

# Représentations complexes des groupes finis et marches aléatoires centrales

Louis Mallet-Burgues

## Table des matières

<b>I Représentations complexes des groupes finis</b>	<b>1</b>
I.1 Définitions . . . . .	1
I.2 Opérations sur les représentations . . . . .	2
I.3 Représentations irréductibles . . . . .	3
I.4 Théorie des caractères et fonctions centrales . . . . .	4
I.5 Théorème fondamental . . . . .	6
I.6 Table de caractères . . . . .	9
I.7 Projecteurs et composantes isotypiques . . . . .	14
I.8 Anneau des caractères . . . . .	15
<b>II Théorie de Fourier sur les groupes finis</b>	<b>15</b>
II.1 Théorie de Fourier non-commutative . . . . .	15
II.2 Théorie de Fourier pour les fonctions centrales . . . . .	17
II.3 Principe d'incertitude de Donoho-Stark . . . . .	18
<b>III Marches aléatoires sur les groupes finis</b>	<b>20</b>
III.1 Généralités . . . . .	20
III.2 Valeurs propres de la transformée de Fourier de $p$ et caractères critiques . . . . .	21
III.3 Fréquence de passages en un point . . . . .	24
III.4 Nombre de sites visités . . . . .	25

## Introduction

Le but de cette note est d'introduire la théorie des représentations complexes d'un groupe fini  $G$  d'un point de vue moderne en centrant l'étude sur l'algèbre de groupe  $\mathbb{C}[G]$ , puis d'appliquer la théorie de Fourier à l'étude de certaines marches aléatoires sur les groupes finis. La plupart des résultats démontrés ici sont vrais pour  $K$  un corps algébriquement clos de caractéristique 0 à la place de  $\mathbb{C}$ .

## I Représentations complexes des groupes finis

### I.1 Définitions

Soit  $G$  un groupe fini. L'objet central de notre discussion est l'algèbre de groupes  $\mathbb{C}[G]$ , définie de la façon suivante :

$$\mathbb{C}[G] = \bigoplus_{g \in G} \mathbb{C}g$$

avec la seule structure de produit qui étend la loi de groupe de  $G$ , autrement dit le produit de  $g$  et de  $h$  dans  $\mathbb{C}[G]$  est exactement  $gh$ , pour tous  $g, h \in G$ .

Il s'agit d'une  $\mathbb{C}$ -algèbre de dimension finie, commutative si et seulement si  $G$  est commutatif. On a un morphisme de groupes injectif naturel :

$$G \longrightarrow \mathbb{C}[G]^\times$$

où  $A^\times$  désigne l'ensemble des éléments inversibles d'une  $\mathbb{C}$ -algèbre  $A$ , qui vérifie la propriété universelle suivante : pour toute  $\mathbb{C}$ -algèbre  $A$  et tout morphisme de groupes  $f : G \longrightarrow A^\times$  il existe un unique morphisme de  $\mathbb{C}$ -algèbres  $\mathbb{C}[G] \longrightarrow A$  qui étende  $f$ .

En termes catégoriques, le foncteur  $G \mapsto \mathbb{C}[G]$  est adjoint à gauche du foncteur  $A \mapsto A^\times$ .

Une *représentation complexe* (de dimension finie) de  $G$  peut-être définie de plusieurs façons équivalentes.

**Définition 1.** Une représentation complexe (de dimension finie) de  $G$  est (au choix) :

- Un  $\mathbb{C}[G]$ -module à gauche de type fini (ou de dimension finie sur  $\mathbb{C}$ , c'est équivalent).
- Un  $\mathbb{C}$ -espace vectoriel de dimension finie  $V$  muni d'un morphisme de groupes  $\rho : G \longrightarrow \text{GL}(V)$ .
- Un  $\mathbb{C}$ -espace vectoriel de dimension finie  $V$  muni d'une action  $G \times V \longrightarrow V$  linéaire, au sens où pour tout  $g \in G$ , l'application  $V \longrightarrow V$  qui envoie  $x$  sur  $gx$  est  $\mathbb{C}$ -linéaire.

Ces différents points sont tous équivalents (notez qu'un morphisme  $G \longrightarrow \text{GL}(V)$  équivaut, par l'adjonction vue précédemment, à un morphisme d'algèbres  $\mathbb{C}[G] \longrightarrow L(V)$ , c'est à dire à une structure de  $\mathbb{C}[G]$ -module sur  $V$  compatible à la structure de  $\mathbb{C}$ -espace vectoriel).

Souvent, on notera  $V$  ou  $(V, \rho)$  une représentation. Un morphisme de représentations  $f : V \longrightarrow W$  est, de façon équivalente, un morphisme de  $\mathbb{C}[G]$ -modules ou une application  $\mathbb{C}$ -linéaire compatible à l'action de  $G$ . Dans la littérature, on appelle aussi cela un "entrelacement" de  $V$  et  $W$ .

La catégorie  $\text{Rep}(G, \mathbb{C})$  des représentations complexes du groupe  $G$  est donc équivalente à la catégorie des  $\mathbb{C}[G]$ -modules. Dans tout ce texte, on ne considérera que des représentations de dimension finie et on ne le précisera plus. Cela revient donc à regarder la catégorie des  $\mathbb{C}[G]$ -modules de type fini.

**Définition 2.** Si  $V$  est un  $\mathbb{C}[G]$ -module, on définit  $V^G = \{x \in V \mid \forall g \in G \quad gx = x\}$  l'espace des points fixes de la représentation.

## I.2 Opérations sur les représentations

Soit  $G$  un groupe fini et  $V, W$  deux représentations de  $G$ . On peut définir les représentations suivantes :

- La représentation *triviale*  $\mathbb{C}$  (avec l'action  $g \cdot x = x$ ).
- La représentation *régulière*, c'est simplement  $\mathbb{C}[G]$  vu comme  $\mathbb{C}[G]$ -module.
- La somme directe  $V \oplus W$  qui est simplement la somme directe comme  $\mathbb{C}[G]$ -modules.
- Le produit tensoriel  $V \otimes W$  qui est le produit tensoriel au dessus de  $\mathbb{C}$  muni de l'action  $g \cdot (v \otimes w) = gv \otimes gw$ . On prendra garde au fait que ce n'est pas le produit tensoriel de  $\mathbb{C}[G]$ -modules (qui d'ailleurs n'a pas vraiment de sens en l'état car ce ne sont pas des bimodules).
- La représentation  $\text{Hom}(V, W)$  qui, en tant qu'espace vectoriel est  $\text{Hom}_{\mathbb{C}}(V, W)$ , muni de l'action suivante : pour tout  $g \in G$ ,  $f \in \text{Hom}(V, W)$  et  $x \in V$ , on a :

$$(gf)(x) = gf(g^{-1}x).$$

Encore une fois, cette représentation n'est pas  $\text{Hom}_{\mathbb{C}[G]}(V, W)$ . En revanche, il est immédiat de vérifier que :

$$\text{Hom}_{\mathbb{C}[G]}(V, W) = \text{Hom}(V, W)^G.$$

On notera  $\text{Hom}_G(V, W)$  cet ensemble : c'est l'ensemble des morphismes de représentations de  $V$  vers  $W$ .

- La représentation duale  $V^* = \text{Hom}(V, \mathbb{C})$  avec  $\mathbb{C}$  la représentation triviale. L'action est donc donnée par  $(gf)(x) = f(g^{-1}x)$ .

On peut alors immédiatement vérifier la proposition suivante.

**Proposition 3.** On a un isomorphisme canonique de représentations de  $G$  :

$$V^* \otimes W \longrightarrow \text{Hom}(V, W)$$

qui envoie  $f \otimes w$  sur  $v \mapsto f(v)w$ .

*Démonstration.* C'est un isomorphisme d'espaces vectoriels et il suffit de voir qu'il est compatible à l'action de  $G$ . □

### I.3 Représentations irréductibles

Soit  $G$  un groupe fini. Une représentation  $V$  est *irréductible* si  $V \neq 0$  et si  $V$  n'a pas d'autre sous- $\mathbb{C}[G]$ -module que  $0$  et  $V$ . On parle aussi de  $\mathbb{C}[G]$ -module *simple*.

Le théorème suivant montre que toute représentation (de dimension finie toujours) est somme directe de représentations irréductibles.

**Théorème 4.** (*Maschke*) Tout  $\mathbb{C}[G]$ -module de type fini (i.e. de dimension finie sur  $\mathbb{C}$ ) est semi-simple, c'est à dire est somme directe de  $\mathbb{C}[G]$ -modules simples.

*Démonstration.* Il suffit de montrer que tout sous- $\mathbb{C}[G]$ -module d'un  $\mathbb{C}[G]$ -module de type fini admet un supplémentaire qui est un  $\mathbb{C}[G]$ -module, puis de raisonner par récurrence forte sur la dimension.

Soit donc  $V$  un  $\mathbb{C}[G]$ -module fini et  $W$  un sous- $\mathbb{C}[G]$ -module de  $V$ . On choisit un produit scalaire hermitien quelconque sur  $V$ ,  $[\bullet, \bullet]$ , et on le moyenne via la formule suivante :

$$\langle x, y \rangle = \frac{1}{|G|} \sum_{g \in G} [gx, gy]$$

de sorte que  $\langle \bullet, \bullet \rangle$  est  $G$ -invariant et on considère alors l'orthogonal de  $W$  pour ce nouveau produit scalaire. □

On est donc amenés à étudier en détail les représentations irréductibles, qui sont les briques de base pour construire toutes les autres représentations. Un des résultats majeurs de la théorie des représentations est qu'il n'y en a qu'un nombre fini à isomorphisme près, et que ce nombre est exactement le nombre  $c(G)$  de classes de conjugaisons dans  $G$ .

Le résultat suivant utilise fondamentalement le fait que  $\mathbb{C}$  est algébriquement clos.

**Lemme 5.** (*Schur*) Soient  $V$  et  $W$  deux  $\mathbb{C}[G]$ -modules *simples*. Tout  $G$ -morphisme de  $V$  dans  $W$  est soit nul soit un isomorphisme.

De plus :

$$\text{Hom}_G(V, V) = \mathbb{C} \text{id}_V.$$

*Démonstration.* Le premier point est clair en regardant l'image et le noyau d'un tel morphisme, qui sont des sous- $\mathbb{C}[G]$ -modules, donc soit nul soit tout l'espace. Le second point se montre en considérant un espace propre du morphisme, qui est aussi un sous- $\mathbb{C}[G]$ -module. □

## I.4 Théorie des caractères et fonctions centrales

L'outil principal de la théorie des représentations sur  $\mathbb{C}$  est la théorie des caractères. À chaque  $\mathbb{C}[G]$ -module  $V$ , on associe un *caractère*  $\text{Tr}_V$  défini par :

$$\text{Tr}_V(g) = \text{Tr}(g | V)$$

qui signifie la trace de  $g$  vu comme endomorphisme de  $V$ .

Le caractère  $\text{Tr}_V$  est une fonction  $G \rightarrow \mathbb{C}$  invariante par conjugaison, aussi appelée *fonction centrale*. On note  $L^2(G)$  l'espace des fonctions de  $G$  dans  $\mathbb{C}$  et  $L_c^2(G)$  le sous-espace des fonctions centrales.

On munit  $L^2(G)$  du produit scalaire hermitien suivant :

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

Faisons tout de suite quelques remarques très simples mais fondamentales.

