La transformée de Fourier sur un groupe fini et quelques-unes de ses applications

Elise Raphael

Semestre d'automne 2009-2010

Contents

Introduction

Nous allons dans ce mémoire aborder la transformée de Fourier sur un groupe fini et quelques-unes de ses applications. Pour ce faire nous allons déterminer le dual d'un groupe fini, en commençant par les groupes cycliques puis en généralisant aux groupes abéliens finis. Nous introduirons ensuite la transformée de Fourier. Nous verrons que la transformée de Fourier est utilisée dans ses applications sous des formes un peu différentes (Sommes de Gauss, transformée de Walsh) à travers un exemple d'application théorique qu'est la démonstration de la loi de réciprocité quadratique, puis de la transformée de Walsh (et ses applications pratiques).
A la fin de ce mémoire se trouve un lexique, qui donne de brèves définitions, propriétés et démonstrations qui m'ont été utiles pour comprendre ce sujet.

1 Transformée de Fourier sur un groupe fini

Rappels sur les groupes finis

On rappelle que l'ensemble G muni d'une loi de composition interne $\cdot$ est un groupe si $\cdot$ est associative, possède un élément neutre et si tout élément de G a un inverse pour $\cdot$. Un groupe est dit commutatif ou abélien si la loi $\cdot$ est commutative.
On dit que G est un groupe fini si son cardinal est fini. Le cardinal est alors noté $|G|$ et est appelé ordre du groupe.
L'ordre d'un élément g est le plus petit élément de l'ensemble $\{k \in \mathbb{N}^* | g^k = 1\}$, où l'on a noté 1 l'élément neutre pour la loi $\cdot$. Si $|G| = n$,on a $g^n = 1 \, \forall g \in G$. L'ordre k d'un élément g divise donc l'ordre de $|G|$.
Un groupe fini engendré par un singleton $\{g\}$ est dit cyclique, et peut être noté $G = \langle g \rangle$.
On rappelle également le théorème de Lagrange :
Soit G un groupe fini et H un sous-groupe de G, alors l'ordre de H divise l'ordre de G.
Nous sommes maintenant prêts à aborder la première partie.

1.1 Dual d'un groupe fini

On s'intéresse aux fonctions qui transportent la structure d'un groupe : les morphismes de G (groupe fini) dans un sous-groupe de $\mathbb{C}^*$.

Soit G un groupe fini. Un **caractère** χ est un morphisme du groupe G (additif ou multiplicatif) dans le groupe multiplicatif $\mathbb{C}^*$. On note $\widehat{G}$ l'ensemble des caractères : c'est le **dual** de G. $\widehat{G}$ est un groupe pour la multiplication des applications :

$$\forall (\chi_1, \chi_2) \in \widehat{G}^2, \chi_1\chi_2 : x \longmapsto \chi_1(x)\chi_2(x)$$

Peut-on déterminer plus précisément les caractères d'un groupe fini ?

Proposition
Soit G un groupe fini tel que $|G| = n$. Les éléments de $\widehat{G}$ sont en fait les

morphismes de G dans le groupe des racines énièmes de l'unité :

$$\mathbb{U}_n = \left\{ exp(\frac{2ik\pi}{n}) \Big| 0 \leq k < n \right\}$$

En particulier :

$$\forall g \in G : |\chi(g)| = 1 \text{ et } \chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$$

Démonstration
On note 1 l'élément neutre de G. Pour tout élément $g \in G$ on a $g^n = 1$. Ceci entraîne : $\forall \chi \in \widehat{G}$, $\chi(g)^n = \chi(g^n) = 1$. Donc χ est à valeurs dans $\mathbb{U}_n$.
Cette proposition nous permet également de dire que $\widehat{G}$ est un groupe fini commutatif, car il existe un nombre fini d'applications de G dans $\mathbb{U}_n$, qui sont tous deux des groupes finis. Enfin, tout élément χ de $\widehat{G}$ est constant sur les classes de conjugaison de G :
$\forall g, h \in G\ \chi(h^{-1}gh) = \chi(h^{-1}\chi(g)\chi(h) = \chi(e)\chi(g) = \chi(g)$.

On note $\mathbb{C}[G]$ l'ensemble des fonctions de G dans $\mathbb{C}$. C'est un $\mathbb{C}$-espace vectoriel.
On aimerait y définir un produit scalaire. On rappelle que sur $\mathbb{R}^n$ le produit scalaire est défini comme suit :

$$\forall x, y \in \mathbb{R}^n \quad \langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$$

On a alors $\langle x, x \rangle = \sum_{i=1}^{n} (x_i)^2$ d'où $\langle x, x \rangle = 0 \Leftrightarrow x = 0$ et $\langle x, x \rangle \geq 0$.
Or sur $\mathbb{C}$ ceci est faux car il n'y a pas d'ordre. Si on définit sur $\mathbb{C}^n$ un second produit scalaire tel que

$$\forall x, y \in \mathbb{C},\ \langle x, y \rangle = \sum_{i=1}^{n} x_i \overline{y_i}$$

On a alors $\langle x, x \rangle = \sum_{i=1}^{n} x_i \overline{x_i} = \sum_{i=1}^{n} |x_i|^2 \geq 0$
On récupère donc la positivité. Attention cependant : le produit scalaire défini sur $\mathbb{R}$ est une forme bilinéaire, tandis que celui défini sur $\mathbb{C}$ n'est que sesquilinéaire. Cette démarche nous amène assez naturellement à la définition suivante :

Définition
On définit sur $\mathbb{C}[G]$ un **produit scalaire hermitien** par:

$$\forall f, g \in \mathbb{C}[G] \quad \langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$$

On définit également une **norme** $\| \cdot \|_2$ sur $\mathbb{C}[G]$ par $\|f\|_2^2 = \langle f, f \rangle$.
On introduit une base canonique afin d'étudier les fonctions de $\mathbb{C}[G]$.
Proposition
Une base de $\mathbb{C}[G]$ est donnée par les fonctions $(\delta_g)_{g \in G}$ suivantes :

$$\delta_g(h) = \begin{cases} 1 \text{ si } h = g \\ 0 \text{ si } h \neq g \end{cases}$$

Démonstration
$\forall f \in \mathbb{C}[G]$, on a $\sum_{x\in G} f(g)\delta_g = f$. Donc la famille des (δ_i) est génératrice.
De plus, $\forall \delta_i$, δ_j le produit hermitien donne :

$$< \delta_i, \delta_j > = \frac{1}{|G|} \sum_{x\in G} \delta_i(x)\delta_j(x)$$
$$= \begin{cases} 1 \text{ si } i = j \\ 0 \text{ sinon} \end{cases}$$

Donc cette famille est orthonormée pour le produit hermitien. Comme les fonctions qui la composent sont non nulles, la famille est donc libre. Par conséquent cette famille est une base de $\mathbb{C}[G]$.
Cependant cette base ne prend pas vraiment en compte la structure de G, et nous allons être amenés à déterminer une autre base, qui tout en restant simple à calculer, se comporte plus agréablement lors des calculs que nous serons amenés à faire.

1.1.1 Dual d'un groupe cyclique

Nous allons dans un premier temps étudier le dual des groupes finis les plus "simples", à savoir les groupes cycliques.
Proposition
Soit $G = \left\{1, g_0, g_0^2, ..., g_0^{n-1}\right\}$ un groupe cyclique de cardinal n et de générateur g_0. Soit ω une racine primitive n^{ieme} de l'unité, par exemple $\omega = e^{\frac{2i\pi}{n}}$. Les éléments de $\widehat{G}$ sont de la forme, pour $j \in \{0, 1, ..., n-1\}$:

$$\chi_j : \begin{cases} G \longrightarrow \mathbb{C}^* \\ g_0^k \longmapsto (\omega^j)^k = e^{\frac{2i\pi jk}{n}} \end{cases}$$

Démonstration
Pour déterminer un caractère χ, il nous faut calculer sa valeur sur chacun des éléments de G, c'est-à-dire calculer $\chi(g_o^k)$ pour $k \in \{0, 1, \ldots, n-1\}$, ce qui donne :

$$\chi(g_0^k) = \chi(g_0)^k = (\omega^j)^k = \omega^{jk}$$

Dans cette égalité on a noté $\omega^j = \chi(g_0)$ avec $0 \leq j \leq n-1$ puisque cette quantité est racine n-ième de l'unité.
Donc $\chi \in \widehat{G}$ est bien un des $\{\chi_0, \ldots, \chi_{n-1}\}$. Réciproquement, on constate que pour $j \in \{0, \ldots, n-1\}$ les applications χ_j sont bien des morphismes de G dans $\mathbb{C}^*$, et donc appartiennent bien au dual de G.

Proposition
G et $\widehat{G}$ sont isomorphes.
Démonstration
On identifie les éléments de $\mathbb{Z}/n\mathbb{Z}$ avec leur représentant $j \in \{0, \ldots, n_1\}$ et on définit l'application suivante :

$$\psi : \begin{cases} \mathbb{Z}/n\mathbb{Z} \longrightarrow \widehat{G} \\ \quad j \longmapsto \chi_j \end{cases}$$

Cette application est un morphisme bijectif donc $\widehat{G} \simeq \mathbb{Z}/n\mathbb{Z} \simeq G$. Remarquons toutefois que cet isomorphisme n'est pas canonique, car il dépend de la racine primitive de l'unité ω choisie.

Prenons l'exemple du groupe cyclique $\mathbb{Z}/12\mathbb{Z}$. On choisit ici comme racine primitive de l'unité $\omega = e^{\frac{2i\pi}{12}}$. On peut alors définir comme suit les 4 premiers caractères de ce groupe :

$$\chi_0 : (g_0)^k \longmapsto 1$$
$$\chi_1 : (g_0)^k \longmapsto e^{\frac{ik\pi}{6}}$$
$$\chi_2 : (g_0)^k \longmapsto e^{\frac{ik\pi}{3}}$$
$$\chi_3 : (g_0)^k \longmapsto e^{\frac{ik\pi}{2}}$$

Pour déterminer complètement ces caractères, il reste à choisir un générateur de $\mathbb{Z}/12\mathbb{Z}$. Les générateurs d'un groupe cyclique additif $\mathbb{Z}/n\mathbb{Z}$ sont les classes d'équivalences des éléments premiers avec n. Ici on peut donc choisir 1, 5, 7 ou 11 comme générateur, mais nous irons au plus simple en prenant 1. Voici la figure correspondant à ces caractères, où on a distingué partie réelle et partie imaginaire.

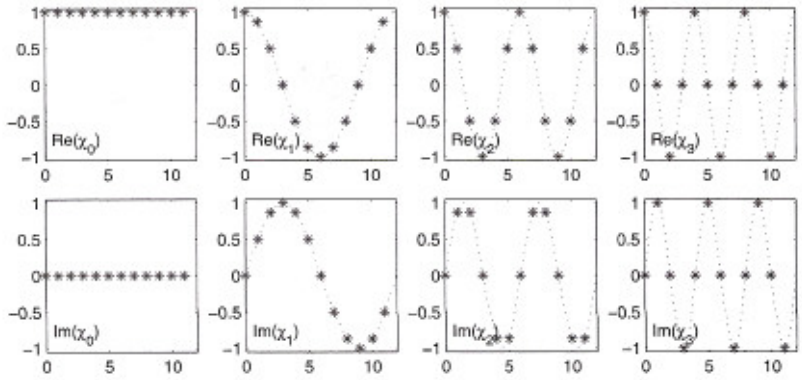


FIG. 1.1 – *Les quatres premiers caractères du groupe* $\mathbb{Z}/12\mathbb{Z}$

Proposition
Soit G un groupe cyclique. $\widehat{G}$ forme une base orthonormale de $\mathbb{C}[G]$, c'est-à-dire :

$$\forall (p,q) \in \{0,\dots,n-1\}^2,\ \langle \chi_p, \chi_q \rangle = \delta_p^q$$

où on a noté

$$\delta_p^q = \begin{cases} 0 \text{ si } p \neq q \\ 1 \text{ si } p = q \end{cases}$$

Démonstration
On peut supposer que $G = \mathbb{Z}/n\mathbb{Z}$. On note $\widehat{G} = \{\chi_i\}_{i=0}^{n-1}$, avec $\chi_i(k) = \omega^{ik}$. on a alors :

$$\forall (p,q) \in \{0,\dots,n-1\}^2,\ \langle \chi_p, \chi_q \rangle = \frac{1}{n}\sum_{i=0}^{n-1} (\omega^{p-q})^i = \delta_p^q$$

La dernière égalité s'obtient en sommant les termes de la série géométrique de raison ω^{p-q}.
La famille des $\{\chi_i\}_{i=0}^{n-1}$ est donc orthonormale (donc libre) et comme $|\widehat{G}| = dim_{\mathbb{C}}(\mathbb{C}[G])$ elle forme une base de $\mathbb{C}[G]$.

