RÉPUBLIQUE ALGÉRIÈNNE DÉMOCRATIQUE ET POPULAIRE.
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
UNIVERSITÉ MOULOUD MAMMERI, TIZI-OUZOU
Faculté de Sciences
Département de Mathématiques

Mémoire de Master de Mathématiques Appliquées
Option : Processus Aléatoires et Statistique de la Décision

LA FORMULE DE PLANCHEREL

ET LES CHAINES DE MARKOV

sous la direction de
Mr BOUDIBA Mohand Arezki

présenté le 8 /10 /2012 par
BOUGHRARA SABRINA

devant le Jury :

Mr. HAMADOUCHE DJAMEL, Professeur, UMMTO, Président
Mr. BOUDIBA Mohand Arezki, Maître de Conférence, UMMTO, Rapporteur
Mr. BERKOUN Youcef, Maître de Conférence, UMMTO, Examinateur.
Mme. HARMIM DEHBIA, Chargée de Recherche, UMMTO, Examinatrice

Remerciements

Je tiens à exprimer toute ma reconnaissance à ***M.Boudiba Med-Arezki*** *pour l'honneur qu'il m'a fait en assurant la direction, le suivi scientifique et téchnique du présent memoire. Je le remercie aussi pour sa grande contribution à l'aboutissement de ce travail, et pour son immense disponibilité malgré son emploi de temps chargé.*

Mes vives remerciements s'adressent aussi au Président et à l'ensemble des membres du jury pour l'honneur qu'ils me font en acceptant de juger et d'éxaminer ce travail.

Je remercie également tous ceux qui ont contribué de prés ou de loin à la réalisation de ce modeste travail.

Par ailleurs, je remercie aussi les camarades étudiants et amis du Master pour la collaboration et la discussion tout au long de ce travail. Nous avons compris ensemble que c'est du choc des idées que jaillisse la lumière pour l'avancement de la science.

Dédicace

J'éxprime ma gratitude à ma famille qui m'a toujours soutenue et encouragée dans la voie que je m'étais fixée. Je remercie mes parents BOUGHRARA Said et CHALLAL Tassadit avec que j'ai vecu dans un climat toujours serein à l'abri de tous soucis affectifs.

Je remércie également mon frére unique Aissa, mes soeurs, mes tantes, oncles, cousins et mes cousines qui sont venus me soutenir lors de ma présentation.

Sans oublier mes deux chères amies Akila et Kahina et tous mes collègues en master qui m'ont accompagné durant les deux années master 1 et 2.

Table des matières

Introduction

L'étude de processus de Markov $(X_n)_n$ engendrés par des produits de composition de fonctions aléatoires indépendantes $(F_n)_n$ est intensément étudié ces derniéres années. Le modèle le plus simple de ce type de processus est constitué par les marches aléatoires. La généralisation introduite par rapport aux marches aléatoires tient dans le type de fonction F_n. Ce qui est nouveau depuis quelques années, c'est qu'en général ces fonctions F_n ne sont pas linéaires et donc le modéle des marches aléatoires ne convient pas tout à fait. Depuis les travaux de Furstehberg dans les années 80, de nombreux auteurs se sont intéressés à ce type de Processus : Letac, Diaconis, Guivarc'h, Bougerol, Mirek,..De nombreux traveaux sont consacrés chaque année à l'étude des propriétés de ce type de processus.

L'absence d'une théorie générale pour ce type de processus, fait qu'au niveau des méthodes d'étude, un appareillage mathématique élaboré et varié est nécéssaire. Furstenberg utilise des algébres et des groupes de Lie ; Diaconis developpe l'analyse de Fourier ; Guivarc'h les opérateurs de Doeblin-Fortet ; Mirek la théorie ergodique,...

Les problèmes posés par l'étude de ces processus sont la rechérche de conditions sur les F_n pour assurer la convergence du processus itéré $F_1 \circ F_2 \cdots \circ F_n$, ou de donner quelque caractérisation utile sur le comportement assymptotique.

Nous nous intéressons au cas où le processus itératif est produit par la double recurrence $X_{n+1} = a_n X_n + b_n X_{n-1}$ et $(X_n)_n$ est à valeurs dans le groupe $\mathbb{Z}/p\mathbb{Z}$. Cela nous a amené à rassembler les éléments de base sur les marches aléatoires et l'Analyse de Fourier, à partir des ouvrages classiques : Naimark et Stern, Serre et Rudin...La formule de Placherel apparait comme

un élément crucial. Dans le premier chapitre nous introduisons le modèle général de marche aléatoire et les notions d'action de groupe sur un ensemble. Le deuxième chapitre est consacré aux représentations linéaires d' un groupe fini. Dans le troisième chapitre nous nous interessons à la transformée de Fourier et à la formule de Plancherel. Le quatrième chapitre est consacré à l'application de la formule de Plancherel à l'étude des chaînes de Markov $X_{n+1} = a_n X_n + b_n X_{n-1}$.

Chapitre 1

Marches aléatoires

1.1 Action d'un groupe sur un ensemble

Pour définir le modèle général d'une marche aléatoire, nous avons besoin de définir l'action d'un groupe sur un ensemble.

Définition 1. *Soient (G,.) un groupe d'élément neutre e et E un ensemble. On dit que G opère dans E, si on a une application*

$$\begin{array}{rcl} \varphi : G \times E & \longrightarrow & E \\ (g, x) & \longmapsto & \varphi(g, x) = g * x \end{array}$$

tel que :

$$1)\ \forall g_1,\ g_2 \in G,\ \forall x \in E,\ g_1 * (g_2 * x) = (g_1.g_2) * x.$$

$$2)\ \forall x \in E,\ e * x = x.$$

3) **Action fidèle :** *Soient E un ensemble et G un groupe agissant sur E. On dit que l'action de G sur E est fidèle si elle est injective.*

4) **Action transitive :** *On dit que G opère transitivement sur E si : $\forall x$, $y \in E$, $\exists g \in G$ tel que : $g * x = y$.*
Et si $\forall x,\ y \in E, \exists!\ g \in G$ tel que : $g * x = y$, l'action de G sur E est dite simplement transitive.

Remarques

1) ***Orbites :*** La relation $\exists g \in G$ tel que : $y = g * x$ est une relation d'équivalence sur E.
Les classes d'équivalences pour cette relation sont appelées de E suivants G ou G-orbites de E.
L'orbite de $x \in E$, sous l'action de G est $O_x = \{y \in E | \exists g \in G, g * x = y\}$.
Donc G opère transitivement sur E s'il y a une seule orbite et dans ce cas on dit que E sous l'action de G est un *espace homogène.*

2) Si l'action de G sur E n'est pas transitive, on aura plusieurs orbites.

3) L'action de G sur chaque orbite est transitive.

Exemples

Exemple 1
Soit $(G, .)$ un groupe et $E = G$. Définissons l'opération $*$ en posant :

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (g_1, g_2) & \longmapsto & g_1 * g_2 = g_1.g_2. \end{array}$$

Alors $*$ est une action du groupe G sur lui-même. En effet : $\forall g_1, g_2$ et $g \in G$, nous avons

$$g_1 * (g_2 * g) = g_1 * (g_2.g) = g_1.(g_2.g)$$
$$= g_1.g_2.g = (g_1.g_2).g = (g_1.g_2) * g.$$

D'autre part $\forall g \in G$, $g * e = g.e = g$.

L'action $*$ est fidèle. En effet $\forall g, x$ et $y \in G$, nous avons

$$g * x = g * y \Longleftrightarrow g.x = g.y \Longrightarrow x = g^{-1}.g.y = (g^{-1}.g).y = e.y = y.$$

L'action $*$ est transitive. En effet $\forall g_1, g_2 \in G, \exists g \in G$ tel que $g * g_1 = g_2$. Nous avons, $g_2 = g_2 * e = g_2.e = g_2.g_1.g_1^{-1} = g_2.g_1^{-1}.g_1 = g.g_1 = g * g_1$ $(g = g_2.g_1^{-1})$.

Exemple 2
Soient E un espace vectoriel réel et $GL(E)$ l'ensemble défini par

$$GL(E) = \{f : E \to E, f \text{ linéaire et bijective } \}.$$

$(GL(E), \circ)$ est un groupe non abélien. En effet,
i) $\forall f_1, f_2 \in GL(E)$, $f_1 \circ f_2 \in GL(E)$, car :
f_1, f_2 sont linéaires bijectives (par définition de $GL(E)$) et $f_1 \circ f_2 = f_1(f_2)$ est aussi linéaire bijective i.e $f_1 \circ f_2 \in GL(E)$.

ii) $\forall f \in GL(E)$, $f \circ Id_E = f(Id_E) = f$ et aussi $Id_E \circ f = f$, alors Id_E est l'élément neutre de $GL(E)$.

iii) $\forall f \in GL(E)$, f bijective, donc f est inversible i.e $\exists f^{-1} \in GL(E)$ tel que : $f \circ f^{-1} = f^{-1} \circ f = Id_E$.

Soit $*$ l'opération dans E définie par :

$$\begin{aligned} G \times E &\longrightarrow E \\ (f, x) &\longrightarrow f * x = f(x). \end{aligned}$$

Alors $*$ définit une action du groupe $GL(E)$ dans E.

En effet : $\forall f_1,\ f_2 \in G,\ \forall x \in E$,

$$f_1 * (f_2 * x) = f_1 * (f_2(x)) = f_1(f_2(x)) = (f_1 \circ f_2)(x) = (f_1 \circ f_2) * x.$$

De plus nous avons

$$\forall x \in E,\ Id_E * x = Id_E(x) = x.$$

L'action $*$ est fidèle. En effet $\forall f \in G$ et $\forall x, y \in E$, nous avons,
$f * x = f * y \Longleftrightarrow f(x) = f(y) \Longrightarrow x = y$, car f est injective (f est bijective).

L'action $*$ est transitive. En effet $\forall x, y \in E, \exists f \in G$ tel que : $f * x = y$.
Car on a : f bijective i.e : on a une seule solution qui vérifie que $f(x) = y$ et $x = f^{-1}(y)$.
Donc : $\forall x, y \in E, \exists f$ inversible $\in G$ tel que $f * x = y$.

Exemple 3
Soit G groupe commutatif, dans G on a déjà la translation τ_a, $a \in G$, $\tau_a(g) = g.a$.
Considérons l'action de G sur lui-même $*$, définie par

$$\begin{aligned} g : G &\longrightarrow G \\ g_1 &\longmapsto g * g_1 = g g_1. \end{aligned}$$

Alors : $*$ est une action de groupe G sur lui-même. En effet :
$\forall g_1, g_2$ et $g \in G$, nous avons

$$g * (g_1 * g_2) = g * (g_1 g_2) = g(g_1 g_2)$$

$$= gg_1 g_2 = (gg_1)g_2 = (gg_1) * g_2.$$

D'autre part $\forall g \in G$, $g * e = ge = g$.

L'action $*$ est fidèle. En effet $\forall g, x$ et $y \in G$, nous avons

$$g * x = g * y \Longleftrightarrow gx = gy \Longrightarrow x = g^{-1}gy = (g^{-1}g)y = ey = y.$$

L'action $*$ est transitive. En effet $\forall g_1, g_2 \in G, \exists g\ (g = g_2 g_1^{-1}) \in G$ tel que : $g * g_1 = g_2$, en effet on a : $g * g_1 = g_2 \Longleftrightarrow gg_1 = g_2 \Longleftrightarrow g = g_2 g_1^{-1}$.

1.2 Modèle général d'une marche aléatoire dans un groupe

Nous sommes en mesure de définir une marche aléatoire par l'action d'un groupe sur un ensemble.

Définition 2. *Soient $(G, .)$ un groupe, $(E, \mathcal{E})$ un ensemble mesurable et $*$ une action de G sur E. Soit $(Y_n)_n$ une suite de variables aléatoires i.i.d de loi μ à valeurs dans G et X_0 une variable aléatoire indépendante des Y_n à valeur dans E. On considère la marche aléatoire à gauche dans E, définie par X_0 et $\forall n > 0$, $X_n = Y_n * X_{n-1}$.*

Si le groupe G est commutatif, la marche aléatoire à gauche et la marche aléatoire à droite coinsident.

Propsition 1. *Soit $(G, .)$ un groupe discrêt engendré par la famille dénombrable $\{g_1, g_2, ...\}$. Soit $(Y_n)_n$ une suite de variable aléatoire à valeur dans G, i.i.d telle que :*

$$P(Y_i = g_i) > 0, \forall i \geq 1.$$

les classes éssenteilles de la marche aléatoire $(X_n)_n$ définie ci-dessus sont les orbites de G dans E.
En particulier $(X_n)_n$ irréductible si l'action de G sur E est irréductible.

Démonstration. cf [G.LARABI- Mémoire de magister] □

Propsition 2. *Soient $(G,.)$ un groupe topologique, $(Y_n)_n$ une suite de v.a i.i.d de loi μ et $(X_n)_n$ la marche aléatoire dans G engendrée par $(Y_n)_n$ et . l'action naturelle de G sur lui-même, alors le noyau P de la marche aléatoire $(X_n)_n$ est définie par*

$$P(g,A) = \mu(g^{-1}A),\ \forall g \in G,\ A \in \mathcal{B}_G.$$

Démonstration. cf [K.TEDLOUT mémoire de master] □

Cette formule généralise une formule de même type pour les marches aléatoires sur le groupe additif $\mathbb{R}$ (resp.$\mathbb{Z}$), car si $(X_n)_n$ est la marche aléatoire dans le groupe $\mathbb{R}$ (resp.$\mathbb{Z}$) engendrée par une suite de v.a $(Y_n)_n$ i.i.d de loi μ et $+$ l'action naturelle de $\mathbb{R}$ (resp.$\mathbb{Z}$) sur lui-même, alors $(X_n)_n$ à pour noyau

$$P(x,A) = \mu(A-x),\ \forall x \in \mathbb{R}\ et\ A \in \mathcal{B}_{\mathbb{R}}.$$

Chapitre 2

Eléments sur les représentations linéaires d'un groupe fini

Rappelons que si V est un espace vectoriel de dimension n sur $\mathbb{C}$, l'ensemble des applications linéaires bijectives de V dans V forme un groupe appelé groupe linéaire de V, on le note par $GL(V)$.
Si $e_1, e_2, ..., e_n$ est une base de V, le groupe $GL(V)$ est isomorphe au groupe $GL_n(\mathbb{C})$ des matrices carrées $n \times n$ inversibles à coefficients dans $\mathbb{C}$ par l'isomorphisme,

$$f \mapsto (a_{ij})$$

$$f(e_j) = \sum_{j=1}^{n} a_{ij} e_i,$$

l'élément a_{ij} est placé en ième ligne et jème colonne. $GL_n(\mathbb{C})$ est un groupe multiplicatif, en effet :

(i) $\forall A, B \in GL_n(\mathbb{C})$, $A.B \in GL_n(\mathbb{C})$.
Le fait que :
- $A \in GL_n(\mathbb{C})$, A est une matrice de [n,n] et $detA \neq 0$.
- $B \in GL_n(\mathbb{C})$, B est une matrice de [n,n] et $detB \neq 0$.

