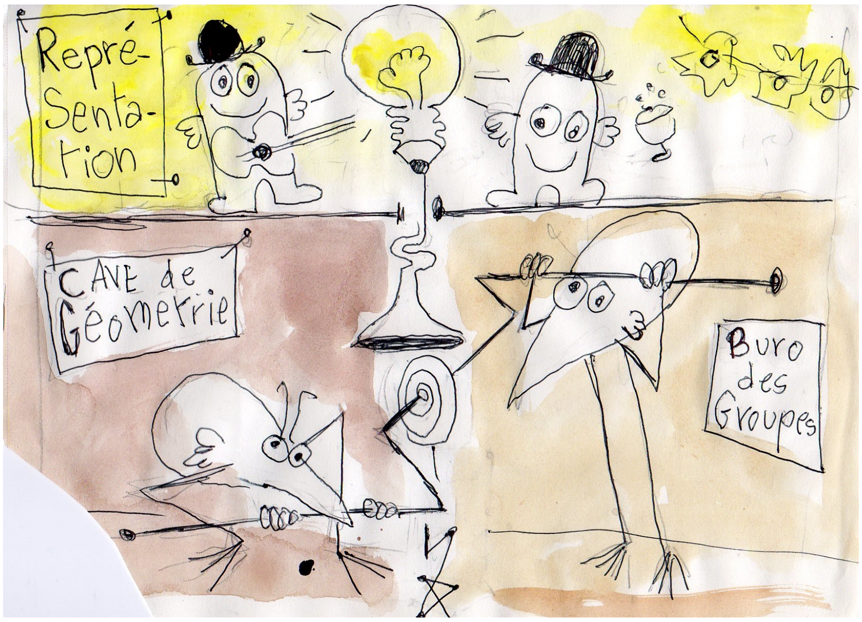
Représentations et Caractères d'un groupe fini sur un $\mathbb{C}$-espace-Leçon 107



0. Le 6 minutes

Aux confins de la théorie des groupes et de la géométrie (linéaire) trône la théorie des représentations. Une représentation n'est rien d'autre qu'une action *linéaire* d'un groupe sur un espace V. Il s'agit donc de plonger un groupe (ou un quotient du groupe) dans un groupe de matrices.

Ici, nous allons nous intéresser aux représentations d'un groupe fini sur le corps des complexes[1].

Le but de la théorie est de comprendre toutes les représentations possibles d'un groupe fini fixé G, à isomorphisme près, c'est-à-dire à changement de base près[2]. La première idée est d'utiliser la finitude du groupe, elle se résume en un autre mot : *moyenner*. Prendre

1. Et ce, pour plusieurs raisons : le corps est algébriquement clos, de caractéristique nulle, et on a une notion de positivité *via* les formes hermitiennes.
2. Soyons raisonnables !

la moyenne sur le groupe va permettre de montrer une propriété de semi-simplicité : tout sous-espace G-stable possède un supplémentaire G-stable, c'est le théorème de Maschke. Une représentation est alors somme directe de sous-représentations "minimales" dites irréductibles (que l'on appellera "irreps" dans la suite). Elles se caractérisent par le lemme de Schur qui assure qu'un morphisme entre deux irreps qui commute à l'action de G est soit nul, soit iso. La classification à isomorphisme près des G-représentations (à isomorphisme près !) devient abordable : il suffit de classer celles qui sont irréductibles.

C'est ici qu'intervient la théorie des caractères, introduite par Frobenius et Schur. Le caractère d'une représentation est une fonction de G dans $\mathbb{C}$, associée à la représentation, qui se définit par la trace de la matrice associée à g dans G, il ne dépend que de sa classe d'isomorphisme. Il s'agit d'un objet simple et concret, un outil de calcul qui va *caractériser* la représentation à isomorphisme près.

On dote l'espace des fonctions de G vers $\mathbb{C}$ d'une forme hermitienne G-invariante sur l'espace des fonctions, et là, miracle, le lemme de Schur implique que les caractères des irreps forment une famille orthonormée ; il s'agit même une base orthonormée de l'espace des fonctions constantes sur les classes de conjugaison de G.