**Remarque 6.** L'espace  $L^2(G)$  est de dimension  $|G|$  et  $L_c^2(G)$  est de dimension  $c(G)$  le nombre de classes de conjugaison de  $G$ .

On a un isomorphisme d'espaces vectoriels :

$$L^2(G) \longrightarrow \mathbb{C}[G]$$

qui envoie  $f$  sur  $\sum_{g \in G} f(g)g$ . Cet isomorphisme identifie  $L_c^2(G)$  au centre de l'algèbre  $\mathbb{C}[G]$  :

$$\begin{array}{ccc} L^2(G) & \xrightarrow{\sim} & \mathbb{C}[G] \\ \uparrow & & \uparrow \\ L_c^2(G) & \xrightarrow{\sim} & Z(\mathbb{C}[G]) \end{array}$$

Deux représentations isomorphes ont le même caractère, puisque si  $V \xrightarrow{f} W$  est un isomorphisme de représentations, on a pour tout  $g \in G$ ,  $(g | W) \circ f = f^{-1} \circ (g | V)$  donc  $\text{Tr}(g | V) = \text{Tr}(g | W)$ .

On dispose des formules suivantes pour  $V$  et  $W$  des  $\mathbb{C}[G]$ -modules, qui se vérifient en calculant avec des bases de  $V$  et  $W$  :

$$\text{Tr}_{V \oplus W} = \text{Tr}_V + \text{Tr}_W \quad \text{Tr}_{V \otimes_{\mathbb{C}} W} = \text{Tr}_V \text{Tr}_W \quad \text{Tr}_{V^*} = \overline{\text{Tr}_V}.$$

De l'isomorphisme 3 on déduit alors :

$$\text{Tr}_{\text{Hom}(V, W)} = \overline{\text{Tr}_V} \text{Tr}_W.$$

Le lemme suivant est crucial.

**Lemme 7.** (*Reynolds*) On définit l'élément de Reynolds :

$$R = \frac{1}{|G|} \sum_{g \in G} g \in Z(\mathbb{C}[G]).$$

Il vérifie la propriété suivante :

$$Rg = gR = R$$

pour tout  $g \in G$  et c'est un projecteur :

$$R^2 = R.$$

Pour tout  $\mathbb{C}[G]$ -module  $V$ , l'image du projecteur  $(R | V)$  est exactement l'espace des points fixes  $V^G$ .

Ainsi, si  $V$  est fini, on a :

$$\text{Tr}(R | V) = \dim V^G$$

autrement dit :

$$\langle 1, \text{Tr}_V \rangle = \dim V^G.$$

En particulier, si  $V$  et  $W$  sont deux  $\mathbb{C}[G]$ -modules, on a :

$$\langle \text{Tr}_V, \text{Tr}_W \rangle = \dim \text{Hom}_G(V, W).$$

*Démonstration.* Les premières propriétés sont faciles à vérifier. Ensuite si  $Rx$  est dans l'image de  $(R | V)$ , on a pour tout  $g$  :

$$gRx = Rx$$

car  $gR = R$  donc  $Rx \in V^G$ , et si  $y \in V^G$ , alors  $Ry = y$  donc  $Ry$  est dans l'image de  $(R | V)$ . Le reste s'en déduit en calculant la trace du projecteur, et le dernier point vient de :

$$\langle \text{Tr}_V, \text{Tr}_W \rangle = \langle 1, \overline{\text{Tr}_V} \text{Tr}_W \rangle = \langle 1, \text{Tr}_{\text{Hom}(V, W)} \rangle = \dim \text{Hom}(V, W)^G = \dim \text{Hom}_G(V, W).$$

□

On note  $\widehat{G} \subseteq L_c^2(G)$  l'ensemble des caractères de représentations irréductibles de  $G$ .

**Corollaire 8.** (*Orthonormalité des caractères*) Deux représentations irréductibles sont isomorphes si et seulement si elles ont le même caractère, et l'ensemble  $\widehat{G}$  est une famille orthonormée de  $L^2(G)$ .

*Démonstration.* On calcule, pour  $V$  et  $W$  deux représentations irréductibles de  $G$  :

$$\langle \text{Tr}_V, \text{Tr}_W \rangle = \dim \text{Hom}_G(V, W) = \delta_{V \cong W}$$

d'après le lemme de Schur 5.

Si  $V \cong W$ , alors les caractères sont les mêmes. Si  $\text{Tr}_V = \text{Tr}_W$ , alors :

$$\delta_{V \cong W} = \langle \text{Tr}_V, \text{Tr}_V \rangle = \delta_{V \cong V} = 1$$

donc  $V \cong W$ .

□

Le corollaire suivant permet d'obtenir, en calculant des produits scalaires, la décomposition d'un  $\mathbb{C}[G]$ -module en somme directe d'irréductibles.

**Corollaire 9.** Soit  $V$  un  $\mathbb{C}[G]$ -module, que l'on décompose ainsi en somme directe d'irréductibles :

$$V \cong \bigoplus_{\chi \in \widehat{G}} W_\chi^{n_\chi}$$

avec  $W_\chi$  un  $\mathbb{C}[G]$ -module simple de caractère  $\chi$  (unique à isomorphisme près).

On a alors :

$$n_\chi = \langle \chi, \text{Tr}_V \rangle$$

et en particulier il y a unicité d'une telle décomposition.

On en déduit que deux  $\mathbb{C}[G]$ -modules finis sont isomorphes si et seulement si ils ont le même caractère.

*Démonstration.* On a :

$$\mathrm{Tr}_V = \sum_{\chi} n_{\chi} \chi$$

donc  $\langle \chi', \mathrm{Tr}_V \rangle = \sum_{\chi} n_{\chi} \langle \chi', \chi \rangle = n_{\chi'}$  par orthonormalité des caractères.  $\square$

**Remarque 10.** Notez que le caractère  $\mathrm{Tr}_V$  sait beaucoup de chose de la représentation  $V$  (on verra plus tard qu'il la détermine à isomorphisme près). Par exemple, la dimension de  $V$  est  $\mathrm{Tr}_V(1)$ . Ainsi, de façon générale, on posera pour  $\chi \in L^2(G)$  :

$$\dim(\chi) = \chi(1).$$

## I.5 Théorème fondamental

Le but de cette partie est d'établir le théorème fondamental 11 de la théorie des représentations complexes d'un groupe fini  $G$ , qui donne une décomposition de l'algèbre  $\mathbb{C}[G]$  comme produit d'algèbres de matrices et dont un corollaire surprenant est la finitude de  $\widehat{G}$  et le calcul exact de son cardinal.

La première étape est de décomposer la représentation *régulière* (c'est à dire le  $\mathbb{C}[G]$ -module  $\mathbb{C}[G]$ ) en somme d'irréductibles. Pour cela on commence par calculer son caractère :

$$\mathrm{Tr}_{\mathbb{C}[G]}(g) = \mathrm{Tr}(g | \mathbb{C}[G]).$$

Or  $g$  permute la base  $G$  de  $\mathbb{C}[G]$  donc sa trace est le nombre de points fixes de la permutation de  $G$  associée, c'est à dire  $|G|$  si  $g = 1$  et 0 sinon :

$$\mathrm{Tr}_{\mathbb{C}[G]} = |G| \delta_1.$$

On en déduit la formule suivante, pour tout  $f \in L^2(G)$  :

$$\langle \mathrm{Tr}_{\mathbb{C}[G]}, f \rangle = f(1).$$

On utilise alors le corollaire précédent pour calculer les multiplicités :

$$n_{\chi}(\mathbb{C}[G]) = \langle \chi, \mathrm{Tr}_{\mathbb{C}[G]} \rangle = \overline{\chi(1)} = \dim(\chi)$$

en notant  $\dim(\chi)$  pour  $\dim(W_{\chi})$  avec  $W$  un  $\mathbb{C}[G]$ -module simple de caractère  $\chi$ .

On a donc :

$$\mathbb{C}[G] \cong \bigoplus_{\chi \in \widehat{G}} W_{\chi}^{\dim(\chi)}$$

comme  $\mathbb{C}[G]$ -modules, avec  $W_{\chi}$  la (à isomorphisme près) représentation irréductible de caractère  $\chi$ , ce qui donne d'ailleurs l'égalité suivante :

$$|G| = \sum_{\chi \in \widehat{G}} \dim(\chi)^2.$$

En particulier, il n'y a qu'un nombre fini de représentations irréductibles de  $G$  à isomorphisme près. On va être beaucoup plus précis et déterminer ce nombre grâce au théorème suivant.

**Théorème 11.** (*Théorème fondamental de la théorie des représentations complexes des groupes finis*)

On a un isomorphisme de  $\mathbb{C}$ -algèbres :

$$\eta : \mathbb{C}[G] \cong \prod_{\chi \in \widehat{G}} \mathrm{Hom}(W_{\chi}, W_{\chi})$$

donné par  $g \mapsto (g | W_\chi)_\chi$ . avec  $W_\chi$  une représentation irréductible de caractère  $\chi$ . En prenant les centres, on obtient un isomorphisme :

$$Z(\mathbb{C}[G]) \cong \mathbb{C}^{|\widehat{G}|}$$

d'où l'on déduit :

$$|\widehat{G}| = c(G)$$

est le nombre de classes de conjugaison de  $G$ .

De plus,  $\widehat{G}$  est une base orthonormale de l'espace  $L_c^2(G)$  des fonctions centrales.

*Démonstration.* Le morphisme  $\eta$  est injectif car si  $\eta(x) = 0$  avec  $x \in \mathbb{C}[G]$ , on a que  $x$  agit comme 0 sur chaque  $W_\chi$ , or  $\mathbb{C}[G]$  est somme directe de  $W_\chi$  donc  $x$  agit comme 0 dans  $\mathbb{C}[G]$ , donc  $x \cdot 1 = 0$  et  $x = 0$ .

Il est surjectif car les deux espaces ont la même dimension d'après ce qui précède.

En prenant la dimension des centres on obtient :

$$|\widehat{G}| = c(G)$$

et donc  $\widehat{G}$  engendre  $L_c^2(G)$  et en est une base orthonormale. □

**Corollaire 12.** Une représentation  $V$  est irréductible si et seulement si son caractère  $\text{Tr}_V$  est de norme 1.

*Démonstration.* On décompose  $V$  en somme d'irréductibles :

$$V = \bigoplus_{\chi} W_\chi^{n_\chi}$$

et on obtient, par orthonormalité des caractères :

$$\|\text{Tr}_V\|^2 = \sum_{\chi} n_\chi$$

qui vaut 1 si et seulement si  $V$  est irréductible. □

**Proposition 13.** L'isomorphisme réciproque de  $\eta$  est donné par :

$$\eta^{-1} : \prod_{\chi} \text{Hom}(W_\chi, W_\chi) \longrightarrow \mathbb{C}[G]$$

qui à  $(\varphi_\chi) \in \prod_{\chi} \text{Hom}(W_\chi, W_\chi)$  associe :

$$\eta^{-1}((\varphi_\chi)) = \frac{1}{|G|} \sum_{g \in G} \sum_{\chi \in \widehat{G}} \dim(\chi) \text{Tr}(g^{-1} \varphi_\chi | W_\chi) g.$$

*Démonstration.* Puisque  $\eta$  est un isomorphisme, il suffit de vérifier, en notant  $\mu$  l'application définie dans l'énoncé, que :

$$\mu \circ \eta = \text{id}.$$

Par linéarité, il suffit de le montrer pour  $h \in G$ . On a alors :

$$\mu \circ \eta(h) = \frac{1}{|G|} \sum_{g \in G} \sum_{\chi \in \widehat{G}} \dim(\chi) \text{Tr}(g^{-1} h | W_\chi) g = \frac{1}{|G|} \sum_{g \in G} \text{Tr}(g^{-1} h | \mathbb{C}[G]) g = h$$

par le calcul du caractère de la représentation régulière. □

On en déduit les formules suivantes.