Et d'autre part : $det(A.B) = det(A).det(B) \neq 0$.
D'où : $A.B \in GL_n(\mathbb{C})$ et la loi . est interne.

(ii) On sait que si : $A \in GL_n(\mathbb{C})$, A est de $[n, n]$ et le $detA \neq 0 \Leftrightarrow$ A est inversible.
Donc : $\forall A \in GL_n(\mathbb{C}), \exists A^{-1} \in GL_n(\mathbb{C})$ tel que :

$AA^{-1} = A^{-1}A = I_n$.
Donc : $(GL_n(\mathbb{C}), .)$ admet un élément neutre I_n.

(iii) $\forall A, B, C \in GL_n(\mathbb{C})$, $(A.B).C = A.(B.C)$
et par conséquent $(GL_n(\mathbb{C}), .)$ est un groupe.

Définition 1. *Soit V un espace vectoriel complexe et $(G, .)$ un groupe fini. On appelle représentation linéaire du groupe G, tout homomorphisme ρ du groupe $(G, .)$ dans $GL(V)$*

$$\rho : G \longrightarrow GL(V)$$

$$s \longrightarrow \rho(s)$$

tel que :
$\rho(s.t) = \rho(s)\rho(t)$, $\forall s$, $t \in G$.

- Si V un espace vectoriel de dimension n et ρ une représentation linéaire de G, on dit que ρ est une représentation de degré n.
-Si V est un espace vectoriel pour la représentation ρ, on dit que ρ est triviale si, pour tout $s \in G$, $\rho(s) = Id_V$.

Propsition 1. *Si ρ est une représentation linéaire du groupe $(G, .)$, alors :*
(1) $\rho(e) = Id$, *avec e l'élément neutre de G et Id est l'élément neutre de $GL(V)$.*
(2) $\rho(s^{-1}) = (\rho(s))^{-1}, \forall s \in G$.

Démonstration.
(1) On a : $\forall s \in G$, $\rho(e) = \rho(s.s^{-1}) = \rho(s)\rho(s^{-1})$.
D'autre part : $\forall s \in G$, $\rho(s) = \rho(e.s) = \rho(e)\rho(s) = \rho(s)\rho(e)$.
Donc : $\rho(e) = Id$.

(2) On a : $\forall s \in G, \rho(s)\rho(s^{-1}) = \rho(e) = Id$, d'aprés 1.
De même $\rho(s^{-1})\rho(s) = \rho(s^{-1}.s) = \rho(e) = Id$.
Donc $\rho(s^{-1})\rho(s) = \rho(s)\rho(s^{-1}) = Id$.
Et par suite $\rho(s^{-1}) = (\rho(s))^{-1}$.
□

Exemples de représentations

(a)*Somme directe de représentation*
Soient G un groupe fini, ρ^1 et ρ^2 deux représentations linéaires des sous-espaces vectoriels V_1 et V_2, si $V = V_1 \oplus V_2$, l'application $\rho_s : G \longrightarrow GL(V)$ définie par :
$\rho_s(x_1 \oplus x_2) = (\rho_s^1 \oplus \rho_s^2)(x_1 \oplus x_2) = \rho_s(x_1) \oplus \rho_s(x_2)$, $\forall s \in G$, $\forall x_1 \in V_1$, $x_2 \in V_2$ est une représentation linéaire de G. Si on choisit $(e_i)_i$ la base de V associée à la décomposition en somme directe i.e si $(e_{i_1})_{i_1}$ la base de V_1 et $(e_{i_2})_{i_2}$ la base de V_2, alors : $e_i = e_{i_1} \oplus e_{i_2}$,
Soient : $r_{i_1 j_1}$ les coefficients de la matrice R_1 de la représentation ρ^1,
$r_{i_2 j_2}$ les coefficients de la matrice R_2 de la représentation ρ^2.
La matrice de ρ, $R(s)$ est donnée par :

$$R(s) = \sum_{i_1=1}^{n} r_{i_1 j_1} e_{j_1} \oplus \sum_{i_2=1}^{n} r_{i_2 j_2} e_{j_2} = \sum_{i=1}^{n} r_{ij} e_j.$$

Donc

$$R(s) = \begin{pmatrix} R_1(s) & 0 \\ 0 & R_2(s) \end{pmatrix}.$$

En effet :$\rho_{st} = \rho_{st}^1 \oplus \rho_{st}^2 = \rho_s^1 \rho_t^1 \oplus \rho_s^2 \rho_t^2 = (\rho_s^1 \oplus \rho_s^2)(\rho_t^1 \oplus \rho_t^2) = \rho_s \rho_t$.

(b) *La représentation régulière*
Si G est un groupe d'ordre n et V un espace vectoriel sur $\mathbb{C}$ de dimension n de base indexée par les éléments de G notés $(e_t)_{t \in G}$, ρ_s l'application de V dans V, la représentation linéaire ρ est définie par : $\rho_s(e_t) = e_{st}$.
En effet : $\forall s, h$ et $t \in G$, $\rho_{sh}(e_t) = e_{sht} = \rho_s(\rho_h(e_t)) = \rho_s \rho_h(e_t)$.
La représentation ρ est appelée *représentation régulière de G* .

(c) *La représentation de permutation*
Soit E un ensemble fini, à n éléments, par exemple $E = \{x_1, x_2, ..., x_n\}$, que l'on peut identifier avec l'ensemble $\{1, 2, ..., n\}$.
Soit $S_n = \{S : E \longrightarrow E, \text{bijective}\}$. $S_n =$ est le groupe symétrique d'ordre n, i.e. le groupe des permutations de $\{1, 2, ..., n\}$. Vérifions que $(S_n, \circ)$ est un groupe. Nous avons :

$\forall \sigma_1, \sigma_2 \in S_n$. Par définition σ_1 et σ_2 sont des bijections de E dans E et donc $\sigma_1 \circ \sigma_2$ et $\sigma_2 \circ \sigma_1$ sont des bijections de E dans E, donc $\sigma_1 \circ \sigma_2$,

$\sigma_2 \circ \sigma_1 \in S_n$.
$\forall \sigma \in S_n$, $\exists \sigma^{-1} \in S_n$ (σ est une bijection de E dans E), $\sigma \circ \sigma^{-1} = \sigma\sigma^{-1} = \sigma^{-1}\sigma = Id$.
$\forall \sigma_1$, σ_2, et $\sigma_3 \in S_n$, $\sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1\sigma_2\sigma_3$.

Soit $\sigma \in S_n$, on note σ par :

$$\begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix},$$

où $\{\sigma(1), \sigma(2),...,\sigma(n)\}$ est un nouvel ordre de $\{1, 2, ..., n\}$.

Pour $x \in E$, $s \in S_n$, on note $sx = s(x)$.
Soit S_n le groupe de permutation de l'ensemble fini E et soit V un espace vectoriel de dimension n ayant la base $(e_x)_{x\in E}$ indexée par les éléments de E. Soit ρ la représentation linéaire du groupe S_n, définie par

$$\begin{aligned} \rho_s : V &\longrightarrow V \\ e_x &\longmapsto \rho_s(e_x) = e_{sx}. \end{aligned}$$

En effet : $\forall s$, $t \in S_n$ et $x \in E$, on a $\rho_{st}(e_x) = e_{stx} = \rho_{s\circ t(x)} = e_{s(t(x))} = \rho_s(e_{tx}) = \rho_s(\rho_t(e_x)) = \rho_s\rho_t(e_x)$.
On dit que e_s transforme e_{sx}.
La représentation ρ est appelée *représentation de permutation associée à E.*

2.1 Sous-représentations

Définition 2. *Soit G un groupe fini et ρ une représentation de G. On dit qu'un sous-espace vectoriel W de l' espace vectoriel V est stable par G, si pour tous $x \in W$ et $s \in G$, $\rho_s x \in W$ (on dit aussi que W est invariant).*

Définition 3. *Soient G groupe, W un sous-espace stable par G, la représetation linéaire ρ^W definie par : $\rho_s^W x = \rho_s x$ avec, $s \in G$ et $x \in W$ est appelée sous-représentation de V.*

Exemple
Soit ρ la représentation régulière de G.
$W = \{x \in V, x = \sum_{t\in G} e_t\}$, avec $(e_t)_t$ la base de V.

Nous avons par définition de W et de la représentation regulière ρ de V, $\rho_s(x) = \rho_s(\sum_{t\in G} e_t) = \sum_{t\in G} \rho_s(e_t) = \sum_{t\in G} e_{st}$, s fixé et $t \in G$, $st \in G$.
Donc : $\sum_{t\in G} e_{st} = \sum_{u\in G} e_u \in W$ (par définition de W) i.e $\rho_s(x) \in W$.
Il en résulte que : W est un sous-espace stable par ρ_s, $\forall s \in G$.
D'où : ρ est une sous-représentation de V.

Rappelons que si W sous-espace vectoriel de V, le sous-espace W' est le supplémentaire de W si $V = W \oplus W'$, i.e :
(1) $\forall z \in V$, $\exists\ x, y$ uniques, tel que $x \in W$, $y \in W'$ et $z = x + y$.
(2) $W \cap W' = \{0\}$.

Théorème 1. *Soit $\rho : G \to GL(V)$ une représentation linéaire de G dans V et soit W sous-espace vectoriel de V stable par G. Il existe un supplémentaire W^0 de W dans V qui est stable par G.*

Démonstration.

(a) Montrons l'exitence de W^0 :
Soit W' un supplémentaire quelconque de W dans V, p le projecteur de V sur W parallèlement à W', notons p^0 la moyenne des transformés de p par les éléments de G, avec :

$$p^0 = \frac{1}{|G|} \sum_{t\in G} \rho_t p \rho_t^{-1}.$$

Par hypothèse on a : p applique V dans W et ρ_t représentation de W (ρ_t conserve W).
Donc : p^0 applique V dans W. En outre, si $x \in W$, on a $\rho_t^{-1}x \in W$, $\forall t \in G$, puisque W est stable (par hypothèse). Par conséquent, pout tout $x \in W$, on a : $p\rho_t^{-1}x = \rho_t^{-1}x$ (p le projecteur de V sur W associé à la décomposition $V = W \oplus W'$), alors $\rho_t p \rho_t^{-1}x = \rho_t\rho_t^{-1}x = x$ et $p^0x = x$.
Ainsi, p^0 est un projecteur de V sur W, correspondant à un certain supplémentaire W^0 de W dans V. En outre on a, $\forall s \in G$, $\rho_s p^0 = p^0\rho_s$.

En effet :

$$\begin{aligned}\rho_s p^0 \rho_s^{-1} &= \rho_s(\frac{1}{|G|}\sum_{t\in G}\rho_t p \rho_t^{-1})\rho_s^{-1} = \frac{1}{|G|}\sum_{t\in G}\rho_s\rho_t p \rho_t^{-1}\rho_s^{-1} \\ &= \frac{1}{|G|}\sum_{t\in G}\rho_s\rho_t p(\rho_s\rho_t)^{-1} = \frac{1}{|G|}\sum_{t\in G}\rho_{st} p \rho_{st}^{-1} \\ &= p^0.\end{aligned}$$

D'où : l'existence de W^0.

(b) Montrons que : W^0 est stable :
Soit maintenant : $x \in W^0$, $s \in G$, $p^0\rho_s x = \rho_s p^0 x = 0$ ie : $\rho_s x \in W^0$
D'où : W^0 est stable par G. □

2.2 La représentation irréductible

Définition 4. *Une représentation ρ est irréductible si l'espace vectoriel V ne contient pas de sous-espaces stables par le groupe G différents de $\{0\}$ et de V. On dit que V est irréductible ou simple.*

Théorème 2. *Toute représentation est somme directe de repésentations irréductibles.*

Démonstration.

Soient ρ une représentation linéaire de l'espace vectoriel V, W^0 un sous-espace vectoriel supplémentaire de W et $\rho^{'}$, ρ^0 sont les représentations linéaires des sous-espaces W et W^0 .
On montre le théorème utilisons la recurrence :

(1) Si $\dim(V) = 0$:
On a : $V = W \oplus W^0$ (d'aprés le théorème 1)
Comme : $\dim(V) = \dim(W) + \dim(W^0)$
Et : $\dim(V) = 0 \Leftrightarrow \dim(W) + \dim(W^0) = 0$
Donc : $\dim(W) = \dim(W^0) = 0$
D'où : $\rho^{'}$, ρ^0 famille vide de représentations irréductibles, car leurs espaces de représentations W, W^0 sont vides.

Et : ρ somme directe de la famille vide des représentations irréductibles.

(2) Si $\dim(V) = n \geq 1$:
On a d'aprés le théorème 1 : $V = W \oplus W^0$ avec : $\dim(W) < \dim(V)$ et : $\dim(W^0) < \dim(V)$.

Supposons que : $\rho^{'}$ et ρ^0 sont des sommes directes des représentations irréductibles, i.e :
$\rho^{'} = \rho_1^{'} \oplus ... \oplus \rho_n^{'}$ et $\rho^0 = \rho_1^0 \oplus ... \oplus \rho_n^0$.
On a : $\rho^{'} \oplus \rho^0 = \rho_1^{'} \oplus ... \oplus \rho_n^{'} \oplus \rho_1^0 \oplus ... \oplus \rho_n^0 = \rho_1^{'} \oplus \rho_1^0 ... \oplus \rho_n^{'} \oplus \rho_n^0 = \rho_1 \oplus ... \oplus \rho_{n-1} \oplus \rho_n$, avec $\rho_i = \rho_i^{'} \oplus \rho_i^0$ et $i = 1, ..., n$.

Supposons que cette proposition est vraie jusqu'à $(n-1)$ on la démontre pour n.
Posons $\rho_1 \oplus ... \oplus \rho_{n-1} = \rho^k$, ρ^k est somme directe des représentations irréductibles.
D'autre part on a : $\rho_n = \rho_n^{'} \oplus \rho_n^0$ i.e ρ_n est aussi somme directe des représentations irréductibles .
Donc : $\rho^{'} \oplus \rho^0 = \rho^k \oplus \rho_n$, et d'aprés l'hypotèse de recurrence, on a une somme directe des représentations irréductibles est irréductible, alors $\rho^k \oplus \rho_n$ est irréductible, donc $\rho^{'} \oplus \rho^0$ il en est aussi, i.e ρ somme directe de représentations irréductibles.