1.1.2 Dual d'un groupe abélien

Il s'agit maintenant de considérer le dual d'un groupe abélien et de voir si on peut étendre les propriétés démontrées pour le cas cyclique à ce cas plus général. Dans ce but, nous allons admettre les propriétés suivantes :
Lemme - Prolongement de caractères
Soit G un groupe fini commutatif et $H \subset G$ un sous-groupe . Tout caractère χ de H peut être prolongé en un caractère de G.
La preuve de ce lemme s'effectue par analyse et synthèse en faisant une récurrence sur l'indice de H dans G.
Théorème
Soit G un groupe abélien fini. Il existe des entiers strictement positifs $n_1, \ldots, n_r$ uniquement déterminés tels que n_k divise n_{k+1}, et tels qu'on ait l'isomorphisme :

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

Corollaire
Soit G un groupe fini commutatif. Alors G est isomorphe à $\widehat{G}$. En particulier $\widehat{G}$ est de même ordre que G.
Constatons que dans le cas d'un groupe abélien fini, l'isomorphisme entre g et son dual n'est pas non plus canonique ; il dépend en effet de choix arbitraires pour décrire la structure du groupe.

Relations d'orthogonalité

On cherche ici à étendre l'orthogonalité des caractères obtenue dans le cas cyclique au cas d'un groupe abélien quelconque.
Lemme

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

Démonstration
Si χ est le caractère trivial, i.e $\chi(g) = 1 \, \forall g \in G$ la propriété est démontrée.
Supposons maintenant $\chi \neq 1$. Soit $t \in G$ tel que $\chi(t) \neq 1$. On a alors

$$\chi(t) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(tg) = \sum_{h \in G} \chi(h)$$

où on a noté $h = tg$ (la fonction qui à g associe tg est une bijection de G). On en déduit

$$(\chi(t) - 1) \sum_{g \in G} \chi(g) = 0 \Longrightarrow \sum_{g \in G} \chi(g) = 0$$

Proposition
Soit G un groupe fini abélien. Alors $\widehat{G}$ est une famille orthonormale d'éléments

:

$$\forall(\chi_1,\chi_2)\in G^2, \langle\chi_1,\chi_2\rangle = \begin{cases} 0 \text{ si } \chi_1 \neq \chi_2 \\ 1 \text{ si } \chi_1 = \chi_2 \end{cases}$$

De plus $\widehat{G}$ est une base de $\mathbb{C}[G]$.
Démonstration

$$\langle\chi_1,\chi_2\rangle = \frac{1}{G}\sum_{g\in G}\chi_1(g)\overline{\chi_2}(g) = \frac{1}{G}\sum_{g\in G}\chi_1(g)\chi_2^{-1}(g)$$

Si on pose $\chi = \chi_1\chi_2^{-1}$, alors $\chi_1 = \chi_2 \Leftrightarrow \chi = 1$, et sinon $\chi \neq 1$.
Il suffit alors d'appliquer le lemme précédent pour trouver la propriété. Ensuite, comme la famille des éléments est orthonormale, elle est libre et par un argument de dimension on obtient la deuxième partie de la proposition.
Proposition
Soit g et h deux éléments de G. On a alors

$$\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi(h)} = \begin{cases} 0 \text{ si } g \neq h \\ |G| \text{ si } g = h \end{cases}$$

La démonstration de cette propriété se fait en passant par le dual de $\widehat{G}$, appelé aussi bidual de G. Il existe un isomorphisme canonique de G dans son bidual qui nous permet de parvenir au résultat.

1.2 Transformée de Fourier

1.2.1 Définitions

Définition
Pour$f \in \mathbb{C}[G]$, on définit, pour $\chi \in \widehat{G}$, le coefficient de Fourier $c_f(\chi)$ par :

$$\forall\chi\in\widehat{G},\ c_f(\chi) =< f,\chi >$$

Définition
L'application transformée de Fourier, notée $\mathcal{F}$, est définie par :

$$\mathcal{F} : \begin{cases} \mathbb{C}[G] \longrightarrow \mathbb{C}[\widehat{G}] \\ f \longmapsto \widehat{f} \end{cases}$$

où $\widehat{f}$ est définie par

$$\forall\chi\in\widehat{G},\ \widehat{f}(\chi) = |G|c_f(\overline{\chi} = \sum_{x\in G} f(x)\chi(x)$$

Prenons maintenant un exemple pour voir ce que fait cette transformée :

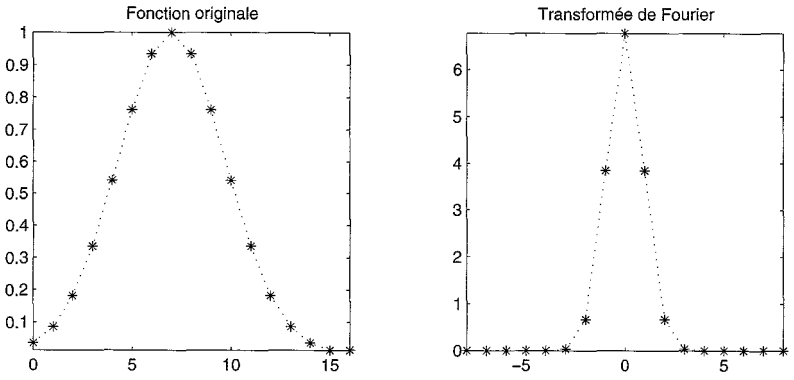


FIG. 1.2 – *Exemple de transformée de Fourier*

Proposition
Pour $f \in \mathbb{C}[G]$, on a la formule d'inversion :

$$f = \sum_{\chi \in \widehat{G}} c_f(\chi)\chi = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi^{-1}$$

Démonstration
La famille des (χ_i) est une base de $\mathbb{C}[G]$ donc si on décompose f dans cette base on obtient :

$$\begin{aligned} f &= \sum_{\chi \in \widehat{G}} \chi < f, \chi > \\ &= \sum_{\chi \in \widehat{G}} \chi \left(\frac{1}{|G|} \sum_{x \in G} f(x)\overline{\chi}(x) \right) \\ &= \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi \left(\sum_{x \in G} f(x)\chi(x)^{-1} \right) = \frac{1}{G} \sum_{\chi \in \widehat{G}} \chi \widehat{f}(\chi^{-1}) \end{aligned}$$

Proposition
c et $\mathcal{F}$ sont des isomorphismes d'espaces vectoriels de $\mathbb{C}[G]$ dans $\mathbb{C}[\widehat{G}]$.
Démonstration
Montrons d'abord l'injectivité : si $c_f = 0$ alors par la formule d'inversion $f = 0$. on termine avec un argument de dimension : comme G et $\widehat{G}$ ont même cardinal, les espaces $\mathbb{C}[G]$ et $\mathbb{C}[\widehat{G}]$ ont même dimension $|G|$.Donc c est bien un isomorphisme.
Les arguments pour $\mathcal{F}$ sont identiques : si $\widehat{f} = 0$, on obtient par la formule d'inversion $f = 0$ et par le même argument de dimension, $\mathcal{F}$ est un isomorphisme.

Proposition - Formule de Plancherel

Pour $f, g \in \mathbb{C}[G]^2$ on a les formules suivantes :

$$\begin{aligned}\sum_{s\in G} f(s)\overline{g(s)} &= |G| \sum_{\chi\in\widehat{G}} c_f(\chi)\overline{c_g(\chi)} \\ &= \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\overline{\widehat{g}(\chi)}\end{aligned}$$

Démonstration
On décompose f et g sous la forme donnée par la formule d'inversion :

$$f(s) = \sum_{\chi\in\widehat{G}} c_f(\chi)\chi(s) \text{ et } g(s) = \sum_{\chi\in\widehat{G}} c_g(\chi)\chi(s)$$

Ce qui nous donne :

$$\sum_{s\in G} f(s)\overline{g(s)} = |G| < f, g >= |G| \sum_{(\chi_1,\chi_2)\in\widehat{G}^2} c_f(\chi_1)\overline{c_g(\chi_2)} < \chi_1, \chi_2 >$$

L'orthogonalité des caractères nous donne ensuite le résultat voulu.

1.2.2 Produit de convolution

G désigne toujours un groupe abélien fini. Nous travaillons depuis le début dans $\mathbb{C}[G]$, l'espace vectoriel des fonctions de $\mathbb{C}$ dans G. On souhaite lui conférer une structure d'algèbre, ce que l'on pourrait faire en introduisant le produit de fonctions défini par

$$\forall (f_1, f_2) \in \mathbb{C}[G]^2, \forall g \in G,\ (f_1 \cdot f_2)(g) = f_1(g)f_2(g)$$

Cependant on va plutôt introduire un autre produit, nommé produit de convolution, pour lequel la transformée de Fourier se comporte de manière pratique.
Définition
Pour f_1, f_2 deux fonctions de $\mathbb{C}[G]$, le produit de convolution $f_1 * f_2$ est donné par :

$$\forall g \in G,\ (f_1 * f_2)(g) = \sum_{(h,k)\in G^2 hk=g} f_1(h)f_2(k) = \sum_{h\in G} f_1(h)f_2(h^{-1}g)$$

Proposition
Le produit de convolution est commutatif, associatif, et l'application $(f_1, f_2) \longrightarrow f_1 * f_2$ est bilinéaire. On munit ainsi l'espace vectoriel $\mathbb{C}[G]$ d'une structure d'algèbre.
Exemple de calcul de convolution
On considère la fonction "porte" sur $\mathbb{Z}/6\mathbb{Z}$ définie comme suit :

$$\begin{aligned}f(0) &= 0 \\ f(1) &= 0 \\ f(2) &= 1 \\ f(3) &= 1 \\ f(4) &= 1 \\ f(5) &= 0\end{aligned}$$