On illustre la théorie avec des exemples de "groupes de petits cardinaux" où l'on sait calculer tous les caractères irréductibles donc, tous les caractères. On prend l'habitude de résumer les résultats obtenus dans une *table de caractères*, c'est-à-dire un tableau à double entrée dont les colonnes sont associées aux classes de conjugaison du groupe, et dont les lignes sont associées aux caractères irréductibles. Cette table donne de précieux renseignements sur le groupe qu'il faut pouvoir décoder, même si l'on sait qu'elle ne permet pas de retrouver le groupe à isomorphisme près.

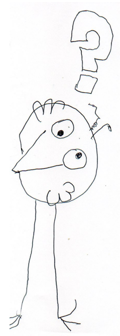
Pour finir, si on doit associer la théorie des représentations à une idée fondamentale des mathématiques, ce serait encore une fois l'idée de dualité. En effet, si un espace E de dimension finie sur $\mathbb{K}$ peut se voir à travers ses morphismes de E vers $\mathbb{K}$, on peut tenter de comprendre un groupe G à travers ses morphismes de G dans $\mathbb{C}^*$. Pour ce qui est des groupes abéliens finis, on obtient une dualité parfaite, mais pour les groupes finis en général, la théorie s'effondre : par exemple, pour l'énorme groupe $\mathfrak{S}_n$, on ne récupère que le morphisme trivial et la signature. Il faut alors remplacer $\mathbb{C}^* = \mathrm{GL}_1(\mathbb{C})$ par $\mathrm{GL}_n(\mathbb{C})$ pour retrouver les propriétés (mais pas toutes !) du groupe G.

Peaux de banane et pièges classiques.

Dans cette section , nous allons voir comment éviter de paraître ridicule en parlant de choses savantes sans savoir exactement ce que l'on fait et pourquoi on le fait. C'est là le piège principal de la leçon. En effet, la théorie fournit des recettes de cuisine assez faciles à suivre et les étudiants croient parfois maîtriser la théorie des représentations en en maîtrisant en réalité que les recettes.

1. Il y a souvent confusion entre caractère et représentation. Il ne faut jamais oublier que le but est de comprendre comment représenter un groupe à l'aide de matrices. La représentation est le but, et le caractère est l'outil.
2. Il y a aussi une confusion qui provient du vocabulaire même. On appelle représentation un morphisme de G dans $\mathrm{GL}_n(\mathbb{K})$ mais aussi l'espace V sur lequel le groupe G agit linéairement. En fait, je préfère appeler V un "G-module", ce qui signifie en gros qu'il possède une structure linéaire et une action linéaire de G, le défaut de

cette notation est de ne pas préciser sur quel corps on le considère, on pourrait dire "G-module sur le corps $\mathbb{K}$" si la précision est utile.