□

2.3 La représentation induite

Classe à gauche modulo un sous-groupe

Définition 5. *Soient G un groupe fini, H un sous-groupe de G et soit $s \in G$, sH l'ensemble des produits st, avec $t \in H$. On dit que sH est la classe à gauche modulo H contenant s.*

Remarques
- Deux éléments s, $s^{'}$ de G sont dits congrus modulo s'ils appartiennent à la même classe à gauche, i.e : si $s^{-1}s^{'}$ appartient à H. On écrit alors $s^{'} \equiv s(mod.H)$.

- L'ensemble des classes à gauche $mod.H$ est noté G/H, c'est une partition de G.

-Si G a g éléments et H a h éléments, G/H a g/h éléments, l'entier g/h est l'indice de H dans G et se note $(G : H)$.

-Si on choisit un élément de toute classe à gauche $mod.H$, on obtient une partie R de G, appelée un système de représentants de G/H et $\forall s \in G$, s s'écrit de façon unique comme suit : $s = rt$, avec $r \in R$ et $t \in H$.

Notation
Soient G un groupe fini et H un sous-groupe de G, ρ une représentation linéaire de G dans l'espace vectoriel V et ρ_H sa restriction à H. Soit W un sous-espace vectoriel de V stable par ρ_t, $t \in H$, θ une représentation linéaire de H dans W, si $s \in G$, l'espace vectoriel $\rho_s W$ ne dépend que de la classe à gauche sH de s, en effet :
$\forall s \in G$, $t \in H$, on a $\rho_{st}W = \rho_s\rho_t W = \rho_s W$, puisque W est stable par les ρ_t ($\rho_t W = W$, $\forall t \in H$). Si σ est une classe à gauche $mod.H$, on peut donc définir un sous-espace W_σ de V comme étant $\rho_s W$ pour tout $s \in \sigma$.

Définition 6. *Soient G un groupe fini, V un espace vectoriel, on dit que la représentation ρ de G dans V est induite par la représentation θ de H dans W si V est égal à la somme des W_σ ($\sigma \in G/H$) et si cette somme est une somme directe, autrement dit si : $V = \oplus_{\sigma \in G/H} W_\sigma$.*

Propsition 2. *Toute représentation irréductible de G est équivalente à l'une des représentations induites corréspondantes de G.*

Démonstration. Cf. [Serre]. □

2.4 Produit tensoriel de deux représentations

Définition 7. *Soient V_1, V_2 deux espaces vectoriels. On appelle produit tensoriel de V_1, V_2 un espace vectoriel W muni d'une application :*

$$\phi : V_1 \times V_2 \to W$$

$$(x_1, x_2) \mapsto \phi(x_1, x_2) = x_1 \otimes x_2$$

tel que :
(1) $x_1 \otimes x_2$ *dépend linéairement de chacune des variables* x_1 *et* x_2.
(2) *Si* (e_{i_1}) *est une base de* V_1 *et* (e_{i_2}) *est la base de* V_2, *la formule de produit* $e_{i_1} \otimes e_{i_2}$ *est une base de* W.
- Donc si $W = \phi(V_1 \times V_2)$, W *est appelé produit tensoriel de* $V_1 \times V_2$ *est noté* $V_1 \otimes V_2$.

Propriété

(1) $\dim(W) = \dim(V_1 \otimes V_2) = \dim(V_1).\dim(V_2)$ (d'aprés la définition).

Définition 8. *Soient :* $\rho^1 : G \to GL(V_1)$ *et :* $\rho^2 : G \to GL(V_2)$ *deux représentations d'un groupe* G *et soit* (x_1, x_2) *dans* $V_1 \otimes V_2$ *et* $(\rho_s^1 \otimes \rho_s^2)(x_1 \otimes x_2) = \rho_s^1(x_1) \otimes \rho_s^2(x_2)$.

On définit l'élément ρ_s, $\forall s \in G$ *de* $GL(V_1 \otimes V_2)$ *par :*

$$\begin{aligned} \rho_s : V_1 \times V_2 &\longrightarrow GL(V_1 \otimes V_2) \\ (x_1, x_2) &\longmapsto \rho_s(x_1 \otimes x_2) = \rho_s^1(x_1) \otimes \rho_s^2(x_2). \end{aligned}$$

Par suite on a :

$$\begin{aligned} \rho_s^1 : V_1 &\longrightarrow GL(V_1) \\ x_1 &\longmapsto \rho_s^1(x_1). \\ \rho_s^2 : V_2 &\longrightarrow GL(V_2) \\ x_2 &\longmapsto \rho_s^2(x_2). \end{aligned}$$

Donc :

$$\begin{aligned} \rho_s^1 \otimes \rho_s^2 : V_1 \otimes V_2 &\longrightarrow GL(V_1 \otimes V_2) \\ (x_1, x_2) &\longmapsto (\rho_s^1 \otimes \rho_s^2)(x_1 \otimes x_2) = \rho_s^1(x_1) \otimes \rho_s^2(x_2), \end{aligned}$$

ρ_s élément de $GL(V_1 \otimes V_2)$ tel que : $\rho_s = \rho_s^1 \otimes \rho_s^2$.
D'où : $\rho_s(x_1 \otimes x_2) = (\rho_s^1 \otimes \rho_s^2)(x_1 \otimes x_2) = \rho_s^1(x_1) \otimes \rho_s^2(x_2)$.
ρ_s une représentation linéaire de G dans $V_1 \otimes V_2$ appelée le produit tensoriel des représentations des données (ρ_s^1, ρ_s^2).

Remarque
Soient : (e_{i_1}) une base de V_1, $r_{i_1j_1}$ la matrice de ρ_s^1 par rapport à cette base. (e_{i_2}) une base de V_2, $r_{i_2j_2}$ la matrice de ρ_s^2 par rapport à cette base.
Donc : $\rho_s^1(e_{j_1}) = \sum_{i_1} r_{i_1j_1} e_{i_1}$, $\rho_s^2(e_{j_2}) = \sum_{i_2} r_{i_2j_2} e_{i_2}$.

On a : $\rho_s(e_{j_1} \otimes e_{j_2}) = (\rho_s^1 \otimes \rho_s^2)(e_{j_1} \otimes e_{j_2}) = \rho_s^1(e_{j_1}) \otimes \rho_s^2(e_{j_2})$
$= (\sum_{i_1} r_{i_1j_1}(s)e_{i_1}) \otimes (\sum_{i_2} r_{i_2j_2}(s)e_{i_2}) = \sum_{i_1i_2}(r_{i_1j_1}(s)e_{i_1}) \otimes (r_{i_2j_2}(s)e_{i_2}) = \sum_{i_1,i_2}(r_{i_1j_1}(s).r_{i_2j_2}(s))(e_{i_1} \otimes e_{i_2})$.

La matrice de ρ_s est donc formée des $(r_{i_1j_1}(s).r_{i_2j_2}(s))$, on reconait là le produit tensoriel des matrices de ρ_s^1 et ρ_s^2.

2.5 Lemme de Schur

Définition 9. *Deux représentations ρ_1, ρ_2 du groupe G dans les espaces V_1, V_2 sont dites équivalentes s'il éxiste un opérateur linéaire f de V_1 dans V_2 qui applique bijectivement V_1 sur V_2 et satisfait à la condition :*

$$f\rho_s^1 = \rho_s^2 f, \forall s \in G$$

Cette équivalence est notée par $\rho^1 \sim \rho^2$.

Lemme 1. *Soit $\rho^1 : G \longrightarrow GL(V_1)$ et $\rho^2 : G \longrightarrow GL(V_2)$ deux représentations irréductibles du groupe G et soit f un opérateur de V_1 dans V_2 qui satisfait à la condition : $\rho_s^2 f = f\rho_s^1$ pour tout $s \in G$.*
Alors : ou bien f applique bijectivement V_1 sur V_2 et donc $\rho^1 \sim \rho^2$ ou bien $f = 0$.

Démonstration.

On a $f : V_1 \longrightarrow V_2$, posons $W = f(V_1)$, alors W est un sous-espace de V_2. D'autre part : $\forall y \in W$, $\exists x \in V_1$ tel que : $f(x) = y$, alors
$\rho_s^2 y = \rho_s^2 f(x) = f(\rho_s^1 x)$ et comme ρ_s^1 est la représentation de G dans V_1, donc $f(\rho_s^1 x) \in f(V_1) = W$,$\forall s \in G$, $x \in V_1$, d'où : $\rho_s^2 f(x) \in W$.
Il en résulte que W est invariant par ρ_s^2, mais ρ_s^2 est une représentation irréductible, i.e $W = \{0\}$ ou $W = V_2$.
Dans le premier cas i.e $W = \{0\}$, $f = 0$, car on a $f(V_1) = W = \{0\}$, alors $\forall x \in V_1$, $f(x) = 0$, donc $f = 0$

Considérons le cas où $W = V_2$: f applique V_1 sur V_2. Démontrons que f est bijectif.
Posons $W^{'} = \ker f = \{x : f(x) = 0\}$, on a $\forall x \in W^{'}, f(x) = 0$ et $\rho_s^2 f(x) = f(\rho_s^1 x) = \rho_s^2 0 = 0$, donc $\rho_s^1 x \in W^{'}$, il en résulte que $\ker f$ est invariant.
Et comme ρ_s^2 est une représentation irréductible, alors $\ker f = \{0\}$ ou $\ker f = V_1$, mais $V_2 = W$, donc $\ker f = \{0\}$.
D'autre part on a : $\dim f(V_1) = \dim(Imf) = \dim V_2$ et $\dim(\ker f) = 0$, d'où f est bijectif et $V_2 = W \oplus \ker f$.

□

Lemme 2. *Soit ρ une représentation irréductible de dimenssion finie du groupe G dans l'espace V. Alors chaque opérateur linéaire $f^{'}$ dans l'espace V qui est permutable à tous les opérateurs ρ_s, $s \in G$, est de la forme $f^{'} = \lambda.Id_V$, où λ est un nombre.*

Démonstration.

D'aprés lemme 1 on a : $f^{'}\rho_s = \rho_s f^{'}$, $\forall s \in G$.
puisque $f^{'}$ est un opérateur linéaire dans un espace de dimension finie, il possède au moins une valeur propre λ.
Posons $f = f^{'} - \lambda.Id_V$, alors f n'est pas une bijection sur V.
D'autre part on a, $f\rho_s = \rho_s f$ pour tous les $s \in G$, i.e f satisfait à la condition du lemme 1 pour $\rho_s^1 \sim \rho_s^2$, $V_1 = V_2$. Puisque f n'est pas bijectif, on a donc $f = 0$, i.e $f^{'} - \lambda.Id_V = 0$, $f^{'} = \lambda.Id_V$. □

Corollaire 1. *Soit h une application linéaire de V_1 dans V_2 et posons :*

$$h^0 = \frac{1}{|G|}\sum_{s\in G}(\rho_s^2)^{-1} h \rho_s^1.$$

Alors :
(1) *Si ρ^1 et ρ^2 ne sont pas équivalentes, on a $h^0 = 0$.*
(2) *Si $V_1 = V_2$, $\rho^1 \sim \rho^2$, h^0 est une homothétie de rapport $\frac{1}{n}tr(h)$, avec $n = dim(V_1)$.*

Démonstration.

On a $\rho_t^2 h^0 = h^0 \rho_t^1$, $\forall t \in G$. En effet :

$$(\rho_t^2)^{-1} h^0 \rho_t^1 = \frac{1}{|G|}\sum_{s\in G}(\rho_t^2)^{-1}(\rho_s^2)^{-1} h \rho_s^1 \rho_t^1$$

$$= \frac{1}{|G|}\sum_{s\in G}(\rho_s^2\rho_t^2)^{-1}h\rho_s^1\rho_t^1$$

$$= \frac{1}{|G|}\sum_{s\in G}(\rho_{st}^2)^{-1}h\rho_{st}^1 = h^0.$$

D'où : $(\rho_t^2)^{-1}h^0\rho_t^1 = h^0$ i.e : $h^0\rho_t^1 = \rho_t^2 h^0$.
En appliquant lemme de Schur à $f = h^0$ pour $f = 0$, on a $h^0 = 0$ et dans le lemme 2, h^0 égal à un scalaire λ.
D'autre part on a dans ce dérnier cas :

$$tr(h^0) = \frac{1}{|G|}\sum_{s\in G} tr((\rho_s^1)^{-1}h\rho_s^1) = tr(h).$$

et comme $tr(h^0) = tr(\lambda) = n.\lambda$, alors : $n\lambda = tr(h)$, d'où : $\lambda = \frac{1}{n}tr(h)$.

En explicitant ce corollaire en supposant que ρ^1 et ρ^2 sont données sous forme matricielle :

$\rho_s^1 = (r_{i_1j_1}(s))$, $\rho_s^2 = (r_{i_2j_2}(s))$ et h défini par une matrice $(x_{i_2i_1})$ et de même h^0 est définie par $(x^0_{i_2i_1})$. On a par définition de h^0 :

$$x^0_{i_2i_1} = \frac{1}{|G|}\sum_{s\in G} r_{i_2j_2}(s^{-1})x_{j_2j_1}r_{j_1i_1}(s).$$

□

Le membre de droite est une forme linéaire par rapport aux $x_{j_2j_1}$, dans le cas 1, cette forme s'annule pour tout système de valeurs des $x_{j_2j_1}$, ses coefficients sont donc nuls. D'où :

Corollaire 2. *D'aprés le cas* 1*, on a*

$$\frac{1}{|G|}\sum_{s\in G} r_{i_2j_2}(s^{-1})r_{j_1i_1}(s) = 0$$

Et d'aprés le cas 2*, on a*

$$\frac{1}{|G|}\sum_{j_1,j_2} r_{i_2j_2}(s^{-1})x_{j_2j_1}r_{j_1i_1}(s) = \frac{1}{n}\sum_{j_1,j_2}\delta_{i_2i_1}\delta_{j_2j_1}x_{j_2j_1}$$

Démonstration.