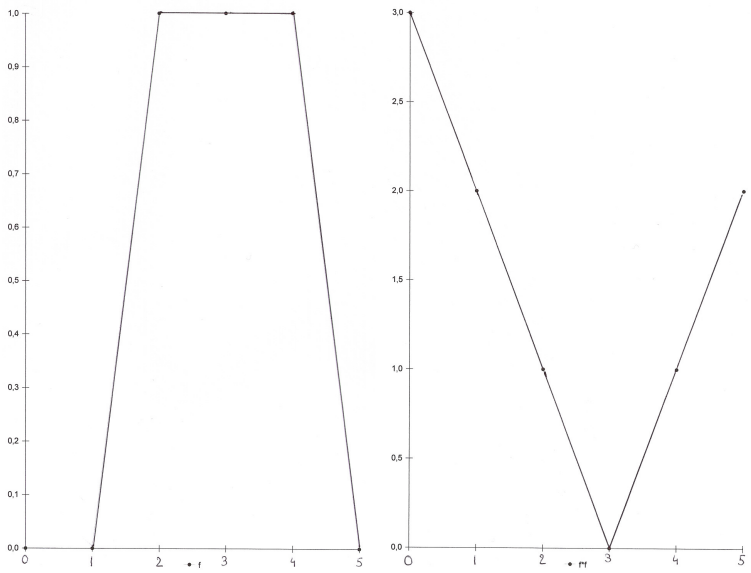
On va calculer le produit de convolution $f * f$.Comme on se trouve sur le groupe $(\mathbb{Z}/6\mathbb{Z}, +)$, la formule donne:

$$(f * f)(g) = \sum_{h \in G} f(h)f(g-h)$$

Ce qui nous donne :

$$\begin{aligned}
f * f(0) &= f(0)f(0) + f(1)f(-1) + f(2)f(-2) + f(3)f(-3) + f(4)f(-4) + f(5)f(-5) \\
&= f(2)f(4) + f(3)f(3) + f(4)f(2) = 3 \\
f * f(1) &= f(2)f(1-2) + f(3)f(1-3) + f(4)f(1-4) = f(2)f(5) + f(3)f(4) + f(4)f(3) = 2 \\
f * f(2) &= f(2)f(2-2) + f(3)f(2-3) + f(4)f(2-4) = f(2)f(0) + f(3)f(5) + f(4)f(4) = 1 \\
f * f(3) &= f(2)f(1) + f(3)f(0) + f(4)f(5) = 0 \\
f * f(4) &= f(2)f(2) + f(3)f(1) + f(4)f(0) = 1 \\
f * f(5) &= f(2)f(3) + f(3)f(2) + f(4)f(1) = 2
\end{aligned}$$

On voit que l'on obtient une fonction en "triangle".



Voyons maintenant comment se comporte la transformée de Fourier avec ce produit.

Théorème
Pour f, g deux fonctions de $\mathbb{C}[G]$ on a :

$$\widehat{f * g} = \widehat{f} \cdot \widehat{g} \text{ et } c_{f*g} = |G| c_f \cdot c_g$$

La transformée de Fourier $\mathcal{F}$ est donc un isomorphisme d'algèbre de $(\mathbb{C}[G], *)$ dans $(\mathbb{C}[\widehat{G}], \cdot)$.
Cette propriété de convolution est largement utilisée, puisqu'elle permet de transformer un calcul de convolution de deux fonctions en un calcul de produit terme à terme.

1.3 Application aux équations et dénombrement de solutions

1.3.1 Dénombrement de solutions

Nous allons voir dans cet exemple comment utiliser les caractères (et les relations d'orthogonalité dont on dispose) pour effectuer un dénombrement de solutions. Soit G un groupe abélien fini, et soit $\phi : G^n \longrightarrow G$. Pour $h \in G$, on note $N(h)$ le nombre de n-uplets $(g_1, ..., g_n)$ tels que $\phi(g_1, ..., g_n) = h$.
Utilisons dans un premier temps la base de $\mathbb{C}[G]$ formée par les fonctions $(\delta_g)_{g\in G}$. On écrit alors :

$$N(h) = \sum_{(g_1,\ldots,g_n)\in G^n} \delta_0 \left(\phi(g_1, \ldots, g_n) - h\right)$$

On rappelle ensuite que $\delta_0 = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \chi$, et on remplace dans l'équation ci-dessus :

$$N(h) = \frac{1}{|G|} \sum_{(x_1,\ldots,x_n)\in G^n} \sum_{\chi\in\widehat{G}} \chi \left(\phi(g_1, \ldots, g_n) - h\right)$$

Enfin, la propriété suivante nous donne la dernière étape :

$$\sum_{\chi\in\widehat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} 0 \text{ si } g \neq h \\ |G| \text{ si } g = h \end{cases}$$

D'où

$$N(h) = \frac{1}{|G|} \sum_{(g_1,\ldots,g_n)\in G^n} \sum_{\chi\in\widehat{G}} \chi \left(\phi(g_1, \ldots, g_n)\right) \overline{\chi}(h)$$

1.3.2 Fonction indicatrice

Soit G un groupe abélien fini et $A \subset G$. On note f_A la fonction indicatrice de A. On appelle fonction indicatrice de A relativement à G la fonction f_A définie de G dans $\{0, 1\}$ par

$$f_A(x) = \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases}$$

Nous allons sur cet exemple observer les liens entre la transformée de Fourier de f_A et la distribution des éléments de A dans G.
1. Regardons d'abord la norme de f_A et la transformée de Fourier de f_1 en χ_0.

$$\|f_A\|_2^2 = \langle f_A, f_A\rangle \ = \frac{1}{|G|} \sum_{x\in G} f_A(x)\overline{f_A}(x) = \frac{|A|}{|G|}$$

D'où $\|f_A\|_2 = \sqrt{\frac{|A|}{|G|}}$. La transformée de Fourier de f_1 sur le caractère trivial donne quant à elle :

$$\widehat{f_A}(\chi_0) = \sum_{x\in G} f_A(x)\chi_0(x) = |A|$$

On définit maintenant la fonction

$$\Phi(A) = \max\left\{|\widehat{f_A}(\chi)| \backslash \chi \in \widehat{G}, \chi \neq \chi_0\right\}$$

2. On cherche à encadrer $\Phi(A)$. Supposons dans un premier temps que $|A| \leq \frac{1}{2}|G|$. On obtient facilement une majoration par le cardinal de A . En effet

$$|\widehat{f_A}(\chi)| = \sum_{x \in G} f_A(x)\chi(x) \leq \sum_{x \in G} |\chi(x)| \leq |A|$$

En utilisant la formule de Plancherel on obtient l'égalité $\|\widehat{f_A}\|_2^2 = |G|\|f_A\|_2^2 = |A|$. On peut majorer $\|\widehat{f_A}\|_2^2$ comme suit :

$$|G|\|\widehat{f_A}\|_2^2 \leq |\widehat{f_A}(\chi_0)|^2 + (|G|-1)\Phi(A)^2 = |A|^2 + (|G|-1)\Phi(A)^2$$

Ce qui nous donne, en utilisant le fait que $|A| \leq \frac{1}{2}|G|$:

$$\Phi(A)^2 \geq \frac{|A|(|G|-|A|)}{|G|-1} \geq \frac{|A|}{2}$$

donc

$$\sqrt{\frac{|A|}{2}} \leq \Phi(A) \leq |A|$$

3. On se place désormais dans le cas où $|A| > \frac{1}{2}|G|$. Nous allons montrer qu'on a $\Phi(A) = \Phi(G\backslash A)$ où $G\backslash A$ désigne le complémentaire de A dans G. On note $B = G\backslash A$. On a $f_B = 1 - f_A$ donc $\widehat{f_B} = \widehat{1} - \widehat{f_A} = |G|\delta_{\chi_0} - \widehat{f_A}$. ceci nous donne, pour $\chi \neq \chi_0$, $\widehat{f_B} = \widehat{f_A}$, donc $\Phi(A) = \Phi(B)$. On obtient alors l'encadrement suivant :

$$\sqrt{\frac{|G|-|A|}{2}} \leq \Phi(A) \leq |G| - |A|$$

En fait, on se rend compte que plus $\Phi(A)$ s'approche de la borne inférieure de son encadrement, plus les éléments de A sont distribués uniformément dans G.

2 Loi de réciprocité quadratique

Prenons l'équation $y^2 = x$ dans $\mathbb{Z}/n\mathbb{Z}$. Cette équation n'admet pas toujours de solutions : pour s'en rendre compte, regardons quelques exemples très simples. L'équation $y^2 = 2$ a-t-elle une solution dans $\mathbb{Z}/3\mathbb{Z}$? La méthode "expérimentale" est de calculer les carrés de chacun des éléments de $\mathbb{Z}/3\mathbb{Z}$: $1^2 \equiv 1[3], 2^2 = 4 \equiv 1[3]$. Donc 2 n'est pas un carré modulo 3.
Prenons maintenant $y^2 = 4$ dans $\mathbb{Z}/5\mathbb{Z}$. On a $1^2 = 1[5]$, $2^2 = 4[5]$, $3^2 \equiv 4[5]$ et enfin $4^2 \equiv 1[5]$. Il y a donc deux solutions, 2 et 3. On se rend vite compte que pour vérifier si 41 est un carré modulo 97 , c'est moins drôle... Mais que faire dans ce cas pour les grands nombres ?
Il existe une loi appelée loi de réciprocité quadratique qui relie deux nombres premiers impairs p et q : si on sait si p est un carré modulo q, on sait aussi l'inverse. Le but de ce chapitre est de démontrer cette loi l'aide de la transformée de Fourier.
Nous allons d'abord introduire quelques définitions concernant les résidus quadratiques.

2.1 Résidus quadratiques

On dit que x est **résidu quadratique** modulo n s'il existe y tel que $y^2 = x[n]$.
Symbole de Legendre
Si p est premier impair, on définit le symbole de Legendre :

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

Lemme d'Euler
Soit p un nombre premier impair. On a , pour tout élément $x \in \mathbb{F}_p^*$:

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

Démonstration
p est premier donc $\mathbb{Z}/p\mathbb{Z}$ est intègre, donc le morphisme $f : x \longmapsto x^2$ a pour noyau le sous-groupe $\{1, -1\}$ c'est-à-dire $Ker(f) = \{x \in \mathbb{F}_p^* \mid x^2 = 1[p]\} = \{-1, 1\}$
Montrons maintenant que $Im(f) = \{x | x^{\frac{p-1}{2}} = 1\}$. L'image de f est l'ensemble $(\mathbb{F}_p^*)^2$ des carrés de $\mathbb{F}_p^*$. Par un théorème d'isomorphisme il vient $|Im(f)| = \frac{|\mathbb{F}_p^*|}{|Ker(f)|} = \frac{p-1}{2}$.
Montrons que $Im(f) \subset \{x | x^{\frac{p-1}{2}} = 1\}$. Soit $x \in Im(f)$ alors $x = y^2$. On a $x^{\frac{p-1}{2}} = y^{p-1} = 1$ par le théorème de Fermat. On conclut en montrant que le cardinal de $\{x | x^{\frac{p-1}{2}} = 1\}$ est égal à $\frac{p-1}{2}$: en effet cela représente le nombre de racines d'un polynôme de degré $\frac{p-1}{2}$, qui est inférieur ou égal à $\frac{p-1}{2}$. Comme $Im(f) \subset \{x | x^{\frac{p-1}{2}} = 1\}$ et $|Im(f)| = \frac{p-1}{2}$, on en déduit l'égalité.

Il découle du lemme d'Euler la propriété suivante :

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

En effet $\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = (a)^{\frac{p-1}{2}}(b)^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

2.2 Caractères additifs et multiplicatifs

Dans la première partie nous nous étions intéressés aux groupes cycliques munis d'une addition, puis aux groupes finis commutatifs. Ici nous allons désormais travailler sur un corps fini $\mathbb{F}_q$, avec $q = p^r$ où p est un nombre premier. C'est un corps de caractéristique p, et il peut être de vu comme un espace vectoriel de dimension r sur son corps premier $\mathbb{F}_p$.

