Université Bordeaux I

Master CSI

Année 2004-2005

UE Mathématiques discrètes de la transformée de Fourier

Christine Bachoc

Bibliography

[1] Gabriel Peyré, *L'algèbre discrète de la transformée de Fourier* (ellipses 2004)

[2] Joachim von zur Gathen, Jürgen Gerhard, *Modern computer algebra*, second edition, CUP 2003

Chapter 1

Introduction

Ce cours traite des aspects *algébriques et discrets* de la transformée de Fourier. Dans un premier temps on traite les groupes commutatifs. On verra rapidement des applications, par exemple à la multiplication rapide des grands entiers, ou bien à la cryptographie. Ensuite on abordera le cas des groupes non commutatifs.

Chapter 2

Rappels de théorie des groupes

Dans cette partie, on rappelle des notions essentielles pour la suite vues en Licence, et qui doivent être parfaitement connues et maîtrisées.

2.1 Groupe, ordre d'un élément, ordre d'un groupe, théorème de Lagrange

Un groupe G est un ensemble non vide, muni d'une opération notée le plus généralement ., qui a les propriétés suivantes:

1. Elle est interne, c'est-à-dire associe à tout couple $(x, y) \in G^2$ un élément $x.y = xy \in G$.
2. Elle est associative: (xy)z=x(yz) pour tout $x, y, z \in G$.
3. Elle a un élément neutre noté 1 ou e, vérifiant $x.1 = 1.x = x$ pour tout $x \in G$.
4. Tout élément $x \in G$ a un inverse $x^{-1} \in G$, c'est-à-dire vérifiant $x.x^{-1} = x^{-1}.x = 1$.

Si, de plus, $xy = yx$ pour tout $x, y \in G$, on dit que le groupe est commutatif ou abélien. Dans ce cas, la loi est souvent notée $+$, le neutre 0 et l'inverse, appelé opposé, est noté $-x$.

Exemples: le groupe multiplicatif $\mathbb{C}^*$; $(\mathbb{Z}, +)$; $\mathbb{Z}/n\mathbb{Z}$. Le groupe des racines n-ièmes de l'unité dans $\mathbb{C}$. Le groupe symétrique S_n. Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

Un sous-groupe H d'un groupe G est une partie de G qui est un groupe pour la même opération que G. Exemple: $\mathbb{Z}$ est un sous-groupe de $\mathbb{C}$. $2\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Pour montrer qu'un sous-ensemble H de G est un sous-groupe de G, il suffit de montrer que:

1. H est non vide
2. Pour tout $x, y \in H$, xy^{-1} (ou $x - y$ dans le cas d'une notation additive) est dans H.

L'ordre d'un élément x d'un groupe G est le plus petit entier k non nul, s'il existe, vérifiant $x^k = 1$. S'il n'existe pas on dit que x est d'ordre infini. C'est la période de la suite des puissances de x. Ainsi, si x est d'ordre 3, la suite de ses puissances successives donne: $1, x, x^2, x^3 = 1, x, x^2, 1, \ldots$. Notons que, si x est d'ordre k, alors $x^{-1} = x^{k-1}$ puisque $x.x^{k-1} = 1$. Cela montre que l'ensemble $\{1, x, x^2, \ldots, x^{k-1}\}$ est un sous-groupe de G, appelé groupe cyclique engendré par x, et noté $< x >$.

Plus généralement, l'ordre d'un groupe est le nombre de ses éléments. Ainsi, l'ordre du groupe engendré par x est égal à l'ordre de x.

Exemples: ordre dans $\mathbb{Z}/n\mathbb{Z}$ et dans $(\mathbb{Z}/n\mathbb{Z})^*$.

On rappelle le théorème de Lagrange:

Théorème 1 *L'ordre d'un sous-groupe est un diviseur de l'ordre du groupe. En particulier, l'ordre d'un élément d'un groupe divise l'ordre de ce groupe.*

2.2 Groupes cycliques

Un groupe cyclique est un groupe engendré par un élément. Un tel élément s'appelle un générateur du groupe. L'exemple typique de groupe cyclique fini est $\mathbb{Z}/n\mathbb{Z}$. Un autre exemple naturel: le groupe des racines n-ièmes de l'unité dans $\mathbb{C}$: $\mathbb{U}_n := \{e^{2ik\pi/n}, 0 \leq k \leq n-1\}$.

On voit facilement que, si x est un générateur d'un groupe cyclique d'ordre n, alors les autres générateurs de G sont les x^k avec $1 \leq k \leq n$ et $(k, n) = 1$. La fonction φ d'Euler en compte le nombre:

$$\varphi(n) := \mathrm{card}\{k, 1 \leq k \leq n \mid (k, n) = 1\}.$$

On a les propriétés suivantes, qui permettent de calculer $\varphi(n)$ pour tout n:

- Si p premier, $\varphi(p^k) = p^k - p^{k-1}$.
- Si $(m, n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$

Le nombre $\varphi(n)$ est aussi (presque par définition) le nombre d'éléments du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

Proposition 1 *Tout sous-groupe et tout quotient d'un groupe cyclique est aussi cyclique. Pour tout diviseur d de l'ordre d'un groupe cyclique, il existe dans ce groupe un unique sous-groupe d'ordre d, et ce groupe contient exactement $\varphi(d)$ éléments d'ordre d.*

En effet, si x est un générateur, l'unique sous-groupe d'ordre d est le groupe engendré par $x^{n/d}$, et les éléments d'ordre d sont les $x^{kn/d}$ avec $(k, d) = 1$.

Comme dans un groupe cyclique d'ordre n il y a exactement $\varphi(d)$ éléments d'ordre d pour tout diviseur d de n, on a l'identité:

$$n = \sum_{d|n} \varphi(d).$$

Exemple: le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p - 1$.

Exemple: Tout groupe d'ordre premier est cyclique.

2.3 Homomorphismes, quotients

Un homomorphisme $f : G \to H$ est une application vérifiant $f(xy) = f(x)f(y)$ pour tout $x, y \in G$. C'est un isomorphisme si f est bijective. Le noyau et l'image de f sont respectivement $\ker f = \{s \in G \mid f(x) = 1\}$ et $\mathrm{Im}\, f = \{f(x) \mid x \in G\}$. Ce sont des sous-groupes respectifs de G et H.

Pour montrer qu'un homomorphisme $f : G \to H$ est un isomorphisme, il suffit de montrer que $\ker f = \{1\}$ et que $|G| = |H|$.

Exemple: Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. En effet, si x est un générateur de ce groupe on définit un isomorphisme $f : \mathbb{Z}/n\mathbb{Z} \to G$ par $f(k \mod n) = x^k$. Cette définition est licite car, si $k \mod n = k' \mod n$, alors $x^k = x^{k'}$.

La notion de quotient est plus subtile, nous la rappelons dans le cas des groupes commutatifs (dans le cas non commutatif il faut la notion de sous-groupe distingué). Si G est un groupe commutatif, et si H est un sous-groupe de G, on

construit un troisième groupe noté G/H, appelé quotient de G par H, de la façon suivante (on note G additivement):

- les éléments de G/H sont les ensembles $x + H$ (on dit aussi les classes) où $x+H = \{x+y \mid y \in H\}$. Noter que l'on peut très bien avoir $x+H = x'+H$ (en fait exactement quand $x - x' \in H$). On note $s : G \to G/H$ l'application définie par $s(x) = x + H$.

- l'opération de groupe sur G/H est définie par: $(x + H) + (x' + H) = (x+x')+H$. Attention, cette définition n'a de sens que si on montre sa cohérence, c'est-à-dire: si $x + H = y + H$ et $x' + H = y' + H$ alors $(x + x') + H = (y+y')+H$. Remarquer que l'application s (appelée surjection canonique) devient un homomorphisme de groupes.

Par soucis de légèreté, on note souvent la classe $x + H$ par: $x \mod H$ ou $\overline{x}$ ou $s(x)$. Dans une ligne de calcul on met souvent un seul "mod H" au bout (et "mod n" pour "mod $n\mathbb{Z}$").

Exemple: $G = \mathbb{Z}$, $H = n\mathbb{Z}$, on retrouve $\mathbb{Z}/n\mathbb{Z}$.

L'ordre de G/H est égal au quotient des ordres de G et H: $|G/H| = |G|/|H|$.

Théorème 2 (Théorème de factorisation) *Soit $f : G \to H$ un homomorphisme de G dans H. Soit $K = \ker f$ et soit $s : G \to G/K$ la surjection canonique. On définit une application $\overline{f} : G/K \to H$ par: $\overline{f}(s(x)) = f(x)$ et celle-ci est un homomorphisme injectif. C'est bien sûr un isomorphisme de G/K sur $\operatorname{Im} f$.*

2.4 Groupes abéliens finis

On connait maintenant une famille de groupes abéliens finis: les produits directs de groupes cycliques, c'est-à-dire les groupes de la forme

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}. \tag{2.1}$$

On peut montrer, et c'est un résultat non trivial, que tout groupe abélien fini est isomorphe à l'un de ces groupes. Une autre question qui se pose alors est de décider quand deux de ces groupes sont isomorphes. On a une solution complète et algorithmique à ces problèmes dans la théorie des *diviseurs élémentaires* et *l'algorithme de réduction de Smith.* Ces notions seront étudiées dans le cours "Algèbre et calcul formel".