3. Le mieux pour éviter toute confusion est de savoir interpréter toutes les définitions de base de façon matricielle. Il faut savoir comment interpréter une sous-représentation (matrice triangulaire par blocs), une somme directe de représentations (matrice diagonale par blocs), un morphisme de représentation (commutation de matrices). Voir [1, p. 255].
4. Attention, on met sur un G-module V deux formes hermitiennes. Une classique notée $(\, , \,)$, indépendante de G, et l'autre G-invariante donnée par
$$(v, w)_G = \frac{1}{|G|} \sum_{g \in G} (g \cdot v, g \cdot w).$$
Il ne faut pas les confondre. C'est la seconde qui fournit un supplémentaire G-stable à toute sous-représentation.
5. Ne passons pas à côté des choses simples ! Il serait ridicule de faire défiler la théorie sans comprendre ce qu'est la théorie des représentations pour le groupe trivial et pour $\mathbb{Z}/2\mathbb{Z}$. Pour le groupe trivial, un G-module est tout simplement un espace vectoriel. Pour $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$, les représentations correspondent aux matrices telles que $A^2 = \mathrm{I}_n$ (ici, $A = \rho(\overline{1})$), c'est-à-dire les matrices de symétries. Un endomorphisme de représentation correspond à une matrice qui commute avec A. Deux représentations ρ et ρ' sont isomorphes (toujours pour le groupe $\mathbb{Z}/2\mathbb{Z}$) si les deux matrices A et A' correspondantes sont conjuguées. Une matrice symétrique (en caractéristique différente de 2) est diagonalisable, ce qui correspond au théorème de Maschke, et les valeurs propres sont 1 et -1, ce qui correspond au fait que l'on a deux irreps : $\overline{1} \mapsto 1$ et $\overline{1} \mapsto -1$. Les sous-espaces propres $\mathrm{Ker}(A - \mathrm{Id})$ et $\mathrm{Ker}(A + \mathrm{Id})$ sont les *composantes isotypiques* de la représentation pour les deux irréductibles de $\mathbb{Z}/2\mathbb{Z}$. Que se passe-t-il pour $\mathbb{Z}/n\mathbb{Z}$? Voir exemple [1, XIII-1.1.7, 1.2.3].
6. De la même manière, trouver une représentation en degré d du groupe diédral D_n signifie trouver, dans $\mathcal{M}_d(\mathbb{C})$ deux matrices C et S telles que $C^n = \mathrm{I}_d$, $S^2 = \mathrm{I}_d$ et $SCS^{-1} = C^{-1}$. Cela vient du fait que D_n est engendré par deux éléments vérifiant les relations correspondantes, voir [1, Remarque XIII-B.2.2].
7. Quand on applique le théorème de Maschke (ou théorème de semi-simplicité) on obtient $V = \oplus_{i=1}^m V_i$ où les V_i sont des irreps. On regroupe ensuite la somme directe en représentations isomorphes : $V \simeq \oplus_{i=1}^k m_i V_i$, attention, c'est un isomorphisme et non pas une égalité (même si par abus de notation on arrive parfois à noter des égalités). Les $m_i V_i$ sont les composantes isotypiques. La composante isotopique associée à une représentation irréductible est unique, elle est entièrement déterminée par V. La première composante isotopique à connaître est le sous-espace V^G des éléments invariants par tout G ; c'est la composante isotopique de la représentation triviale. Comme elle est de degré 1, la multiplicité est donc $m = \dim V^G$. Pour revenir à l'exemple de $\mathbb{Z}/2\mathbb{Z}$, m est la dimension du sous-espace propre de A pour la valeur propre 1.
8. Quand G est un groupe fini, on a le théorème de Lagrange qui assure qu'une représentation vérifie $\rho(g)^n = \mathrm{I}_n$ pour $n = |G|$. C'est ceci qui implique que $\rho(g)$ est

diagonalisable sur $\mathbb{C}$, mais si G est infini, la diagonalisabilité n'est pas acquise ! Penser à la représentation de $(\mathbb{Z}, +)$ telle que $n \mapsto \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$.

9. Attention, quand on dit que le caractère caractérise, il ne caractérise la représentation qu'à isomorphisme près. On ne peut pas récupérer une représentation à partir de son caractère, *Hey ! What did you expect ?*

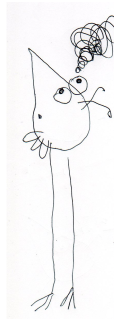
I. Les fondamentaux

Il est fondamental de savoir construire des représentations d'un groupe G donné. Voici les outils de base.