Prenons un exemple : le plus petit groupe fini $\mathbb{Z}/2\mathbb{Z}$, c'est-à-dire $(\mathbb{F}_2, +, \times)$ dont les éléments sont $0, 1$. C'est bien un corps car 2 est premier, et sa caractéristique est $2 : 1 + 1 = 0$, 1 étant l'élément neutre pour la multiplication et 0 celui pour l'addition. On a les tables de loi suivantes :

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

Considérons maintenant $\mathbb{F}_2[X]$. les polynômes de degré 2 sont $X^2, X^2+X, X^2+1, X^2+X+1$. On voit que X^2 admet 0 comme racine double ; X^2+X est une fonction identiquement nulle sur $\mathbb{F}_2$; et enfin X^2+1 admet 1 comme racine. Seul X^2+X+1 est irréductible dans $\mathbb{F}_2[X]$: en effet $1+1+1=1$ et $0+0+1=1$. On construit alors l'extension correspondante $\mathbb{F} = \mathbb{F}_2[X]/(X^2+X+1)\mathbb{F}_2[X]$. $\mathbb{F}$ est un corps, et ses éléments sont les suivants : $\{0, 1, X, X+1\}$.Voici ses tables :

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

*	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

On note dorénavant $\mathbb{F} = \mathbb{F}_4$. c'est un espace vectoriel de dimension 2 sur $\mathbb{F}_2$, de base $(1, x)$.

Revenons maintenant au cas général.Nous pouvons dégager sur notre corps deux structures de groupe : on peut considérer $\mathbb{F}_q$ comme un groupe additif , et le groupe multiplicatif $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$, qui est un groupe cyclique d'ordre $p-1$.Ceci nous conduit à considérer deux types de caractères : les caractères additifs et multiplicatifs.

Définition

Les éléments de $\widehat{\mathbb{F}_q}$ sont appelés caractères additifs. Ce sont donc les morphismes :

$$\psi : (\mathbb{F}_q, +) \longrightarrow (\mathbb{C}^*, *)$$

Les éléments de $\widehat{\mathbb{F}_q^*}$ sont appelés caractères multiplicatifs. Ce sont donc les morphismes :

$$\chi : (\mathbb{F}_q^*, *) \longrightarrow (\mathbb{C}^*, *)$$

Les caractères les plus simples à déterminer sont les caractères multiplicatifs, car le groupe $\mathbb{F}_q^*$ est cyclique. Soit donc ζ un générateur de $\mathbb{F}_q^*$, de sorte que l'on ait $\mathbb{F}_q^* = \{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$. On peut alors donner les $q-1$ caractères multiplicatifs :

$$\forall j \in \{0, 1, \ldots, q-1\},\ \chi_j : \begin{cases} \mathbb{F}_q^* \longrightarrow \mathbb{C}^* \\ \zeta^k \longmapsto e^{\frac{2i\pi}{q-1}jk} \end{cases}$$

On obtient un isomorphisme entre $\mathbb{F}_q^*$ et son dual $\widehat{\mathbb{F}_q^*}$. cet isomorphisme n'est toutefois pas canonique puisqu'il résulte d'un choix de racine primitive ζ.

Passons maintenant aux caractères multiplicatifs. Ceux-ci vont nous demander plus de travail, en effet le groupe additif $\mathbb{F}_q$ n'est pas cyclique. Cependant on va s'aider du fait que le groupe additif $\mathbb{F}_q$ est isomorphe au groupe produit $(\mathbb{Z}/p\mathbb{Z})^r$, et $\mathbb{Z}/p\mathbb{Z}$ est un groupe cyclique.

Afin de simplifier la description du dual on introduit la notion suivante.

Définition

Soit $\mathbb{F}_q$ un corps fini contenant un sous-corps $\mathbb{F}_p$ de cardinal p. On note $r = [\mathbb{F}_q : \mathbb{F}_p]$ la dimension de $\mathbb{F}_q$ en tant que $\mathbb{F}_p$-espace vectoriel , de sorte que le cardinal de $q = p^r$.

Soit $\alpha \in \mathbb{F}_q$. on définit l'**application trace** de $\mathbb{F}_q$ sur $\mathbb{F}_p$ de la manière suivante :

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{r-1}}$$

On notera désormais $Tr_{\mathbb{F}_q/\mathbb{F}_p} = Tr$.
Si on reprend notre exemple avec $\mathbb{F}_4$: $\mathbb{F}_4$ est un corps fini contenant le sous-corps$\mathbb{F}_2$ et on a $r = 2$. Alors :

$$\begin{aligned} Tr(0) &= 0 \\ Tr(1) &= 1 + 1^2 = 2 = 0 \\ Tr(x) &= x + x^2 = x + x + 1 = 1 \\ Tr(x+1) &= x + 1 + (x+1)^2 = x + 1 + x^2 + 2x + 1 = 1 \end{aligned}$$

Voici maintenant quelques propriétés sur les corps finis.
Proposition
Soit K un corps fini de caractéristique p.
(i) Soit k un sous-corps de K de cardinal s. Un élément $x \in K$ appartient à k si et seulement si $x^s = x$.
(ii) L'application $\Phi : x \longmapsto x^p$ est un morphisme appelé morphisme de Frobenius. les itérés $\Phi^k : x \longmapsto x^{p^k}$ sont aussi des morphismes.

Regardons la propriété (i) sur notre exemple : $0^2 = 0$ et $0 \in \mathbb{F}_2$, $1^2 = 1$ et $1 \in \mathbb{F}_2$. En revanche $x^2 = x + 1$ et $(x+1)^2 = x$ et $x, x+1 \notin \mathbb{F}_2$.
Proposition
La trace de K sur k est une forme k-linéaire non nulle à valeurs dans k.
Démonstration
On montre dans un premier temps que pour $\alpha \in K$, on a $Tr_{K/k}(\alpha) \in k$, donc que $\alpha^s \in k$. D'après les propriétés précédentes, cela équivaut à $Tr_{K/k}(\alpha)^s = Tr_{K/k}(\alpha)$. On utilise ensuite la linéarité du morphisme $x \longmapsto x^s$ (qui est un itéré de Frobenius) et on obtient :

$$Tr_{K/k}(\alpha)^s = \alpha^s + \alpha^{s^2} + \cdots + \alpha^{s^t}$$

Comme K^* est un groupe de cardinal s^{t-1}, on a $\alpha^{s^{t-1}} = 1 \; \forall \alpha \in K^*$, donc $\alpha^s = \alpha$ ce qui nous donne $Tr_{K/k}(\alpha)^s = Tr_{K/k}(\alpha)$.
Montrons maintenant que l'application trace n'est pas triviale, i.e qu'il existe $\alpha \in K$ tel que $Tr_{K/k}(\alpha) \neq 0$. Si $Tr_{K/k}(\alpha) = 0$ cela signifie que α est racine du polynôme de degré s^{t-1}

$$P(X) = X + X^s + \cdots + X^{s^{t-1}}$$

Ce polynôme a donc au plus s^{t-1} racines, et comme K a s^t éléments il existe bien $\alpha \in K$ tel que $Tr_{K/k}(\alpha) \neq 0$. Donc l'application trace est non nulle. Enfin, comme pour tout $\lambda \in k$ on a $\lambda^s = \lambda$

$$Tr_{K/k}(\lambda\alpha) = (\lambda\alpha) + (\lambda\alpha)^s + \cdots + (\lambda\alpha)^{s^{t-1}} = \lambda(Tr_{K/k}(\alpha)$$

Donc l'application trace est k-linéaire.

Nous sommes désormais en mesure de fournir une description complète des caractères additifs de $\mathbb{F}_q$. On introduit d'abord un caractère dit canonique, qui ne dépend pas de la façon dont on construit le corps $\mathbb{F}_q$.
Définition

On définit le caractère additif canonique ψ_1, élément de $\widehat{\mathbb{F}_q}$ par

$$\psi_1 : \begin{cases} \mathbb{F}_q \longrightarrow \mathbb{C}^* \\ x \longmapsto e^{\frac{2i\pi}{p}Tr(x)} \end{cases}$$

On peut maintenant définir les autres caractères à partir du caractère canonique.

Proposition
Soit, pour $a \in \mathbb{F}_q$, l'application

$$\psi_a : \begin{cases} \mathbb{F}_q \longrightarrow \mathbb{C}^* \\ x \longmapsto \psi_1(ax) \end{cases}$$

C'est un caractère additif, $\psi_a \in \widehat{\mathbb{F}_q}$ et réciproquement tout caractère additif s'écrit de cette manière.
Démonstration
Il est clair que les ψ_a sont des caractères. Montrons qu'ils sont tous différents. Comme la trace est non identiquement nulle, le caractère canonique est non trivial.On prend $a \neq b \in \mathbb{F}_q$. On peut trouver $c \in \mathbb{F}_q$tel que

$$\frac{\psi_a(c)}{\psi_b(c)} = \frac{\psi_1(ac)}{\psi_1(bc} = \psi_1(a-b)c) \neq 1$$

On a donc $\psi_a \neq \psi_b$, ce qui veut dire qu'il y a q caractères distincts. or on sait que $|\widehat{\mathbb{F}_q}| = |G| = q$, donc nous avons construit tous les caractères additifs.
Nous avons donc construit un isomorphisme entre $\mathbb{F}_q$ et son dual $\widehat{\mathbb{F}_q}$ par l'application $a \longmapsto \psi_a$. on note $\psi_0 = 1$ le caractère trivial, à ne pas confondre avec χ_0, qui n'est pas défini en 0, bien qu'on le prolonge souvent en $\tilde{\chi_0}$, auquel cas ils coïncident.
Nous allons maintenant énoncer des propriétés des caractères additifs et multiplicatifs, découlant des relations d'orthogonalité montrées en première partie.
Proposition
Soient a, b des éléments de $\mathbb{F}_q$. On a alors :

$$\sum_{x \in \mathbb{F}_q} \psi_a(x)\overline{\psi_b(x)} = \begin{cases} 0 \text{ si } a \neq b \\ q \text{ si } a = b \end{cases}$$

$$\sum_{x \in \mathbb{F}_q} \psi_a(x) = 0 \text{ si } a \neq 0$$

$$\sum_{x \in \mathbb{F}_q} \psi_x(a)\overline{\psi_x(b)} = \begin{cases} 0 \text{ si } a \neq b \\ q \text{ si } a = b \end{cases}$$

Proposition
Soient a, b des éléments de $\mathbb{F}_q^*$, et soient χ et τ deux éléments de $\widehat{\mathbb{F}_q^*}$. On a alors:

$$\sum_{x \in \mathbb{F}_q^*} \chi(x)\overline{\tau(x)} = \begin{cases} 0 \text{ si } \chi \neq \tau \\ q-1 \text{ si } \chi = \tau \end{cases}$$

$$\sum_{x\in\mathbb{F}_q^*}\chi(x)=0 \text{ si } \chi\neq\chi_0$$

$$\sum_{x\in\mathbb{F}_q^*}\chi(a)\overline{\chi(b)}=\begin{cases}0 \text{ si } a\neq b\\ q \text{ si } a=b\end{cases}$$

2.3 Sommes de Gauss

Définition
Soient $\chi\in\mathbb{F}_q^*$, $\psi\in\mathbb{F}_q$ des caractères respectivement multiplicatif et additif. On définit la **somme de Gauss** $G(\chi,\psi)$ associée à ces deux caractères par :

$$G(\chi,\psi)=\sum_{x\in\mathbb{F}_q^*}\chi(x)\psi(x)$$

Quel est le lien entre la somme de Gauss et la transformée de Fourier ? On peut définir la transformée de Fourier sur le groupe multiplicatif $\mathbb{F}_q^*$:

$$\forall f\in\mathbb{C}\left[\mathbb{F}_q^*\right],\ \mathcal{F}_{mul}(f):\begin{cases}\widehat{\mathbb{F}_q^*}\longrightarrow\mathbb{C}\\ \\ \chi\longmapsto\sum_{x\in\mathbb{F}_q^*}f(x)\chi(x)\end{cases}$$

On peut donc écrire la somme de Gauss comme la transformée de Fourier multiplicative d'un caractère additif, c'est-à-dire :

$$\forall\psi\in\widehat{\mathbb{F}_q},\ \forall\chi\in\mathbb{F}_q^*,\ \ G(\chi,\psi)=\mathcal{F}_{mul}(\psi)(\chi)$$