Le théorème chinois, vu en Licence, est une première étape dans cette direction.

Théorème 3 *Si* $(a, b) = 1$*,* $\mathbb{Z}/ab\mathbb{Z}$ *est isomorphe à* $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$*.*

L'isomorphisme est obtenu en factorisant l'homomorphisme $f : \mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ défini par: $f(n) = (n \mod a, n \mod b)$. Le noyau de f est $\ker f = ab\mathbb{Z}$ grâce à la propriété $(a, b) = 1$; les deux groupes ayant même ordre, cela suffit à montrer que l'homomorphisme f est un isomorphisme.

L'application inverse est d'une grande utilité pratique. En d'autres termes, étant donnés des entiers s et t, il existe un unique entier $k \mod ab$ tel que: $k \equiv s \mod a$ et $k \equiv t \mod b$. Pour calculer k en fonction de s et t il faut utiliser une relation de Bezout: $au + bv = 1$. Alors $k = sbv + tau$ convient.

Finalement, remarquons qu'il est souvent facile de démontrer que deux groupes ne sont *pas* isomorphes, en trouvant une propriété de groupe qui les distingue. Ainsi, si deux groupes n'ont pas le même ordre, ou bien n'ont pas le même nombre d'éléments d'ordre donné, ils ne peuvent pas être isomorphes.

Chapter 3

Transformée de Fourier sur un groupe fini

L'objectif est d'étudier les fonctions à valeurs complexes définies sur un groupe fini G. Pour cela, on étudie d'abord celles qui sont des homomorphismes, ce sont les caractères du groupe. Afin d'analyser une fonction quelconque, on la décomposera suivant ceux-ci.

3.1 Caractères d'un groupe fini

Définition 1 *Soit G un groupe fini. Un caractère de G est un homomorphisme $\chi : G \to \mathbb{C}^*$.*

La notation $\mathbb{C}^*$ désigne bien sûr le groupe *multiplicatif* $(\mathbb{C}^*, \times)$.

Soit $\chi : G \to \mathbb{C}^*$ un caractère de G. Si $g \in G$, pour tout entier k, $\chi(g^k) = \chi(g)^k$. En particulier, si g est d'ordre k, on a $\chi(g)^k = 1$.

Petite parenthèse sur les racines de l'unité dans $\mathbb{C}$: on appelle racines de l'unité les nombres complexes $z \in \mathbb{C}$ tels qu'il existe un entier n avec $z^n = 1$. C'est un groupe pour la multiplication, noté $\mathbb{U}$. On a:

$$\mathbb{U}_n := \{z \in \mathbb{C} \mid z^n = 1\} = \{e^{2i\pi k/n}, 0 \leq k \leq n-1\}$$

est le *groupe des racines n-ièmes de l'unité*. C'est un groupe (multiplicatif) cyclique. Les $z \in \mathbb{U}_n$ tels que $z^a \neq 1$ pour tout $0 < a < n$ s'appellent les racines primitives n-ièmes de l'unité. Ce sont les générateurs du groupe $\mathbb{U}_n$, il y en a

exactement $\varphi(n)$, qui sont les $e^{2i\pi k/n}$ avec $1 \leq k \leq n-1$ et $(k,n)=1$. Bien sûr, $\mathbb{U} = \cup_{n\geq 0}\mathbb{U}_n$.

Lemme 1 *Les sous-groupes finis de $\mathbb{U}$ sont exactement les $\mathbb{U}_n$. En particulier ils sont cycliques.*

Preuve: : Soit G un sous-groupe fini de $\mathbb{U}$, d'ordre n. Par le théorème de Lagrange, tout élément z de G vérifie $z^n = 1$. Donc $G \subset \mathbb{U}_n$; comme $\mathbb{U}_n$ est exactement d'ordre n, on a $G = \mathbb{U}_n$.

□

Retournons aux caractères de G. Ainsi, si G est d'ordre n, on a forcément pour tout $g \in G$, $\chi(g) \in \mathbb{U}_n$.

Proposition 2 *Soit G un groupe fini d'ordre n. Soit $\chi : G \to \mathbb{C}^*$ un caractère de G.*

1. $\mathrm{Im}\,\chi \subset \mathbb{U}_n$.
2. *Pour tout $g \in G$, $\chi(g^k) = \chi(g)^k$. En particulier, l'ordre de $\chi(g)$ divise l'ordre de g.*
3. *Pour tout $g \in G$, $|\chi(g)| = 1$, $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$.*

On peut multiplier les caractères. Si χ_1 et χ_2 sont deux caractères de G, on définit le produit $\chi_1\chi_2$ par: $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$. On obtient bien ainsi un caractère $\chi_1\chi_2 : G \to \mathbb{C}^*$.

Proposition 3 *L'ensemble $\widehat{G}$ des caractères de G est un groupe pour la multiplication. On l'appelle aussi le dual de G.*

Exemples: décrire $\widehat{G}$ pour $G = \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, S_3.

Une propriété importante des caractères d'un groupe fini, mais qui n'a d'intérêt que dans le cas des groupes non commutatifs est la suivante:

Proposition 4 *Soit χ un caractère d'un groupe G. Pour tout $g, h \in G$, $\chi(ghg^{-1}) = \chi(h)$. En particulier, χ est constant sur les classes de conjugaison de G.*

Preuve: : Cela résulte de la commutativité de $\mathbb{C}^*$. En effet, $\chi(ghg^{-1}) = \chi(g)\chi(h)\chi(g)^{-1} = \chi(h)\chi(g)\chi(g)^{-1} = \chi(h)$.

□

Exercice: décrire les caractères de S_4 (utiliser la proposition précédente).

3.2 Dual d'un groupe cyclique

Considérons le cas d'un groupe G cyclique d'ordre n. Soit g un générateur fixé de G. Comme tout élément de G est de la forme g^k, et que $\chi(g^k) = \chi(g)^k$, on voit qu'un caractère χ de G est entièrement déterminé par $\chi(g)$. D'un autre côté, on doit choisir $\chi(g)$ parmi les racines n-ièmes de l'unité de $\mathbb{C}^*$. On peut ainsi définir n caractères $\chi_0 = 1, \chi_1, \ldots, \chi_{n-1}$ de G par:

$$\chi_k(g) = e^{2i\pi k/n}.$$

Il faut remarquer que, d'une part, $\chi_k = \chi_1^k$, et, d'autre part, que cette indexation des caractères de G dépend du choix fait pour le générateur de G.

On a démontré:

Proposition 5 *Soit G un groupe cyclique d'ordre n et soit g un générateur fixé de G. Le groupe dual $\widehat{G}$ est égal à l'ensemble $\{\chi_0, \chi_1, \ldots, \chi_{n-1}\}$, où χ_k est défini par:*

$$\chi_k(g) = e^{2i\pi k/n}.$$

Le groupe $\widehat{G}$ est cyclique, d'ordre n, engendré par χ_1 (on a $\chi_k = \chi_1^k$).

Remarque: L'application $g^k \to \chi_k$ définit un isomorphisme entre G et $\widehat{G}$ dit *non canonique* car il dépend du choix d'un générateur de G.

3.3 Dual d'un groupe abélien fini; bidual

On sait qu'un groupe abélien fini est produit direct de groupes cycliques (théorème admis); comme on sait décrire le dual d'un groupe cyclique, il nous reste à décrire le dual d'un produit direct de groupes.

Théorème 4 *Soit G_1 et G_2 deux groupes finis. L'application*

$$\begin{aligned} f : \widehat{G_1} \times \widehat{G_2} &\longrightarrow \widehat{G_1 \times G_2} \\ (\chi_1, \chi_2) &\longmapsto f((\chi_1, \chi_2)) \end{aligned}$$

où $\chi = f((\chi_1, \chi_2))$ est défini par: $\chi(g_1, g_2) = \chi_1(g_1)\chi_2(g_2)$ est un isomorphisme.

Noter que le théorème décrit explicitement les caractères de $\widehat{G_1 \times G_2}$ en fonction de ceux de $\widehat{G_1}$ et de $\widehat{G_2}$. Exemple: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Corollaire 1 *Le dual d'un groupe abélien fini est (non canoniquement) isomorphe à ce groupe; en particulier ils ont même ordre.*

Par contre, on a un isomorphisme cette fois canonique entre un groupe G abélien fini et son *bidual*.

3.4 L'algèbre de groupe $\mathbb{C}[G]$

On note $\mathbb{C}[G]$ l'ensemble des fonctions (cette fois sans propriété particulière) $f : G \to \mathbb{C}$. C'est une algèbre sur $\mathbb{C}$, c'est-à-dire:

- Un anneau pour l'addition et la multiplication des fonctions, définies respectivement par: $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ et $(f_1 f_2)(x) = f_1(x) f_2(x)$. Le zéro de cet anneau est la fonction $f = 0$ constante égale à 0; l'unité est la fonction $f = 1$ constante égale à 1.
- Un $\mathbb{C}$-espace vectoriel, pour la multiplication des scalaires définie par $(\lambda f)(x) = \lambda f(x)$.