**Proposition 14.** (*Formules de décalage*)

Soient  $\chi, \tau \in \widehat{G}$  des caractères et soient  $\varphi \in \text{Hom}(W_\chi, W_\chi)$  et  $\psi \in \text{Hom}(W_\tau, W_\tau)$ . On a la formule suivante :

$$\frac{1}{|G|} \sum_{g \in G} \text{Tr}(g^{-1}\varphi | W_\chi) \text{Tr}(g\psi | W_\tau) = \frac{\delta_{\chi, \tau}}{\dim(\chi)} \text{Tr}(\varphi\psi | W_\chi).$$

Notez que  $\text{Tr}(\varphi\psi)$  n'a de sens que si  $\chi = \tau$ .

Ensuite, pour tous  $u, v \in G$ , on a :

$$\langle \chi(u\bullet), \tau(v\bullet) \rangle = \frac{\delta_{\chi, \tau}}{\dim(\chi)} \chi(u^{-1}v).$$

*Démonstration.* On va exploiter le fait que  $\eta \circ \eta^{-1} = \text{id}$ . Soit donc  $\varphi \in \text{Hom}(W_\chi, W_\chi)$ . On considère  $\Phi$  la famille dans  $\prod_{\tau \in \widehat{G}} \text{Hom}(W_\tau, W_\tau)$  qui vaut  $\varphi$  en  $\chi$  et 0 ailleurs. De  $\eta \circ \eta^{-1} = \text{id}$ , on tire pour tout  $\tau$  :

$$\delta_{\chi, \tau} \cdot \varphi = (\eta^{-1}(\Phi) | W_\tau) = \left( \frac{1}{|G|} \sum_{g \in G} \dim(\chi) \text{Tr}(g^{-1}\varphi | W_\chi) g | W_\tau \right).$$

Soit alors  $\psi \in \text{Hom}(W_\tau, W_\tau)$ , on compose par  $\psi$  et on prend la trace :

$$\delta_{\chi, \tau} \cdot \text{Tr}(\varphi\psi | W_\chi) = \frac{1}{|G|} \sum_{g \in G} \dim(\chi) \text{Tr}(g^{-1}\varphi | W_\chi) \text{Tr}(g\psi | W_\tau).$$

Notez que  $\text{Tr}(\varphi\psi)$  n'a de sens que si  $\chi = \tau$ .

On en déduit la première formule. Pour la seconde, on peut considérer  $\varphi$  l'endomorphisme de multiplication par  $u$  sur  $W_\chi$  et  $\psi$  celui de multiplication par  $v$  sur  $W_\tau$ , pour obtenir :

$$\frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}u) \tau(gv) = \frac{\delta_{\chi, \tau}}{\dim(\chi)} \chi(uv).$$

Or on a  $\chi(g^{-1}) = \overline{\chi(g)}$  donc :

$$\frac{1}{|G|} \sum_{g \in G} \overline{\chi(gu^{-1})} \tau(gv) = \frac{\delta_{\chi, \tau}}{\dim(\chi)} \chi(uv)$$

car  $\chi$  est une fonction centrale. On a donc bien :

$$\langle \chi(u\bullet), \tau(v\bullet) \rangle = \frac{\delta_{\chi, \tau}}{\dim(\chi)} \chi(u^{-1}v).$$

□

**Remarque 15.** (*Représentations de dimension 1 et cas des groupes abéliens*) Remarquons que toute représentation de dimension 1 de  $G$  est irréductible, et elle correspond à un morphisme  $G \rightarrow \text{GL}_1(\mathbb{C}) = \mathbb{C}^\times$ . Ainsi, l'ensemble des représentations de dimension 1 de  $G$  s'identifie au groupe dual de  $G$ ,  $\text{Hom}(G, \mathbb{C}^\times)$ . De plus, un tel morphisme tue le groupe dérivé  $D(G)$  donc se factorise par l'abélianisé  $\text{Ab}(G) = G/D(G)$ . On peut donc identifier l'ensemble des caractères de dimension 1 de  $G$  au groupe dual de l'abélianisé de  $G$ .

Si maintenant  $G$  est commutatif, toute représentation irréductible  $V$  de  $G$  est de dimension 1 car il existe un vecteur propre à tout  $G$  puisque les éléments de  $G$  agissant sur  $V$  sont codiagonalisables (ils sont d'ordre fini et ils commutent deux à deux). Ainsi  $\widehat{G}$  s'identifie au dual de  $G$ .

Il est très facile de décrire l'ensemble des caractères irréductibles d'un produit direct.

**Proposition 16.** (*Dual d'un produit direct*) Soient  $G$  et  $H$  deux groupes finis. On a :

$$\mathbb{C}[G \times H] \cong \mathbb{C}[G] \otimes \mathbb{C}[H]$$

avec le produit défini par  $(x \otimes y)(x' \otimes y') = xx' \otimes yy'$ .

De plus on a une bijection :

$$\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$$

via  $V \otimes W \leftrightarrow (V, W)$ .

*Démonstration.* On a un isomorphisme d'espaces vectoriels :

$$\mathbb{C}[G] \otimes \mathbb{C}[H] \longrightarrow \mathbb{C}[G \times H]$$

via  $g \otimes h \mapsto (g, h)$  car il envoie une base sur une base. Il suffit alors de vérifier qu'il est multiplicatif, ce qui est clair. Pour chaque  $\chi, \tau$  caractères irréductibles de  $G$  et  $H$  respectivement, on choisit  $V_\chi$  une représentation de  $G$  de caractère  $\chi$  et  $W_\tau$  une représentation de  $H$  de caractère  $\tau$  et on peut former la représentation  $V_\chi \otimes W_\tau$  et voir que, si  $\chi \otimes \tau$  désigne son caractère, on a :

$$\chi \otimes \tau(g, h) = \chi(g)\tau(h).$$

On en déduit immédiatement que ces caractères forment une base orthonormée de  $L_c^2(G \times H)$  car  $c(G \times H) = c(G) \times c(H)$ , avec  $c(G)$  le nombre de classes de conjugaison de  $G$ . □

## I.6 Table de caractères

Soit  $G$  un groupe fini. Bien souvent, une façon de comprendre le groupe  $G$  est d'établir la liste de ses représentations irréductibles. Puisqu'il y a autant de caractères irréductibles que de classes de conjugaison (par 11), on est amenés à remplir un tableau carré de taille  $c(G)$  par  $c(G)$ , avec chaque ligne indexée par un caractère et chaque colonne par une classe de conjugaison. Les entrées du tableau sont alors les  $\chi(c)$  avec  $\chi \in \widehat{G}$  et  $c \in C(G)$  une classe de conjugaison ( $C(G)$  est l'ensemble des classes de conjugaison de  $G$ ). Notez que  $\chi(c)$  est bien défini car  $\chi$  est une fonction centrale.

Les remarques suivantes permettent de remplir la table de caractère quand il ne manque qu'une colonne ou qu'une seule ligne.

**Remarque 17.** Pour tous  $\chi, \psi \in \widehat{G}$ , on a  $\langle \chi, \psi \rangle = \delta_{\chi, \psi}$  ce qui signifie que :

$$\sum_{c \in C(G)} |c| \overline{\chi(c)} \psi(c) = \delta_{\chi, \psi} |G|$$

et donne des relations d'orthogonalité pour les lignes de la table. En particulier, avec  $\chi = 1$  et  $\psi \neq 1$ , on obtient que :

$$\sum_{c \in C(G)} |c| \psi(c) = 0.$$

Considérons alors la matrice suivante, carrée de taille  $c(G)$  :

$$M_{\chi, c} = \sqrt{\frac{|c|}{|G|}} \chi(c).$$

Par ce qui précède,  $M$  est une matrice unitaire (au sens où  $M^*M = \text{id}$ ) et donc sa transposée est aussi unitaire. On en déduit la relation suivante pour toutes classes  $c, d \in C(G)$  :

$$\sum_{\chi \in \widehat{G}} \sqrt{|c||d|} \chi(c) \overline{\chi(d)} = |G| \delta_{c,d}.$$

En particulier, on a :

$$\sum_{\chi \in \widehat{G}} |\chi(c)|^2 = \frac{|G|}{|c|}.$$

Notez qu'avec  $c = 1$  on retrouve que :

$$\sum_{\chi \in \widehat{G}} \dim(\chi)^2 = |G|$$

ce qui restreint fortement les dimensions possibles des représentations irréductibles de  $G$ .

Le théorème suivant permet de restreindre encore plus les dimensions possibles.

**Théorème 18.** (*Propriété d'intégralité*) Pour tout  $\chi \in \widehat{G}$ , on a la relation de divisibilité suivante :

$$\dim(\chi) \mid |G|.$$

*Démonstration.* On part de l'identité  $\langle \chi, \chi \rangle = 1$ , qui s'écrit :

$$|G| = \sum_{g \in G} |\chi(g)|^2.$$

Notons  $C(G)$  l'ensemble des classes de conjugaison de  $G$ . Puisque  $\chi$  est centrale, on a aussi :

$$|G| = \sum_{c \in C(G)} |c| \cdot |\chi(c)|^2.$$

On pose alors, pour toute classe de conjugaison  $c$  :

$$\alpha_c = \sum_{g \in c} g \in Z(\mathbb{Z}[G])$$

qui est dans le centre de  $\mathbb{Z}[G]$ . L'anneau  $Z(\mathbb{Z}[G])$  est fini sur  $\mathbb{Z}$  donc  $\alpha_c$  est entier sur  $\mathbb{Z}$ . Ainsi  $(\alpha_c | W_\chi)$  est un élément de  $Z(\text{Hom}(W_\chi, W_\chi))$  entier sur  $\mathbb{Z}$ , donc c'est une homothétie de rapport  $\chi(\alpha_c)/\dim(\chi)$  entier sur  $\mathbb{Z}$ . On a donc montré que :

$$\lambda_c := \sum_{g \in c} \frac{\chi(g)}{\dim(\chi)} = \frac{\chi(c)|c|}{\dim(\chi)} \in \overline{\mathbb{Z}}.$$

On a :

$$|G| = \sum_{c \in C(G)} \dim(\chi) \overline{\chi(c)} \lambda_c.$$

On a donc :

$$\frac{|G|}{\dim(\chi)} = \sum_{c \in C(G)} \overline{\chi(c)} \lambda_c \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$$

ce qui conclut. □

**Exemple 19.** Si  $G$  est abélien, les caractères irréductibles de  $G$  forment le groupe  $\widehat{G}$  des morphismes de  $G$  vers  $\mathbb{C}^\times$  et les classes de conjugaison sont exactement les éléments de  $G$ , donc il est facile de remplir la table de caractères.

Si  $G$  est cyclique de générateur  $t$  d'ordre  $n \geq 1$ , les caractères de  $G$  sont les  $\chi_\omega$  pour  $\omega \in \mathbb{U}_n$  donnés par  $\chi_\omega(t) = \omega$ , et la table consiste en les  $\chi_\omega(t^k) = \omega^k$ .