De même on peut définir la transformée de Fourier sur le groupe additif $\mathbb{F}_q$. Cela nécessite cependant d'étendre les caractères multiplicatifs $\chi\in\widehat{\mathbb{F}_q^*}$ en fonctions $\tilde{\chi}\in\mathbb{C}[\mathbb{F}_q]$ en posant $\tilde{\chi}(0)=0$. La transformée additive est alors définie comme suit :

$$\forall f\in\mathbb{C}[\mathbb{F}_q],\ \mathcal{F}_{add}(f):\begin{cases}\widehat{\mathbb{F}_q}\longrightarrow\mathbb{C}\\ \\ \psi\longmapsto\sum_{x\in\mathbb{F}_q}f(x)\psi(x)\end{cases}$$

On obtient alors une autre écriture de la somme de Gauss :

$$\forall\psi\in\widehat{\mathbb{F}_q},\ \forall\chi\in\mathbb{F}_q^*,\ \ G(\chi,\psi)=\mathcal{F}_{add}(\tilde{\chi})(\psi)$$

Ceci nous permet de décomposer un caractère multiplicatif en série de Fourier additive.
Proposition
Soit $\chi\in\widehat{\mathbb{F}_q^*}$. on a

$$\chi=\frac{1}{q}\sum_{\psi\in\widehat{\mathbb{F}_q}}G(\chi,\overline{\psi})\psi$$

Démonstration
On décompose la fonction $\tilde{\chi}$ en série de Fourier, ce qui nous donne :

$$\tilde{\chi}=\sum_{\psi\in\widehat{\mathbb{F}_q}}\langle\tilde{\chi},\psi\rangle\psi$$

Ensuite on a $\langle \tilde{\chi}, \psi \rangle = \frac{1}{q} G(\chi, \overline{\psi}$, ce qui termine la démonstration.
Nous allons maintenant énoncés quelques propriétés facilitant le calcul des sommes de Gauss.

Propriétés des sommes de Gauss

On rappelle que p est la caractéristique du corps $\mathbb{F}_q$, i.e $q = p^r$. Alors, si on note $\chi \in \widehat{\mathbb{F}_q^*}$ et $\psi \in \widehat{\mathbb{F}_q}$:

$$\text{(i) pour a et b} \in \mathbb{F}_q, \text{on a } G(\chi, \psi_{ab}) = \overline{\chi(a)} G(\chi, \psi_b)$$

$$\text{(ii) } G(\chi, \overline{\psi}) = \chi(-1) G(\chi, \psi)$$

$$\text{(iii) } G(\overline{\chi}, \psi) = \chi(-1) \overline{G(\chi, \psi)}$$

Démonstration
(i) $G(\chi, \psi_{ab}) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \psi_{ab}(x) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \psi_b(ax)$
On effectue ensuite un changement de variable en posant $y = ax$.On obtient alors :
$G(\chi, \psi_{ab}) = \sum_{y \in \mathbb{F}_q^*} \chi(y) \chi(a^{-1}) \psi_b(y) = \chi(a^{-1}) G(\chi, \psi_b)$
(ii) La seconde propriété s'obtient à partir de la (i) en posant $b = -1$. En effet $G(\chi, \overline{\psi_a}) = G(\chi, \psi_{-a}) = \chi(-1) G(\chi, \psi_a)$
(iii) On utilise (ii) en passant à la conjugaison :

$$\overline{G(\chi, \overline{\psi})} = \overline{\sum_{x \in g} \chi(x) \overline{\psi}(x)} = \sum_{x \in G} \overline{\chi(x)} \psi(x) = G(\overline{\chi}, \psi)$$

Or $\overline{G(\chi, \overline{\psi})} = \overline{\chi(-1) G(\chi, \psi)} = \overline{\chi(-1)}\, \overline{G(\chi, \psi)}$. Comme $\chi(-1) \in \mathbb{R}$, on obtient le résultat demandé : $G(\overline{\chi}, \psi) = \chi(-1) \overline{G(\chi, \psi)}$.

Cependant on est dans la pratique généralement incapable de calculer simplement la valeur de ces sommes de Gauss. Pour le moment on dispose seulement de la majoration $|G(\chi, \psi)| \leq q - 1$. La proposition suivante nous permet d'en savoir plus.

Proposition Calcul des sommes de Gauss

$$G(\chi, \psi) = \begin{cases} q - 1 \text{ si } \chi = \chi_0 \text{ et } \psi = \psi_0 \\ -1 \text{ si } \chi = \chi_0 \text{ et } \psi \neq \psi_0 \\ 0 \text{ si } \chi \neq \chi_0 \text{ et } \psi = \psi_0 \end{cases}$$

Dans les autres cas (pour $\chi \neq \chi_0$ et $\psi \neq \psi_0$) on a $|G(\chi, \psi)| = q^{\frac{1}{2}}$ et
$G(\chi, \psi) G(\overline{\chi}, \psi) = q \chi(-1)$.

Démonstration
(i) $\forall x \in \mathbb{F}_q^*$, $\chi_0(x) = 1$ et $\psi_0(x) = 1$. D'où $G(\chi_0, \psi_0) = \left|\mathbb{F}_q^*\right| = q - 1$.
(ii) Si $\chi = \chi_0$ et $\psi \neq \psi_0$ alors $G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^*} \psi(x)$. Or on sait par les propriétés des caractères additifs que $\sum_{x \in \mathbb{F}_q} \psi(x) = 0$ quand $\psi \neq \psi_0$. Donc $G(\chi, \psi) = \left(\sum_{x \in \mathbb{F}_q} \psi(x)\right) - \psi(0) = -1$.
(iii) Si $\chi \neq \chi_0$ et $\psi = \psi_0$ alors $G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^*} \chi(x) = 0$. Ceci est en effet une propriété des caractères multiplicatifs.
Pour le cas général, on se sert du fait que la fonction qui à un caractère additif

ψ associe la somme de Gauss $G(\chi,\psi)$ est la transformée de Fourier additive de la fonction $\tilde{\chi}$. On utilise alors la formule de Plancherel:

$$\begin{aligned}\langle G(\chi,\cdot),G(\chi,\cdot)\rangle &= \frac{1}{q}\sum \mathcal{F}_{add}(\tilde{\chi})\overline{\mathcal{F}_{add}(\tilde{\chi})}\\ &= \sum \tilde{\chi}\overline{\tilde{\chi}} = q\langle\tilde{\chi},\tilde{\chi}\rangle = q\end{aligned}$$

On choisit maintenant un caractère multiplicatif ψ_a.

$$\begin{aligned}\langle G(\chi,\psi_a),G(\chi,\psi_a)\rangle &= \frac{1}{q}\sum_{b\in\mathbb{F}_q} G(\chi,\psi_{ab})\overline{(\chi,\psi_{ab})}\\ &= \frac{1}{q}\sum_{b\in\mathbb{F}_q} |\chi(b)|^2|G(\chi,\psi_a)|^2\\ &= \langle\chi,\chi\rangle|G(\chi,\psi_a)|^2 = |G(\chi,\psi_a)|^2\end{aligned}$$

D'après l'égalité précédente, on a alors $|G(\chi,\psi_a)|^2 = q$ i.e $|G(\chi,\psi_a)| = q^{\frac{1}{2}}$. La dernière égalité est donnée par :

$$G(\chi,\psi)G(\overline{\chi},\psi) = \chi(-1)|G(\chi,\psi)|^2 = \chi(-1)q$$

puisque nous venons de montrer que $|G(\chi,\psi)| = q^{\frac{1}{2}}$. Il est alors naturel de vouloir connaître la valeur de $\chi(-1)$, ce que nous permet de faire la proposition suivante.

Proposition

Soit χ un caractère multiplicatif et m son ordre dans $\mathbb{F}_q$, c'est-à-dire le plus petit entier k tel que $\chi^k = \chi_0$.

Alors $\chi(-1) = 1 \Leftrightarrow m$ est pair et $\frac{q-1}{m}$ est impair.

Démonstration

Dans un premier temps montrons que m est pair. On sait que $\widehat{\mathbb{F}_q^*}$ est un groupe cyclique d'ordre $q-1$, donc $\chi^{q-1} = \chi_0$. Ceci implique que m divise $q-1$.

De plus χ est à valeurs dans $\mathbb{U}_m$, et $(-1) \in \mathbb{U}_m \Leftrightarrow m$ est pair.

m est pair, donc comme m divise $q-1$, on a $q-1$ pair donc q impair. On note g_0 un générateur de $\mathbb{F}_q^*$. Alors $\chi(g_0)$ est une racine m^{ieme} primitive de l'unité et on a :

$$\chi(-1) = \chi(g_0^{\frac{q-1}{2}}) = \zeta^{\frac{q-1}{2}}$$

Donc on a $\chi(-1) = -1$ si et seulement si $\zeta^{\frac{q-1}{2}} = \zeta^{\frac{m}{2}}$, c'est-à-dire si $\frac{q-1}{2} \equiv \frac{m}{2}$ modulo m. Ceci est équivalent à $\frac{q-1}{m} \equiv 1$ modulo 2, ce qui signifie que , $\frac{q-1}{m}$ est impair.

2.4 Loi de réciprocité quadratique

2.4.1 Le caractère quadratique

Quel est donc le lien entre ce que nous avons fait jusqu'à maintenant et l'introduction de ce chapitre concernant les résidus quadratiques ? Voici un exemple de caractère multiplicatif qui nous servira pour la démonstration de la loi de réciprocité quadratique.

Caractère quadratique

Soit q un entier impair. On définit un caractère multiplicatif $\eta \in \mathbb{F}_q^*$ de la manière suivante :

$$\forall x \in \mathbb{F}_q^*,\ \eta(x) = \begin{cases} 1 \text{ si x est un carré dans } \mathbb{F}_q \\ -1 \text{ sinon} \end{cases}$$

On voit que η correspond en fait à $\chi_{\frac{q-1}{2}}$. De plus, quand $q = p$ est un nombre premier, on a $\eta(x) = \left(\frac{x}{p}\right)$, c'est-à-dire le symbole de Legendre.

2.4.2 Signes des sommes de Gauss

Nous allons maintenant nous intéresser de plus près au caractère quadratique, afin de pouvoir démontrer la loi de réciprocité quadratique. Dans un premier temps nous utiliserons un endomorphisme T de $\mathbb{C}[\mathbb{F}_q^*]$,défini comme suit :

$$\forall f \in \mathbb{C}[\mathbb{F}_q^*],\ T_f : \begin{cases} \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^* \\ a \longmapsto \sum\limits_{x \in \mathbb{F}_q^*} f(x)\psi_a(x) \end{cases}$$

Cet endomorphisme est très proche de la transformée de Fourier additive, puisqu'on a , si on note $\tilde{f}$ la fonction f prolongée en 0 par $f(0) = 0$:

$$\forall f \in \mathbb{C}[\mathbb{F}_q^*],\ T_f(a) = \mathcal{F}_{add}(\tilde{f})(\psi_a)$$

Pourquoi utiliser cet opérateur au lieu de la transformée de Fourier additive? En fait il rend les formules dans lesquelles interviennent les sommes de Gauss plus simples. par exemple, on a :

$$\forall \chi \in \widehat{\mathbb{F}_q^*}, \forall \psi \in \widehat{\mathbb{F}_q},\ T_\chi(x) = G(\chi, \psi_x) = \overline{\chi}(x)G(\chi, \psi_1)$$

Pour la suite des démonstrations on se restreindra au cas où $q = p$. L'opérateur T alors s'exprime de la manière suivante :

$$\forall f \in \mathbb{C}[\mathbb{F}_p^*],\ T_f : \begin{cases} \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^* \\ a \longmapsto \sum\limits_{x \in \mathbb{F}_p^*} f(x)\zeta^{ax} \quad \text{où on a noté } \zeta = e^{\frac{i\pi}{p}} \end{cases}$$

Voici un lemme qui fait le lien entre le caractère quadratique et T :
Lemme Soit $\eta \in \widehat{\mathbb{F}_p^*}$ le caractère quadratique sur le corps $\mathbb{F}_p$. On a alors :

$$det(T) = (-1)^{\frac{p-1}{2}} i^{\frac{(p-1)(p-3)}{4}} p^{\frac{p-3}{2}} G(\eta, \psi_1)$$

Démonstration
Il s'agit d'écrire la matrice de T dans la base des caractères multiplicatifs $\{\chi_0, ..., \chi_{p-2}\}$ Les deux seuls caractères à valeurs réelles sont χ_0 et η, on pourra regrouper les autres caractères par paires $(\chi, \overline{\chi})$ et se servir de la relation $T_\chi(x) = G(\chi, \psi_x) = \overline{\chi}(x)G(\chi, \psi_1)$.