On a d'aprés le cas 1 de corollaire 1 si ρ_s^1 n'est pas équivalente à ρ_s^2, $h^0 = 0$ et comme $(r_{i_1j_1}(s))$ est la forme matricielle de ρ^1, $(r_{i_2j_2}(s))$ est la forme matricielle de ρ^2 et $(x_{i_2i_1})$ est la matrice de h, alors :

$$\frac{1}{|G|}\sum_{s\in G} r_{i_2j_2}(s^{-1})x_{j_2j_1}r_{j_1i_1}(s) = 0,$$

pour tout système de valeurs des $x_{j_2j_1}$, ses coefficients sont nuls, donc

$$\frac{1}{|G|}\sum_{s\in G} r_{i_2j_2}(s^{-1})r_{j_1i_1}(s) = 0.$$

D'aprés le cas 2 de corollaire 1 on a :$\rho^1 \sim \rho^2$, $h^0 = \lambda$ et comme $(x^0_{i1j_1})$ est la matrice de l'application linéaire h^0 alors $x^0_{i_1j_1} = \lambda\delta_{i_2i_1}$, avec :

$$\delta_{i_2i_1} = \begin{cases} 1, & \text{si } i_1 = i_2 \\ 0, & \text{si } i_1 \neq i_2 \end{cases}$$

On a $\lambda = \frac{1}{n}tr(h)$ et comme $tr(h) = \sum \delta_{j_2j_1}x_{j_2j_1}$, alors $\lambda = \frac{1}{n}\sum \delta_{j_2j_1}x_{j_2j_1}$ et comme

$$x^0_{i_2i_1} = \frac{1}{|G|}\sum_{s\in G} r_{i_2j_2}(s^{-1})x_{j_2j_1}r_{j_1i_1}(s) = \lambda\delta_{i_2i_1},$$

Il en résulte que,

$$\lambda\delta_{i_2i_1} = \frac{1}{n}\sum_{j_1j_2}\delta_{j_2j_1}x_{j_2j_1}\delta_{i_2i_1} = \frac{1}{n}\sum_{j_1j_2}\delta_{j_2j_1}\delta_{i_2i_1}x_{j_2j_1}.$$

D'où l'égalité. □

En égalant les coefficients des $x_{j_2j_1}$, on obtient comme ci-dessus :

Corollaire 3. *D'aprés le cas* (2)*, on a*

$$\frac{1}{|G|}\sum_{s\in G} r_{i_2j_2}(s^{-1})r_{j_1i_1}(s) = \frac{1}{n}\delta_{i_2i_1}\delta_{j_2j_1} = \begin{cases} 1/n, & si\ i_1 = i_2, j_1 = j_2 \\ 0, & sinon \end{cases}$$

Démonstration.

D'aprés le corollaire 2, on a :

$$\frac{1}{|G|}\sum_{s,j_1,j_2} x_{j_2j_1} r_{i_2j_2}(s^{-1}) r_{j_1i_1}(s) = \frac{1}{n}\sum_{j_1,j_2} \delta_{i_2i_1}\delta_{j_2j_1}x_{j_2j_1}$$

Et comme les coefficients des $x_{j_2j_1}$ sont tous égals et on a $\delta_{i_2i_1}$, $\delta_{j_2j_1}$ soit égals à 1 soit égals à 0, alors on obtient,

$$\frac{1}{|G|}\sum_{s} r_{i_2j_2}(s^{-1}) r_{j_1i_1}(s) = \frac{1}{n}\delta_{i_2i_1}\delta_{j_2j_1}$$

Et

$$\frac{1}{n}\delta_{i_2i_1}\delta_{j_2j_1} = \begin{cases} \frac{1}{n}, & \text{si } i_1 = i_2, j_2 = j_1 \\ 0, & \text{si } i_1 \neq i_2, j_2 \neq j_1 \end{cases}$$

□

2.6 Théorie des caractères

2.6.1 Caractères d'une représentation

Définition 10. *Si ρ est une représentation du groupe G on appelle caractère de la représenation ρ l'application χ définie par :*

$$\chi_\rho(s) = trace(\rho(s)), \forall s \in G$$

Définition 11. *Soit G groupe fini, t et t' deux éléments du groupe G, t est dit conjugué avec t' s'il existe $s \in G$ tel que $t' = sts^{-1}$ et la relation $t\mathcal{R}t' \iff t$ et t' conjugués définit une relation d'équivalence sur G. Les classes d'équivalences pour cette relation sont appelées classes de conjugaison.*

Définition 12. *Une fonction centrale d'un groupe G est une fonction définie sur G à valeurs dans $\mathbb{C}$ constante sur les classes de conjugaison de G.*

Propsition 3. *Si χ est le caractère d'une représentation ρ de degré n, on a :*
(1) $\chi_\rho(st) = \chi_\rho(ts)$ *(χ est dite fonction centrale).*
(2) $\chi_\rho(e) = n$, *avec e est l'élément neutre de G.*
(3) $\chi_{\rho^1\oplus\rho^2}(s) = \chi_{\rho^1}(s) + \chi_{\rho^2}(s)$.
(4) $\chi_\rho(tst^{-1}) = \chi_\rho(s)$.
(5) $\chi_{\rho^1\otimes\rho^2}(s) = \chi_{\rho^1}(s).\chi_{\rho^2}(s)$.

Démonstration.

(1) On a : $\chi_\rho(st) = tr(\rho(st))$.

Et : $tr(\rho(st)) = tr(\rho_{st}) = tr(\rho_s\rho_t) = tr(\rho_t\rho_s) = tr(\rho_{ts}) = \chi_\rho(ts)$.

(2) On a : ρ repésentation de degré n ie : la dimension de l'espace de représentation V du groupe G est égal à n.
D'autre part on a : si e est l'élément neutre de G, $\rho(e) = Id_V$, donc : $\chi_\rho(e) = tr(\rho_e) = tr(\rho(e)) = tr(Id_V) = n$.

(3) Soit R_s^1 la matrice de la représentation ρ^1 et R_s^2 la matrice de la représentation ρ^2, la représentation $\rho^1 \oplus \rho^2$ est donnée par :

$$R_s = \begin{pmatrix} R_s^1 & 0 \\ 0 & R_s^2 \end{pmatrix}$$

Donc :
$\chi(s) = tr(R_s) = tr(R_s^1 + R_s^2) = tr(R_s^1) + tr(R_s^2) = \chi_1(s) + \chi_2(s)$.

(4) D'aprés (1), on a : $\chi(uv) = \chi(vu)$, alors si on pose : $u = ts$, $v = t^{-1}$, on a donc : $\chi(tst^{-1}) = \chi(t^{-1}ts) = \chi(s)$.

(5) Soient : $r_{i_1j_1}$ la matrice de ρ^1, $r_{i_2j_2}$ la matrice de ρ^2, on a :
$\chi_1(s) = \Sigma_{i_1} r_{i_1i_1}(s)$, $\chi_2(s) = \Sigma_{i_2} r_{i_2i_2}(s)$.

$\chi_{\rho^1\otimes\rho^2}(s) = tr(\rho_s^1 \otimes \rho_s^2) = \Sigma_{i_1,i_2} r_{i_1i_1}(s) r_{i_2i_2}(s) = \Sigma_{i_1} r_{i_1i_1}(s) \Sigma_{i_2} r_{i_2i_2}(s)$
$= tr(\rho^1(s))tr(\rho^2(s)) = \chi_{\rho^1}(s).\chi_{\rho^2}(s)$. □

2.6.2 Othogonalité des caractères

Définition 13. *Soit V un espace vectoriel sur $\mathbb{C}$, on appelle forme hérmitienne sur V toute application*

$$\begin{array}{rcl} \varphi : V \times V & \longrightarrow & \mathbb{C} \\ (x, y) & \longmapsto & < x, y >= \varphi(x, y) \end{array}$$

tel que :

(a) φ linéaire par rapport à la première variable i.e :
(i) $\forall x,\ y,\ z \in V,\ \varphi(x+y,z) = \varphi(x,z) + \varphi(y,z)$.
(ii) $\varphi(\lambda x, y) = \lambda\varphi(x,y)$.

(b) φ antilinéaire par rapport à la deuxième variable i.e :
(i) $\forall x,\ y,\ z \in V,\ \varphi(x, y+z) = \varphi(x,y) + \varphi(x,z)$.
(ii) $\forall x,\ y \in V,\ \varphi(x,y) = \overline{\varphi(y,x)}$.
(iii) $\forall \lambda \in \mathbb{C},\ x,\ y \in V,\ \varphi(x,\lambda y) = \bar{\lambda}\varphi(x,y)$.

On dit que φ est positive si $\forall x \in V,\ \varphi(x,x) \geq 0$ et définie positive si φ est positive et $\forall x \in V,\ \varphi(x,x) = 0 \Longleftrightarrow x = 0$.
Un produit scalaire hérmitien sur V est une φ forme hérmitienne sur V définie psitive.

Soit $\mathbb{L}^2_\mu(\Omega, \mathbb{A}) = \{f : \Omega \longrightarrow \mathbb{C},\ tel\ que : \int_\Omega |f|^2\ d\mu < \infty\}$

Propsition 4. *Pour f et $g \in \mathbb{L}^2_\mu(\Omega, \mathbb{A})$ l'application*

$$(f,g) \longrightarrow < f\ ,\ g > = \int_\Omega f\bar{g}\ d\mu$$

définit un produit scalaire sur $\mathbb{L}^2_\mu$.

Démonstration.

Pour f et $g \in \mathbb{L}^2_\mu(\Omega, \mathbb{A})$, montrons que $< f\ ,\ g >$ à toujours un sens. L'inégalité de Holder assure que si p et q sont conjugués ($p.q = p + q$), alors si $f \in \mathbb{L}^p$ et $g \in \mathbb{L}^q$, $fg \in \mathbb{L}^1$. D'aprés cette inégalité si $f \in \mathbb{L}^2_\mu$ et $g \in \mathbb{L}^2_\mu$, comme $\mathbb{L}^2_\mu$ est en dualité avec lui-même, alors $|fg| \in \mathbb{L}^1$ et donc $\int |fg| d\mu$ existe toujours et comme $|fg| = \sqrt{fg.\bar{f}\bar{g}} = \sqrt{f\bar{g}.g\bar{f}}$, donc $|f\bar{g}| \leq |fg|$, d'où $\int f\ \bar{g}\ d\mu$ existe toujours.

Montrons que $< f\ ,\ g >$ est une forme hérmitienne, définie positive :
(1) $< f\ ,\ g >$ est une forme hérmitienne :

(a) φ linéaire par rapport à la première variable
(i) $\forall f,\ g,\ h \in \mathbb{L}^2_\mu,\ < f+g\ ,\ h > = \int (f+g)\bar{h}\ d\mu = \int (f\bar{h} + g\bar{h})\ d\mu = \int f\bar{h}\ d\mu + \int g\bar{h}\ d\mu = < f\ ,\ h > + < g\ ,\ h >$.

(ii) $\forall f, g \in \mathbb{L}^2_\mu, \lambda \in \mathbb{C}, < \lambda f , g >= \int \lambda\, f\bar{g}\, d\mu = \lambda \int f\bar{g}\, d\mu = \lambda < f , g >$.

(b) φ antilinéaire par rapport à la deuxième variable. Nous avons
(i) $\forall f, g, h \in \mathbb{L}^2_\mu, < f , g + h >= \int f\overline{(g+h)}\, d\mu = \int f\bar{g}\, d\mu + \int f\bar{h}\, d\mu = < f , g > + < f , h >$.

(ii) $\forall f, g \in \mathbb{L}^2_\mu, < f , g >= \int f\bar{g}\, d\mu = \int \overline{\bar{f}g}\, d\mu = \int \overline{g\bar{f}}\, d\mu = \overline{< g , f >}$.

(iii) $\forall f, g \in \mathbb{L}^2_\mu, \lambda \in \mathbb{C}, < f , \lambda g >= \int f\overline{\lambda g}\, d\mu = \bar{\lambda} \int f\bar{g}\, d\mu = \bar{\lambda} < f , g >$.

(2) On montre que $< f , g > \geq 0$ i.e : $\forall f \in \mathbb{L}^2_\mu, < f , f > \geq 0$:
On a $< f , f >= \int |f|^2\, d\mu$ et comme $|f|^2 \geq 0$, alors $\int |f|^2\, d\mu \geq 0$, d'où $< f , f > \geq 0$.

(3) Il reste à montrer que : $< f , g >$ définie positive, i.e :
$< f , f >= 0 \Longleftrightarrow f = 0$, $\mu p.p$. Il suffit de montrer que $< f , f >= 0 \Longrightarrow f = 0$ $\mu p.p$ et $f = 0 \Longrightarrow < f , f >= 0$ $\mu.p.p$.
(i) On a si $f = 0 \Longrightarrow |f|^2 = 0$, alors : $\int |f|^2 = 0$, d'où $< f , f >= 0$, $\mu p.p$.

(ii) Si $< f , f >= 0$, on montre que $f = 0$:
On a : $|f|^2 \in \mathbb{L}^1$, $|f|^2 \geq 0$, supposons que $|f|^2 > 0$, i.e : $f \neq 0$.
En particulier $\exists \varepsilon > 0$, tel que : $\mu\{x, |f|^2(x) > \varepsilon\} > 0$, l'inégalité de Tchebetchev associée pour $f \in \mathbb{L}^2_\mu$, $f > 0$, $\forall \varepsilon > 0$,

$$\mu\{x, f(x) > \sqrt{\varepsilon}\} \leq \frac{\int f d\mu}{\sqrt{\varepsilon}}.$$

Pour ε choisi, on a $\mu\{x, f(x) > \sqrt{\varepsilon}\} = 0$, mais d'aprés ce qu'on a supposé $(f > 0)$ on est arrivé à un résultat contradictoire, d'aprés l'hypothèse on a $f \geq 0$, donc $f = 0$, $\mu p.p$.

Il en résulte que $< f , g >$ pour $f, g \in \mathbb{L}^2$ définie un produit scalaire dans $\mathbb{L}^2$. □

Propsition 5. $\mathbb{L}^2$ *muni de produit scalaire* $< . , . >$ *est un espace de Hilbet.*

Démonstration.