Notons qu'on a :

$$\text{Hom}(G \times H, \mathbb{C}^\times) = \text{Hom}(G, \mathbb{C}^\times) \times \text{Hom}(H, \mathbb{C}^\times)$$

et comme tout groupe abélien fini est produit direct de groupes cycliques et tout groupe cyclique est isomorphe à son dual, on a aussi que tout groupe abélien fini est isomorphe à son dual (de façon non-canonique a priori).

**Exemple 20.** (*Table de caractères de  $H_8$* ) Considérons le groupe quaternionique  $H_8$  dont les huit éléments sont  $\pm 1, \pm i, \pm j, \pm k$  avec :

$$i^2 = j^2 = k^2 = ijk = -1.$$

Les classes de conjugaison sont les suivantes :

- La classe triviale notée 1.
- La classe avec seulement  $-1$ , notée  $-1$  (il engendre le centre du groupe).
- La classe de  $\pm i$ , notée  $I$ .
- La classe de  $\pm j$ , notée  $J$ .
- La classe de  $\pm k$ , notée  $K$ .

L'abélianisé de  $H_8$  est  $H_8/\langle -1 \rangle = \langle i, j \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$ . Il y a donc 4 caractères irréductibles de dimension 1 et le dernier doit être de dimension 2 pour avoir :

$$\sum_{\chi} \dim(\chi)^2 = |H_8|.$$

Notons 1 le caractère trivial,  $\alpha, \beta, \alpha\beta$  les trois autres caractères de  $\text{Ab}(H_8)$ , et  $\chi$  le caractère de dimension 2. Les quatre premières lignes sont automatiques à remplir puisqu'on peut décrire explicitement  $1, \alpha, \beta, \alpha\beta$ . La dernière s'obtient par la remarque 17.

	1	-1	I	J	K
1	1	1	1	1	1
$\alpha$	1	1	-1	1	-1
$\beta$	1	1	1	-1	-1
$\alpha\beta$	1	1	-1	-1	1
$\chi$	2	-2	0	0	0

**Exemple 21.** (*Table de caractères de  $D_4$* ) Considérons le groupe diédral  $D_4$  des symétries du carré, engendré par la rotation  $r$  et la réflexion  $f$  avec les relations :

$$r^4 = f^2 = (fr)^2 = 1.$$

Il a un sous-groupe distingué d'ordre 4, engendré par  $r$ , qui est d'indice 2 et donc  $|D_4| = 8$ . Les classes de conjugaison sont les suivantes :

- La classe triviale notée 1.
- La classe avec seulement  $r^2$ , notée  $r^2$ .

- La classe avec  $r$  et  $r^{-1}$ , notée  $R$ .
- La classe avec  $f$  et  $rf r^{-1}$ , notée  $F$ .
- La classe avec  $fr$  et  $rf$ , notée  $FR$ .

L'abélianisé de  $D_4$  est  $D_4/\langle r^2 \rangle = \langle r, f \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$ . Il y a donc 4 caractères irréductibles de dimension 1 et le dernier doit être de dimension 2 pour avoir :

$$\sum_{\chi} \dim(\chi)^2 = |D_4|.$$

On peut d'ailleurs facilement décrire ce dernier caractère  $\chi$  : c'est le caractère de la représentation de  $D_4$  agissant sur  $\mathbb{C}^2$  (par rotations et réflexions).

Il est clair qu'on est dans la même situation que dans l'exemple 20 et qu'on a donc la même table de caractères (avec des noms différents) :

	1	$r^2$	$R$	$F$	$FR$
1	1	1	1	1	1
$\alpha$	1	1	-1	1	-1
$\beta$	1	1	1	-1	-1
$\alpha\beta$	1	1	-1	-1	1
$\chi$	2	-2	0	0	0

On remarque que les groupes  $H_8$  et  $D_4$  ont la même table de caractères. Pourtant, ils ne sont pas isomorphes car ils n'ont pas le même nombre d'éléments d'ordre 4. Ceci entraîne en particulier qu'ils ont la même algèbre de groupes :

$$\mathbb{C}[H_8] \cong \mathbb{C}[D_4]$$

car l'algèbre de groupes est entièrement déterminée, d'après 11 par la dimension des représentations irréductibles. La réciproque est fautive, par exemple deux groupes abéliens de même cardinal  $n$  ont la même algèbre de groupe  $\mathbb{C}^n$  mais pas nécessairement la même table de caractères (voir  $\mathbb{Z}/4\mathbb{Z}$  et  $(\mathbb{Z}/2\mathbb{Z})^2$  par exemple).

**Définition 22.** Deux groupes  $G$  et  $H$  sont *matriciellement équivalents* si  $\mathbb{C}[G] \cong \mathbb{C}[H]$ .

D'après l'isomorphisme fondamental 11, ceci revient à dire qu'ils ont les mêmes dimensions de représentations irréductibles. Notez qu'on ne demande pas que l'isomorphisme vienne d'un morphisme de  $G \rightarrow H$  : si c'était le cas, ce morphisme serait injectif donc serait un isomorphisme.

Si deux groupes  $G$  et  $H$  sont matriciellement équivalents via un isomorphisme fixé  $\mathbb{C}[G] \xrightarrow{\varphi} \mathbb{C}[H]$ , il y a une bijection canonique entre les représentations irréductibles à isomorphisme près de  $G$  et celles de  $H$  (car ce sont les  $\mathbb{C}[G]$ -modules simples) et donc entre  $\widehat{G}$  et  $\widehat{H}$  mais ça ne suffit pas à dire que les tables de caractères sont les mêmes.

De ce qui précède, on a que  $H_8$  et  $D_4$  sont matriciellement équivalents, et qu'en fait deux groupes abéliens sont matriciellement équivalents si et seulement si ils ont le même cardinal.

La dénomination "matriciellement équivalents" s'explique par la caractérisation suivante.

**Proposition 23.** Deux groupes finis  $G$  et  $H$  sont matriciellement équivalents si et seulement  $|G| = |H| = n$  et si il existe  $M_{g \in G, h \in H}$  une matrice carrée de taille  $n$ ,  $N_{h \in H, g \in G}$  une matrice carrée de taille  $n$ , avec :

$$MN = I$$

au sens où :

$$\sum_h M_{gh} N_{hk} = \delta_{g,k}$$

pour tous  $g, k \in G$ , et avec de plus la condition suivante pour tout  $g \in G$  et  $h, h' \in H$  :

$$M_{g, hh'} = \sum_{xy=g} M_{x,h} M_{y,h'}.$$

*Démonstration.* C'est immédiat en traduisant la condition  $\varphi^{-1}(hh') = \varphi^{-1}(h)\varphi^{-1}(h')$  sur la matrice de  $\varphi$ .  $\square$

Mentionnons ensuite d'autres manières de produire des représentations (irréductibles) à partir d'autres et donc de remplir la table de caractères.

Premièrement, si  $\chi \in \widehat{G}$  et si  $\alpha$  est un caractère de dimension 1, alors  $\chi\alpha$  est le caractère de la représentation  $W_\chi \otimes W_\alpha$  et il est irréductible car :

$$\|\chi\alpha\| = 1$$

puisque  $\alpha$  est à valeurs dans le cercle unité. Ainsi, on peut toujours multiplier une ligne par une ligne qui correspond à un caractère de dimension 1 et obtenir une nouvelle ligne de la table de caractères (sauf si on l'avait déjà obtenue avant).

Une autre idée est de faire agir le groupe de Galois absolu. Pour éviter de parler des automorphismes de  $\mathbb{C}$ , on va noter que toute la théorie que l'on a faite s'applique à n'importe quel corps de caractéristique 0 (pour pouvoir moyenner sur tout le groupe) algébriquement clos (pour avoir le lemme de Schur) et donc qu'on aurait aussi pu classifier les représentations à coefficients dans  $\overline{\mathbb{Q}}$  le corps des nombres algébriques. On obtient exactement les mêmes tables de caractères (car on sait qu'il y a  $c(G)$  représentations irréductibles, qu'elles soient complexes ou algébriques, et le caractère d'une représentation est à valeurs dans  $\overline{\mathbb{Q}}$  car les valeurs propres des éléments de  $G$  sont des racines de l'unité).

On obtient alors une action de  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  sur  $\widehat{G}$  : si  $\chi \in \widehat{G}$ , on trouve une représentation  $\rho_\chi : G \rightarrow \text{GL}_{\dim(\chi)}(\overline{\mathbb{Q}})$  qui lui correspond et on pose, pour  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ,  $\rho_\chi^\sigma(g) = \sigma(\rho_\chi(g))$ . Il lui correspond alors le caractère  $\chi^\sigma$  défini par :

$$\chi^\sigma(g) = \sigma(\chi(g)).$$

Comme les valeurs propres de  $g$  sont des racines de l'unité, si  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\text{ab}})$  avec  $\mathbb{Q}^{\text{ab}}$  la plus grande extension abélienne de  $\mathbb{Q}$  contenue dans  $\overline{\mathbb{Q}}$ , on a  $\chi^\sigma = \chi$ . On a donc une action de  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\text{ab}}$  sur  $\widehat{G}$ .

**Remarque 24.** Soit  $V$  une représentation de  $G$  de caractère  $\chi = \text{Tr}_V$ . On définit le noyau de  $V$ , noté  $\text{Ker}(\chi)$ , comme le noyau du morphisme associé à la représentation :  $G \rightarrow \text{GL}(V)$ .

Ce noyau peut se lire sur le caractère  $\chi$  de la façon suivante :

$$\text{Ker}(\chi) = \{g \in G \mid \chi(g) = \dim(\chi)\}.$$

En effet, si  $g \in G$ ,  $g$  est d'ordre fini donc l'endomorphisme de  $V$  associé,  $(g \mid V)$ , est diagonalisable et ses valeurs propres comme endomorphisme de  $V$  sont de module 1 et on a :

$$(g \mid V) = \text{id}_V \iff \text{Spec}(g \mid V) = \{1\} \iff \text{Tr}(g \mid V) = \dim V$$

par le cas d'égalité de l'inégalité triangulaire.

## I.7 Projecteurs et composantes isotypiques

Parlons maintenant des composantes isotypiques d'un  $\mathbb{C}[G]$ -module. De l'isomorphisme fondamental :

$$\mathbb{C}[G] \cong \prod_{\chi} \text{Hom}(W_{\chi}, W_{\chi})$$

on déduit une équivalence de catégories :

$$\mathbb{C}[G] - \text{Mod} \simeq \prod_{\chi} \text{Hom}(W_{\chi}, W_{\chi}) - \text{Mod}$$

dont la réciproque est donnée par  $(V_{\chi})_{\chi} \mapsto \bigoplus_{\chi} V_{\chi}$  (c'est un principe général que  $A \times B - \text{Mod} \cong A - \text{Mod} \times B - \text{Mod}$ ).

Le sens direct s'explique de la façon suivante : pour tout  $\chi$  on a un élément  $\pi_{\chi}$  dont l'image par  $\eta$  dans  $\prod_{\tau} \text{Hom}(W_{\tau}, W_{\tau})$  est 0 en  $\tau \neq \chi$  et  $\text{id}_{W_{\chi}}$  en  $\tau = \chi$ .