On l'appelle *algèbre du groupe G*.

Une base naturelle de $\mathbb{C}[G]$ est constituée des δ_x, $x \in G$, définis par:

$$\begin{cases} \delta_x(x) = 1 \\ \delta_x(h) = 0 \text{ pour tout } h \neq x \end{cases}$$

Toute fonction $f : G \to \mathbb{C}$ s'écrit $f = \sum_{x \in G} f(x)\delta_x$. C'est la représentation "naturelle" des fonctions. Il est immédiat de vérifier que $\{\delta_x, x \in G\}$ est une base de $\mathbb{C}[G]$; en particulier, cela montre que la dimension de $\mathbb{C}[G]$ est égale à l'ordre de G.

Nous avons vu un autre ensemble de n éléments de $\mathbb{C}[G]$: ce sont les caractères de G. Nous alors voir que, lorsque G est commutatif, ils forment une autre base de $\mathbb{C}[G]$; c'est le passage d'une base à l'autre qui va nous permettre d'analyser les fonctions sur G. Introduisons d'abord un produit hermitien sur $\mathbb{C}[G]$.

Définition 2 *Soit, pour tout* $f_1, f_2 \in \mathbb{C}[G]$

$$< f_1, f_2 >= \frac{1}{|G|} \sum_{x \in G} f_1(x)\overline{f_2(x)}.$$

On définit ainsi un produit hermitien sur $\mathbb{C}[G]$*. La base* $\{\delta_x, x \in G\}$ *est une base orthogonale pour ce produit scalaire, et* $< \delta_x, \delta_x >= \frac{1}{|G|}$ *pour tout* $x \in G$*.*

Proposition 6 *Soit* G *un groupe abélien fini. L'ensemble des caractères de* G *forme une base orthonormée pour le produit hermitien défini ci-dessus.*

Preuve: Il nous faut calculer $< \chi_1, \chi_2 >$ pour deux caractères de G. Remarquons d'abord que $< \chi_1, \chi_2 >=< \chi_1{\chi_2}^{-1}, 1 >$. En effet,

$$\begin{aligned} < \chi_1, \chi_2 > &= \frac{1}{|G|} \sum_{x \in G} \chi_1(x)\overline{\chi_2(x)} \\ &= \frac{1}{|G|} \sum_{x \in G} \chi_1(x)\chi_2(x)^{-1} \\ &= \frac{1}{|G|} \sum_{x \in G} (\chi_1{\chi_2}^{-1})(x) \\ &=< \chi_1{\chi_2}^{-1}, 1 > . \end{aligned}$$

En posant $\chi = \chi_1{\chi_2}^{-1}$, il nous reste à calculer $< \chi, 1 >$. Lorsque $\chi = 1$, on a $\sum_{x \in G} \chi(x) = |G|$ soit $< \chi, 1 >= 1$. Supposons maintenant que $\chi \neq 1$. Il existe donc un élément $b \in G$ tel que $\chi(b) \neq 1$. Comme $hG = G$, on a

$$\begin{aligned} S := \sum_{x \in G} \chi(x) &= \sum_{x \in G} \chi(bx) \\ &= \sum_{x \in G} \chi(b)\chi(x) \\ &= \chi(b) \sum_{x \in G} \chi(x) \\ &= \chi(b)S \end{aligned}$$

soit $S = \chi(b)S$, que l'on peut écrire dans $\mathbb{C}$: $(1 - \chi(b))S = 0$. Comme $\chi(b) \neq 1$, on peut en déduire que $S = 0$.

On a donc démontré que les éléments de $\widehat{G}$ forment une famille orthonormée. Comme il y en a exactement $|G|$, ils forment bien une base.

□

On a démontré les *relations d'orthogonalité* entre caractères. Elles sont extrêmement utiles, et nous les rappelons dans la proposition suivante, associées aux relations duales.

Proposition 7 *(Relations d'orthogonalité:) Soit G un groupe commutatif fini.*

1. *Pour tout $\chi_1, \chi_2 \in \widehat{G}$,*

$$\sum_{x \in G} \chi_1(x)\overline{\chi_2(x)} = \begin{cases} |G| \text{ si } \chi_1 = \chi_2 \\ 0 \text{ sinon} \end{cases}$$

et, en particulier:

$$\sum_{x \in G} \chi_1(x) = \begin{cases} |G| \text{ si } \chi_1 = 1 \\ 0 \text{ sinon} \end{cases}$$

2. *Pour tout $x, y \in G$,*

$$\sum_{\chi \in \widehat{G}} \chi(x)\overline{\chi(y)} = \begin{cases} |G| \text{ si } x = y \\ 0 \text{ sinon} \end{cases}$$

et, en particulier:

$$\sum_{\chi \in \widehat{G}} \chi(x) = \begin{cases} |G| \text{ si } x = 1 \\ 0 \text{ sinon} \end{cases}$$

Preuve: On a déjà démontré les premières. Les deuxièmes relations d'orthogonalité se démontrent soit directement, soit en remarquant que ce sont les relations d'orthogonalité des caractères du groupe dual $\widehat{G}$. En effet, les caractères de $\widehat{G}$ sont en correspondance avec les éléments de G via l'application (qui est un isomorphisme):

$$\begin{aligned} g \in G \longrightarrow \chi_g : \widehat{G} &\longrightarrow \mathbb{C}^* \\ \chi &\longmapsto \chi(g) \end{aligned}$$

□

3.5 Transformée de Fourier

On suppose désormais que notre groupe G est abélien fini.

C'est seulement un changement de base!

Soit $f \in \mathbb{C}[G]$. On peut décomposer f sur les deux bases orthonormées que l'on connait: $\{\sqrt{|G|}\delta_x \mid x \in G\}$ et $\{\chi \mid \chi \in \widehat{G}\}$. Cela donne:

$$f = \sum_{x \in G} f(x)\delta_x = \sum_{\chi \in \widehat{G}} c_f(\chi)\chi$$

où $c_f(\chi) =< f, \chi >$. L'usage est de noter:

Définition 3 *On appelle transformée de Fourier de f et on note $\widehat{f}$ l'élément de $\mathbb{C}[\widehat{G}]$ défini par:*

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

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

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

C'est bien sûr un isomorphisme d'espaces vectoriels.

Théorème 5 *Soit $f, g \in \mathbb{C}[G]$. On a:*

- *(Formule d'inversion)*

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

- *(Formule de Plancherel)*

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

Preuve: : On a déjà vu la première. La deuxième résulte du calcul de $< f, g >$ dans les deux bases.

□

3.6 Produit de convolution

Le produit des fonctions est une multiplication naturelle sur $\mathbb{C}[G]$; toutefois le produit de convolution est plus adéquat parce qu'il se comporte mieux vis à vis de la transformée de Fourier.

Définition 4 *Soit $f, g \in \mathbb{C}[G]$. On définit le produit de convolution $f * g$ de f et g par:*

$$(f * g)(x) = \sum_{y,z \in G | yz = x} f(y)g(z) = \sum_{y \in G} f(y)g(y^{-1}x).$$

Théorème 6 *Le produit de convolution munit $\mathbb{C}[G]$ d'une structure d'algèbre. De plus, pour tout $f, g \in \mathbb{C}[G]$,*

$$\widehat{f * g} = \widehat{f}\widehat{g}.$$

La transformée de Fourier $\mathcal{F}$ est un isomorphisme d'algèbres de $(\mathbb{C}[G], *)$ sur $(\mathbb{C}[\widehat{G}], .)$.

Preuve: On calcule $\widehat{f * g}(\chi)$ pour $\chi \in \hat{G}$.

$$\begin{aligned}
\widehat{f * g}(\chi) &= \sum_{x \in G} (f * g)(x)\chi(x) \\
&= \sum_{x \in G} \big(\sum_{y,z \in G | yz = x} f(y)g(z) \big)\chi(x) \\
&= \sum_{y,z \in G} f(y)g(z)\chi(yz) = \sum_{y,z \in G} f(y)g(z)\chi(y)\chi(z) \\
&= \big(\sum_{y \in G} f(y)\chi(y) \big) \big(\sum_{z \in G} f(z)\chi(z) \big) \\
&= \widehat{f}(\chi)\widehat{g}(\chi)
\end{aligned}$$

On a donc bien $\mathcal{F}(f * g) = \mathcal{F}(f)\mathcal{F}(g)$.

□

3.7 Formule de Poisson

On termine avec une formule, très utile, qui analyse le comportement d'une fonction sur un sous-groupe. Nous en verrons une application à la théorie des codes (formule de Mac Williams).

Définition 5 *Soit H un sous-groupe de G. L'orthogonal de H, noté $H^\perp$, est:*

$$H^\perp := \{\chi \in \widehat{G} \mid \chi(H) = \{1\}\}.$$

Proposition 8 *$H^\perp$ est un sous-groupe de $\widehat{G}$. On a: $H^\perp \simeq \widehat{G/H}$. En particulier, $|H^\perp| = |G|/|H|$.*

Preuve: Il est clair que $H^\perp$ est un sous-groupe de $\widehat{G}$.