1. On peut construire à partir d'un groupe un certain nombre de représentations : les représentations classiques (la triviale, la régulière [1, XIII-1.1.10]), les représentations par permutations à partir d'actions de groupe sur des ensembles finis. En effet, toute action du groupe G sur un ensemble fini X fournit une représentation par matrices de permutations, [1, XIII-3.11]. Le caractère de cette représentation est l'application qui envoie g sur le nombre d'invariants de g sur X. La représentation régulière a l'avantage d'être fidèle (injective) ; cela provient des permutations de l'action du groupe G à gauche sur lui-même.
2. *La construction de représentations*, voir [1, XIII-1.3] : on utilise la somme directe, la dualité, les homomorphismes de représentations pour construire à partir de quelques représentations classiques beaucoup d'autres représentations.
3. Si G est un groupe abélien, alors les matrices de représentations commutent et sont diagonalisables : elle sont codiagonalisables et donc, les irreps sont de dimension 1. On a ainsi n irreps et elles forment même un groupe pour la multiplication des fonctions, noté $\widehat{G}$. C'est le début d'une belle dualité ! Par exemple, le groupe G va s'identifier au bidual, voir [1, Annexe XIII-A, 1.2.3] et la théorie de Fourier peut s'appliquer.
4. Le théorème de Maschke : toute sous-représentation possède un supplémentaire stable. La version avec l'orthogonal pour la forme G-invariante est valable uniquement sur $\mathbb{C}$. La version avec les noyaux d'un projecteur G-invariant a l'avantage d'être valable sur tout corps de caractéristique ne divisant pas $|G|$, voir [1, XIII-1.7].
5. La théorie des caractères : le caractère associé à une représentation ρ est la fonction qui envoie g dans G sur la trace $\mathrm{tr}(\rho(g))$. Le lemme de Schur, [1, XIII-2.1], en est le point de départ. Il dit qu'un morphisme d'irreps est soit iso soit nul, et (sur $\mathbb{C}$) s'il est iso, c'est une homothétie. C'est ce résultat fondamental qui implique que les caractères des irreps forment un système orthonormé pour la norme hermitienne G-invariante des fonctions de G vers $\mathbb{C}$, [1, XIII-2.5.6]. Mieux ! Si on se restreint aux fonctions constantes sur les classes de conjugaison de G, on montre avec un peu plus d'effort que l'ensemble des caractères irréductibles en forme une base, [1, XIII-2.6.1]. Comme corollaire, [1, XIII-2.7], le nombre d'irreps (à iso près) est égal au nombre de classes de conjugaison : la table de caractères est une matrice carrée !
6. *La déconstruction de représentations* : la base unitaire des caractères permet alors de comprendre comment une représentation complexe se décompose en représentations irréductibles, à isomorphisme près. En effet, $V \simeq \sum_i m_i V_i$ implique au niveau des

caractères $\chi_V = \sum_i m_i \chi_{V_i}$, et $m_i = \langle \chi_{V_i}, \chi_V \rangle$ car la base des χ_{V_i} est unitaire. Comme corollaire, on obtient que si deux représentations possèdent un même caractère, elles sont isomorphes : le caractère caractérise, [1, XIII-2.5.7].

7. Savoir construire une table de caractères, utiliser pour cela la somme des carrés des degrés, l'orthogonalité des lignes, la pseudo-orthogonalité des colonnes, voir les annexes de [1, XIII]. La connaissance botanique des petits groupes : $\mathbb{Z}/n\mathbb{Z}$ (où la table de caractères est une matrice de Vandermonde), D_n, $\mathfrak{S}_n$, et $\mathfrak{A}_n$, pour $n = 3, 4$, voire 5. Il sera apprécié de faire provenir certaines représentations d'actions de groupe sur l'espace affine (avec des dessins, même s'ils sont moches, c'est pas grave) sur le triangle, le carré, le n-gone, le tétraèdre, voire l'icosaèdre.



II. Questions classiques du jury.

1. Un groupe abélien fini a toutes ses irreps de degré 1. Et réciproquement ?

   Oui, voir par exemple [1, Exercice XIII-E1].

2. Deux groupes ayant la même table de caractères sont isomorphes. Vrai ou faux ?

   Faux, on a des contre-exemples. Le premier exemple est que la table de caractères de H_8 et de D_4 sont les mêmes alors qu'ils sont non isomorphes, voir [1, Exercice XIII-21].

3. Peut-on trouver la table de caractères d'un sous-groupe H à partir de la table des caractères d'un groupe G donné ?

   En théorie oui : toutes les représentations de G sont dans la représentation régulière de G et comme $H \subset G$, la représentation régulière de H est une sous-représentation de la représentation régulière de G, vue comme restriction d'une représentation de G. On a donc toutes les représentations de H dans les représentations de G. Du coup, en pratique, on prend une à une les représentations de G et on regarde leur décomposition en caractères de H, quand l'indice de H est petit, on s'en sort, voir [1, Annexe XIII-D].