Cet élément s'appelle le *projecteur isotypique sur  $\chi$*  et le foncteur  $\mathbb{C}[G] - \text{Mod} \simeq \prod_{\chi} \text{Hom}(W_{\chi}, W_{\chi}) - \text{Mod}$  envoie un  $\mathbb{C}[G]$ -module  $V$  sur la famille des :

$$V_{\chi} = \pi_{\chi} V.$$

Ainsi on a :

$$V = \bigoplus_{\chi} \pi_{\chi} V.$$

Si  $V$  est fini, on peut le décomposer en somme d'irréductibles :

$$V \cong \bigoplus_{\chi} W_{\chi}^{n_{\chi}}$$

et on a alors  $\pi_{\chi} V \cong W_{\chi}^{n_{\chi}}$ , ce qui est clair en inspectant  $\eta(\pi_{\chi})$ .

Ainsi  $\pi_{\chi} V$  donne la composante en puissance de  $W_{\chi}$  dans la somme directe.

On peut décrire explicitement  $\pi_{\chi}$  grâce à 13.

**Lemme 25.** (*Expression du projecteur isotypique*) On a :

$$\pi_{\chi} = \frac{\dim(\chi)}{|G|} \sum_{g \in G} \overline{\chi(g)} g \in \mathbb{C}[G].$$

On en déduit qu'un élément  $x \in V$  est dans la composante  $V_{\chi}$  si et seulement si :

$$\frac{\dim(\chi)}{|G|} \sum_{g \in G} \overline{\chi(g)} gx = x.$$

Pour les caractères de dimension 1, il existe une description très simple.

**Proposition 26.** (*Composante isotypique d'un caractère de dimension 1*) Soit  $V$  un  $\mathbb{C}[G]$ -module et  $\chi$  un caractère de  $V$  de dimension 1. On a :

$$V_{\chi} = \{x \in V \mid \forall g \in G \quad gx = \chi(g)x\}.$$

*Démonstration.* L'inclusion de droite à gauche est facile par le lemme 25.

La deuxième inclusion s'obtient en remarquant que :

$$g\pi_{\chi} = \frac{1}{|G|} \sum_{h \in G} \overline{\chi(h)} gh = \frac{1}{|G|} \sum_h \overline{\chi(g^{-1}h)} h = \chi(g)\pi_{\chi}$$

car  $\chi$  est de dimension 1, donc multiplicatif. □

## I.8 Anneau des caractères

Soit  $G$  un groupe fini. On note  $\mathbb{Z}[\widehat{G}]$  le sous-anneau de  $L^2_{\mathbb{C}}(G)$  (pour le produit usuel des fonctions sur  $G$ ) engendré par les éléments de  $\widehat{G}$ . Puisque  $\widehat{G}$  est stable par produit (car le produit tensoriel de deux représentations de dimension 1 est une représentation de dimension 1, encore irréductible),  $\mathbb{Z}[\widehat{G}]$  a pour  $\mathbb{Z}$ -base les éléments de  $\widehat{G}$  :

$$\mathbb{Z}[\widehat{G}] = \bigoplus_{\chi \in \widehat{G}} \mathbb{Z}\chi.$$

C'est l'anneau des caractères de  $\widehat{G}$ , et ses éléments s'appellent des caractères virtuels (tout caractère virtuel est la différence de deux caractères de représentations de  $G$ ).

## II Théorie de Fourier sur les groupes finis

Le but de cette partie est d'expliquer comment construire une théorie de Fourier sur un groupe fini  $G$ . Il est possible de construire deux théories de Fourier, une plus générale que l'autre : une qui porte sur les fonctions sur  $G$  (appelée théorie de Fourier non-commutative) et une qui porte seulement sur les fonctions centrales sur  $G$  (théorie de Fourier commutative). Notez que si  $G$  est abélien, ces deux théories sont exactement les mêmes.

### II.1 Théorie de Fourier non-commutative

Soit  $G$  un groupe fini. On veut construire une théorie de Fourier pour les fonctions sur  $G$ . Pour cela, on commence par choisir un système de représentations irréductibles unitaires, au sens suivant.

Dans la suite, la notation  $U(n)$  désigne le groupe des matrices unitaires de taille  $n$  à coefficients complexes.

**Définition 27.** Un système de représentations unitaires de  $G$  est la donnée, pour chaque  $\chi \in \widehat{G}$ , d'un morphisme de groupes  $\rho_{\chi} : G \rightarrow U(\dim(\chi))$  tel que la représentation associée soit de caractère  $\chi$ . Ainsi, on a :

$$\rho_{\chi}(g)^* = \rho_{\chi}(g^{-1})$$

où  $*$  est la notation pour la matrice adjointe (transposée de la conjuguée complexe).

**Proposition 28.** Il existe un système de représentations unitaires.

*Démonstration.* Pour chaque  $\chi \in \widehat{G}$ , prenons  $W_{\chi}$  une représentation irréductible de caractère  $\chi$  et munissons-la d'un produit scalaire  $G$ -invariant, comme dans la preuve du théorème de Maschke 4.

Les éléments de  $G$  agissent alors comme des isométries pour ce produit scalaire, et il suffit de choisir une base orthonormée.  $\square$

On fixe dans la suite un tel système de représentations unitaires. On définit  $\mathcal{O}(\widehat{G})$  comme la  $\mathbb{C}$ -algèbre (éventuellement non-commutative)  $\prod_{\chi \in \widehat{G}} M_{\dim(\chi)}(\mathbb{C})$ . On verra les éléments de cet anneau comme des fonctions définies sur  $\widehat{G}$  à valeurs dans des espaces de matrices : si  $\alpha \in \mathcal{O}(\widehat{G})$  et  $\chi \in \widehat{G}$ , on note  $\alpha(\chi) \in M_{\dim(\chi)}(\mathbb{C})$  la valeur en  $\chi$  de  $\alpha$ . On utilise alors l'isomorphisme  $\eta$  du théorème 11 :

$$L^2(G) \cong \mathbb{C}[G] \cong \prod_{\chi} M_{\dim(\chi)}(\mathbb{C}) = \mathcal{O}(\widehat{G}).$$

Cet isomorphisme envoie  $f \in L^2(G)$  sur  $\tilde{f}$  qui est définie ainsi :

$$\tilde{f}(\chi) = \sum_{g \in G} f(g) \rho_\chi(g) \in M_{\dim(\chi)}(\mathbb{C}).$$

Cette formule sera notre définition de la transformée de Fourier (non-commutative) de  $f$ . Il existe des dizaines d'autres conventions, mais on choisira celle-ci car elle donne des formules simples pour la convolution.

**Définition 29.** (*Convolution dans  $L^2(G)$* ) De l'isomorphisme  $L(G) \cong \mathbb{C}[G]$ , on peut munir  $L^2(G)$  d'une unique structure d'algèbre qui fait de cet isomorphisme un isomorphisme d'algèbres :

$$u * v(g) = \sum_{xy=g} u(x)v(y) = \sum_{x \in G} u(x)v(x^{-1}g).$$

Ainsi l'algèbre  $(L^2(G), *)$  est isomorphe à  $\mathbb{C}[G]$  et comme  $Z(\mathbb{C}[G])$  est une sous-algèbre de  $\mathbb{C}[G]$ ,  $L_c^2(G)$  est stable par convolution.

Par construction, on a les formules suivantes.

**Proposition 30.** Pour tous  $u, v \in L^2(G)$ , on a :

$$\widetilde{u * v} = \tilde{u} \cdot \tilde{v}.$$

En particulier, pour tout  $n \geq 0$  :

$$\widetilde{u^{*n}} = \tilde{u}^n.$$

On peut aussi définir un produit scalaire sur  $\mathcal{O}(\widehat{G})$ , via la formule suivante :

$$\langle \alpha, \beta \rangle = \sum_{\chi \in \widehat{G}} \text{Tr}(\alpha^*(\chi)\beta(\chi)) \frac{\dim(\chi)}{|G|^2}.$$

Ce produit scalaire est défini de telle sorte que la transformée de Fourier soit une isométrie. En effet, on a pour tous  $f, g \in L^2(G)$  :

$$\begin{aligned} \langle \tilde{f}, \tilde{g} \rangle &= \sum_{\chi \in \widehat{G}} \text{Tr}(\tilde{f}^*(\chi)\tilde{g}(\chi)) \frac{\dim(\chi)}{|G|^2} = \sum_{x, y \in G} \sum_{\chi \in \widehat{G}} \overline{f(x)g(y)} \text{Tr}(\rho_\chi(x^{-1})\rho_\chi(y)) \frac{\dim(\chi)}{|G|^2} \\ &= \sum_{x, y \in G} \sum_{\chi \in \widehat{G}} \overline{f(x)g(y)} \chi(x^{-1}y) \frac{\dim(\chi)}{|G|^2} \\ &= \frac{1}{|G|^2} \sum_{x, y \in G} \overline{f(x)g(y)} \text{Tr}_{\mathbb{C}[G]}(x^{-1}y) \\ &= \frac{1}{|G|} \sum_{x \in G} \overline{f(x)g(x)} = \langle f, g \rangle. \end{aligned}$$

en utilisant que  $\sum_{\chi} \dim(\chi)\chi = \text{Tr}_{\mathbb{C}[G]}$  où  $\mathbb{C}[G]$  est la représentation régulière de  $G$ . On en déduit la formule de Plancherel :

$$\|f\|^2 = \sum_{\chi} \text{Tr}(\tilde{f}^*(\chi)\tilde{f}(\chi)) \frac{\dim(\chi)}{|G|^2}.$$

De la description explicite de l'isomorphisme inverse  $\eta^{-1}$  13 une formule de transformée de Fourier inverse.

**Proposition 31.** Pour tout  $\alpha \in \mathcal{O}(\widehat{G})$ , on pose :

$$\check{\alpha}(x) = |G| \langle \widetilde{\delta}_x, \alpha \rangle = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \dim(\chi) \operatorname{Tr}(\rho_\chi(x)^* \alpha(\chi))$$

avec  $\delta_x$  la fonction indicatrice de  $\{x\}$ .

L'application  $\check{\bullet}$  est alors la bijection réciproque de  $\widetilde{\bullet}$ .

*Démonstration.* On peut soit le prouver en partant de 13, soit se dire que si  $\check{\bullet}$  désigne la réciproque de  $\widetilde{\bullet}$ , on a :

$$\check{\alpha}(\chi) = |G| \langle \delta_x, \check{\alpha} \rangle = |G| \langle \widetilde{\delta}_x, \alpha \rangle.$$

□

La proposition suivante est facile à vérifier.

**Proposition 32.** On note  $i : G \rightarrow G$  l'application  $x \mapsto x^{-1}$ . On a alors, pour tout  $f \in L^2(G)$  :

$$(\widetilde{f})^* = \widetilde{f \circ i}.$$

De plus, pour tous  $\alpha, \beta, \gamma \in \mathcal{O}(\widehat{G})$ , on a :

$$\langle \alpha \beta, \gamma \rangle = \langle \beta, \alpha^* \gamma \rangle$$

et de façon duale, pour tous  $f, g, h \in L^2(G)$  on a :

$$\langle f * g, h \rangle = \langle g, \overline{f \circ i} * h \rangle.$$

En appliquant cette formule à  $f = \delta_x$ , on obtient :

$$\langle \delta_x * g, h \rangle = \langle g, \delta_{x^{-1}} * h \rangle.$$

Notez que  $\delta_x * \bullet$  est un opérateur de translation sur  $L^2(G)$ .