On définit un homomorphisme $\phi : H^\perp \to \widehat{G/H}$ en posant: $\phi(\chi) = \overline{\chi}$, défini par: $\overline{\chi}(x + H) = \chi(x)$. Le point essentiel est que cette définition est valide car elle ne dépend pas du choix du représentant choisi modulo H, grâce au fait que $\chi(H) = \{1\}$. ϕ est clairement injectif. Si $\chi' \in \widehat{G/H}$, on définit χ en composant les applications $G \to^s G/H \to^{\chi'} \mathbb{C}^*$, c'est-à-dire $\chi = \chi' s$. Alors, $\chi \in H^\perp$ et $\chi' = \phi(\chi)$. L'application ϕ est donc surjective; on a donc démontré que c'est un isomorphisme.

□

Théorème 7 *(Formule de Poisson) Soit $f \in \mathbb{C}[G]$, et $H \subset G$ un sous-groupe de G. On a:*

$$\sum_{x \in H} f(x) = \frac{1}{|H^\perp|} \sum_{\chi \in H^\perp} \widehat{f}(\chi).$$

Preuve: On applique la formule de Plancherel en prenant pour g la fonction indicatrice de H:

$$g(x) = \begin{cases} 1 \text{ si } x \in H \\ 0 \text{ sinon} \end{cases}$$

Il reste à calculer $\hat{g}$. On a:

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

où la dernière égalité résulte des relations d'orthogonalités appliquées à la restriction χ_H de χ à H. La condition $\chi_H = 1$ équivaut à $\chi \in H^\perp$. La formule de Plancherel devient donc:

$$\sum_{x \in H} f(x) = \frac{|H|}{|G|} \sum_{\chi \in H^\perp} \hat{f}(\chi).$$

□

Chapter 4

Transformée de Walsh et fonctions booléennes

Dans ce chapitre, nous considérons le cas particulier $G = (\mathbb{Z}/2\mathbb{Z})^n$. Nous allons décrire un algorithme rapide de calcul de la transformée de Fourier, appelée dans ce cas transformée de Walsh, et ses applications à l'étude des propriétés des fonctions booléennes.

4.1 Transformée de Walsh

4.1.1 Caractères de $(\mathbb{Z}/2\mathbb{Z})^n$

Comme $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$, on peut voir G comme le $\mathbb{F}_2$-espace vectoriel de dimension n: $\mathbb{F}_2^n$. On le munit du produit scalaire usuel:

$$x \cdot y = \sum_{i=1}^{n} x_i y_i.$$

Notons que, si $u \in \mathbb{F}_2$, est défini modulo 2, le nombre $(-1)^u \in \mathbb{R}$ est bien défini.

Définition 6 *A tout $y \in \mathbb{F}_2^n$ on peut associer un caractère χ_y de $\mathbb{F}_2^n$ défini par:*

$$\chi_y(x) = (-1)^{x \cdot y}.$$

Proposition 9 *L'application $y \to \chi_y$ est un isomorphisme d'espaces vectoriels entre $\mathbb{F}_2^n$ et $\widehat{\mathbb{F}_2^n}$.*

Preuve: La démonstration directe est facile. En fait, ce n'est qu'une redite de ce que nous avons déjà vu sur les caractères d'un produit direct. Rappelons que $\widehat{Z/2\mathbb{Z}} = \{\chi_0, \chi_1\}$, où $\chi_0 = 1$ et $\chi_1(1) = -1$. Un caractère χ de $\mathbb{F}_2^n$ est donné par le choix d'une séquence de n caractères de $\mathbb{Z}/2\mathbb{Z}$, par exemple: $(\chi_0, \chi_0, \chi_1, \dots)$. Alors $\chi(x) = \chi_0(x_1)\chi_0(x_2)\chi_1(x_3)\dots$. Il suffit de remarquer que, si l'on associe à cette séquence l'élément $y \in \mathbb{F}_2^n$ dont les coordonnées successives sont 0 pour χ_0 et 1 pour χ_1, ici $y = (0, 0, 1, \dots)$, alors

$$(-1)^{x\cdot y} = (-1)^{\sum_{i=1}^n x_i y_i} = \prod_{i=1}^{n} (-1)^{x_i y_i} = \chi_0(x_1)\chi_0(x_2)\chi_1(x_3)\cdots = \chi(x).$$

On peut y voir aussi l'identification usuelle entre un espace vectoriel et son dual, donnée par le choix d'un produit scalaire.

□

Remarque 1 *Dans cette identification entre $\mathbb{F}_2^n$ et son dual, l'orthogonal d'un sous-groupe H (i.e. un sous-espace vectoriel!), est l'orthogonal au sens usuel pour le produit scalaire $x \cdot y$:*

$$H^\perp = \{y \in \mathbb{F}_2^n \mid x \cdot y = 0 \textit{ pour tout } x \in H\}.$$

La transformée de Fourier est dans ce contexte appelée *transformée de Walsh* et devient l'application

$$\begin{aligned} \mathcal{W} : \mathbb{C}[\mathbb{F}_2^n] &\longrightarrow \mathbb{C}[\mathbb{F}_2^n] \\ f &\longmapsto \widehat{f} \end{aligned}$$

où $\widehat{f}$ est définie par:

$$\widehat{f}(x) = \sum_{y \in \mathbb{F}_2^n} f(y)(-1)^{x\cdot y}.$$

Dans la base des δ_x, la matrice de $\mathcal{W}$ est la matrice

$$W_{2^n} = ((-1)^{x\cdot y})_{x,y\in\mathbb{F}_2^n}.$$

dont on ordonne les lignes et les colonnes suivant l'ordre lexicographique. C'est aussi l'ordre naturel des entiers de 0 à $2^n - 1$ identifiés avec leur écriture binaire. Cette matrice est clairement symétrique et vérifie (grâce aux relations d'orthogonalité)

$$W_{2^n} W_{2^n} = 2^n \operatorname{Id} .$$

4.2 Transformée de Walsh rapide

Le calcul de $\mathcal{W}f$ nécessite à priori $(2^n)^2$ opérations dans $\mathbb{C}$ puisque il s'agit de calculer le produit de la matrice W_{2^n} par le vecteur des valeurs prises par f. Nous allons voir un procédé récursif qui permet de passer à $n2^n$ opérations.

Pour $x \in \mathbb{F}_2^n$, notons $x' \in \mathbb{F}_2^{n-1}$ le $(n-1)$-uplet constitué des $n-1$ dernières coordonnées de x, de sorte que $x = (0, x')$ ou $x = (1, x')$. On a bien sur: $x \cdot y = x_1 y_1 + x' \cdot y'$. Dans le calcul de $\widehat{f}$, nous allons partager $\mathbb{F}_2^n$ en deux ensembles, suivant la valeur du premier bit.

$$\begin{aligned}
\widehat{f}(x) &= \sum_{y \in \mathbb{F}_2^n} f(y)(-1)^{x \cdot y} \\
&= \sum_{y' \in \mathbb{F}_2^{n-1}} f(0, y')(-1)^{x' \cdot y'} + \sum_{y' \in \mathbb{F}_2^{n-1}} f(1, y')(-1)^{x_1 + x' \cdot y'} \\
&= \begin{cases} \sum_{y' \in \mathbb{F}_2^{n-1}} (f(0, y') + f(1, y'))(-1)^{x' \cdot y'} \text{ si } x = (0, x') \\ \sum_{y' \in \mathbb{F}_2^{n-1}} (f(0, y') - f(1, y'))(-1)^{x' \cdot y'} \text{ si } x = (1, x') \end{cases}
\end{aligned}$$

On définit alors deux éléments f^+ et f^- de $\mathbb{C}[\mathbb{F}_2^{n-1}]$:

$$\begin{cases} f^+(y') = f(0, y') + f(1, y') \\ f^-(y') = f(0, y') - f(1, y') \end{cases}$$

L'expression trouvée pour $\widehat{f}$ montre que $\widehat{f}(x)$ s'exprime comme une transformée de Walsh *à l'ordre* $n-1$:

$$\begin{cases} \widehat{f}(0, x') = \widehat{f^+}(x') \\ \widehat{f}(1, x') = \widehat{f^-}(x') \end{cases}$$

Notons $T(2^n)$ le nombre d'opérations nécessaires au calcul de $\widehat{f}$. On doit calculer les deux fonctions sur $\mathbb{F}_2^{n-1}$: f^+, f^-, ce qui nécessite 2^n opérations. Ensuite, on est ramenés au calcul de deux transformées de Walsh sur $\mathbb{F}_2^{n-1}$. Donc:

$$\begin{aligned} T(2^n) &= 2^n + 2T(2^{n-1}) \\ &= 2^n + 2(2^{n-1} + 2T(2^{n-2})) \\ &= \dots \\ &= n2^n + 2^n T(1) = n2^n \end{aligned}$$

L'algorithme de calcul de $\widehat{f}$ est décrit par le schéma suivant, appelé *schéma papillon*:

Ce type d'algorithme est connu sous le nom de "diviser pour régner" (divide and conquer algorithm).