4. Le lemme de Schur assure que l'ensemble des endomorphismes d'une représentation irréductible est un corps. Est-il nécessairement commutatif ?

   Oui pour $\mathbb{C}$, puisqu'on obtient les homothéties, et donc le corps $\mathbb{C}$ lui-même. Mais non pour $\mathbb{R}$, voir par exemple [1, Exercice XIII-E.13], où l'on trouve le corps des quaternions.

5. Il est indispensable de savoir répondre à la question "Que peut-on lire dans la table de caractères d'un groupe fini G ?" Citons en vrac : le treillis des sous-groupes distingués [1, Exercice XIII-E.25], donc en particulier, la simplicité de G (à savoir illustrer sur le groupe simple $\mathfrak{A}_5$), le groupe dérivé, [1, Exercice XIII-E.26], le centre de G, [1, Exercice XIII-E.28], la cyclicité du centre, [1, Exercice XIII-E.29], le nombre de racines carrées d'un élément g de G, [1, Exercice XIV-A.9], et selon une remarque judicieuse de Jean-Pierre Serre, l'existence de sous-groupe isomorphes à un groupe de type donné (plus difficile), [1, Exercice XIV-A.14].

III. Extensions du domaine de la théorie.

1. Liens avec les probas : en théorie des représentations des groupes finis, on fabrique beaucoup d'indicateurs à l'aide de moyennes. Il est naturel de les interpréter en termes probabilistes. On peut montrer par exemple que la moyenne du nombre d'invariants dans le groupe $\mathfrak{S}_n$ est 1, et la variance est également 1, [1, Exercice XIII-E.20].
2. Propriétés des actions de groupes. Soit G un groupe fini agissant sur un ensemble fini X. Soit V la représentation par permutation issue de cette action. L'action est transitive si et seulement si $\dim V^G = 1$, plus précisément, $\dim(V^G)$ est égal au nombre d'orbites, voir [1, XIII-3.11]. Elle est de plus doublement transitive si et seulement si l'orthogonal de V^G (pour la forme hermitienne G-invariante) est irréductible, donc, si son caractère est de norme 1, [1, XIII-3.11].
3. Cas où G est abélien, en lien avec la transformée de Fourier discrète. La transformée de Fourier des fonctions sur $\mathbb{R}$ de période 2π peut être vue comme l'étude des représentations du cercle $S^1 \simeq \mathbb{R}/2\pi\mathbb{R}$. La théorie des représentations d'un groupe fini abélien G peut être vue comme une version discrète. Le théorème de décomposition, la formule inverse, le théorème de Parseval, le lien avec la convolution y ont leurs analogues discrets. On en tire un bel algorithme de transformée rapide (FFT), [1, XIII-A.1.26].
4. Les liens étroits entre arithmétique et représentations qui ont fait les beaux jours de la recherche peuvent être exploités à un oral d'agrégation. Par exemple : le degré d'une représentation irréductible divise l'ordre du groupe, [1, Exercice XIII-E.35]. Autre résultat profond : toute ligne de la table de caractères (pour un degré $d > 1$) possède au moins un zéro, [1, Exercice XIII-E.35-E.36].
5. Formule de Molien. Il s'agit d'un joli lien entre théorie des représentations et combinatoire. Si G est un groupe fini, on peut étudier l'action linéaire de G sur un espace V à l'aide d'une série génératrice appelée série de Molien.
6. L'indicateur de Frobenius-Schur ou comment, à partir du caractère d'une représentation irréductible, voir qu'elle peut se réaliser sur $\mathbb{R}$, [1, Théorème XIV-2.3.1].
7. Plus facile et plutôt amusant : les idées de l'analyse harmonique s'appliquent à la géométrie. L'analyse harmonique sur un triangle (on peut en déduire le théorème de Napoléon) et sur un quadrilatère (théorème de Thébault, exercice E.49) et sur un cube (juste pour le fun), [1, Exercice XIII-E.46-E.49].