## II.2 Théorie de Fourier pour les fonctions centrales

On va adapter la théorie précédente au cas des fonctions centrales. Notez qu'il est possible de démontrer les résultats de cette partie sans faire appel à la précédente, simplement en partant du fait que  $\widehat{G}$  forme une base orthonormale de  $L_c^2(G)$  (voir 11).

Soit donc  $G$  un groupe fini. On définit  $L^2(\widehat{G})$  comme l'espace des fonctions de  $\widehat{G}$  dans  $\mathbb{C}$ , que l'on munit du produit de fonctions terme à terme. On peut alors voir  $L^2(\widehat{G})$  comme le centre de l'algèbre  $\mathcal{O}(\widehat{G})$  (voir la partie précédente) puisque :

$$Z(\mathcal{O}(\widehat{G})) = \prod_{\chi \in \widehat{G}} Z(M_{\dim(\chi)})(\mathbb{C}) = \prod_{\chi} \mathbb{C} = L^2(\widehat{G})$$

en identifiant une matrice d'homothétie de rapport  $\lambda$  avec le scalaire  $\lambda$ .

On munit alors  $L^2(\widehat{G}) \subseteq \mathcal{O}(\widehat{G})$  du produit scalaire induit, c'est à dire que pour tous  $\alpha, \beta \in L^2(\widehat{G})$  on a :

$$\langle \alpha, \beta \rangle = \sum_{\chi} \operatorname{Tr}((\alpha(\chi) \operatorname{id})^* \beta(\chi) \operatorname{id}) \frac{\dim(\chi)}{|G|^2}$$

ce qui donne après simplification :

$$\langle \alpha, \beta \rangle = \sum_{\chi} \overline{\alpha(\chi)} \beta(\chi) \frac{\dim(\chi)^2}{|G|^2}.$$

En munissant  $L^2(G)$  du produit de convolution, on a alors des isomorphismes d'algèbres :

$$L^2(G) \longrightarrow \mathbb{C}[G] \xrightarrow{\eta} \mathcal{O}(\widehat{G})$$

et la composée de ces isomorphismes est la transformée de Fourier non-commutative, qui est une isométrie. En prenant le centre de ces algèbres, on obtient des isomorphismes d'algèbres commutatives :

$$L_c^2(G) \longrightarrow Z(\mathbb{C}[G]) \longrightarrow L^2(\widehat{G}).$$

On laisse en exercice le fait que  $L_c^2(G)$  est le centre de  $L^2(G)$  pour la convolution.

La composée est alors un isomorphisme d'algèbres et une isométrie pour les produits scalaires induits, et on l'appelle transformée de Fourier commutative. On la note  $\widehat{\bullet}$  et on note son inverse  $\check{\bullet}$ .

Résumons ses propriétés.

**Théorème 33.** Soit  $f \in L_c^2(G)$ . On a :

$$\widehat{f}(\chi) = \sum_{x \in G} f(x) \frac{\chi(x)}{\dim(\chi)}.$$

On a naturellement  $\widehat{f * g} = \widehat{f} \widehat{g}$  et  $\widehat{f^{*n}} = (\widehat{f})^n$ . La transformée de Fourier inverse est donnée, pour tout  $\alpha \in L^2(\widehat{G})$  par :

$$\check{\alpha}(x) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \dim(\chi)^2 \alpha(\chi) \overline{\chi}(x).$$

On dispose aussi d'une formule de Plancherel :

$$\|f\|^2 = \sum_{\chi} |\widehat{f}(\chi)|^2 \frac{\dim(\chi)^2}{|G|^2}.$$

*Démonstration.* On la laisse au lecteur, ce sont simplement des cas particuliers des formules de la partie précédente. Il est tout à fait possible d'essayer de les démontrer directement d'ailleurs.  $\square$

**Remarque 34.** Encore une fois, il existe de nombreuses conventions, on a choisi celle-ci parce qu'elle est compatible avec la théorie non-commutative et parce qu'elle donne des formules très simples pour la convention. Elle est aussi agréable du point de vue probabiliste comme on le verra dans la partie sur les marches aléatoires. Une convention plus utilisée est  $\widehat{f}(\chi) = \langle \chi, f \rangle$  de façon à avoir  $f = \sum_{\chi} \widehat{f}(\chi) \chi$  pour la transformée inverse.

### II.3 Principe d'incertitude de Donoho-Stark

Soit  $G$  un groupe fini et  $f \in L^2(G)$ . On appelle support de  $f$ , noté  $\text{Supp}(f)$ , l'ensemble des  $x \in G$  tels que  $f(x) \neq 0$  et de même on définit le support de  $\widetilde{f}$  comme l'ensemble des  $\chi \in \widehat{G}$  tels que  $\widetilde{f}(\chi) \neq 0$ .

Le principe d'incertitude en théorie de Fourier stipule que si  $f$  a un petit support, alors  $\widetilde{f}$  a un

grand support, et inversement.

Remarquons qu'on a les cas extrêmes suivants : si  $f = \delta_x$  (support réduit à un point), alors  $\tilde{f}(\chi) = \rho_\chi(x) \neq 0$  (car c'est une matrice inversible) donc  $\text{Supp}(\tilde{f}) = \widehat{G}$ , et si  $f = 1$  (support  $G$ ), alors  $\tilde{f}(\chi) = \sum_x \rho_\chi(x) = \rho_\chi(R)$  avec  $R = \sum_{x \in G} x \in \mathbb{C}[G]$  l'élément de Reynolds, de sorte que  $\tilde{f}(\chi)$  est la projection sur l'espace des points fixes de la représentation  $\mathbb{C}^{\dim(\chi)}$ , et par irréductibilité, cet espace de points fixes est 0 sauf si  $\chi$  est la représentation triviale, donc  $\tilde{f}(\chi) = \delta_{\chi,1} \text{id}$ .

Ce principe peut prendre la forme de la jolie inégalité suivante :

**Théorème 35.** (*Principe d'incertitude de Donoho-Stark*) Notons  $d_G$  le maximum des dimensions des représentations irréductibles de  $G$  (en particulier  $d_G \mid |G|$  d'après 18). Soit  $f \in L^2(G)$  une fonction non nulle. On a :

$$|\text{Supp } f| \times |\text{Supp } \tilde{f}| \geq \frac{|G|}{d_G^2}$$

Notons que la constante  $d_G$  vaut 1 si et seulement si  $G$  est abélien.

*Démonstration.* On définit une norme infinie sur  $L^2(G)$  et une norme infinie sur  $\mathcal{O}(\widehat{G})$ , toutes deux notées  $\|\bullet\|_\infty$  et définies de la façon suivante. Pour  $u \in L^2(G)$  on pose :

$$\|u\|_\infty = \sup_{x \in G} |f(x)|.$$

Pour  $\alpha \in \mathcal{O}(\widehat{G})$ , on pose :

$$\|\alpha\|_\infty = \sup_{\chi \in \widehat{G}} \sqrt{\text{Tr}(\alpha(\chi)^* \alpha(\chi))}$$

c'est à dire le maximum des normes de Frobenius des  $\alpha(\chi)$ .

On peut alors écrire :

$$\tilde{f}(\chi) = \sum_{x \in \text{Supp}(f)} f(x) \rho_\chi(x).$$

On a donc :

$$\|\tilde{f}\|_\infty \leq \sum_{x \in \text{Supp}(f)} |f(x)| \sqrt{d_G} \leq \|f\|_\infty |\text{Supp}(f)| \sqrt{d_G}.$$

car la norme de Frobenius de  $\rho_\chi(x)$  est  $\sqrt{\dim(\chi)}$  puisque  $\rho_\chi(x)$  est unitaire.

Écrivons maintenant la transformée de Fourier inverse 31 :

$$f(x) = \frac{1}{|G|} \sum_{\chi \in \text{Supp}(\tilde{f})} \dim(\chi) \text{Tr}(\rho_\chi(x)^* \tilde{f}(\chi))$$

donc par Cauchy-Schwarz pour le produit scalaire hermitien  $A, B \mapsto \text{Tr}(A^* B)$  :

$$\|f\|_\infty \leq \frac{|\text{Supp}(\tilde{f})| d_G^{3/2}}{|G|} \|\tilde{f}\|_\infty.$$

En rassemblant les deux inégalités et en utilisant que  $f \neq 0$ , on en déduit :

$$|\text{Supp } f| \times |\text{Supp } \tilde{f}| \geq \frac{|G|}{d_G^2}.$$

□

Si  $f$  est centrale,  $\tilde{f}$  et  $\widehat{f}$  ont le même support donc on a immédiatement le corollaire suivant.

**Corollaire 36.** Soit  $f \in L_c^2(G)$  une fonction centrale non-nulle, on a aussi :

$$|\text{Supp } f| \times |\text{Supp } \widehat{f}| \geq \frac{|G|}{d_G^2}.$$

### III Marches aléatoires sur les groupes finis

#### III.1 Généralités

Soit  $G$  un groupe fini. Une loi de probabilité sur  $G$  est une fonction  $p \in L^2(G)$  qui vérifie  $\sum_{x \in G} p(x) = 1$  et  $p \geq 0$ . On peut interpréter la transformée de Fourier de  $p$  de façon probabiliste.

**Lemme 37.** Soit  $X$  une variable aléatoire sur  $G$  de loi  $p$ . On a :

$$\tilde{p}(\chi) = \mathbb{E}(\rho_\chi(X)).$$

*Démonstration.* En effet :

$$\tilde{p}(\chi) = \sum_{x \in G} p(x) \rho_\chi(x) = \mathbb{E}(\rho_\chi(x)).$$

□

Une marche aléatoire sur  $G$  de loi  $p$  est la donnée d'une suite  $X_1, X_2, \dots$  de variables aléatoires indépendantes de même loi  $p$ . Le  $n$ -ème pas de la marche est défini par :

$$S_n = X_n X_{n-1} \dots X_1$$

avec  $S_0 = 1_G$  par convention. On note  $p_n \in L^2(G)$  la loi de  $p$ . On a alors :

$$p_n = p^{*n}.$$

En effet, par indépendance :

$$p_n(a) = \sum_{x_n x_{n-1} \dots x_1 = a} p(x_n) \dots p(x_1) = p^{*n}(a).$$

Notons que  $p^{*0} = \delta_{1_G}$  est le neutre pour la convolution, et c'est bien  $p_0$ .

On en déduit la formule suivante pour la transformée de Fourier de  $p_n$  :

$$\tilde{p}_n = (\tilde{p})^n.$$

La transformée de Fourier inverse donne alors :

$$p_n(x) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \dim(\chi) \operatorname{Tr}(\rho_\chi(x)^* \tilde{p}(\chi)^n).$$

On peut généraliser cette formule ainsi. On note  $X$  une variable aléatoire de loi  $p$ .

**Proposition 38.** Soit  $f \in L^2(G)$ . On a :

$$\mathbb{E}(f(S_n)) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \dim(\chi) \operatorname{Tr}((\tilde{p}(\chi)^n)^* \tilde{f}(\chi)).$$

*Démonstration.* On a :

$$f(x) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \dim(\chi) \operatorname{Tr}(\rho_\chi(x)^* \tilde{f}(\chi))$$

donc :

$$f(S_n) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \dim(\chi) \operatorname{Tr}(\rho_\chi(X_1)^* \dots \rho_\chi(X_n)^* \tilde{f}(\chi)).$$

donc par indépendance :

$$\mathbb{E}(f(S_n)) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \dim(\chi) \operatorname{Tr} \left( \mathbb{E} \left( \rho_\chi(X)^* \right)^n \widetilde{f}(\chi) \right)$$

et on conclut avec le lemme 37.  $\square$

**Remarque 39.** On ne retrouve pas exactement la formule précédente pour  $f = \delta_x$ , on obtient sa conjuguée mais comme une probabilité est réelle c'est bien la même chose.