Exemple: $n = 3$

	000	001	010	011	100	101	110	111
f	0	1	0	0	1	0	0	0
$\hat{f}$	2	0	2	0	0	-2	0	2

4.3 Fonctions booléennes

Définition 7 *Une fonction booléenne est une application $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Pour tout $1 \leq i \leq n$, on note X_i la fonction booléenne définie par: $X_i(x) = x_i$.*

Proposition 10 *La somme et le produit de fonctions booléennes est une fonction booléenne. On a: $X_i^2 = X_i$. Tout polynôme en les X_i, dont les exposants valent 0 ou 1 et à coefficients dans $\mathbb{F}_2$, définit une fonction booléenne. Réciproquement, toute fonction booléenne a une expression unique sous la forme d'un polynôme en les X_i, dont les exposants valent 0 ou 1. Cette expression s'appelle la* forme algébrique de f. *Par définition, le degré de f est le degré de ce polynôme.*

Preuve: On montre que l'ensemble M des monômes en les X_i, , dont les exposants valent 0 ou 1, forme une base de l'espace des fonctions booléennes. Soit $a \in \mathbb{F}_2^n$; on note encore δ_a la fonction définie au chapitre précédent, dont on considère maintenant les valeurs modulo 2. On sait que l'ensemble des δ_a forme une

base de l'espace des fonctions booléennes. On vérifie facilement que

$$\delta_a = \prod_{i=1}^{n}(X_i + a_i + 1),$$

ce qui montre que δ_a est combinaison linéaire d'éléments de M, et donc que M est une famille génératrice. Pour montrer que c'est une base, il suffit de montrer que M a le bon cardinal, soit 2^n. Il est clair qu'il y a autant de monômes que de parties de l'ensemble $\{1, 2, \ldots, n\}$, soit 2^n.

□

Les fonctions de degré 1 sont les fonctions de la forme $f(x) = a_0 + a_1x_1 + \cdots + a_nx_n$, où les a_i sont dans $\mathbb{F}_2$. Notons $\phi_a(x) := a_1x_1 + \cdots + a_nx_n = a \cdot x$. Les fonctions ϕ_a et $1 + \phi_a$ sont les fonctions affines de la variable x; en quelque sorte les fonctions les plus simples parmi les fonctions booléennes. Notons Aff l'ensemble de ces fonctions; c'est un $\mathbb{F}_2$-espace vectoriel de dimension $n + 1$.

Il est important, dans les applications cryptographiques, de savoir déterminer quand une fonction booléenne donnée est "proche" de l'une des fonctions affines. Pour cela, la transformée de Walsh est extrêmement utile.

Tout d'abord, donnons un sens à la notion de distance entre fonctions booléennes.

Définition 8 *On définit la distance (de Hamming) de deux fonctions booléennes f et g par:*

$$d(f, g) := \mathrm{card}\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}.$$

C'est une distance au sens métrique du terme.
On définit la distance d'une fonction booléenne f aux fonctions affines par:

$$d(f, \mathrm{Aff}) := \min\{d(f, \phi) \mid \phi \in \mathrm{Aff}\}.$$

La distance de f aux fonctions affines se calcule grâce à la transformée de Walsh de la fonction $f^* : x \to (-1)^{f(x)}$.

Théorème 8
1. $d(f, \phi_y) = 2^{n-1} - \frac{1}{2}\mathcal{W}(f^*)(y)$.
2. $d(f, \mathrm{Aff}) = 2^{n-1} - \frac{1}{2}\max\{|\mathcal{W}(f^*)(y)| \mid y \in \mathbb{F}_2^n\}$.
3. $d(f, \mathrm{Aff}) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

4. *f atteint cette borne si et seulement si $|\mathcal{W}(f^*)(y)| = 2^{n/2}$ pour tout $y \in \mathbb{F}_2^n$. Une telle fonction booléenne s'appelle une* fonction courbe.

5. *Si n est pair, il existe des fonctions courbes, par exemple $f = \sum_{i=1}^{n/2} x_i x_{n/2+i}$.*

Preuve:

1. On a:

$$\begin{aligned}\mathcal{W}(f^*)(y) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+x\cdot y} \\ &= \mathrm{card}\{x \in \mathbb{F}_2^n \mid f(x) = x\cdot y\} - \mathrm{card}\{x \in \mathbb{F}_2^n \mid f(x) \neq x\cdot y\} \\ &= 2^n - 2d(f, \phi_y).\end{aligned}$$

2. On remarque que $d(f, \phi_y) + d(f, 1+\phi_y) = 2^n$; si $d(f, \phi_y) = 2^{n-1} - \delta$, alors $d(f, 1+\phi_y) = 2^{n-1} + \delta$, donc $\min(d(f, \phi_y), d(f, 1+\phi_y)) = 2^{n-1} - \frac{1}{2}|\mathcal{W}(f^*)(y)|$, d'où l'expression pour $d(f, \mathrm{Aff})$.

3. Par la formule de Plancherel, on a:

$$\sum_{y\in\mathbb{F}_2^n} |\mathcal{W}(f^*)(y)|^2 = 2^n \sum_{x\in\mathbb{F}_2^n} |f^*(x)|^2 = 2^{2n}.$$

   donc $\max(|\mathcal{W}(f^*)(y)|) \geq 2^{n/2}$, ce qui conduit à $d(f, \mathrm{Aff}) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

4. Le mieux que l'on puisse faire est: $|\mathcal{W}(f^*)(y)| = 2^{n/2}$ pour tout $y \in \mathbb{F}_2^n$, ce qui équivaut, en vertu de ce qui précède, à $d(f, \mathrm{Aff}) = 2^{n-1} - 2^{\frac{n}{2}-1}$. Comme $d(f, \mathrm{Aff})$ est un entier, il est nécessaire que n soit pair.

5. On "coupe en deux" les éléments de $\mathbb{F}_2^n$: on pose $x = (x^{(1)}, x^{(2)})$, et $y = (y^{(1)}, y^{(2)})$. Alors, $f(x) = x^{(1)} \cdot x^{(2)}$.

$$\begin{aligned}\mathcal{W}(f^*)(x) &= \sum_{y\in\mathbb{F}_2^n}(-1)^{y^{(1)}\cdot y^{(2)}+x\cdot y} \\ &= \sum_{y^{(1)},y^{(2)}\in\mathbb{F}_2^{n/2}}(-1)^{y^{(1)}\cdot y^{(2)}+x^{(1)}\cdot y^{(1)}+x^{(2)}\cdot y^{(2)}} \\ &= \sum_{y^{(1)}\in\mathbb{F}_2^{n/2}}(-1)^{x^{(1)}\cdot y^{(1)}}\left(\sum_{y^{(2)}\in\mathbb{F}_2^{n/2}}(-1)^{(y^{(1)}+x^{(2)})\cdot y^{(2)}}\right)\end{aligned}$$

En vertu des relations d'orthogonalité,

$$\sum_{y^{(2)}\in\mathbb{F}_2^{n/2}}(-1)^{(y^{(1)}+x^{(2)})\cdot y^{(2)}} = \begin{cases}2^{n/2} \text{ si } x^{(2)} = y^{(1)} \\ 0 \text{ sinon}\end{cases}$$

donc:

$$\mathcal{W}(f^*)(x) = 2^{n/2}(-1)^{x^{(1)}\cdot x^{(2)}}$$

et on a bien $|\mathcal{W}(f^*)(x)| = 2^{n/2}$ pour tout x.

□

Remarque 2 *Lorsque n est impair, on ne connait pas la valeur maximale de $d(f, \mathrm{Aff})$, Cela correspond en théorie des codes au rayon de recouvrement des codes de Reed-Muller d'ordre 1. On ne connait pas non plus toutes les fonctions courbes.*

En cryptographie, on utilise souvent des fonctions booléennes pour filtrer ou combiner des sources de bits pseudo-aléatoires. Des attaques sur ces systèmes sont possibles lorsque la fonction booléenne est trop proche d'une fonction affine. On peut donc utiliser la transformée de Walsh rapide pour calculer les fonctions affines les plus proches d'une fonction booléenne donnée. La recherche de fonctions booléennes ayant de bonne propriétés cryptographiques, et la discussion sur ce que sont de bonne propriétés cryptographiques, est un domaine de recherches actuelles très actif.

Exercice: (Le générateur de Geffe:) Soit $f(x) = x_1x_2 + x_2x_3 + x_3$. Calculer par Walsh rapide $\mathcal{W}(f^*)$ et en déduire les fonctions affines les plus proches de f.