On a $||.||$ la norme associée au produit scalaire est la norme euclidienne, i.e $||f|| =< f , f >^{\frac{1}{2}}$, $\forall f \in \mathbb{L}^2$ et on a $< f , f >= \int |f|^2\, d\mu = ||f||_2^2$, i.e :

la norme euclidienne coincide avec la $||.||$ de $\mathbb{L}^2$, donc $\mathbb{L}^2$ muni de produit scalaire $< f\ ,\ g >$, $f,\ g \in \mathbb{L}^2$ est un espace euclidien d'aprés Le Théorème de Fisher-Riesz, $\mathbb{L}^2$ est complet pour $||.||_2 = ||.||$.
Donc $\mathbb{L}^2$ muni de produit scalaire $< .\ ,. >$ est un espace hérmitien complet et donc $\mathbb{L}^2$ est un espace de Hilbert.
□

L'espace $\mathbb{L}^2_\mu(G)$

Soit G groupe fini et $\mathbb{L}^2_\mu(G) = \{f : G \longrightarrow \mathbb{C}, \int |f|^2\ d\mu < \infty\}$, pour

$$\mu(ds) = \frac{1}{|G|},\ \forall s \in G,$$

d'aprés la formule de produit scalaire dans $\mathbb{L}^2$, nous avons pour $f, g \in \mathbb{L}^2(G)$,

$$< f\ ,\ g >= \int f(s)\ \overline{g(s)}\mu(ds) = \sum_{s\in G} f(s)\overline{g(s)}\frac{1}{|G|} = \frac{1}{|G|}\sum_{s\in G} f(s)\overline{g(s)}$$

Remarquons que si χ est un caractère sur G alors $\chi \in \mathbb{L}^2_\mu(G)$. De plus nous avons

Théorème 3. *i) Si χ est le caractère d'une représentation irréductible, on a :*

$< \chi, \chi >= 1$ *(autrement dit χ est de longueur 1).*

ii) Si χ et $\chi^{'}$ sont les caractères de deux représentations irréductibles non équivalentes, on a $< \chi, \chi' >= 0$ (autrement dit, χ et χ' sont orthogonaux)

Démonstration.

i) Soit ρ une représentation irréductible de caractère χ et soit $(r_{ij})_{i,j}$ la matrice de représentation ρ.
On a : $\chi(t) = \sum_i r_{ii}(t)$, d'où :

$$< \chi, \chi >=< \sum_i r_{ii}, \sum_j r_{jj} >= \sum_i \sum_j < r_{ii}, r_{jj} >= \sum_{i,j} < r_{ii}, r_{jj} > .$$

D'aprés le corollaire (3), on a $< r_{ii}, r_{jj} >= \delta_{ij}/n$, où n est le degré de ρ.
Et comme les indices i, j prennent chacun n valeurs et $i = j$, donc :

$$< \chi, \chi >= (\sum_{i,j} \delta_{ij})/n = n/n = 1$$

ii) Soient ρ, $\rho^{'}$ deux représentations irréductibles non équivalentes des caractères χ, $\chi^{'}$ et soit $(r_{ij})_{i,j}$, $(r_{i'j'})_{i',j'}$ les matrices de représentations ρ, $\rho^{'}$. Donc

$$< \chi, \chi^{'} >= \sum_{i,j} < r_{ii}, r_{j'j'} > .$$

Et comme les indices i, $j^{'}$ ont des valeurs différentes, alors d'aprés le corollaire (3), $\delta_{ij'} = 0$. Donc :

$$< \chi, \chi^{'} >= 0.$$

□

Remarque

On appelle *caractère irréductible* tout caractère de représentation irréductible.

Théorème 4. *Soit ρ une représentation linéaire de G dans l'espace vectoriel V, φ le caractère irréductible de ρ, supposons que V décompose en somme directe des sous-espaces vectoriels des représentations irréductibles,*

$$\rho = \rho^1 \oplus ... \oplus \rho^k.$$

Alors, si ρ^j est une représentation irréductible de caractère χ, le nombre des ρ^i équivalentes à ρ^j est égal au produit scalaire $(\varphi|\chi) =< \varphi, \chi >$.

Démonstration.

Soit χ_i le caractère de ρ^i, d'aprés la proposition 1, si χ_1 et χ_2 deux caractères des représentations ρ^1 et ρ^2,alors $\chi_{\rho^1 \oplus \rho^2} = \chi_{\rho^1} + \chi_{\rho^2} = \chi_1 + \chi_2$, donc on a

$$\varphi = \chi_1 + ... + \chi_k$$

Et $< \varphi, \chi >=< \chi_1 + ... + \chi_k, \chi >=< \chi_1, \chi > +...+ < \chi_k, \chi >$.
D'autre part on a d'aprés le théorème 3

$$< \chi_i, \chi >= \begin{cases} 1, & \text{si } \chi_i = \chi \\ 0, & \text{sinon} \end{cases}$$

Et dans le cas où $\chi_i = \chi$, la représentation ρ^i de caractère χ_i équivalente à la représentation ρ^j de caractère χ et à chaque fois qu'on a le résultat on a la valeur 1 pour l'équivalence, d'où on peut compter le nombre de fois où ρ^i équivalente à ρ^j. □

Corollaire 4. *Le nombre des ρ^i équivalentes à ρ^j ne dépend pas de la décomposition choisie.*

Démonstration.
On a :$< \varphi, \chi >=< \chi_1, \chi > +...+ < \chi_k, \chi >$.
Et $\rho^i \sim \rho^j$ si et seulement si $\chi = \chi_i$, i.e si ces deux représentations ont le même caractère donc l'équivalence dépend des équivalence entre les représentations et non pas de leurs décompositions. □

Corollaire 5. *Deux représentations de même caractère sont équivalentes.*

Démonstration.

Le corollaire 1 montre que deux représentations de même caractère contiennent le même nombre de fois toute représentation irréductible donnée, i.e si χ et $\chi^{'}$ leurs caractères, alors $< \chi, \chi^{'} >= 1$, d'aprés le théorème 3 ces représentations sont irréductibles équivalentes et on a toute représentation irréductible est une représentation, d'où le résultat. □

Propsition 6. *Si χ_1, χ_2, ... , χ_n sont les différents caractères irréductribles du groupe G et si ρ^1, ρ^2, ... , ρ^n désignent des représentations corréspondantes, toute représentation ρ de caractère φ est égale à une somme directe telle que :*

$$\rho = m_1\rho^1 \oplus ... \oplus m_n\rho^n, m_i \text{ entier } \geq 0.$$

et $\varphi = m_1\chi_1 + ... + m_n\chi_n$, alors $< \varphi, \chi_i >= m_i$, avec $i = 1, ..., n$.

Démonstration.

On a φ est le caractère de ρ, avec $\varphi = m_1\chi_1 + ... + m_n\chi_n$, on a donc :
$< \varphi, \chi_i >=< m_1\chi_1 + ... + m_n\chi_n, \chi_i >=< m_1\chi_1, \chi_i > +...+ < m_n\chi_n, \chi_i >$
$= m_1 < \chi_1, \chi_i > +... + m_n < \chi_n, \chi_i >= m_i < \chi_i, \chi_i >= m_i, i = 1, ..., n.$
□

Propsition 7. *Soient χ_1, χ_2, ... , χ_h les caractères des représentations irréductibles ρ^1, ρ^2, ... , ρ^h du groupe G, si n_1, n_2, ... , n_h les degrés des représentations ρ^1, ρ^2, ... , ρ^h, alors elles sont aussi les degrés de leurs caractères.*

Démonstration.

On a χ_1, χ_2, ... , χ_h les caractères des ρ^1, ρ^2, ... , ρ^h, alors $\chi_1(s) = \chi_{\rho^1}(s)$, $\chi_2(s) = \chi_{\rho^2}(s)$, ... , $\chi_h(s) = \chi_{\rho^h}(s)$, $\forall s \in G$, on a par définition de caractère de représentation, $\chi_{\rho^i}(s) = tr(\rho^i(s))$, d'aprés l'hypothèse on a : n_i est le degré de représentation de ρ^i, i.e si V_i est l'espace de représentation de ρ^i, n_i est la dimension de V_i et comme $\chi_{\rho^i}(e) = tr(\rho^i(e)) = tr(Id_{V_i}) = n_i$ (e est l'élément neutre de G), donc $n_i = \chi_{\rho^i}(e) = \chi_i(e)$.

□

2.6.3 Décomposition de la représentation régulière

Propsition 8. *Le caractère r_G de la représentation régulière ρ dans l'espace vectoriel V est donné par les formules :*

$$r_G = \begin{cases} |G|, & si\ s = e \\ 0, & sinon \end{cases}$$

Démonstration.

On a ρ est la représentation régulière de G, alors le degré de ρ est égal au $|G|$.
Comme $r_G(s) = tr(\rho(s))$, alors si $s = e$, $tr(\rho(s)) = tr(\rho(e)) = tr(Id_V) = |G|$ et pour $s \neq e$, on a $tr(\rho_s) \neq |G|$.
D'autre part on a si $(e_t)_{t\in G}$ est la base de V, ρ_s transforme e_t en e_{st}, i.e : $\rho_s(e_t) = e_{st}$ et si $s \neq e$, on a $st \neq et$, ce qui montre que les termes diagonaux de la matrice ρ_s sont nuls, en particulier on a $tr(\rho_s) = 0$, d'où $r_G(s) = 0$. □

Corollaire 6. *Chaque représentation irréductible ρ^i est contenue dans la représentation régulière ρ un nombre de fois égal à son degré n_i.*

Démonstration.

Soit χ_i le caractère de ρ^i et r_G est le caractère de ρ, d'aprés le théorème 4, le nombre de représentations irréductibles est égal à $< \chi_i, r_G >$. Or, on a

$$< \chi_i, r_G >= \frac{1}{|G|} \sum_{s\in G} \chi_i(s) r_G(s^{-1}),$$

alors pour $s = e$,

$$< \chi_i, r_G >= \frac{1}{|G|}\sum_{s\in G}\chi_i(e)r_G(e) = \frac{1}{|G|}|G|\chi_i(e)$$

$$= \chi_i(e) = \chi_{\rho^i}(e) = tr(\rho^i(e)) = tr(Id_{V_i}) = n_i.$$

□

2.6.4 Nombre des représentations irréductibles

Propsition 9. *Soit f une fonction centrale sur le groupe G et soit $\rho : G \longrightarrow GL(V)$ une représentation linéaire de G. Soit ρ_f l'application linéaire de l'espace vectoriel V de dimension n dans lui-même définie par la formule :*

$$\rho_f = \sum_{t\in G} f(t)\rho_t.$$

Si ρ est irréductible de degré n et de caractère χ, ρ_f est une homothètie de rapport λ donnée par :

$$\lambda = \frac{1}{n}\sum_{t\in G} f(t)\chi(t) = \frac{g}{n} < f, \chi^* > .(g = |G|, \chi^* = \chi^{-1})$$

Démonstration.

On a : $\rho_f = \sum_{t\in G} f(t)\rho_t$, alors

$$\begin{aligned}\rho_s^{-1}\rho_f\rho_s &= \sum_{t\in G}\rho_s^{-1}f(t)\rho_t\rho_s = \sum_{t\in G} f(t)\rho_s^{-1}\rho_t\rho_s = \sum_{t\in G} f(t)\rho_s^{-1}\rho_{ts} \\ &= \sum_{t\in G} f(t)\rho_{s^{-1}}\rho_{ts} = \sum_{t\in G} f(t)\rho_{s^{-1}ts}.\end{aligned}$$

En posant $u = s^{-1}ts$, $t = sus^{-1}$, on a $t \in G$ et $s \in G$, alors $s^{-1}ts \in G$, i.e $u \in G$, donc :

$$\sum_{t\in G} f(t)\rho_{s^{-1}ts} = \sum_{u\in G} f(sus^{-1})\rho_u$$

D'autre part on a f est centrale, i.e $u = sus^{-1}$, alors

$$\sum_{u\in G} f(sus^{-1})\rho_u = \sum_{u\in G} f(u)\rho_u = \rho_f.$$

Donc : $\rho_s^{-1}\rho_f\rho_s = \rho_f$, il en résulte que $\rho_f\rho_s = \rho_s\rho_f$ et d'aprés le lemme 2 on a, ρ_f est une homothétie λ et $tr(\lambda) = \lambda tr(Id_V) = \lambda.n$
on a : $tr(\rho_f) = \sum_{t\in G} f(t)tr(\rho_t) = \sum_{t\in G} f(t)\chi(t) = n\lambda$ et

$$< f, \chi >= \frac{1}{g}\sum_{t\in G} f(t)\chi(t)^*.$$

D'où :

$$\lambda = \frac{1}{n}\sum_{t\in G} f(t)\chi(t) = g\frac{1}{g}(\frac{1}{n}\sum_{t\in G} f(t)(\chi(t)^*)^*)$$

$$= \frac{g}{n}(\frac{1}{g}\sum_{t\in G} f(t)(\chi(t)^*)^*) = \frac{g}{n} < f, \chi^* > .$$

□

Propsition 10. *Si H est l'espace vectoriel des fonctions centrales sur le groupe G, les caractères irréductibles χ_1, χ_2,...,χ_h des représentations de G, appartiennent à H.*

Démonstration.

D'aprés la proposition 9, on a

$$\lambda = \frac{g}{n} < f\ ,\ \chi^* >,$$

alors :

$$< f\ ,\ \chi^* >= \frac{n\lambda}{g}$$

D'aprés la définition de la forme hérmitienne on a : f et χ dans le même espace vectoriel, donc l'espace vectoriel H des fonctions centrale est le même pour les caractères irréductibles.

□

Théorème 5. *Les caractères χ_1, χ_2,...,χ_h forment une base orthonormale de H.*

Démonstration.

Le théorème 3 montre que les χ_i forment un système orthonormal dans H.

Il reste à montrer qu'ils engendrent H et pour cela il suffit de montrer que tout élément de H orthogonal aux χ_i^* est nul. Or soit f un tel élément.

Pour toute représentation ρ de G, posons $\rho_f = \sum_{t\in G} f(t)\rho_t$. Puisque f est orthogonale aux χ_i^*, la proposition 8 montre que ρ_f est nul lorsque ρ est irréductible, par décomposition en somme directe on en conclut que ρ_f est toujours nul (car on a un système orthonormal, i.e ρ n'est pas équivalente à aucune représentation résultatante de la décomposition). Appliquons ceci à la représentation régulière et calculons le transformé du vecteur de base e_1 par ρ_f. On a :

$$\rho_f e_1 = \sum_{t\in G} f(t)\rho_t(e_1) = \sum_{t\in G} f(t)e_t.$$

Comme $\rho_f = 0$, alors on a $\rho_f\, e_1 = 0$, la formule ci-dessus montre que $f(t) = 0$ (car $\rho_t e_1 = e_t \neq 0$), d'où $f = 0$.

□

Définition 14. *Une famille ρ^1, ρ^2, ... , ρ^m de représentation de groupe G s'appelle système complet de représentation irréductible, si :*
(a) les représentation ρ^1, ρ^2, ... , ρ^m sont irréductibles et non équivalentes deux à deux.
(b) Chaque représentation irréductible du groupe G est équivalente à une des représentations ρ^1, ρ^2, ... , ρ^m.

Théorème 6. *Soit G un groupe fini et soient ρ^1, ρ^2, ... , ρ^m des représentations linéaire de G. Si ρ^1, ρ^2, ... , ρ^m forment un système complet de représentations irréductibles du groupe G, alors les éléments matriciaux $x_{ij}^k(s)$, $k = 1, ..., m$, i, $j = 1, ..., n_k$ de toutes ces représentations forment un système orthogonal complet dans $\mathbb{L}^2(G)$.*

Démonstration.

L'orthogonalité de ce système a été démontré dans le théorème 3, alors il reste à montrer que ce système est complet.
(Cf.[1] pour la démontrer que le système est complet)

□

Théorème 7. *Le nombre des représentations irréductibles de G (à isomorphisme prés) est égal au nombre des classes de G.*

Démonstration.

Soient C_1, C_2,...,C_k les différentes classes de G.
Dire qu'une fonction f sur G est centrale sur G équivaut à dire qu'elle est constante sur chaque classe du G (par définition), elle est donc détérminée par ses valeurs propres λ_i sur les classes C_i, qu'elles peuvent être choisies arbitraurement, donc la dimension de l'espace de f est égal au nombre de ses valeurs propres et comme ces dérnières ont été choisies par rapport à les classes de G, alors le nombre des valeurs propres égal au nombre des classes de G, d'où la dimension de l'espace vectoriel H est égal à k.
D'autre part d'aprés le théorème 5, cette dimension est égal au nombre des représentations irréductibles du groupe G.