Dans ce qui précède, on a utilisé le lemme suivant.

**Lemme 40.** Soient  $A$  et  $B$  deux matrices aléatoires indépendantes (sur un univers fini) telles que le produit  $AB$  a du sens. Alors :

$$\mathbb{E}(AB) = \mathbb{E}(A)\mathbb{E}(B).$$

*Démonstration.* On a :

$$\mathbb{E}(AB)_{ij} = \mathbb{E}((AB)_{ij}) = \mathbb{E} \left( \sum_k A_{ik} B_{kj} \right) = \sum_k \mathbb{E}(A_{ik}) \mathbb{E}(B_{kj})$$

ce qui donne la formule voulue.  $\square$

**Proposition 41.** La marche aléatoire  $X$  va partout où elle a le droit d'aller, au sens où :

$$\bigcup_{N \geq 0} \operatorname{Supp} S_N = \langle \operatorname{Supp} X \rangle$$

où  $\operatorname{Supp}$  désigne le support de la loi d'une variable aléatoire et  $\langle \bullet \rangle$  est la notation pour "sous-groupe engendré". Ce sous-groupe est appelé *groupe engendré par la marche  $X$* .

*Démonstration.* L'inclusion de gauche à droite est claire. Ensuite, on a  $\operatorname{Supp} X \subseteq \bigcup_{N \geq 0} \operatorname{Supp} S_N$ , et il suffit donc de montrer que cette réunion est un groupe : elle contient le neutre (prendre  $N = 0$ ) et elle est stable par produit puisque si la marche peut aller en  $a$  en  $k$  étapes et en  $b$  en  $\ell$  étapes avec des probabilités non nulles, alors elle peut, par indépendance des  $X_i$ , aller en  $ba$  en  $k + \ell$  étapes avec probabilité non nulle. Il n'y a pas besoin de vérifier que c'est stable par inverse puisque  $G$  est fini.  $\square$

On dit que la marche aléatoire *engendre*  $G$  si le groupe engendré par la marche est  $G$ .

### III.2 Valeurs propres de la transformée de Fourier de $p$ et caractères critiques

On considère une loi de probabilité  $p$  sur un groupe fini  $G$  et  $X$  une variable aléatoire de loi  $p$ . On suppose que la marche aléatoire associée engendre  $G$ , autrement dit que le support de  $p$  engendre  $G$ . On note  $\|\bullet\|$  la norme d'opérateur sur  $M_n(\mathbb{C})$  associée à la norme euclidienne sur  $\mathbb{C}^n$ . Par le lemme 37, on a :

$$\|\widetilde{p}(\chi)\| \leq 1$$

car  $\rho_\chi(X)$  est unitaire donc de norme 1. Ainsi le rayon spectral de  $\widetilde{p}(\chi)$  est inférieur ou égal à 1 :

$$\operatorname{Spec}(\widetilde{p}(\chi)) \subseteq \{z \mid |z| \leq 1\}.$$

**Définition 42.** Un caractère  $\chi \in \widehat{G}$  est *critique* (pour la marche aléatoire de loi  $p$ ) si le rayon spectral de  $\widetilde{p}(\chi)$  vaut 1.

La proposition suivante est fondamentale.

**Proposition 43.** (*Caractérisation des caractères critiques*) Soit  $\chi \in \widehat{G}$ . C'est un caractère critique si et seulement si  $\chi$  est de dimension 1 et pour tout  $g \in \text{Supp}(p)$  on a  $\rho_\chi(g) = \lambda$  pour un certain  $\lambda$  de module 1 (autrement dit  $\rho_\chi(X) = \lambda$  presque sûrement). En particulier, si  $\chi \neq 1$ , alors 1 n'est pas valeur propre de  $\widetilde{p}(\chi)$  et donc  $1 - \widetilde{p}(\chi)$  est inversible.

Cet unique  $\lambda$  est la *valeur critique* de  $\chi$ . Les caractères critiques sont donc constants sur le support.

**Remarque 44.** Notez que si  $p(1) > 0$ , alors la seule valeur critique possible est 1 et donc le seul caractère critique est le caractère trivial.

*Démonstration.* Supposons que  $\widetilde{p}(\chi)$  possède une valeur propre  $\lambda$  de module 1 associée à un vecteur propre  $u \in \mathbb{C}^{\dim(\chi)}$  unitaire. On a donc :

$$\mathbb{E}(\rho_\chi(X)u) = \lambda u$$

et donc :

$$1 = \|\lambda u\| = \|\mathbb{E}(\rho_\chi(X)u)\| \leq \mathbb{E}(\|\rho_\chi(X)u\|) = \mathbb{E}(\|u\|) = 1$$

donc on est dans le cas d'égalité de l'inégalité triangulaire pour une norme euclidienne et les  $\rho_\chi(X)u$  est presque sûrement sur la demi-droite portée par  $\lambda u$ , et comme ils sont de norme 1 :

$$\rho_\chi(X)u = \lambda u$$

presque sûrement. Ainsi, pour tout  $g$  dans le support de  $p$  on a  $\rho_\chi(g)u = \lambda u$  donc le sous-groupe de  $G$  qui stabilise  $\text{Vect}(u)$  contient le support de  $p$ , et puisque  $p$  engendre  $G$ , on en déduit que  $\text{Vect}(u)$  est stable par  $G$ .

Or  $\rho_\chi$  est une représentation irréductible donc ceci entraîne qu'elle est de dimension 1. On peut donc supposer  $u = 1$  et en déduire que pour tout  $g \in \text{Supp}(p)$  :

$$\rho_\chi(g) = \lambda.$$

La réciproque est claire. Si  $\lambda = 1$ , on obtient que le support de  $p$  agit trivialement donc  $G$  agit trivialement donc  $\chi = 1$ . □

**Proposition 45.** Les caractères critiques pour  $p$  forment un sous-groupe cyclique  $\Gamma$  de  $\text{Hom}(G, \mathbb{C}^\times)$ . Le cardinal de ce groupe est appelé *ordre critique* de la marche aléatoire. De plus, un caractère critique est entièrement déterminé par sa valeur critique.

Si  $\kappa$  est l'ordre critique de la marche aléatoire, on a une réunion disjointe :

$$\bigsqcup_{i=0}^{\kappa-1} \text{Supp}(p_i) \subseteq G$$

avec toujours  $p_i = p^{*i}$ . On a d'ailleurs l'inégalité suivante :

$$\kappa \leq |\text{Supp}(\widetilde{p})| d_G^2$$

avec  $d_G$  la dimension de la plus grande représentation irréductible de  $G$ .

*Démonstration.* Il est clair que les caractères critiques forment un sous-groupe de  $\text{Hom}(G, \mathbb{C}^\times)$  car ce sont les caractères de dimension 1 constants sur le support de  $p$ . On a alors un morphisme :

$$\Gamma \longrightarrow \mathbb{C}^\times$$

qui envoie  $\chi$  sur sa valeur critique (valeur sur le support de  $p$ ). Ce morphisme est injectif car le support de  $p$  engendre  $G$ , et un sous-groupe fini de  $\mathbb{C}^\times$  est cyclique donc  $\Gamma$  est cyclique.

Ensuite, prenons  $\chi$  un générateur de  $\Gamma$  et notons  $\lambda$  sa valeur critique, qui est donc une racine primitive  $\kappa$ -ème de l'unité. Ainsi  $\chi$  vaut 1 sur  $\text{Supp}(p_0)$ ,  $\lambda$  sur  $\text{Supp}(p)$ ,  $\lambda^2$  sur  $\text{Supp}(p_2)$  et ainsi de suite, et comme les valeurs  $1, \lambda, \dots, \lambda^{\kappa-1}$  sont distinctes, ces ensembles doivent être disjoints. On en déduit :

$$\sum_{i=0}^{\kappa-1} |\text{Supp}(p_i)| \leq |G|$$

et en appliquant l'inégalité de Donoho-Stark 35 on obtient :

$$|G| \geq \sum_{i=0}^{\kappa-1} \frac{|G|}{d_G^2 |\text{Supp}(\tilde{p}_i)|}$$

et on sait que  $\tilde{p}_i = (\tilde{p})^i$  donc  $\text{Supp}(\tilde{p}_i) \subseteq \text{Supp}(\tilde{p})$  et donc :

$$|G| \geq \kappa \frac{|G|}{d_G^2 |\text{Supp}(\tilde{p})|}$$

d'où l'inégalité annoncée. □

**Remarque 46.** Notons que :

$$\kappa \mid \text{pgcd}\{k \geq 1 \mid p_k(1) > 0\}.$$

En effet, si  $p_k(1) > 0$ , il existe  $x_1, \dots, x_k \in \text{Supp}(p)$  qui vérifient  $x_1 \dots x_k = 1$  et donc pour tout  $\chi \in \Gamma$  de valeur critique  $\lambda$  on a  $\lambda^k = \chi(x_1) \dots \chi(x_k) = 1$  et donc  $\kappa \mid k$ .

On peut se demander si il y a égalité entre  $\kappa$  et  $\text{pgcd}\{k \geq 1 \mid p_k(1) > 0\}$ , mais c'est faux : voici un exemple qui je pense est minimal, on prend  $G = \mathbb{U}_{12}$  et une loi  $p$  de support  $\{\zeta_4, \zeta_6\}$  avec  $\zeta_4$  d'ordre 4 et  $\zeta_6$  d'ordre 6. Ici, le pgcd des temps de retour (la deuxième quantité) vaut  $\text{pgcd}(4, 6) = 2$  alors que  $\kappa$  vaut 1 car le seul caractère d'ordre 2 n'est pas constant sur le support.

**Remarque 47.** Dans le cas où il y a un deux éléments inverses l'un de l'autre dans le support de  $p$ , l'ordre critique vaut 1 ou 2.

On verra que les caractères critiques interviennent différemment dans les calculs. Le lemme suivant sera très utile dans la suite.

**Lemme 48.** Soit  $A \in M_d(\mathbb{C})$  une matrice de rayon spectral  $R$ . On a alors :

$$A^n = O(R^n n^{d-1})$$

quand  $n$  tend vers l'infini, et en particulier pour tout  $r > R$  on a  $A^n = O(r^n)$ .