	000	001	010	011	100	101	110	111
f	0	1	0	0	0	1	1	1
f^*	1	-1	1	1	1	-1	-1	-1
	2	-2	0	0	0	0	2	2
	2	-2	2	-2	2	2	-2	-2
$\mathcal{W}(f^*)$	0	4	0	4	0	4	-4	0

On trouve $\max|\mathcal{W}(f^*)| = 4$ donc $d(f, \mathrm{Aff}) = 2^2 - 2 = 2$. De plus, $\mathcal{W}(f^*)(y) = 4$ pour $y = 001, 011, 101$, correspond à $d(f, X_3) = d(f, X_2 + X_3) = d(f, X_1 + X_3) = 2$ tandis que $\mathcal{W}(f^*)(110) = -4$ signifie $d(f, 1 + X_1 + X_2) = 2$. Il y a exactement quatre fonctions affines à distance 2 de f.

Chapter 5

Transformée de Fourier discrète

5.1 Définition

La transformée de Fourier discrète (DFT) est extrêmement utile en théorie du signal. C'est en fait une transformée de Fourier sur $\mathbb{Z}/N\mathbb{Z}$, et on peut en calculer les valeurs par un algorithme rapide (FFT) analogue à celui du chapitre précédent. Nous verrons en application comment calculer rapidement le produit de polynômes à coefficients complexes.

Nous notons $f = (f[0], f[1], \ldots, f[N-1])$ un N-uplet de nombres complexes, i.e. un élément de $\mathbb{C}^N$. Cette notation provient de la théorie du signal: un tel N-uplet peut être l'échantillonage d'une fonction $\tilde{f}$ de la variable réelle t, représentant en général le temps, définie sur un intervalle $[a, b]$; alors

$$f[k] = \tilde{f}(a + k\frac{b-a}{N}).$$

Définition 9 *Soit $w_N := e^{\frac{2i\pi}{N}}$. L'application DFT_N est définie par:*

$$\begin{aligned} \mathrm{DFT}_N : \mathbb{C}^N &\longrightarrow \mathbb{C}^N \\ f &\longmapsto \widehat{f} \end{aligned}$$

où:

$$\widehat{f}[k] = \sum_{n=0}^{N-1} f[n] w_N^{-nk}.$$

Faisons le lien avec la transformée de Fourier définie au Chapitre 3. Le groupe $G = \mathbb{Z}/N\mathbb{Z}$ a pour caractères les applications: χ_k définies par: $\chi_k(n \mod N) = w_N^{-nk}$. Notons encore f l'application de $\mathbb{Z}/N\mathbb{Z}$ dans $\mathbb{C}$ associée à $f = (f[0], \ldots, f[N-1])$, c'est-à-dire $f(k \mod N) = f[k]$. Alors il est clair que:

$$(\mathrm{DFT}_N f)[k] = (\mathcal{F}f)(\chi_k).$$

Pour cette raison, on note de la même façon: $\widehat{f} = \mathrm{DFT}_N f = \mathcal{F}f$. Attention toutefois à ne pas confondre ces applications...

Les résultats du Chapitre 3 s'applique en particulier à la transformée de Fourier discrète; ainsi, la formule d'inversion (Théorème 5) montre que DFT est inversible et que DFT^{-1} est encore une DFT, où on a remplacé w_N par w_N^{-1}. En termes matriciels, notons V_{w_N} la matrice de taille $N \times N$ définie par:

$$V_{w_N}[i,j] := w_N^{-(i-1)(j-1)} \text{ pour tout } 1 \leq i,j \leq N.$$

La matrice de DFT_N dans la base canonique de $\mathbb{C}^N$ est V_{w_N} et celle de DFT_N^{-1} est $\frac{1}{N} V_{w_N^{-1}}$. On a bien sûr:

$$V_{w_N} V_{w_N^{-1}} = N \,\mathrm{Id}_N\,.$$

La formule de Plancherel (Théorème 5) devient:

$$\sum_{k=0}^{N-1} f[k]\overline{g[k]} = \frac{1}{N} \sum_{k=0}^{N-1} \widehat{f}[k]\overline{\widehat{g}[k]}.$$

En termes matriciels, la matrice $\frac{1}{\sqrt{N}} V_{w_N}$ est unitaire.

5.2 Transformée de Fourier rapide (FFT)

Nous allons voir deux versions en quelque sorte duales de cet algorithme rapide: une version dite en décimation temporelle et l'autre en décimation fréquentielle. L'idée de base est toujours de couper en deux récursivement les intervalles d'entiers. Remarquons d'abord que le calcul élémentaire, en supposant connues les puissances successives de w_N, nécessite $2N$ opérations pour $\widehat{f}[k]$ et donc $2N^2$ opérations dans $\mathbb{C}$ en tout.

Nous allons supposer que $N = 2^p$ est une puissance de 2.

FFT en décimation temporelle: Dans l'expression pour $\widehat{f}[k]$, on sépare la somme suivant que n est pair ou non. Cela donne:

$$\begin{aligned}\widehat{f}[k] = \sum_{n=0}^{N-1} f[n] w_N^{-nk} &= \sum_{n=0}^{N/2-1} f[2n] w_N^{-2nk} + \sum_{n=0}^{N/2-1} f[2n+1] w_N^{-(2n+1)k} \\ &= \sum_{n=0}^{N/2-1} f[2n] w_{N/2}^{-nk} + w_N^{-k} \sum_{n=0}^{N/2-1} f[2n+1] w_{N/2}^{-nk}\end{aligned}$$

en remarquant que $w_N^2 = w_{N/2}$. On voit apparaître deux vecteurs de taille $N/2$:

$$\begin{cases} f_0 := (f[2n])_{0 \le n \le N/2-1} \\ f_1 := (f[2n+1])_{0 \le n \le N/2-1} \end{cases}$$

avec, pour $0 \le k \le N/2 - 1$:

$$\begin{cases} \widehat{f}[k] & = \widehat{f_0}[k] + w_N^{-k} \widehat{f_1}[k] \\ \widehat{f}[N/2+k] & = \widehat{f_0}[k] - w_N^{-k} \widehat{f_1}[k] \end{cases}$$

Attention à l'interprétation du chapeau: $\widehat{f} = \mathrm{DFT}_N(f)$ tandis que $\widehat{f_0} = \mathrm{DFT}_{N/2}(f_0)$, $\widehat{f_1} = \mathrm{DFT}_{N/2}(f_1)$. On voit que le calcul de $\widehat{f}$ est ramené au calcul de deux DFT de taille $N/2$. Comme pour la transformée de Walsh rapide, le temps de calcul $T(N)$ vérifie $T(N) = 2T(N/2) + 2N$ ce qui conduit à $T(N) = 2N \log(N)$.

Remarque 3 *Pour optimiser l'implémentation, il est préférable qu'à chaque étape, les vecteurs f_0 et f_1 soient les parties gauche et droite de f. Pour cela, on réordonne les $f[k]$ en inversant l'écriture binaire de k. Notons $b(k)$ l'écriture binaire de k et $\sigma(k)$ l'entier d'écriture binaire $\overline{b(k)}$ qui est le réciproque de $b(k)$. On change donc $f = (f[k])_{0 \le k \le N-1}$ en*
$f' = (f[\sigma(k)])_{0 \le k \le N-1}$.

Exemple: Prenons $f = (0, 2, -1, 0, 1, 0, 1, 1)$;

k	0	1	2	3	4	5	6	7
$b(k)$	000	001	010	011	100	101	110	111
$\overline{b(k)}$	000	100	010	110	001	101	011	111
$\sigma(k)$	0	4	2	6	1	5	3	7

k	0	1	2	3	4	5	6	7
f	0	2	-1	0	1	0	1	1
f'	0	1	-1	1	2	0	0	1

Remarquons que

$$(f'[k])_{0\leq k\leq N-1} = (f_{b(k)}[0])_{0\leq k\leq N-1}.$$

On peut donc calculer les valeurs de $\widehat{f_{00}}$, $\widehat{f_{01}}$, $\widehat{f_{10}}$, $\widehat{f_{11}}$, puis de $\widehat{f_0}$, $\widehat{f_1}$, puis de $\widehat{f}$.

k	0	1	2	3	4	5	6	7
$N=1$	$\widehat{f_{000}}[0]$	$\widehat{f_{001}}[0]$	$\widehat{f_{010}}[0]$	$\widehat{f_{011}}[0]$	$\widehat{f_{100}}[0]$	$\widehat{f_{101}}[0]$	$\widehat{f_{110}}[0]$	$\widehat{f_{111}}[0]$
	0	1	-1	1	2	0	0	1
$N=2$	$\widehat{f_{00}}[0]$	$\widehat{f_{00}}[1]$	$\widehat{f_{01}}[0]$	$\widehat{f_{01}}[1]$	$\widehat{f_{10}}[0]$	$\widehat{f_{10}}[1]$	$\widehat{f_{11}}[0]$	$\widehat{f_{11}}[1]$
	1	-1	0	-2	2	2	1	-1
$N=4$	$\widehat{f_0}[0]$	$\widehat{f_0}[1]$	$\widehat{f_0}[2]$	$\widehat{f_0}[3]$	$\widehat{f_1}[0]$	$\widehat{f_1}[1]$	$\widehat{f_1}[2]$	$\widehat{f_1}[3]$
	1	$-1+2i$	1	$-1-2i$	3	$2+i$	1	$2-i$
$N=8$	$\widehat{f}[0]$	$\widehat{f}[1]$	$\widehat{f}[2]$	$\widehat{f}[3]$	$\widehat{f}[4]$	$\widehat{f}[5]$	$\widehat{f}[6]$	$\widehat{f}[7]$
	4	$(-1+2i).$	$1-i$	$-(1+2i).$	-2	$(-1+2i).$	$1+i$	$-(1+2i).$
		$(1-iw_8^{-1})$		$(1+w_8^{-1})$		$(1-iw_8^{-1})$		$(1-w_8^{-1})$