On obtient donc la matrice suivante :

$$\begin{pmatrix} G(\chi_0,\psi_1) & & & & & & \\ & G(\eta,\psi_1) & & & & & \\ & & 0 & G(\chi,\psi_1) & & & \\ & & G(\overline{\chi},\psi_1) & 0 & & & \\ & & & \ddots & & & \\ & & & & 0 & G(\chi_{\frac{p-3}{2}},\psi_1) \\ & & & & G(\overline{\chi_{\frac{p-3}{2}}},\psi_1) & 0 \end{pmatrix}$$

On a vu précédemment que $G(\chi_0,\psi_1) = -1$. On ne connait pour l'instant pas la valeur de $G(\eta,\psi_1)$. Il reste à calculer les sous déterminants de taille 2 :

$$det\begin{pmatrix} 0 & G(\chi,\psi_1) \\ G(\overline{\chi},\psi_1) & 0 \end{pmatrix} = -G(\chi,\psi_1)G(\overline{\chi},\psi_1) = -\chi(-1)p$$

On obtient donc comme valeur du déterminant :

$$\begin{aligned} det(T) &= -G(\eta,\psi_1)(-p)^{\frac{p-3}{2}} \prod_{j=1}^{\frac{p-3}{2}} \chi_j(-1) \\ &= (-1)^{\frac{p-1}{2}} p^{\frac{p-3}{2}} G(\eta,\psi_1) \prod_{j=1}^{\frac{p-3}{2}} \chi_j(-1) \end{aligned}$$

Or $\chi_j(-1) = \chi_1(-1)^j = (-1)^j$. Ce qui nous donne :

$$\begin{aligned} \prod_{j=1}^{\frac{p-3}{2}} \chi_j(-1) &= \prod_{j=1}^{\frac{p-3}{2}} (-1)^j \\ &= (-1)^{1+\ldots+(\frac{p-3}{2}} = (-1)^{\frac{(p-1)(p-3)}{4}} \end{aligned}$$

Ce qui correspond bien à l'expression à démontrer.

Signes des sommes de Gauss

Soit p un nombre premier impair. On note η le caractère quadratique de $\mathbb{F}_p$. Alors

$$G(\eta,\psi_1) = \begin{cases} p^{\frac{1}{2}} \text{ si } p \equiv 1[4] \\ ip^{\frac{1}{2}} \text{ si } p \equiv 3[4] \end{cases}$$

Démonstration

Comme η est à valeurs réelles, on a $\overline{\eta} = \eta$, donc $G(\eta,\psi_1)G(\overline{\eta},\psi_1) = G(\eta,\psi_1)^2 = p\eta(-1)$.

Déterminons maintenant la valeur de $\eta(-1)$. L'ordre de η est 2, donc pair. On a que $\eta(-1) = -1$ si et seulement si $\frac{p-1}{2}$ est impair. on en déduit alors :

$$\eta(-1) = \begin{cases} 1 \text{ si } p \equiv 1[4] \\ -1 \text{ si } p \equiv 3[4] \end{cases}$$

On obtient alors

$$G(\eta,\psi_1) = \begin{cases} \epsilon_p p^{\frac{1}{2}} \text{ si } p \equiv 1[4] \\ \epsilon_p ip^{\frac{1}{2}} \text{ si } p \equiv 3[4] \end{cases} \quad \text{avec } \epsilon_p \in \{1,-1\}$$

Il reste désormais à montrer que $\epsilon_p = 1$, ce qui est la partie la plus longue... Afin de travailler sur une seule équation au lieu des deux ci-dessus, on utilise le fait que

$$i^{\frac{(p-1)^2}{4}} = \begin{cases} 1 \text{ si } p \equiv 1[4] \\ i \text{ si } p \equiv 3[4] \end{cases}$$

On a donc $G(\eta, \psi_1) = \epsilon_p i^{\frac{(p-1)^2}{4}} p^{\frac{1}{2}}$.
On utilise maintenant la valeur du déterminant de T calculée précédemment en remplaçant $G(\eta, \psi_1)$ par l'expression obtenue ci-dessus, ce qui donne :

$$det(T) = \epsilon_p (-1)^{\frac{p-1}{2}} i^{\frac{(p-1)(p-2)}{2}} p^{\frac{p-2}{2}}$$

Pour déterminer ϵ_p il nous faut comparer cette expression de $det(T)$ à son expression dans une autre base. on choisit pour cela la base constituée des fonctions$\{\delta_1, ..., \delta_{p-1}\}$. Dans cette base nous avons :

$$T\delta_k = \sum_{x \in \mathbb{F}_p^*} \delta_x \zeta^{kx}$$

Le calcul du déterminant est simple puisqu'il s'agit d'une matrice de Vandermonde et on obtient :

$$det(T) = det\left(\zeta^{jk}\right)_{1 \leq j,k \leq n} = \prod_{1 \leq m < n \leq p-1} (\zeta^n - \zeta^m)$$

On pose maintenant $\mu = e^{\frac{i\pi}{2}}$, ce qui nous permet de décomposer ce produit en trois sous-produits :

$$\prod_{1 \leq m < n \leq p-1} (\zeta^n - \zeta^m) = \prod_{1 \leq m < n \leq p-1} \left(\mu^{2n} - \mu^{2m}\right) = \prod_{1 \leq m < n \leq p-1} \left(\mu^{m+n}(\mu^{n-m} - \mu^{m-n})\right)$$

$$= \prod_{1 \leq m < n \leq p-1} \mu^{m+n} \prod_{1 \leq m < n \leq p-1} \mu^{(n-m)} - \mu^{-(n-m)}$$

$$= \prod_{1 \leq m < n \leq p-1} \mu^{m+n} \prod_{1 \leq m < n \leq p-1} 2isin\left(\frac{\pi(n-m)}{p}\right)$$

$$= \prod_{1 \leq m < n \leq p-1} \mu^{m+n} \prod_{1 \leq m < n \leq p-1} i \prod_{1 \leq m < n \leq p-1} 2sin\left(\frac{\pi(n-m)}{p}\right)$$

Il reste maintenant à trouver les signes de ces trois produits.
Le plus simple est le produit des sin.En effet on a $1 \leq n - m \leq p - 2$ et $p \geq 2$. Donc chaque terme du produit est positif et on a
$\prod_{1 \leq m < n \leq p-1} 2sin\left(\frac{\pi(n-m)}{p}\right) > 0$. Pour la suite, notons ce produit A, tout ce qui nous intéresse est qu'il est strictement positif.

On s'intéresse désormais au second produit.Il nous faut pour cela déterminer $Card\{(m,n)|1 \leq m < n \leq p-1$. Pour mieux se le représenter, on peut le décomposer en une somme de plusieurs termes. Fixons $m = 1$. On a alors les couples $(1,2)...(1,p-1)$, ce qui donne $(p-2)$ couples.On répète ce raisonnement

jusqu'à $m = p-2$ ce qui donne un unique couple $(p-1, p-2)$. Par conséquent on a

$$Card\{(m,n)|1 \leq m < n \leq p-1\} = \sum_{k=2}^{p-1} p-k = \sum_{k=2}^{p-1} p - \sum_{k=2}^{p-1} k$$
$$= p(p-2) - \frac{p(p-1)-2}{2} \qquad = \frac{(p-1)(p-2)}{2}$$

Donc $\prod_{1\leq m<n\leq p-1} i = i^{\frac{(p-1)(p-2)}{2}}$.
Passons au dernier produit, pour déterminer l'exposant de μ on calcule la somme suivante :

$$\sum_{1\leq m<n\leq p-1} m+n = \sum_{n=2}^{p-1}\sum_{m=1}^{n-1} m+n$$
$$= \sum_{n=2}^{p-1} \frac{3n^2}{2} = \frac{3}{2}\sum_{n=1}^{p-2} n(n-1)$$
$$= \frac{3}{2}\left(\frac{(p-2)(p-3)(2p-3)}{6} + \frac{(p-1)(p-2)}{2}\right)$$
$$= \frac{p(p-1)(p-2)}{2}$$

D'où $\prod_{1\leq m<n\leq p-1} \mu^{m+n} = \mu^{\frac{p(p-1)(p-2)}{2}} = (-1)^{\frac{(p-1)(p-2)}{2}}$.
L'expression de $det(T)$ obtenue est donc :

$$det(T) = (-1)^{\frac{(p-1)(p-2)}{2}} i^{\frac{(p-1)(p-2)}{2}} A$$

En comparant avec la première expression de $det(T)$ que nous connaissons, à savoir :

$$det(T) = \epsilon_p (-1)^{\frac{p-1}{2}} i^{\frac{(p-1)(p-2)}{2}} p^{\frac{p-2}{2}}$$

On obtient $\epsilon_p = +1$.

2.4.3 Démonstration de la loi

Voici l'énoncé de la loi de **réciprocité quadratique**
Pour tous nombre impairs premiers distincts p et r on a :

$$\left(\frac{p}{r}\right)\left(\frac{r}{p}\right) \;=\; (-1)^{\frac{(p-1)(r-1)}{4}}$$

On rappelle que $\left(\frac{p}{r}\right)$ désigne le symbole de Legendre et peut prendre ici deux valeurs distinctes 1 et -1. La valeur 0, cas où r divise p, est exclue car p et r sont premiers et distincts donc premiers entre eux.
Soit η le caractère multiplicatif quadratique de $\mathbb{F}_p$ et ψ_1 le caractère additif canonique.
On sait par le théorème précédent que :

$$G(\eta,\psi_1)^2 = \begin{cases} p & \text{si } p \equiv 1[4] \\ -p & \text{si } p \equiv 3[4] \end{cases}$$
$$= (-1)^{\frac{p-1}{2}} p$$

On note maintenant $G = G(\eta, \psi_1)$. On a

$$G^r \ = \ (G^2)^{\frac{r-1}{2}} G \ = \left((-1)^{\frac{p-1}{2}} p\right)^{\frac{r-1}{2}} \ G$$

A partir de maintenant nous allons effectuer les calculs dans l'anneau R des entiers algébriques, c'est-à-dire des nombres appartenant à $\mathbb{C}$ qui sont racines de polynômes à coefficients entiers. Comme les caractères sont des sommes de racines de l'unité, les valeurs des sommes de Gauss sont des entiers algébriques. Donc $G \in R$ On note (r) l'idéal engendré par r dans R, et on se place dans l'anneau quotient $\frac{R}{(r)}$. Comme l'anneau quotient $\frac{R}{(r)}$ est de caractéristique r on obtient, par la formule du multinôme de Newton

$$G^r = \left(\sum_{x \in mathbbF_p^*} \eta(x)\psi_1(x) \right)^r = \sum_{x \in \mathbb{F}_p^*} (\eta(x))^r (\psi_1(x))^r \text{modulo } r$$