*Démonstration.* Utiliser la décomposition de Dunford-Jordan. □

### III.3 Fréquence de passages en un point

On considère une marche aléatoire  $S_n$  de loi  $p$  sur un groupe fini  $G$  qui engendre  $G$  au sens où le sous-groupe engendré par la marche est  $G$ . Pour  $a \in G$ , on pose :

$$F_n(a) = \frac{1}{n} \sum_{k=0}^{n-1} 1_{S_k=a}$$

qui est la fréquence de passage de la marche aléatoire au point  $a$  après le  $n - 1$ -ème pas. On pose alors :

$$v_n(a) = \mathbb{E}(F_n(a))$$

la fréquence moyenne de passage en  $a$ . On a :

$$v_n(a) = \frac{1}{n} \sum_{k=0}^{n-1} p_k(a) = \frac{1}{n} \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \dim(\chi) \operatorname{Tr} \left( \rho_\chi(a)^* \sum_{k=0}^{n-1} \widetilde{p}(\chi)^k \right).$$

La contribution de  $\chi = 1$  à cette somme est  $\frac{1}{|G|}$  et donc on peut écrire :

$$v_n(a) = \frac{1}{|G|} + \sum_{\chi \neq 1} v_{\chi,n}(a)$$

avec :

$$v_{\chi,n}(a) = \frac{1}{n|G|} \dim(\chi) \operatorname{Tr} \left( \rho_\chi(a)^* \sum_{k=0}^{n-1} \widetilde{p}(\chi)^k \right).$$

Puisque la marche aléatoire engendre  $G$ , pour  $\chi \neq 1$ ,  $1$  n'est pas valeur propre de  $\widetilde{p}(\chi)$  et on a donc :

$$v_{\chi,n}(a) = \frac{\dim(\chi)}{n|G|} \operatorname{Tr} \left( \rho_\chi(a)^* (1 - \widetilde{p}(\chi))^{-1} \right) - \varepsilon_{\chi,n}(a)$$

avec :

$$\varepsilon_{\chi,n}(a) = \frac{\dim(\chi)}{n|G|} \operatorname{Tr} \left( \rho_\chi(a)^* \widetilde{p}(\chi)^n (1 - \widetilde{p}(\chi))^{-1} \right).$$

**Lemme 49.** Si  $\chi$  n'est pas critique, on a :

$$\varepsilon_{\chi,n}(a) = O\left(R_\chi^n n^{\dim(\chi)-2}\right)$$

avec  $R_\chi < 1$  le rayon spectral de  $\widetilde{p}(\chi)$ .

Si  $\chi$  est critique de valeur critique  $\lambda \neq 1$ , alors :

$$\varepsilon_{\chi,n}(a) = \frac{\overline{\chi}(a) \lambda^n}{n|G|(1-\lambda)}.$$

*Démonstration.* On utilise le lemme 48 :

$$\sum_{k=0}^{n-1} \widetilde{p}(\chi)^k = (1 - \widetilde{p}(\chi))^{-1} - \widetilde{p}(\chi)^n (1 - \widetilde{p}(\chi))^{-1} = (1 - \widetilde{p}(\chi))^{-1} + O\left(R_\chi^n n^{\dim(\chi)-1}\right).$$

On en déduit bien l'estimation souhaitée dans le cas non-critique. Le cas critique est clair.  $\square$

On en déduit le théorème suivant.

**Théorème 50.** Soit  $p$  une loi de probabilité sur un groupe fini  $G$  et  $S_n$  une marche aléatoire de loi  $p$  qui engendre  $G$ . On a alors pour tout  $a \in G$  :

$$\nu_n(a) = \frac{1}{|G|} + O\left(\frac{1}{n}\right).$$

Plus précisément, on a pour tout  $R \in ]0, 1[$  strictement plus grand que tous les rayons spectraux des  $\tilde{p}(\chi)$  avec  $\chi$  non-critique :

$$\nu_n(a) = \frac{1}{|G|} + \frac{1}{n|G|} \sum_{\chi \neq 1} \dim(\chi) \operatorname{Tr}(\rho_\chi(a)^* (1 - \tilde{p}(\chi))^{-1}) - \frac{1}{n|G|} \sum_{\chi \neq 1, \text{ critique}} \frac{\bar{\chi}(a) \tilde{p}(\chi)^n}{1 - \tilde{p}(\chi)} + O(R^n)$$

et on peut améliorer le  $O(R^n)$  en  $O(S^n n^{d_G-2})$  avec  $d_G$  la borne supérieure des  $\dim(\chi)$  et  $S$  la borne supérieure des rayons spectraux des  $\tilde{p}(\chi)$  avec  $\chi$  non-critique.

**Remarque 51.** Si  $p(1) > 0$ , la remarque 44 donne :

$$\nu_n(a) = \frac{1}{|G|} + \frac{1}{n|G|} \sum_{\chi \neq 1} \dim(\chi) \operatorname{Tr}(\rho_\chi(a)^* (1 - \tilde{p}(\chi))^{-1}) + O(R^n).$$

Généralisons cette remarque.

**Corollaire 52.** Pour tout  $n$  divisible par l'ordre critique  $\kappa$  (voir 45), on a :

$$\nu_n(a) = \frac{1}{|G|} + \frac{1}{n|G|} \sum_{\chi \neq 1} \dim(\chi) \operatorname{Tr}(\rho_\chi(a)^* (1 - \tilde{p}(\chi))^{-1}) - \frac{1}{n|G|} \sum_{\chi \neq 1, \text{ critique}} \frac{\bar{\chi}(a)}{1 - \tilde{p}(\chi)} + O(R^n).$$

**Remarque 53.** On peut donner une formule plus simple pour le nombre de passages en le neutre :

$$\nu_n(1) = \frac{1}{|G|} + \frac{1}{n|G|} \sum_{\chi \neq 1} \dim(\chi) \operatorname{Tr}((1 - \tilde{p}(\chi))^{-1}) - \frac{1}{n|G|} \sum_{\lambda \in \mathbb{U}_\kappa \setminus \{1\}} \frac{\lambda^n}{1 - \lambda} + O(R^n)$$

et si  $\kappa \mid n$  :

$$\nu_n(1) = \frac{1}{|G|} + \frac{1}{n|G|} \sum_{\chi \text{ non critique}} \dim(\chi) \operatorname{Tr}((1 - \tilde{p}(\chi))^{-1}) + O(R^n).$$

### III.4 Nombre de sites visités

Soit  $X$  une marche aléatoire de loi  $p$  sur un groupe fini  $G$ . On s'intéresse, pour  $n \geq 0$ , au nombre moyen de sites visités par la marche au bout de  $n$  pas. Pour cela, on pose :

$$U_n = \mathbb{P}\left(\bigcap_{k=1}^n (S_k \neq 1)\right)$$

et  $u(z) = \sum_{n \geq 0} U_n z^n$  la série génératrice associée. On note toujours  $p_n$  la loi de  $S_n$ , c'est à dire  $p_n = p^{*n} \in L^2(G)$  et on pose  $\varphi_a(z) = \sum_{n \geq 0} p_n(a) z^n$  de sorte que, par 38 pour  $z$  assez petit :

$$\begin{aligned} \varphi_a(z) &= \sum_{n \geq 0} \frac{1}{|G|} \sum_{\chi} \dim(\chi) \operatorname{Tr}(\rho_\chi(a)^* \tilde{p}(\chi)^n z^n) \\ &= \frac{1}{|G|} \sum_{\chi} \dim(\chi) \operatorname{Tr}(\rho_\chi(a)^* (1 - z \tilde{p}(\chi))^{-1}). \end{aligned}$$

**Lemme 54.** On a :

$$u(z) = \frac{1}{(1-z)\varphi_1(z)}.$$

*Démonstration.* On observe, pour tout  $n \geq 0$  :

$$\begin{aligned} 1 &= \mathbb{P}\left(\bigcup_{k=1}^n (S_k = 1)\right) + U_n \\ &= \sum_{k=1}^n \mathbb{P}(S_k = 1) \mathbb{P}\left(\bigcap_{i=1}^{n-k} (S_i \neq 1)\right) + U_n \\ &= \sum_{k=0}^n p_k(1) U_{n-k} \end{aligned}$$

en décomposant l'évènement  $\bigcup_{k=1}^n (S_k = 1)$  selon la date  $k$  du dernier moment où 1 est atteint par la marche entre les temps 1 et  $n$ . Autrement dit :

$$\frac{1}{1-z} = \varphi_1(z)u(z)$$

et  $\varphi_1(0) = 1$  donc  $\varphi_1$  est inversible dans  $\mathbb{C}[[z]]$ , d'où la formule annoncée.  $\square$

À présent, pour  $a \in G$ , notons  $V_{a,n}$  la probabilité que  $a$  soit visité par la marche pendant les  $n$  premiers pas :

$$V_{a,n} = \mathbb{P}\left(\bigcup_{k=0}^n (S_k = a)\right)$$

En particulier on a toujours  $V_{1,n} = 1$ . On note  $v_a(z) = \sum_{n \geq 0} V_{a,n} z^n$  la série génératrice associée.

**Lemme 55.** On a :

$$v_a(z) = \frac{1}{1-z} \frac{\varphi_a(z)}{\varphi_1(z)}.$$

*Démonstration.* En décomposant s'évènement  $\bigcup_{k=0}^n (S_k = a)$  selon la date  $k$  entre 0 et  $n$  où la valeur  $a$  a été prise par la marche au dernier moment, on obtient :

$$V_{a,n} = \sum_{k=0}^n p_k(a) U_{n-k}$$

donc  $v_a(z) = \varphi_a(z)u(z) = \frac{1}{1-z} \frac{\varphi_a(z)}{\varphi_1(z)}$ .  $\square$

On note à présent  $W_n$  le nombre moyen de sites visités par la marche pendant les  $n$  premiers pas :  $W_n = \mathbb{E}(|\{S_0, S_1, \dots, S_n\}|)$ . On pose  $w(z) = \sum_{n \geq 0} W_n z^n$  la série génératrice associée.

**Lemme 56.** Soit  $A \in M_n(\mathbb{C})$  une matrice. On a, pour  $z$  assez petit :

$$\text{Tr}\left((1-zA)^{-1}\right) = \frac{f'(1/z)}{zf(1/z)}$$

avec  $f(z) = \det(z-A)$  le polynôme caractéristique de  $A$ .

*Démonstration.* On calcule, avec  $\lambda_1, \dots, \lambda_n$  les valeurs propres de  $A$  :

$$\text{Tr}\left((1 - zA)^{-1}\right) = \sum_i \frac{1}{1 - z\lambda_i} = \frac{f'(1/z)}{zf(1/z)}$$

avec :

$$f(z) = \prod_i (z - \lambda_i)$$

le polynôme caractéristique de  $A$ . □

**Proposition 57.** On a :

$$w(z) = \frac{|G|}{(1-z)^2} \left( \sum_{\chi} \dim(\chi) \text{Tr}\left((1 - z\tilde{p}(\chi))^{-1}\right) \right)^{-1}$$

D'après le lemme précédent,  $w(z)$  est donc une fraction rationnelle et ainsi les  $W_n$  vérifient une relation de récurrence linéaire qui permet de les calculer en pratique.

*Démonstration.* Remarquons d'abord que  $w(z) = \sum_{a \in G} v_a(z)$ . En effet, pour tout  $n \geq 0$ ,  $W_n$  est l'espérance de :

$$\sum_{a \in G} 1_{(\exists k \leq n \ S_k = a)}$$

donc  $W_n = \sum_{a \in G} V_{a,n}$ .

On calcule alors :

$$w(z) = \sum_{a \in G} v_a(z) = \frac{1}{(1-z)\varphi_1(z)} \sum_{a \in G} \varphi_a(z)$$

Or la somme des  $p_n(a)$  pour  $a \in G$  vaut 1, autrement dit  $\sum_{a \in G} \varphi_a(z) = \frac{1}{1-z}$ , d'où la formule annoncée. □

**Remarque 58.** La théorie précédente se simplifie grandement quand la marche aléatoire est *centrale*, au sens où la loi  $p$  est une fonction centrale sur  $G$ . En effet, on peut alors tout exprimer en fonction de la transformée de Fourier  $\widehat{p} \in L^2(\widehat{G})$ . On laisse au lecteur le soin de retrouver les formules précédentes dans le cas d'une marche centrale.