explicites à d'autres problèmes fondamentaux, parmi lesquels :

- construire les représentations irréductibles (modules de Specht),
- calculer simplement les valeurs des caractères irréductibles (règle de Murnaghan-Nakayama),
- décomposer certaines représentations induites en somme directe de représentations irréductibles (règle de Young, règle de Pierri, règle de Littlewood-Richardson).

Notons finalement qu'on ne connaît pas de formule combinatoire explicite pour décomposer le produit tensoriel de deux représentations irréductibles en somme directe de représentations irréductibles (problème de Kronecker).