□

Chapitre 3

Caractère d'un groupe, Transformée de Fourier et Formule de Plancherel

3.1 Mesure de Haar

Définition 1. *Soit G groupe topologique localement compact et abelien, pour abreger LCA. Il existe une mesure m sur $(G, \mathcal{B}_G)$ unique à une constante multiplicative près, invariante par translation et finie sur les compacts, appelée mesure de Haar du groupe G.*

(Cf. [9], pour la démonstration de l'existence et l'unicité de m).

Propriété

Soient G groupe additif et LCA et E ensemble Borélien dans le groupe G. Si m la mesure de Haar sur G, alors $m(-E) = m(E)$. Si G est un groupe multiplicatif, on a $m(E^{-1}) = m(E)$.

Démonstration.

Soit $m^{'}$ une mesure sur $(G, \mathcal{B}_G)$ définie par $m^{'}(E) = m(-E)$, où m est une mesure de Haar de G et E ensemble Borélien sur le groupe G, alors $m^{'}$ est une mesure de Haar. En effet :

$\forall x \in G, E \in G, m^{'}(E+x) = m(-E+x) = m(-E)$, car m est une mesure de Haar, alors m est invariante par translation.

Donc : $m^{'}(E+x) = m(-E) = m^{'}(E)$. Il en résulte que $m^{'}$ est aussi invariante par translation.
m est une mesure finie sur les compacts, alors $m^{'}$ l'on est aussi.

Alors m est unique à constante prés, donc $\exists\lambda$, tel que $m^{'}(E) = \lambda m(E)$, ie $m(-E) = m(E)$, $\forall E \in \mathcal{B}_G$.
En particulier si : $-E = E$, on a $\lambda = 1$. Donc $m^{'}(E) = m(E)$ et par suite $m(-E) = m(E)$. $\square$

3.2 Convolution

Définition 2. *Soit G un groupe LCA et m sa mesure de Haar. Soient f, g deux fonctions de $\mathbb{L}^1_m(G)$. On appelle convolution de f et g la fonction notée $f * g$, définie pour $x \in G$, par*

$$(f * g)(x) = \int_G f(x-y)g(y)m(dy).$$

quand cela a un sens ie $\int_G |f(x-y)g(y)|m(dy) < \infty$, ce que l'on supposera dans ce qui suit.

Propriété 1

La convolution est commutative :
$\forall f, g \in \mathbb{L}^1(G)$ et $x \in G$, $(f * g)(x) = (g * f)(x)$

Démonstration.
On a $(f * g)(x) = \int_G f(x-y)g(y)m(dy)$. Soit le changement de variable $z = x - y$. Nous avons $dz = -dy$ ie $dy = -dz$. Donc

$$(f * g)(x) = \int_G f(x-y)g(y)m(dy) = \int_G f(z)g(x-z)m(-dz).$$

Comme $m(-dz) = m(dz)$, d'aprés la propriété ci-dessus, nous avons donc :

$$(f * g)(x) = \int_G f(z)g(x-z)m(dz)$$

Comme par définition

$$(g * f)(x) = \int_G f(z)g(x-z)m(dz),$$

nous avons donc $(f * g)(x) = (g * f)(x)$ et la propriété est démontrée. □

Propriété 2

La convolution est associative :
$\forall f, g, h \in \mathbb{L}^1(G)$ et $x \in G$, $((f * g) * h)(x) = (f * (g * h))(x)$,
en supposant que le produit de convolution $f * (g * h)$ a un sens.

Démonstration.
On a :

$$(f*(g*h))(x) = \int_G f(x-z)(g*h)(z)m(dz) = \int_G \int_G f(x-z)g(z-y)h(y)m(dy)m(dz).$$

En appliquant Fubini, on a :

$$\int_G \int_G f(x-z)g(z-y)h(y)m(dy)m(dz) = [\int_G f(x-z)[\int_G g(z-y)h(y)m(dy)]m(dz)].$$

Soit le changement de variable : $t = z - y$. Nous avons : $m(dt) = m(dz)$.
Donc :

$$\begin{aligned}[\int_G f(x-z)[\int_G g(z-y)h(y)m(dy)]m(dz)] &= [\int_G f(x-t-y)[\int_G g(t)h(y)m(dy)]m(dt)] \\ &= \int_G f((x-y)-t)g(t)m(dt) \int_G h(y)m(dy).\end{aligned}$$

Par définition, on a

$$\begin{aligned}\int_G f((x-y)-t)g(t)m(dt) \int_G h(y)m(dy) &= \int_G (f*g)(x-y)h(y)m(dy) \\ &= ((f*g)*h)(x),\end{aligned}$$

nous avons donc $(f*(g*h))(x) = ((f*g)*h)(x)$ et la propriété est démontrée.
□

Propriété 3

Si $\forall f, g \in \mathbb{L}^1(G)$ et $\forall x \in G$, $\int_G |f(x-y)g(y)|m(dy) < \infty$, alors
$||f * g||_1 \leq ||f||_1.||g||_1$.

Démonstration. On a :

$$||f * g||_1 = \int_G |f * g|dm = \int_G |(f * g)(x)|m(dx)$$

Par définition, on a :

$$\begin{aligned}\int_G |(f*g)(x)|m(dx) &= \int_G [|\int_G f(x-y)g(y)m(dy)|]m(dx)\\ &\leq \int_G\int_G |f(x-y)g(y)|m(dy)m(dx)\\ &= \int_G\int_G |f(x-y)||g(y)|m(dy)m(dx)\end{aligned}$$

En appliquant Fubini, on a :

$$\begin{aligned}\int_G\int_G |f(x-y)||g(y)|m(dy)m(dx) &= \int_G |g(y)|\int_G |f(x-y)|m(dx)m(dy)\\ &= \int_G |g(y)|m(dy)\int_G |f(x-y)|m(dx)\\ &= ||f||_1||g||_1.\end{aligned}$$

□

3.3 Caractères

Définition 3. *Soit G un groupe LCA noté additivement. On appelle caractère sur G toute application continue $\gamma : G \longrightarrow \mathbb{C}$, telle que :*
(i) $\forall s \in G$, $|\gamma(s)| = 1$.
(ii) $\forall s,\ t \in G$, $\gamma(s+t) = \gamma(s)\gamma(t)$ *et* $\gamma(s-t) = \gamma(s)\gamma(t)^{-1}$.

Soit Γ, l'ensemble des caractères de G. Définissons sur Γ la somme de deux caractères, en posant :

$(\gamma_1 + \gamma_2)(s) = \gamma_1(s)\gamma_2(s)$, $\forall \gamma_1,\ \gamma_2 \in \Gamma$ et $s \in G$.
Alors Γ muni de cette loi est un groupe abelien, appelé groupe dual de G.

Propriétés des caractères

Soit G groupe LCA et Γ groupe dual de G. Si $\gamma \in \Gamma$ on note $\gamma(x) = (x, \gamma)$, pour $x \in G$, nous avons alors :

Propriété 1
$\forall x,\, y \in G$ et $\gamma \in \Gamma$, $(x+y,\gamma) = (x,\gamma)(y,\gamma)$

Démonstration.
On a d'aprés la notation ci-dessus : $(x+y,\gamma) = \gamma(x+y)$, $\forall x,\, y \in G$ et $\gamma \in \Gamma$, d'aprés la définition on a, $\gamma(x+y) = \gamma(x)\gamma(y)$, comme $\gamma(x) = (x,\gamma)$ et $\gamma(y) = (y,\gamma)$, alors :

$$(x+y,\gamma) = (x,\gamma)(y,\gamma)$$

□

Propriété 2
$\forall x \in G$ et $\gamma_1,\, \gamma_2 \in \Gamma$, $(x,\gamma_1+\gamma_2) = (x,\gamma_1)(x,\gamma_2)$

Démonstration.
On a : $(x,\gamma_1+\gamma_2) = (\gamma_1+\gamma_2)(x)$, $\forall x \in G$, $\gamma_1,\, \gamma_2 \in \Gamma$, en plus on a :
$(\gamma_1+\gamma_2)(x) = \gamma_1(x)\gamma_2(x)$ et comme $\gamma_1(x) = (x,\gamma_1)$ et $\gamma_2(x) = (x,\gamma_2)$, alors il en résulte que $(x,\gamma_1+\gamma_2) = (x,\gamma_1)(x,\gamma_2)$

□

Propriété 3
$\forall x \in G$, $\gamma \in \Gamma$, $(0,\gamma) = 1$.

Démonstration.
On a : $(0,\gamma) = (x-x,\gamma)$, $\forall x \in G$, d'autre part on a :
$(x-x,\gamma) = \gamma(x-x) = \gamma(x)\gamma(x)^{-1} = 1$, donc $\forall x \in G$, $\gamma \in \Gamma$, $(0,\gamma) = 1$.

□

Propriété 4
$\forall x \in G$, $\gamma \in \Gamma$, $(-x,\gamma) = \overline{(x,\gamma)}$

Démonstration.
On sait que : $(-x,\gamma) = \gamma(-x) = -\gamma(x) = (x,-\gamma)$, d'autre part on a :
$(-x,\gamma) = (0-x,\gamma) = \gamma(0)\gamma(-x) = \gamma(0)\gamma(x)^{-1}$ et d'aprés la propriété 3, on a : $\gamma(0)\gamma(x)^{-1} = 1.\gamma(x)^{-1} = (x,\gamma)^{-1}$, d'où : $(-x,\gamma) = \overline{(x,\gamma)}$. □

3.4 Transformée de Fourier

Définition 4. *$\forall f \in \mathbb{L}^1(G)$, la fonction définie dans Γ, par :*

$$\hat{f}(\gamma) = \int_G f(x)(-x,\gamma)dx = \int_G f(x)\overline{\gamma(x)}dx,\ \forall \gamma \in \Gamma$$

est appelée la transformée de Fourier de f.

Propriété
Soit f, $g \in \mathbb{L}^1(G)$, $\gamma \in \Gamma$, alors on a la formule suivante,

$$\widehat{f * g}(\gamma) = \hat{f}(\gamma)\hat{g}(\gamma)$$

Démonstration.
Par définition, on a :

$$\begin{aligned}\widehat{f * g}(\gamma) &= \int_G (f*g)(x)(-x,\gamma)dx = \int_G (f*g)(x)\overline{\gamma(x)}dx \\ &= \int_G\int_G f(x-y)g(y)\overline{\gamma(x)}dxdy.\end{aligned}$$

En appliquant Fubini, on a :

$$\begin{aligned}\int_G\int_G f(x-y)g(y)\overline{\gamma(x)}dxdy &= \int_G g(y)dy\int_G f(x-y)\overline{\gamma(x)}dx \\ &= \int_G g(y)dy\int_G f(x-y)\gamma(-x)dx\end{aligned}$$

Soit le changement de variable : $t = x - y \Longrightarrow x = t + y$ et $dx = dt$. Donc :

$$\begin{aligned}\int_G g(y)dy\int_G f(x-y)\gamma(-x)dx &= \int_G g(y)dy\int_G f(t)(-t-y,\gamma)dt \\ &= \int_G g(y)dy\int_G f(t)\gamma(-t)\gamma(-y)dt \\ &= \int_G g(y)\gamma(-y)dy\int_G f(t)\gamma(-t)dt \\ &= \int_G f(t)\gamma(-t)dt\int_G g(y)\gamma(-y)dy \\ &= \int_G f(t)\overline{\gamma(t)}dt\int_G g(y)\overline{\gamma(y)}dy \\ &= \hat{f}(\gamma)\hat{g}(\gamma)\end{aligned}$$

Donc : $\widehat{f * g}(\gamma) = \hat{f}(\gamma)\hat{g}(\gamma)$ $\square$

Propsition 1. *Dans le cas où $G = \mathbb{R}$, les caractères de G sont les fonctions $t \mapsto e^{i\alpha t}$, où α est un nombre réel donné.*

Dans le cas où $G = \mathbb{Z}$, les caractères de G sont les fonctions $t \mapsto e^{int}$, avec $n \in \mathbb{Z}$.

Démonstration.

Soient G un groupe LCA additif et Γ est le groupe dual de G et soit γ un caractère sur G défini par : $\gamma(x) = (x, \gamma)$, $\forall x \in G$, $\gamma \in \Gamma$, posons $G = \mathbb{R}$, $\gamma \in \Gamma$, $\exists \delta > 0$, tel que :

$$\int_0^\delta \gamma(t)dt = \alpha \neq 0.$$

On a : $\alpha\gamma(x) = \gamma(x) \int_0^\delta \gamma(t)dt$.
D'aprés la première propriété des caractères on a : $\gamma(x + t) = \gamma(x)\gamma(t)...(1)$

$$\int_0^\delta \gamma(x)\gamma(t)dt = \int_0^\delta \gamma(x + t)dt.$$

Soit le changement de variable : $v = x + t \Longrightarrow t = v - x$,
si $t \longrightarrow 0$, $v \longrightarrow x$ et si : $t \longrightarrow \delta$, $v \longrightarrow \delta + x$. Donc

$$\int_0^\delta \gamma(x + t)dt = \int_x^{\delta+x} \gamma(v)\ dv,$$

γ est continue (par définition de γ), alors γ est dérrivable, donc elle est indéfiniment dérrivale, car on sait que si une fonction une fois dérrivable, alors elle est indéfiniment dérrivable et l'équation (1) est différentielle.
Soit γ' la derrivée continue de γ, alors on a :

$$\gamma(x + t)' = (\gamma(x)\gamma(t))' = \gamma(x)\gamma(t)'.$$

Pour $t = 0$, $\gamma(0) = 1$ (d'aprés la propriété 3). Donc $\gamma'(x) = \gamma'(0)\gamma(x)$.
On pose $A = \gamma'(0)$, alors $\gamma'(x) = A\gamma(x)$.
La solution de l'équation differentielle est : $\gamma(x) = e^{iyx}$, $\forall y \in \mathbb{R}$.

Si $G = \mathbb{Z}$ et $\gamma \in \Gamma$, alors $(1, \gamma) = \gamma(1) = e^{i\alpha}$, $\forall \alpha \in \mathbb{R}$.
De même pour $(n, \gamma) = e^{in\alpha}$.
$\square$

Corollaire 1. *: La transformation de Fourier correspondante à $G = \mathbb{R}$ est :*

$$\hat{f}(y) = \int_{\mathbb{R}} f(x)e^{-iyx}dx, \ \forall y \in \mathbb{R}$$

Propsition 2 (Formule d'inversion de Fourier). *Soit $f \in \mathbb{L}^1(\mathbb{R})$ une fonction telle que $\hat{f} \in \mathbb{L}^1(\mathbb{R})$, alors on a*

$$f(x) = \int_{\mathbb{R}} e^{iyx}\hat{f}(y)dy, \ \forall y \in \mathbb{R}$$

Cette formule est appelée formule d'inversion de Fourier permet de passer $\hat{f}$ à f.