IV. Les développements

1. Critère de double transitivité d'une action. [1, Proposition XIII-3.11.1].
2. Les groupes H_8 et D_4 sont non isomorphes et ont même table de caractères, [1, Exercice XIII-E.21] (jeter aussi un oeil sur [1, Exercice XIV- A.11].
3. On peut retrouver le treillis des sous-groupes distingués de G dans sa table de caractères. E.25 + Critère de simplicité, [1, Exercice XIII-E.27].
4. Un zéro sur chaque ligne dans la table de caractères s'il vous plait ! [1, Exercice XIII-E.36].
5. La table de caractères de $\mathfrak{S}_n$ est à valeurs dans $\mathbb{Z}$, [1, Exercices XIII-E.40 et E.41].

6. A l'opposé si l'ordre de G est impair, aucune ligne non triviale de sa table de caractères n'est réelle, [1, Exercice XIV-A.6].

Annexe. Théorie des représentations sous forme matricielle

Comprendre la théorie sous forme matricielle permet de percevoir les vrais problèmes de façon tangible. Ici, le groupe G sera fini, et l'espace vectoriel V sur lequel G agit linéairement sera de dimension finie notée n sur le corps de complexes.

1. Qu'est-ce qu'une représentation d'un groupe fini G ?

   Il s'agit finalement de trouver une famille de matrices $A(g) \in \mathrm{GL}_n(\mathbb{C})$ pour tout g dans G, telles que si $g = hk$, alors $A(g) = A(h)A(k)$.

2. Qu'est-ce qu'un morphisme de représentations ? Qu'est-ce qu'un automorphisme de représentations ?

   Si V, resp. W, est une représentation de G de degré n, resp. m, dont le système de matrices associées est $A(g)$, resp. $B(g)$, $g \in G$, alors un morphisme de représentations entre V et W est une matrice $M \in \mathcal{M}_{m,n}(\mathbb{C})$ telle que pour tout g dans G, $MA(g) = B(g)M$. Un automorphisme de la représentation V est une matrice P de $\mathrm{GL}_n(\mathbb{C})$ telle que $PA(g)P^{-1} = A(g)$ pour tout g de G.

3. Qu'est-ce qu'une forme hermitienne G-invariante sur le $\mathbb{C}$-espace V ?

   Il s'agit d'une matrice H dans $\mathcal{M}_n(\mathbb{C})$, à symétrie hermitienne, c'est-à-dire $H^* = H$, telle que $A(g)^*HA(g) = H$ pour tout g de G.

4. Comment voit-on matriciellement une sous-représentation ? Et formuler matriciellement le théorème de Maschke.

   On voit que l'on a une sous-représentation s'il existe une matrice de passage $P \in \mathrm{GL}_n(\mathbb{C})$ telle que pour tout $g \in G$, $PA(g)P^{-1}$ a une structure triangulaire par blocs : $\begin{pmatrix} B(g) & X(g) \\ 0 & C(g) \end{pmatrix}$. Le théorème de Maschke dit qu'il existe une matrice Q de $\mathrm{GL}_n(\mathbb{C})$ telle que $QA(g)Q^{-1}$ est diagonale par blocs pour tout g (avec les mêmes tailles de blocs que ci-dessus).

5. Que signifie matriciellement la décomposition de V en irréductibles ?

   Cela signifie qu'il existe P dans $\mathrm{GL}_n(\mathbb{C})$ telle que $PA(g)P^{-1}$ est diagonalisable par blocs pour tout g, avec des blocs les plus petits possibles.

6. Que dit finalement le théorème de Frobenius-Schur ? (Facultatif)

   Si V est irréductible et si $\frac{1}{|G|}\sum_{g\in G}\chi_V(g^2) = 1$, alors il existe P dans $\mathrm{GL}_n(\mathbb{C})$ telle que $PA(g)P^{-1}$ est une matrice réelle pour tout g.

Références

[1] Philippe Caldero et Jérôme Germoni. *Nouvelles Histoires Hédonistes de Groupes et de Géométries, tome second.* Calvage et Mounet, 2018.


1+1