Or $\eta(x) \in \{-1, 1\}$ et r est impair donc $\eta(x)^r = eta(x)$, et $\psi_1(x)^r = \psi_r(x)$. Cela nous donne

$$G^r = \eta(x)\psi_r(x) = G(\eta, \psi_r) = \overline{eta(r)} G = \eta(r) G \text{ modulo } r$$

Nous avons obtenu deux expressions pour G^r, qui sont donc égales :

$$\left((-1)^{\frac{p-1}{2}} p\right)^{\frac{r-1}{2}} \ G = \eta(r) G \text{ modulo } r$$

On multiplie cette égalité par G et en utilisant la valeur de G^2 trouvée précédemment il vient :

$$\left((-1)^{\frac{p-1}{2}} p\right)^{\frac{r-1}{2}} \ (-1)^{\frac{p-1}{2}} p = \eta(r)(-1)^{\frac{p-1}{2}} p \text{ modulo } r$$

Cette égalité est en fait valable sur $\mathbb{Z}/r\mathbb{Z}$. Comme p et r sont premiers entre eux on simplifie par $(-1)^{\frac{p-1}{2}} p$:

$$\eta(r) = \left((-1)^{\frac{p-1}{2}} p\right)^{\frac{r-1}{2}} = (-1)^{\frac{(p-1)(r-1)}{4}} p^{\frac{r-1}{2}} \text{ modulo } r$$

Or nous avons vu lors de le définition du caractère quadratique que lorsque p est premier $\eta(r) = \left(\frac{r}{p}\right)$. La formule d'Euler nous donne $p^{\frac{r-1}{2}} = \left(\frac{p}{r}\right)$. Donc finalement notre égalité devient :

$$\left(\frac{r}{p}\right) = (-1)^{\frac{(p-1)(r-1)}{4}} \left(\frac{p}{r}\right)$$

Il reste à vérifier que cette égalité est valable dans $\mathbb{Z}$: les deux membres de l'égalité sont à valeurs dans $\{-1, 1\}$ et $r \geq 3$ donc nous sommes parvenus au résultat.

Pour conclure ce chapitre dédié à la loi de réciprocité quadratique, reprenons l'exemple que j'avais proposé au début de ce chapitre : 41 est-il un carré modulo 97? 41 et 97 sont deux nombres premiers impairs, on peut donc appliquer la loi de réciprocité quadratique :

$$\left(\frac{41}{97}\right) \left(\frac{97}{41}\right) = (-1)^{\frac{((41-1)(97-1)}{4}} = 1$$

Donc $\left(\frac{41}{97}\right) = \left(\frac{97}{41}\right)$. Or $97 \equiv 15[41]$, donc $\left(\frac{97}{41}\right) = \left(\frac{15}{41}\right) = \left(\frac{3}{41}\right)\left(\frac{5}{41}\right)$ On applique une seconde fois la loi de réciprocité quadratique pour chacun des deux termes et on obtient finalement :

$$\left(\frac{41}{97}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{3}\right)$$

Il est désormais simple de conclure : en effet 1 est un carré modulo 3 mais pas 2, donc $\left(\frac{41}{97}\right) = -1$ ce qui signifie que 41 n'est pas un carré modulo 97.

On peut maintenant se demander s'il est possible d'aller plus loin : peut-on rapidement savoir si un nombre est un cube, ou une quelconque puissance modulo p ? Eisenstein a établi une loi de réciprocité cubique, et Gauss une loi de réciprocité biquadratique. Cependant la théorie des corps de classes est considérée comme véritable la généralisation de cette loi.

3 Transformée de Walsh et applications

3.1 Définitions

La transformée de Walsh est en fait une réécriture de la transformée de Fourier sur un groupe abélien particulier $G = (\mathbb{Z}/2\mathbb{Z})^k$. Quel est le dual d'un tel groupe? En fait, chaque caractère va s'exprimer comme un produit des différents caractères des groupes élémentaires. Donc on va s'intéresser ici aux caractères de $\mathbb{Z}/2\mathbb{Z}$.
$\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. L'élément générateur de ce groupe est 1, et les éléments de $\widehat{G}$ sont les suivants :

$$\chi_0 : \begin{cases} G \longrightarrow \mathbb{C}^* \\ g = 1^k \longmapsto e^{\frac{2ik0\pi}{2}} = 1 \end{cases}$$

χ_0 est le caractère trivial.

$$\chi_1 : \begin{cases} G \longrightarrow \mathbb{C}^* \\ g = 1^k \longmapsto e^{\frac{2ik\pi}{2}} = e^{ik\pi} \end{cases}$$

χ_1 est donc défini par $\chi_1(0) = 1$ et $\chi_1(1) = -1$.
On va maintenant utiliser la forme bilinéaire canonique sur $(\mathbb{Z}/2\mathbb{Z})^k$ définie par :

$$< a, x >= \sum_{i=0}^{k-1} a_i x_i$$

Cela nous permet d'associer à chaque élément $a = \{a_0, ..., a_{k-1}\}$ un caractère :

$$\chi_a : \begin{cases} (\mathbb{Z}/2\mathbb{Z})^k \longrightarrow \{-1, 1\} \\ x = \{x_0, x_1, ..., x_{k-1}\} \longmapsto (-1)^{<a,x>} = (-1)^{a_0 x_0}(-1)^{a_1 x_1}...(-1)^{a_{k-1} x_{k-1}} \end{cases}$$

Les caractères χ_a seront donc vus comme des vecteurs de taille 2^k remplis de 1 et de -1. les éléments de G seront assimilés à des entiers compris entre 0 et $2^k - 1$ de la manière suivante : à $x \in G = (\mathbb{Z}/2\mathbb{Z})^k$ on fait correspondre l'entier $\sum_{i=0}^{k-1} x_i 2^i$.

Prenons un exemple . considérons le groupe $G = (\mathbb{Z}/2\mathbb{Z})^3$, qui est de cardinal 8. Voici ses éléments et l'entier qui leur est assimilé selon la correspondance décrite ci-dessus :

$$(0,0,0) \longrightarrow 0$$
$$(1,0,0) \longrightarrow 1$$
$$(0,1,0) \longrightarrow 2$$
$$(1,1,0) \longrightarrow 3$$
$$(0,0,1) \longrightarrow 4$$
$$(1,0,1) \longrightarrow 5$$
$$(0,1,1) \longrightarrow 6$$
$$(1,1,1) \longrightarrow 7$$

On peut représenter la table de caractères de G comme une matrice carrée d'ordre 8 , notée W_8 dont la ligne i représente les valeurs du caractère χ_i, c'est-à-dire $(W_8)_{ij} = \chi_i(j)$.

$$W_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Voici deux autres exemples de matrices de Walsh :

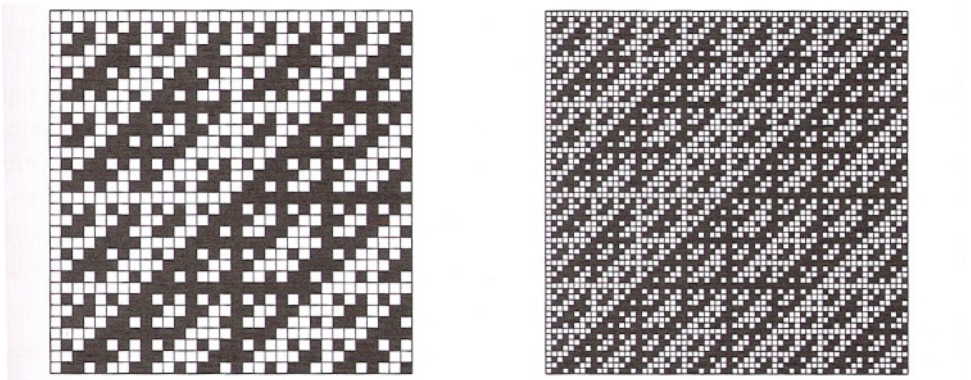


FIG. 2.2 – *Matrices de Walsh W_{32} et W_{64}*

On va maintenant définir la transformée de Walsh.

Définition

On définit la transformée de Walsh $\mathcal{W}_k(f)$ d'un vecteur complexe $f = \{f[0], ..., f[2^k -$

1]} de taille 2^k par :

$$\forall i \in \{0, ..., 2^k - 1\},\ \mathcal{W}_k(f)[i] = \sum_{j=0}^{2^k-1} f[j]\chi_i(j) = 2^k < f, \chi_i >$$

Quel est le lien avec la transformée de Fourier ? Notons $f : (\mathbb{Z}/2\mathbb{Z})^k \longrightarrow \mathbb{C}$ la fonction correspondant au vecteur f, c'est-à-dire le vecteur correspondant à la décomposition de la fonction f dans la base des fonctions de Dirac $\{\delta_x\}_{x\in G}$. Alors le calcul de $\mathcal{W}(f)$ est celui d'une transformée de Fourier :

$$\mathcal{W}(f)[i] = 2^k < f, \chi_i >= 2^k \frac{1}{2^k} \sum_{x\in G} f(x)\overline{\chi_i}(x) = \widehat{f}(\overline{\chi_i}$$

Or χ_i est à valeurs dans $\{-1, 1\}$ donc $\overline{\chi_i} = \chi_i$ et on a

$$\mathcal{W}(f)[i] = \overline{f}(\chi_i)$$

L'opérateur $\mathcal{W}_k : \mathbb{C}^{2^k} \longrightarrow \mathbb{C}^{2^k}$ est une application linéaire , et sa matrice dans la base canonique est W_{2^k}, c'est-à-dire la table des caractères du groupe $(\mathbb{Z}/2\mathbb{Z})^k$. On a par conséquent $\mathcal{W}_k(f) = W_{2^k} f$. Notons bien que le premier f représente la fonction, et le second le vecteur correspondant à cette fonction dans la base des fonctions Dirac.
On utilise maintenant la formule d'inversion de la transformée de Fourier pour calculer celle de la transformée de Walsh :
Proposition
La transformée de Walsh est inversible et son inverse est $\frac{1}{2^k}\mathcal{W}_k$. D'un point de vue matriciel, cela signifie que la matrice W_{2^k} vérifie $W_{2^k} W_{2^k} = 2^k Id_n$.
A quoi sert la transformée de Walsh et comment l'utilise-t-on?
Son intérêt principal est qu'elle permet de décomposer n'importe quelle fonction $f : \{0, ..., 2^k - 1\} \longrightarrow \mathbb{C}$ sur la base orthogonale des caractères de $(\mathbb{F}_2)^k$:

$$\forall i \in \{0..., 2^k - 1\},\ f[i] = \frac{1}{2^k} \sum_{j=0}^{2^k-1} W_k(f)[j]\chi_j[i]$$

Quelques exemples vont nous permettre de voir comment on peut utiliser la transformée de Walsh pour des compressions de signaux, pour l'étude de foncions booléennes

3.2 Applications

3.2.1 Etude statistique

On considère la situation suivante : un fermier veut connaître l'influence de certains paramètres sur sa production de blé. Ces paramètres sont au nombre de trois : l'éclairage(variable a), la quantité d'herbicide (variable b) et la quantité d'engrais (variable c). Chacune de ces variables peut prendre deux valeurs , + (forte quantité) et − (faible quantité). On dispose d'un compte-rendu d'expérience donné par le tableau suivant, qui regroupe les valeurs pour la taille du blé en cm sous les différentes conditions:

a	b	c	α_{abc}
+	+	+	69
-	+	+	81
+	-	+	63
-	-	+	77
+	+	-	61
-	+	-	92
+	-	-	54
-	-	-	89