3.5 Formule de Plancherel

Définition 5. *Soit E un espace euclidien,$<,>$ son produit scalaire. L'adjoint d'un opérateur $T : E \longrightarrow E$ est l'opérateur T^* défini par*

$$\forall x, \ y \in E, \ < T(x) \ , \ y >=< x \ , \ T^*(y) >$$

Les propriétés de l'opérateur adjoint

Soit T^* l'adjoint de l'opérateur T. L'adjoint T^* a les propriétéss suivantes :

Propriété 1
T^* est linéaire.

Démonstration.
Montrons que :
(1) $\forall \alpha \in \mathbb{R}$, $\forall x \in E$, $T^*(\alpha x) = \alpha T^*(x)$.
Par définition, on a : $\forall x \in E$ et $\alpha \in \mathbb{R}$, $< T(x) \ , \ \alpha y >=< x \ , \ T^*(\alpha y) >$.
Et $< x \ , \ T^*(\alpha y) >= \alpha < x \ , \ T^*(y) >=< x \ , \ \alpha T^*(y) >$.
Donc

$$T^*(\alpha x) = \alpha T^*(x).$$

Montrons que :
(2) $\forall x, y \in E$, $T^*(x + y) = T^*(x) + T^*(y)$.
Par définition, on a :

$\forall x$, y et $y^{'} \in E$, $< T(x)\ ,\ y + y^{'} >=< T(x)\ ,\ y > + < T(x)\ ,\ y^{'} >=$
$< x\ ,\ T^{*}(y) > + < x\ ,\ T^{*}(y') >$.
D'autre part, on a : $< T(x)\ ,\ y + y^{'} >=< x\ ,\ T^{*}(y + y') >$.
Donc : $< T(x)\ ,\ y+y^{'} >=< x\ ,\ T^{*}(y+y') >=< x\ ,\ T^{*}(y) > + < x\ ,\ T^{*}(y') >$.
D'où

$$T^{*}(x + y) = T^{*}(x) + T^{*}(y).$$

□

Propriété 2
Soit $T \in \mathrm{End}(E)$, alors
T^{*} est une involution.

Démonstration.

Montrons que :
$(T^{*})^{*} = T$.
Posons : $T^{*} = V$. Par définition, on a :
$\underline{\forall x,\ y\ \in\ E,} < x, T(y) >=< T^{*}(x), y >=< V(x), y >= \overline{< y, V(x) >} =$
$< V^{*}(y), x > = < x, V^{*}(y) >=< x, (T^{*})^{*}(y) >$ et par conséquent :

$$(T^{*})^{*} = T$$

□

Propriété 3
Soient T, $T^{'} \in E$, alors $(T \circ T^{'})^{*} = T^{'*} \circ T^{*}$.

Démonstration.

Par définition, on a : $\forall x, y \in E, < (T \circ T^{'})(x)\ ,\ y >=< (T(T^{'}(x))\ ,\ y >=$
$< T^{'}(x)\ ,\ T^{*}(y) >=< x\ ,\ T^{'*}(T^{*}(y)) >$.
D'autre part on a : $< (T \circ T^{'})(x)\ ,\ y >=< x\ ,\ (T \circ T^{'})^{*}(y) >$.
Donc :$< (T \circ T^{'})(x)\ ,\ y >=< x\ ,\ (T \circ T^{'})^{*}(y) >=< x\ ,\ T^{'*}(T^{*}(y)) >$. Donc

$$(T \circ T^{'})^{*} = T^{'*} \circ T^{*}.$$

□

Propriété 4
Considérons une base orthonormale $B = \{e_1, ..., e_n\}$ de l'espace hémitien E,soit $(x_1, x_2, ..., x_n)$ et $(y_1, y_2, ..., y_n)$ les coordonnées de x et y dans cette base. Désignons par $A = (a_{ij})$ la matrice de T relativement à cette base,

alors la matrice de l'endomorphisme adjoint T^* de T est $A^* = \bar{A}^t$, avec $A^* = b_{ij}$, $i, j = 1, ..., n$.

Démonstration.

On a, par définition : $< x, y >= \sum_{i=1}^{n} x_i \bar{y}_i$.
Les coordonnées de $T(x)$ sont donnés par

$$x'_j = \sum_{i=1}^{n} x_i a_{ji} \quad \text{et} \quad y'_i = \sum_{i=1}^{n} y_i b_{ji}$$

D'où

$$< T(x), y >= \sum_{j=1}^{n} x'_j \bar{y_j} = \sum_{j=1}^{n} \sum_{i=1}^{n} x_i a_{ji} \bar{y_j}$$

$$< x, T^*(y) >= \sum_{j=1}^{n} x_j \bar{y'_j} = \sum_{j=1}^{n} \sum_{i=1}^{n} x_j \bar{b_{ji}} \bar{y_i}$$

Pour que ces deux nombres soient égaux, quels que soient x et y, il faut et il suffit, que :

$$a_{ji} = \bar{b_{ij}} \quad \text{ou} \quad b_{ij} = \bar{a_{ji}},$$

ie que la matrice (b_{ij}) soit la transposée de la conjuguée de A.
Cette matrice se note A^* et se nomme matrice adjointe de A.

$$A^* = {}^t\bar{A}.$$

Ou on a :

$$< x, y >= {}^t x \bar{y}$$

Donc

$$\begin{aligned} < Ax, y > \quad &= \quad < x, A^* y > \\ &\iff {}^t(Ax)\bar{y} = {}^t x(\overline{A^* y}) \\ &\iff {}^t x\, {}^t A \bar{y} = {}^t x \bar{A}^* \bar{y} \\ &\iff {}^t A = \bar{A}^* \\ &\iff A^* = {}^t\bar{A}. \end{aligned}$$

□

Propsition 3 (Formule de Plancherel). *Soit $f \in \mathbb{L}^1(G) \bigcap \mathbb{L}^2(G)$, $x \in G$ et $\gamma \in \Gamma$, alors on a*

$$\int_G |f(x)|^2 dx = \int_\Gamma |\hat{f}(\gamma)|^2 d\gamma$$

i.e.

$$||f||_2 = ||\hat{f}||_2$$

Démonstration. (Cf. [9] pour la démonstration.) □

Dans le cas où G est un groupe fini, nous consiérons $\mathbb{L}^2(G)$ avec $m = \frac{1}{|G|}$.

Rappelons qu'une famille de représentations T^1, T^2, ..., T^m forment un système complet de représentations irréductibles, si :
- T^1, T^2, ..., T^m sont irréductibles et non Ãľquivalente deux à deux.
- Chaque représentation irréductible du groupe G est équivalente à une des reprèsentations T^1, T^2, ..., T^m .

Nous avons alors :

Propsition 4 (Formule de Plancherel pour un groupe fini). *On suppose que l'espace vectoriel V est muni d'un produit scalaire et que les représentations T^k de degrés n_k, $k = 1, ..., m$ admettent $(x^k_{ij}(s))$ comme une représentation matricielle unitaires par rapport au produit scalaire de V.*
Si T^1, T^2, ..., T^m forment un système complet de représentations, alors la famille $(e^k_{ij}(s))_{i,j}$ définie par $e^k_{ij}(s) = \sqrt{n_k} x^k_{ij}(s)$, $\forall s \in G$, forme une base orthonormale de $\mathbb{L}^2_m(G)$ et on a la formule de Plancherel :

$$\forall f \in \mathbb{L}^2_m(G), \ < f, f >= \sum_{k=1}^{m} n_k tr(T^{k*}(f) T^k(f))$$

Démonstration.

D'aprés le théorème 6 de chapitre 2, on a : si la famille de représentations T^1, T^2, ..., T^m forme un système complet du groupe G, alors les éléments des matrices $(x^k_{ij}(s))_{i,j}$, $k = 1, 2, ..., n_m$ forment un système orthogonal complet, donc $e^k_{ij}(s) = \sqrt{n_k} x^k_{ij}(s)$ forme une base orthonormale dans $\mathbb{L}^2(G)$, alors pour toute fonction f dans $\mathbb{L}^2(G)$ vérifie

$$< f, f >= \sum_{k=1}^{m} \sum_{j=1}^{n_k} | < f, e^k_{ij} > |^2$$

D'autre part on a : $< f, e^k_{ij} >= \sqrt{n_k} < f, x^k_{ij} >$, on remplace $< f, e^k_{ij} >$ par sa valeur dans $< f, f >$, on a :

$$< f, f >= \sum_{k=1}^{m} \sum_{i,j=1}^{n_k} n_k | < f, x^k_{ij} > |^2$$

Soit $T^{k^*}(s)$ l'opérateur adjoint à $T^k(s)$ relativement au produit scalaire. Posons

$$T^k(f) = g(f(s)T^{k^*}(s)) = \frac{1}{|G|} \sum_{k=1}^{|G|} f(s)T^{k^*}(s), \ \forall s \in G$$

Les $x^k_{ji}(s)$ sont alors les éléments de la matrice de l'opérateur $T^{k^*}(s)$ relativement à la base de $T^k(s)$, donc

$$tr(T^{k^*}(s)T^k(s)) = \sum_{i,j=1}^{n_k} | < f, x^k_{ij} > |^2$$

On remplace $tr(T^{k^*}(s)T^k(s))$ par sa valeur dans la formule de $< f, f >$, on a

$$< f, f >= \sum_{k=1}^{m} n_k tr(T^{k^*}(s)T^k(s)).$$

□

Remarques

(a) La fonction $T^k(f)$ de l'indice k définie ci-dessus est *la transformée de Fourier de la fonction f.*

(b) La formule $< f, f >= \sum_{k=1}^{m} \sum_{j=1}^{n_k} | < f, e_{ij}^k > |^2$ est *l'égalité de Parceval du groupe* G.

Dans le cas d'un groupe fini G, si m est la mesure uniforme sur G, la formule de Plancherel se simplifie et nous avons :

Propsition 5 (Formule de Plancherel pour un groupe fini.). *Soit G un groupe fini et m est la mesure uniforme sur G. Si f, $g \in \mathbb{L}_m^2(G)$, alors*

$$\sum_{s \in G} f(s)\overline{g(s)} = \frac{1}{|G|} \sum_{\rho} d_\rho \ tr(\hat{f}(\rho)^t \overline{\hat{g}(\rho)}),$$

où ρ parcourt l'ensemble des représentations de G et d_ρ le degré de ρ.

Chapitre 4

Les chaines de Markov $X_{n+1} = a_n X_n + b_n X_{n-1}$

4.1 Application de la formule de Plancherel

Soit $(E, \mathcal{E})$ un espace mesurable et $\mathcal{P}(E)$ l'ensemble des lois de probabilités sur E. On définit une norme sur E, en posant pour $\mu \in \mathcal{P}(E)$,

$$||\mu|| = \sup_{A \in \mathcal{E}} |\mu|(A)$$

où $|\mu|$ est la variation totale de μ.

Dans le cas particulier d'un groupe fini G, si P est une loi sur G, nous avons

$$||P|| = \sum_s P(s)$$

La distance associée à cette norme est appelée la distance de variation. Donc $\mathcal{P}(G)$ devient un espace normé. Toutes les normes sur $\mathcal{P}(E)$ sont équivalentes et la distance de variation est choisie en raison de ses intérprétations en Calcul de Probabilités.

Soit P une loi de probabilité sur le groupe fini G et U la loi uniforme sur G. La définition de $\|.\|$ sur l'ensemble des lois permet de comparer ces deux lois i.e. de dire si ces deux lois sont proches (se ressemblent) ou éloignées (différentes), en considérant leur distance de variation i.e.

$$||P-U|| = \max_{A\subset G} |P(A)-U(A) = \frac{1}{2}\sum_{s\in G}|P(s)-\frac{1}{|G|}|.$$

Lemme 1 (Lemme de la borne supérieure, Diaconis(1984)). *Soit G un groupe fini, P une probabilité et U la loi uniforme sur G, alors on a*

$$||P-U||^2 \leq \frac{1}{4}\sum_{\rho} n\ tr(\hat{P}(\rho)^t\overline{\hat{P}(\rho)}),$$

où la somme est etendue sur toutes les représentations irréductibles non-triviale ρ du groupe G.

Démonstration.

On a

$$||P-U|| = \frac{1}{2}\sum_{s\in G}|P(s)-U(s)|.$$

Donc

$$\begin{aligned} 4||P-U||^2 &= (\sum_{s\in G}|P(s)-U(s)|)^2 \\ &= (\sum_{s\in G}|P(s)-U(s)|)(\sum_{s\in G}|P(s)-U(s)|). \end{aligned}$$

et d'aprés linégalité de Cauchy-schwartz, on a :

$$(\sum_{s\in G}|P(s)-U(s)|)^2 \leq (\sum_{s\in G}|P(s)-U(s)|^2)(\sum_{s\in G}|P(s)-U(s)|^2)$$

D'autre part on a : $0 \leq |P(s)-U(s)| \leq 1$, alors

$$\sum_{s\in G}|P(s)-U(s)|^2 \leq \sum_{s\in G}1 = |G|$$

Donc :

$$(\sum_{s\in G}|P(s)-U(s)|)^2 \leq |G|\sum_{s\in G}|P(s)-U(s)|^2$$

D'aprés la formule de Plancherel, on a

$$\begin{aligned} |G| \sum_{s \in G} |P(s) - U(s)|^2 &= |G| \frac{1}{|G|} \sum_{\rho} n \; tr((\widehat{P - U})(\rho)^t \overline{(\widehat{P - U})(\rho)}) \\ &= \sum_{\rho} n \; tr((\widehat{P - U})(\rho)^t \overline{(\widehat{P - U})(\rho)}) \\ &= \sum_{\rho} n \; tr(((\hat{P}(\rho) - \hat{U}(\rho))^t \overline{(\hat{P}(\rho) - \hat{U}(\rho))}). \end{aligned}$$

Comme on a, si ρ est une représentation triviale alors $\hat{P}(\rho) = 1$ et si ρ est non-triviale $\hat{U}(\rho) = 0$, alors :

$$(\sum_{s \in G} |P(s) - U(s)|)^2 \leq \sum_{\rho} n \; tr(\hat{P}(\rho)^t \overline{\hat{P}(\rho)}).$$

D'où

$$||P - U||^2 \leq \frac{1}{4} \sum_{\rho} n \; tr(\hat{P}(\rho)^t \overline{\hat{P}(\rho)}).$$

□

4.2 Les chaînes de Markov $X_{n+1} = a_n X_n + b_n (mod\, p)$

Les ordinateurs produisent souvent des nombres pseudo-aléatoire utilisant des recurrences, telles que $X_{n+1} = aX_n + b (\text{mod } p)$, avec p un nombre entier fixe (avec $2^{31} - 1$ et 2^{32} étant des choix populaires) et les nombres entiers a et b sont choisis de sorte que les réalisations de $X_0 = 0$, X_1, X_2, ..., aient certaines des propriétés de suites de nombres aléatoires. Cependant, l'ordre de X_n est détérministe et presente une certaine régularité pour les grands échantillons. Pour augmenter "l'aspect aléatoire", un ou plusieurs différents générateurs sont souvent combinés.