FFT en décimation fréquentielle: Maintenant, on coupe en deux l'intervalle $[0, N-1]$ suivant l'ordre naturel. Notons f^0 et f^1 les deux parties de f, on a:

$$\begin{aligned}\widehat{f}[k] &= \sum_{n=0}^{N-1} f[n] w_N^{-nk} \\ &= \sum_{n=0}^{N/2-1} f^0[n] w_N^{-nk} + \sum_{n=0}^{N/2-1} f^1[n] w_N^{-(N/2+n)k} \\ &= \sum_{n=0}^{N/2-1} (f^0[n] + w_N^{-kN/2} f^1[n]) w_N^{-nk}\end{aligned}$$

soit, pour $0 \leq k \leq N/2-1$,

$$\begin{cases} \widehat{f}[2k] & = \sum_{n=0}^{N/2-1}(f^0[n]+f^1[n])w_{N/2}^{-nk} \\ \widehat{f}[2k+1] & = \sum_{n=0}^{N/2-1}(f^0[n]-f^1[n])w_N^{-n}w_{N/2}^{-nk} \end{cases}$$

On voit apparaître deux vecteurs de taille $N/2$:

$$\begin{cases} f^+ := (f^0[n]+f^1[n])_{0\le n\le N/2-1} \\ f^- := (w_N^{-n}(f^0[n]-f^1[n]))_{0\le n\le N/2-1} \end{cases}$$

avec

$$\begin{cases} \widehat{f}[2k] & = \widehat{f^+}[k] \\ \widehat{f}[2k+1] & = \widehat{f^-}[k] \end{cases}$$

et on est ramené au calcul de deux TFD de taille $N/2$. Le temps de calcul est le même que précédemment. Dans notre exemple cela donne:

k	0	1	2	3	4	5	6	7
8	$f[0]$	$f[1]$	$f[2]$	$f[3]$	$f[4]$	$f[5]$	$f[6]$	$f[7]$
	0	2	-1	0	1	0	1	1
4	$f^+[0]$	$f^+[1]$	$f^+[2]$	$f^+[3]$	$f^-[0]$	$f^-[1]$	$f^-[2]$	$f^-[3]$
	1	2	0	1	-1	$2w_8^{-1}$	$2i$	iw_8^{-1}
2	$f^{++}[0]$	$f^{++}[1]$	$f^{+-}[0]$	$f^{+-}[1]$	$f^{-+}[0]$	$f^{-+}[1]$	$f^{--}[0]$	$f^{--}[1]$
	1	3	1	$-i$	$-1+2i$	$(2+i)w_8^{-1}$	$-1-2i$	$-(1+2i)w_8^{-1}$
1	$f^{+++}[0]$	$f^{++-}[0]$	$f^{+-+}[0]$	$f^{+--}[0]$	$f^{-++}[0]$	$f^{-+-}[0]$	$f^{--+}[0]$	$f^{---}[0]$
	4	-2	$1-i$	$1+i$	$(-1+2i).$	$(-1+2i).$	$-(1+2i).$	$-(1+2i).$
					$(1+iw_8^{-1})$	$(1-iw_8^{-1})$	$(1+w_8^{-1})$	$(1-w_8^{-1})$

Il faut remarquer que la dernière ligne donne bien les valeurs de $\widehat{f}[k]$ mais dans le désordre. Plus précisément, on obtient le vecteur $(\widehat{f}(\sigma(k))_{0\le k\le N-1}$.

Dans le cas où N n'est pas une puissance de 2, on peut soit augmenter f par des 0 jusqu'à la prochaine puissance de 2, et se contenter d'un calcul approché de $\widehat{f}$, soit exploiter la factorisation de N: si $N=pq$ on peut découper l'intervalle en p morceaux de taille q, soit encore découper au plus près de la moitié au prix de complications dans l'algorithme.

5.3 Produit de convolution

Le produit de convolution de deux vecteurs f et g correspond au produit de convolution sur $\mathbb{Z}/N\mathbb{Z}$:

$$(f * g)[n] := \sum_{k=0}^{N} f[k]g[n-k]$$

où l'indice $n-k$ est vu modulo N. On peut l'écrire aussi:

$$(f * g)[n] := \sum_{\substack{0 \leq k,l \leq N \\ k+l=n \mod N}} f[k]g[l].$$

La propriété importante, déjà vue au Théorème 6 est:

$$\widehat{f * g}[n] = \widehat{f}[n]\widehat{g}[n], 0 \leq n \leq N-1$$

Le calcul de $\widehat{fg}$ à partir de $\widehat{f}$ et $\widehat{g}$ ne prend que N opérations complexes. Grâce au calcul rapide de la DFT et de son inverse, on peut donc calculer $f * g$ en $O(N \log N)$.

5.4 Application au calcul du produit de deux polynômes de $\mathbb{C}[x]$

Soit $P(x) = p_0 + p_1 x + \cdots + p_{N-1}x^{N-1}$ et $Q(x) = q_0 + q_1 x + \cdots + q_{N-1}x^{N-1}$ deux polynômes de $\mathbb{C}[x]$, de degré au plus égal à $N-1$. Leur produit $PQ = \sum r_k x^k$ a pour coefficients

$$r_k = \sum_{\substack{0 \leq i,j \leq N-1 \\ i+j=k}} p_i q_j.$$

On voit facilement que le calcul des coefficients r_k nécessite par ces formules un nombre d'opérations en $O(N^2)$.

Il est naturel d'associer à P et Q les vecteurs de $\mathbb{C}^N$ formés de leurs coordonnées. On les note respectivement p, q, de sorte que $p[i] = p_i$, $q[i] = q_i$. On aimerait que le produit des polynômes $P(x)Q(x)$ corresponde au produit de convolution $p * q$ dans $\mathbb{C}^N$. Ce n'est pas tout à fait vrai, sauf si on considère les polynômes *modulo* $x^N - 1$.

Proposition 11 *Soit $(p*q)(x)$ le polynôme de degré au plus égal à $N-1$, défini par*

$$(p*q)(x) = \sum_{k=0}^{N-1} (p*q)[k] x^k.$$

On a:

$$P(x)Q(x) = (p*q)(x) \mod x^N - 1.$$

En d'autres termes, l'application

$$\begin{aligned} \mathbb{C}^N &\longrightarrow \mathbb{C}[x]/(x^N-1)\mathbb{C}[x] \\ p &\longmapsto P = \sum_{i=0}^{N-1} p[i] x^i \end{aligned}$$

est un isomorphisme de $\mathbb{C}$-algèbres.

Preuve: Si $PQ = \sum_{k=0}^{2N-2} r_k x^k$, alors

$$PQ \mod x^N - 1 = \sum_{k=0}^{N-1} (\sum_{i=k \mod N} r_i) x^k.$$

$$\begin{aligned} \sum_{i=k \mod N} r_i &= \sum_{i=k \mod N} \sum_{0 \le l,j \le N-1 \atop l+j=i} p_l q_j \\ &= \sum_{0 \le l,j \le N-1 \atop l+j=k \mod N} p_l q_j \\ &= (p*q)[k]. \end{aligned}$$

□

Afin de récupérer exactement le produit PQ des polynômes P et Q, il suffit de choisir $N > \deg(P) + \deg(Q)$. En prenant pour N la plus petite puissance de 2 convenable, grâce au calcul de la convolution par FFT, on obtient

un algorithme de complexité $O(N\log(N))$, c'est-à-dire en $O(d\log(d))$, où $d = \max(\deg(P), \deg(Q))$.

Remarquons que la DFT, vue sur les polynômes de degré au plus égal à $N-1$, n'est autre que l'évaluation aux puissances de w_N:

$$\begin{aligned}\mathrm{DFT}_N(p)[k] &= \sum_{n=0}^{N-1} p[n] w_N^{-nk} \\ &= \sum_{n=0}^{N-1} p_n (w_N^{-k})^n = P(w_N^{-k})\end{aligned}$$

Chapter 6

DFT sur un anneau

Au chapitre précédent, on a pu accélérer la multiplication des polynômes à coefficients complexes grâce à la FFT. En fait la seule propriété de $\mathbb{C}$ que nous utilisons est que $\mathbb{C}$ contient les racines N-ièmes de l'unité. Afin d'obtenir un algorithme rapide de multiplication des polynômes dont les coefficients appartiennent à un anneau A quelconque, par exemple un corps fini, ou bien $\mathbb{Z}$, nous allons généraliser la DFT. C'est facile si l'anneau A contient des racines N-ièmes de 1 pour tout N; sinon, nous verrons comment Schönhage et Strassen contournent le problème, au prix d'un $\log\log(N)$ supplémentaire. Cela conduit aussi à un algorithme rapide pour la multiplication des entiers.