Ces résultats sont donc modélisables par une fonction

$$f : \begin{cases} (\mathbb{Z}/2\mathbb{Z})^3 \simeq \{+,-\}^3 \longrightarrow \mathbb{R} \\ (a,b,c) \longmapsto \alpha_{abc} \end{cases}$$

Afin d'analyser ces résultats , on définit des interactions d'ordre 0, 1, 2 et 3. L'interaction d'ordre 0 est simplement la moyenne :

$$\mu = \frac{1}{8} \sum_{(a,b,c)\in\{+,-\}^3} \alpha_{abc}$$

Les interactions d'ordre 1 sont au nombre de 3 et correspondent à l'effet d'un seul paramètre, les deux autres étant supposés constants :

$$\mu_a = \frac{1}{4}\left(\sum_{(b,c)\in\{+,-\}^2} \alpha_{+bc} - \sum_{(b,c)\in\{+,-\}^3} \alpha_{-bc} \right)$$

$$\mu_b = \frac{1}{4}\left(\sum_{(a,c)\in\{+,-\}^2} \alpha_{a+c} - \sum_{(a,c)\in\{+,-\}^3} \alpha_{a-c} \right)$$

$$\mu_c = \frac{1}{4}\left(\sum_{(a,b)\in\{+,-\}^2} \alpha_{ab+} - \sum_{(a,b)\in\{+,-\}^3} \alpha_{ab-} \right)$$

De la même manière nous avons 3 interactions d'ordre 2:

$$\mu_{ab} = \frac{1}{4}\left(\sum_{c\in\{+,-\}} \alpha_{++c} + \alpha_{--c} \right) - \frac{1}{4}\left(\sum_{c\in\{+,-\}} \alpha_{+-c} + \alpha_{-+c} \right)$$

$$\mu_{bc} = \frac{1}{4}\left(\sum_{a\in\{+,-\}} \alpha_{a++} + \alpha_{a--} \right) - \frac{1}{4}\left(\sum_{a\in\{+,-\}} \alpha_{a+-} + \alpha_{a-+} \right)$$

$$\mu_{ac} = \frac{1}{4}\left(\sum_{b\in\{+,-\}} \alpha_{+b+} + \alpha_{-b-} \right) - \frac{1}{4}\left(\sum_{b\in\{+,-\}} \alpha_{+b-} + \alpha_{-b+} \right)$$

Enfin voici l'interaction d'ordre 3 :

$$\mu_{abc} = \frac{1}{4}\left(\sum_{(b,c)\in\{+,-\}^2 b=c} \alpha_{+bc} - \alpha_{-bc} \right) + \frac{1}{4}\left(\sum_{(b,c)\in\{+,-\}^2 b\neq c} \alpha_{-bc} - \alpha_{+bc} \right)$$

Si on reprend notre fonction f et que l'on assimile la valeur + à 0, la valeur - à 1 et les triplets (a, b, c) à un entier de la même manière que lors de la définition de la transformée de Walsh on obtient :

$$\mu = \frac{1}{8}\sum_{i=0}^{7} f[i]\chi_0 = \frac{1}{8}\mathcal{W}_8(f)[0]$$

$$\mu_a = \frac{1}{4}(f[0] - f[1] + f[2] - f[3] + f[4] - f[5] + f[6] - f[7]) = \frac{1}{4}\mathcal{W}_8(f)[1]$$

En fait, chaque interaction est le résultat de la transformée de Walsh de f pour un j donné. On obtient par conséquent $W_8 f = \tilde{u}$:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} f[0] \\ f[1] \\ f[2] \\ f[3] \\ f[4] \\ f[5] \\ f[6] \\ f[7] \end{pmatrix} = \begin{pmatrix} 8\mu \\ 4\mu_a \\ 4\mu_b \\ 4\mu_{ab} \\ 4\mu_c \\ 4\mu_{ac} \\ 4\mu_{bc} \\ 4\mu_{abc} \end{pmatrix}$$

4 Lexique

Classe de conjugaison La classe de conjugaison de $g \in G$ avec G un groupe est définie comme suit :

$$C_g = \left\{hgh^{-1}, h \in G\right\}$$

Pourquoi les classes de conjugaison nous importent-elles dans le cas présent ? Prenons deux exemples afin de mieux se les représenter.
Soit $\Phi : G \longrightarrow \mathbb{C}^*$ tel que Φ soit un morphisme.On note e l'élément neutre de G. Alors pour g,h $\in G$ on a :

$$\Phi(hgh^{-1}) = \Phi(h)\Phi(g)\Phi(h^{-1}) = \Phi(e)\Phi(g) = \Phi(g)$$

Donc Φ est constante sur les classes de conjugaison.
Prenons maintenant $G = GL_n$. Les classes de conjugaison sont les matrices semblables et le déterminant est constant sur ces classes.
Si G est abélien, alors $C_g = \{g\}$.

Extension algébrique Une extension algébrique L sur un corps K est une extension de corps (exemple : C est une extension de R et contient R comme sous-corps, voir Construction de $\mathbb{C}$) dans laquelle tous les éléments sont algébriques sur K.Un élément $l \in L$ est dit algébrique sur K si et seulement si il existe un polynôme non nul à coefficients dans K ayant l pour racine.

Formule de Newton Cette généralisation de la formule du binôme de Newton donne le développement d'une puissance entière n d'une somme finie de m termes :

$$(x_1 + x_2 + ... + x_m)^n = \sum_{\sum_{i=1}^{m} k_i = n} \binom{n}{k_1 ... k_m} \prod x_i^{k_i}$$

La somme porte sur toutes les combinaisons d'indices entiers naturels $k_1, \ldots, k_m$ tels que $k_1 + k_2 + \cdots + k_m = n$, certains d'entre eux pouvant être nuls. Les nombres suivants sont appelés coefficients multinomiaux.

$$\binom{n}{k_1 ... k_m} = \frac{n!}{k_1! k_2! \ldots k_m!}$$

Démonstration
On procède par récurrence sur m, et on utilise la formule du binôme de Newton. Initialisation : pour $m = 1$, les deux côtés valent x_1^n. On suppose désormais l'égalité vraie au rang m. Montrons qu'elle est encore vraie au rang $m + 1$

$$\begin{aligned}(x_1 + x_2 + \cdots + x_m + x_{m+1})^n &= (x_1 + x_2 + \cdots + (x_m + x_{m+1}))^n \\ &= \sum_{k_1+k_2+\cdots+k_{m-1}+K=n} \binom{n}{k_1, k_2, \ldots, k_{m-1}, K} x_1^{k_1} x_2^{k_2} \cdots x_{m-1}^{k_{m-1}} (x_m + x_{m+1})^K\end{aligned}$$

On applique maintenant le binôme de Newton au terme $(x_m + x_{m+1})^K$:

$$\sum_{k_1+k_2+\cdots+k_{m-1}+K=n} \binom{n}{k_1, k_2, \ldots, k_{m-1}, K} x_1^{k_1} x_2^{k_2} \cdots x_{m-1}^{k_{m-1}} (x_m + x_{m+1})^K$$

$$== \sum_{k_1+k_2+\cdots+k_{m-1}+K=n} \binom{n}{k_1, k_2, \ldots, k_{m-1}, K} x_1^{k_1} x_2^{k_2} \cdots x_{m-1}^{k_{m-1}} \sum_{k_m+k_{m+1}=K} \binom{K}{k_m, k_{m+1}} x_m^{k_m} x_{m+1}^{k_{m+1}}$$

$$= \sum_{k_1+k_2+\cdots+k_{m-1}+k_m+k_{m+1}=n} \binom{n}{k_1, k_2, \ldots, k_{m-1}, k_m, k_{m+1}} x_1^{k_1} x_2^{k_2} \cdots x_{m-1}^{k_{m-1}} x_m^{k_m} x_{m+1}^{k_{m+1}}$$

Ce qui nous permet de passer de l'avant-dernière étape à la dernière étape est que :

$$\frac{n!}{k_1! k_2! \cdots k_{m-1}! K!} \frac{K!}{k_m! k_{m+1}!} = \frac{n!}{k_1! k_2! \cdots k_{m+1}!}$$

Donc

$$\binom{n}{k_1, k_2, \ldots, k_{m-1}, K} \binom{K}{k_m, k_{m+1}} = \binom{n}{k_1, k_2, \ldots, k_{m-1}, k_m, k_{m+1}}$$

Structure d'algèbre Un ensemble E a une structure d'algèbre sur le corps commutatif K s'il est muni de trois lois de composition ($+$ et $\times$ lois de composition interne, $\cdot$ loi de composition externe) satisfaisant aux conditions suivantes : - $(E, +, \times)$ est un espace vectoriel sur K
-la loi $\times$ est distributive par rapport à la loi $+$
-$\forall a, b \in K, \forall x, y \in E\ (a \cdot b) \times (x \cdot y) = (ab) \cdot (x \times y)$.

Vandermonde (Matrice, déterminant) Une matrice de Vandermonde $n \times n$ est de la forme :

$$V = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & ... & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & ... & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & ... & \alpha_n^{n-1} \end{pmatrix}$$

Pour calculer son déterminant,on effectue l'opération $C_i \longleftarrow C_i - \alpha_1 \times C_{i-1}$ (où C_i désigne la colonne i), en partant de la dernière colonne jusqu'à la deuxième. On obtient alors :

$$det(V) = det \begin{pmatrix} 1 & 0 & 0 & ... & 0 \\ 1 & (\alpha_2 - \alpha_1) & \alpha_2(\alpha_2 - \alpha_1) & ... & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & (\alpha_n - \alpha_1) & \alpha_n(\alpha_n - \alpha_1) & ... & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{pmatrix}$$

On développe à partir de la première ligne, ce qui nous donne :

$$det(V) = 1 \times det(\begin{pmatrix} (\alpha_2 - \alpha_1) & \alpha_2(\alpha_2 - \alpha_1) & ... & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ \vdots & \vdots & & \vdots \\ (\alpha_n - \alpha_1) & \alpha_n(\alpha_n - \alpha_1) & ... & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{pmatrix}$$

C'est-à-dire, si on extrait le facteur $\alpha_n - \alpha_1$:

$$det(V) = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)...(\alpha_n - \alpha_1) det \begin{pmatrix} 1 & \alpha_2 & \alpha_2^2 & ... & \alpha_2^{n-2} \\ 1 & \alpha_3 & \alpha_3^2 & ... & \alpha_3^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & ... & \alpha_n^{n-2} \end{pmatrix}$$

Par récurrence on obtient $det(V) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$.

5 Bibliographie

Cette section sera en l'occurrence très brève, puisque j'ai travaillé de manière exclusive à partir du livre suivant : *L'algèbre discrète de la transformée de Fourier*, chapitres I et II, par Gabriel Peyré, aux éditions Ellipses, 2004.

Conclusion

Ce mémoire m'a permis de relier mes enseignements du semestre (Dualité sur un espace vectoriel, Forme bilinéaires, Normes...) tout en abordant un niveau de difficulté supérieur à travers l'algèbre de la transformée de Fourier.
J'ai étudié la transformée de Fourier sous l'angle de la théorie des groupes uniquement, et n'ayant jamais vu auparavant la transformée de Fourier sous forme analytique je n'avais aucune idée de la transformée en elle-même ou des structures qu'elle utilise. Ce qui constitue désormais une raison supplémentaire de découvrir la transformée de Fourier analytique...
En ce qui concerne les applications, je me suis passionnée pour la loi de réciprocité quadratique, et il me reste beaucoup à lire sur d'autres applications de la transformée de Walsh. J'ai été impressionnée par la diversité des applications possibles, aussi bien dans le traitement de l'image que dans le codage et décodage.
La compréhension de l'algèbre utilisée n'a cependant pas été facile, et je commence seulement à prendre un peu de recul et à voir l'étendue des mathématiques touchées par ce sujet.