Dans ce cadre, nous donnons quelques propriétés des chaînes de Markov $X_{n+1} = a_n X_n + b_n (\text{mod } p)$, où les a_n et les b_n sont des suites de variables aléatoires indépendantes, exploitables dans ce sens.

Le générateur du type $X_{n+1} = aX_n (mod\ p)$

Les premiers générateurs de nombres pseudo-aléatoires étaient du type $X_{n+1} = aX_n (\text{mod } p)$ à un taux constant (dire, 1000 fois par seconde), les appels aux générateurs depend du temps d'éxecution de diverses étapes dans le programme ayant pour résultat un multiplicateur aléatoire i.e $a.X_n$.

Le générateur du type $X_{n+1} = aX_n + b_n (mod\ p)$

Nous considérons la chaine de markov $(X_n)_n$ sur $\mathbb{Z}_p$ l'ensemble des entiers modulo p définie par $X_{n+1} = aX_n + b_n (mod\ p)$, où (a_n) et $(b_n)_n$ sont des variables aléatoires indépendantes et de même loi. Notre but de base sera d'éstimer aussi précisement que nous pouvons le nombre n d'étapes requises, si p est impair et b_1, b_2, b_3, ..., sont indépendants avec la loi μ sur $\mathbb{Z}_p$, pour que la suite de nombres produits soit distribuée uniformèment dans $\mathbb{Z}_p$. Pour celà, si U est la loi uniforme, nous devons montrer que $\|P_n - U\|$ est proche de 0, si P_n est la loi de $(X_n)_n$. Commençons par le cas où $a = 1$.

Théorème 1. *Soit p un entier et soit $(X_n)_n$ la chaine de Markov définie par $X_{n+1} = X_n + b_n\ (mod\ p)$ d'espace des états le groupe $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ avec $n > 7$, $n \geq p^2$, où les b_n sont des var i.i.d et de loi P tel que*

$$P[0] = P[1] = P[-1] = \frac{1}{3}.$$

Alors il existe α

$$\alpha = \frac{8}{9}\pi^2$$

tel que :

$$||P^{*n} - U|| \leq e^{-\frac{\alpha n}{p^2}}.$$

Démonstration.

D'aprés l'hypothèse, on a : $P(+1) = P(-1) = P(0) = \frac{1}{3}$, la transformée de Fourier associée à P est : $\hat{P}(j) = \sum_k P(k)Q^{kj}$, avec $Q^{kj} = e^{2\pi jik/p}$, alors

$$\hat{P}(j) = P(1)e^{2\pi ji/p} + P(-1)e^{2\pi ji(-1)/p} + P(0)e^{2\pi ji(0)/p},$$

donc

$$\hat{P}(j) = \frac{1}{3}(1 + e^{2\pi ij/p} + e^{-2\pi ij/p})$$

D'autre part on a :

$$\frac{1}{3}(1 + e^{2\pi ij/p} + e^{-2\pi ij/p}) = \frac{1}{3}(1 + 2(\frac{e^{2\pi ij/p}}{2} + \frac{e^{-2\pi ij/p}}{2}) = \frac{1}{3}(1 + 2\cos\frac{2\pi j}{p}).$$

D'où :

$$\hat{P}(j) = \frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi j}{p}).$$

Soit P^{*n} la mesure de convolution de P à n pas et d'aprés le lemme de la borne supérieure, on a

$$||P^{*n} - U||^2 \leq \frac{1}{4}\sum_{j=1}^{p-1} |\hat{P}^{*n}(j)|^2 = \frac{1}{4}\sum_{j=1}^{p-1} \hat{P}^{2n}(j) = \frac{1}{4}\sum_{j=1}^{p-1}(\frac{1}{3} + \frac{2}{3}\cos\frac{2\pi j}{p})^{2n}$$

D'aure part, on a la formule de Marc Laurin pour $f(x) = \cos(x)$ est donnée par :

$$f(x) = f(0) + xf'(0) + \frac{x^2}{2!}f^{(2)}(0) + \frac{x^3}{3!}f^{(3)}(0) + \frac{x^4}{4!}f^{(4)}(0) + ... + \frac{x^n}{(n)!}f^{(n)}(c).$$

Donc

$$\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!}\cos(c).$$

Alors pour $0 \leq x \leq \frac{\pi}{4}$ et $0 \leq c < x$, on a :

$$1 - \cos(x) - \frac{x^2}{2!} + \frac{x^4}{4!} = \frac{x^6}{6!}\cos(c) > 0$$

Donc

$$1 - \cos x \geq \frac{x^2}{2} - \frac{x^4}{4!} = \frac{x^2}{2}(1 - \frac{x^2}{12}) \geq \frac{x^2}{3}.$$

On a aussi :

$$e^{-x} = 1 - x + \frac{x^2}{2}e^{-c}, o < c < x$$

Alors :

$$e^{-x} - 1 + x = \frac{x^2}{2}e^{-c} > 0.$$

Donc : $1 - x \leq e^{-x}$, alors :

$$\frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi j}{p}) = 1 - \frac{2}{3}(1 - \cos(\frac{2\pi j}{p})) \leq e^{-\frac{2}{3}(1-\cos(\frac{2\pi j}{p}))}$$

Et comme on a : $1 - \cos x \geq \frac{x^2}{3}$, alors :

$$1 - \cos(\frac{2\pi j}{p}) \geq \frac{1}{3}(\frac{2\pi j}{p})^2 = \frac{1}{3}\frac{4\pi^2 j^2}{p^2}$$

Donc :

$$1 - \frac{2}{3}(1 - \cos(\frac{2\pi j}{p})) \leq e^{-\frac{8}{9}\frac{\pi^2 j^2}{p^2}}.$$

Posons : $\frac{8\pi^2}{9} = \alpha$
D'où :

$$1 - \frac{2}{3}(1 - \cos(\frac{2\pi j}{p})) \leq e^{-\frac{\alpha j^2}{p^2}}.$$

Pour : $\frac{\pi}{4} < \frac{2\pi j}{p} \leq \frac{\pi}{2}$ et $\frac{p}{8} \leq j \leq \frac{p}{4}$, le terme général est majoré par :

$$(\frac{1}{3} + \frac{2}{3}\cos(\frac{2\pi j}{p}))^{2n} \leq (\frac{1}{3} + \frac{2}{3\sqrt{2}})^{2n},$$

alors :

$$\begin{aligned}
\sum_{j=1}^{p-1}(\frac{1}{3} + \frac{2}{3}\cos\frac{2\pi j}{p})^{2n} &\leq \sum_{j=1}^{\frac{p}{8}} e^{-\frac{\alpha j^2 2n}{p^2}} + \sum_{j=\frac{p}{8}}^{p-1}(\frac{1}{3} + \frac{2}{3\sqrt{2}})^{2n} \\
&\leq \sum_{j=1}^{\frac{p}{8}} e^{-\frac{\alpha j^2 2n}{p^2}} + \frac{p}{4}(\frac{1}{3} + \frac{2}{3\sqrt{2}})^{2n}
\end{aligned}$$

Posons $n = \gamma p^2$, avec $\gamma > 1$ et $p^2 > 7$

$$\begin{aligned}
\sum_{j=1}^{\frac{p}{8}} e^{-\frac{\alpha j^2 2n}{p^2}} &= \sum_{j=1}^{\frac{p}{8}} e^{-2\alpha j^2 \gamma} \leq \sum_{j=1}^{\frac{p}{8}} e^{-2\alpha j \gamma} \\
&= \frac{1}{e^{2\gamma\alpha}} . \frac{1 - (\frac{1}{e^{2\gamma\alpha}})^{\frac{p}{8}}}{1 - \frac{1}{e^{2\gamma\alpha}}} \\
&\leq \frac{1}{e^{2\gamma\alpha}} \leq e^{-\alpha\gamma}.
\end{aligned}$$

D'autre part, pour n est assez grand $\frac{p}{4}(\frac{1}{3} + \frac{2}{3\sqrt{2}})^{2n} \to 0$.
Donc

$$\|P^{*n} - U\| \leq e^{-\alpha\gamma}$$

D'où le résultat chérché. □

Remarque

Le théorème répond à la question de départ, car il donne une estimation de la distance de P^{*n} à la loi uniforme. Cette distance devient petite quand n est grand.

Théorème 2. *Soit p un entier et soit $(X_n)_n$ la chaine de Markov définie par $X_{n+1} = 2X_n + b_n \ (mod\ p)$ d'espace des états le groupe $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, où les b_n sont des var i.i.d et de loi P tel que*

$$P[1] = P[-1] = \frac{1}{2}.$$

Alors il existe $0 \leq \beta < p$, tel que :

$$\|P^{*n} - U\| = \frac{(\beta+1)[p-(\beta+1)]}{2^n p}.$$

Remarque

Danc ce cas aussi, le théorème répond à la question de départ et même plus, car il donne un calcul exact de la distance de P_n à la loi uniforme. Cette distance devient petite quand n est grand.
Pour $n = \log_2 p + c(p)$, la distence de variation entre la loi de X_n ie P^{*n} et la loi uniforme U tend vers 0.

4.3 La chaine de Markov $X_{n+1} = a_n X_n + b_n X_{n-1} (mod\ p)$

Nous términons ce mémoire par le résultat de Diaconis sur la chaîne de Markov $X_{n+1} = a_n X_n + b_n X_{n-1} (mod\ p)$.

Théorème 3. *Soient P_1 et P_2 deux probabilités sur $\mathbb{Z}_p$, P_1 est choisie arbitrairement et P_2 n'est concentrée sur aucun sous-groupe de $\mathbb{Z}_p^*$. Supposons*

que (a_1, b_1), (a_2, b_2), ..., (a_n, b_n) *sont iid pour* $P_1 \times P_2$. *Si* P^{*n} *est la loi jointe de* (X_n, X_{n-1}), *a et b deux constantes, alors on a*

$$\|P^{*n} - U \times U\| \leq a\ e^{-bn/(p^2 \log p)}$$

Démonstration. Pour établir ce résultat on a besoin de construire la chaîne de Markov $(Y_n)_n$ définie par $Y_n = (X_n, X_{n-1})$ où $X_n = a_n X_{n-1} + b_n X_{n-2}(mod\ p)$. On suppose que p est impair. Nous ne montrerons pas ce résultat. Nous faisons cependant les observations suivantes.

La chaîne de Markov $(Y_n)_n$ sur $\mathbb{Z}_p \times \mathbb{Z}_p$ peut être ecrite sous la forme

$$Y_n = \begin{pmatrix} X_n \\ X_{n-1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ 1 & 0 \end{pmatrix} \begin{pmatrix} X_n \\ X_{n-1} \end{pmatrix} = ... = \prod_{i=0}^{n} \begin{pmatrix} a_i & b_i \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

La chaîne de Markov $(Y_n)_n$ est donc engendrée par une marche aléatoires dans un sous-groupe de matrice de $GL_2(\mathbb{R})$. Un lemme équivalent au lemme de la borne superieure (Cf p. 52) permet alors d'établir le théorème. La démonstration comporte aussi l'introduction du plan projectif.

□

Remarques

(1) Si $n >> p^2 \log p$, la loi jointe P^{*n} de X_n et X_{n-1} est proche de la loi uniforme sur $\mathbb{Z}_p \times \mathbb{Z}_p$.

(2) Si $n = (\log p)^k$ et $k < 3$, la loi P^{*n} est proche de la loi uniforme.

Conclusion

L'étude des chaînes de Markov $X_{n+1} = a_n X_n + b_n (mod\ p)$, a nécéssité la mise en place de l'appareillage mathématique de l'Analyse de Fourier indispensable pour la compréhension de la Formule de Plancherel. Cela nous a pris beaucoup de temps et d'énérgie car necessitant les éléments sur les représentations linéaires de groupe. Les résultats de cette étude, à partir des travaux de Diaconis, sont quelques caractérisations de ces chaînes de Markov, utiles dans la mise en place de générateurs de nombres aléatoires. Outre le fait que l'étude de ces chaînes de Markov n'est pas achevée, les perspectives qui en découlent sont de deux ordres :

(1) Selon Diaconis, la formule de Plancherel, peut être d'un apport intéréssant, pour étudier l'entropie de ces chaînes de Markov, et eventuellement leur recurrence.

(2) Cela fait penser aussi que ces téchniques peuvent servir à caractériser d'autres types de chaînes de Markov itératives.

Bibliographie

[1] M. Naimark et A. Stern, *Théorie des représentations des groupes*
Second Edition, MIR MOSCOU, 1979 .

[2] A. Doneddu, *Espaces euclidiens et hérmitiens. Géométries*
Second Edition, Jean-Pierre Serre, *Représentations linéaires des groupes finis*
Cinquième edition, HERMANN, 1998 .

[3] Persi Diaconis, *Group Representations in Probability and Statistics*
Institute of Mathematical Statistics. Lecture notes-Monograph series Shanti S. Gupta, Series Editor, 1987.

[4] Persi Diaconis and Mehrdad Shahshahani, *Products of random matrices as they arise in the study of random walks on groups*
Thecnical report no. 229, Departement of statistics, Stanford University, California, Novembre 1984.

[5] Ghenima LARABI, *Chaine de markov et applications*
Mémoire de magister, UMMTO, 2008.

[6] Kahina TEDLOUT, *Marches aléatoires et Chaînes de Markov dans un groupe*
Mémoir de Master, UMMTO, 2011.

[7] A. Kolmogorov et S. Fomine, *Eléments de la théorie des fonctions et de l'analyse fonctionnelle*

Second Edition, MIR MOSCOU, 1977.

[8] Walter Rudin, *Fourier analysis on groups*
John Willey and Sons, New York , 1962.

[9] D. Revuz, *Markov Chaîns*
Edition North Holland, 1975.

[10] Marcel Berger, *Géométrie. Action de groupes, espaces affines et projectifs*
CEDIC/FERNAND NATHAN, Paris, 1977.

[11] F. R .K. Chung, P. Diaconis and R. L. Graham, *A Random walk problem involving random number generation*
Technical report No. 212, Departement of statistics, Stanford university, California, 1984.

[12] Jean-Pierre Serre, *Représentations linéaires des groupes finis*
Edition HERMANN, 1998.