6.1 L'anneau A contient une racine primitive N-ième de l'unité

Définition 10 *Soit A un anneau commutatif (et unitaire). On dit que A contient une racine primitive N-ième de l'unité, s'il existe $w_N \in A$ tel que:*

1. $w_N^N = 1$
2. *Pour tout $l < N$, l divisant N, N/l premier, $w_N^l - 1$ n'est pas un diviseur de zéro de A.*

Exemple: $A = \mathbb{C}$, $A = \mathbb{F}_q$ et N divise $q - 1$.

Proposition 12 *Si w_N est une racine primitive N-ième de l'unité dans A, alors $w^l - 1$ n'est pas un diviseur de zéro dans A, pour tout $0 < l < N$. De plus, on a :*

$$\sum_{j=0}^{N-1} w_N^{lj} = 0.$$

Preuve: Remarquons d'abord que, si $w^a - 1$ n'est pas un divideur de zéro, alors $w^b - 1$ non plus dès que b divise a. En effet, cela découle de l'identité:

$$(w^a - 1) = (w^b - 1)(w^{b(a/b-1)} + w^{b(a/b-2)} + \cdots + w^b + 1).$$

Donc, la condition 2. implique que $w_N^l - 1$ n'est pas diviseur de 0 quel que soit l divisant N, $l < N$. Soit maintenant un entier $l < N$ ne divisant pas nécessairement N. Soit $d = \mathrm{pgcd}(l, N)$, et une relation de Bezout $d = lu + Nv$. On a $w_N^d = w_N^{lu}$. Comme d divise N, on sait que $w_N^d - 1$ n'est pas diviseur de zéro; donc $w_N^{lu} - 1$ n'est pas diviseur de zéro; mais l divise lu donc $w_N^l - 1$ n'est pas diviseur de zéro.

On a

$$(w_N^l - 1)(\sum_{j=0}^{N-1} w_N^{lj}) = w_N^{lN} - 1 = 0.$$

On conclut en utilisant le fait que $w_N^l - 1$ n'est pas diviseur de zéro.

□

On est en mesure de définir l'application DFT_N sur A, exactement comme sur $\mathbb{C}$.

Définition 11 *Supposons que l'anneau A contienne une racine primitive N-ième de l'unité w_N. L'application DFT_N est définie par:*

$$\begin{aligned} \mathrm{DFT}_N : A^N &\longrightarrow A^N \\ f &\longmapsto \widehat{f} \end{aligned}$$

où:

$$\widehat{f}[k] = \sum_{n=0}^{N-1} f[n] w_N^{-nk}.$$

Théorème 9 *Sous les mêmes hypothèses, l'application* DFT_N *est* A*-linéaire, et sa matrice dans la base canonique de* A^N *est* V_{w_N} *définie par:*

$$V_{w_N}[i,j] := w_N^{-(i-1)(j-1)} \text{ pour tout } 1 \leq i,j \leq N.$$

et vérifie: $V_{w_N} V_{w_N^{-1}} = N\,\mathrm{Id}_N$.

Le produit de convolution, défini sur A^N *par:*

$$(f * g)[k] = \sum_{\substack{0 \leq i,j \leq N-1 \\ i+j=k \mod N}} f[i]g[j]$$

vérifie:

$$\mathrm{DFT}_N(f * g) = \mathrm{DFT}_N(f)\,\mathrm{DFT}_N(g).$$

Preuve: Il suffit de reprendre les arguments invoqués sur $\mathbb{C}$. La démonstration de l'identité matricielle $V_{w_N} V_{w_N^{-1}} = N\,\mathrm{Id}_N$ utilise les identités de la Proposition 12:

$$\begin{aligned}(V_{w_N} V_{w_N^{-1}})[i,j] &= \sum_{k=1}^{N} V_{w_N}[i,k] V_{w_N^{-1}}[k,j] = \sum_{k=1}^{N} w_N^{-(i-1)(k-1)} w_N^{(k-1)(j-1)} \\ &= \sum_{k=1}^{N} w_N^{(j-i)(k-1)} = \begin{cases} N \text{ si } j-i = 0 \mod N \\ 0 \text{ si } j-i \neq 0 \mod N \end{cases}\end{aligned}$$

Calculons $\mathrm{DFT}_N(f * g)$.

$$\begin{aligned}\mathrm{DFT}_N(f * g)[k] &= \sum_{n=0}^{N-1} (f * g)[n] w_N^{-nk} = \sum_{n=0}^{N-1} \Big(\sum_{\substack{0 \leq i,j \leq N-1 \\ i+j=n \mod N}} f[i]g[j] w_N^{-nk} \Big) \\ &= \sum_{0 \leq i,j \leq N-1} f[i]g[j] w_N^{-(i+j)k} \\ &= \Big(\sum_{0 \leq i \leq N-1} f[i] w_N^{-ik} \Big) \Big(\sum_{0 \leq j \leq N-1} g[j] w_N^{-jk} \Big) \\ &= \mathrm{DFT}_N(f)[k]\,\mathrm{DFT}_N(g)[k].\end{aligned}$$

□

L'algorithme FFT fonctionne sur A exactement comme sur $\mathbb{C}$. Il permet de calculer $\mathrm{DFT}_N(f)$ en $O(N\log(N))$ opérations élémentaires de A. En particulier, on peut l'utiliser pour calculer le produit de deux polynômes de $A[X]$ dont la somme des degrés est au plus égale à N (plus exactement on récupère NPQ; il faut pouvoir divider par N dans A). En effet, on a toujours:

$$PQ = P * Q \mod (x^N - 1).$$

6.2 L'anneau A est quelconque

On ne suppose plus désormais que A contient des racines primitives de l'unité, mais seulement que 2 est inversible dans A (même cette hypothèse peut être relaxée..). Un algorithme, dû à Schönhage et Strassen (1971), permet de multiplier deux polynômes P et Q de $A[x]$ dont la somme des degrés est au plus égale à N en $O(N\log(N)\log\log(N))$ opérations; l'idée est de rajouter à A les racines N-ièmes manquantes, par passage au quotient; si on procède naivement, on perd en complexité. L'idée de SS est de rajouter *les racines $\sqrt{N}$-ièmes de l'unité* à A, comme on va le voir.

On suppose que N est une puissance de 2 et on pose $N = 2^k$. Soit $m \leq t$ deux entiers aussi proches que possible de $\sqrt{N}$ (si k est pair, $m = t = 2^{k/2}$; si k est impair, $m = 2^{(k-1)/2}$ et $t = 2^{(k+1)/2} = 2m$).

On définit des polynômes $P_0, \ldots, P_{t-1}$ et $Q_0, \ldots, Q_{t-1}$ de degrés inférieur à m tels que

$$P = \sum_{j<t} P_j(x)x^{mj},\ Q = \sum_{j<t} Q_j(x)x^{mj}.$$

On pose maintenant:

$$P' = \sum_{j<t} P_j(x)y^j,\ Q' = \sum_{j<t} Q_j(x)y^j$$

de sorte que $P(x) = P'(x, x^m)$, $Q(x) = Q'(x, x^m)$. Nous allons calculer le produit $P'Q'$. Les coefficients de $P'Q'$ sont des polynômes en x, de degré inférieur à $2m$, de sorte qu'il suffit de connaitre leur image dans

$$D := A[x]/(x^{2m} + 1)A[x].$$

Le degré en y de $P'Q'$ est $\deg_y(P'Q') < 2t \leq 4m$. D'autre part, D contient une racine primitive $4m$-ième de l'unité: en effet, soit $w := x \mod x^{2m} + 1$. On a $w^{2m} = -1$ et $w^{4m} = 1$. De plus, $w^{2m} - 1 = -2$ n'est pas un diviseur de zéro de D puisqu'on suppose 2 inversible dans A. On se retrouve donc dans la situation du paragraphe précédent, et on peut appliquer l'algorithme FFT pour calculer $P'Q'$ en $O(m \log(m))$ opérations dans D. Parmi ces opérations, les additions et multiplications par des puissances de x ne coutent que du $O(m)$, tandis que les "vrais" multiplications sont analogues à la multiplication de polynômes de $A[x]$ de degré inférieur à $2m$. Pour ces dernières, on peut appliquer récursivement FFT à l'ordre $2m \simeq \sqrt{N}$; il faut aussi estimer leur nombre. Une analyse plus fine conduit à une complexité totale en $O(N \log N \log\log N)$.

6.3 Le produit d'entiers

Pour se ramener à une situation analogue à celle des polynômes, on utilise la représentation des entiers dans une base b. Tout entier a s'écrit $a = a_0 + a_1 b + \cdots + a_N b^N$. Par exemple, si $b = 2^{64}$, cette écriture traduit la manipulation des entiers en multiprécision par un processeur en 64 bits. Chaque mot a_i est constitué de 64 bits.

La différence essentielle avec la manipulation des polynômes est la gestion des retenues. Sans entrer dans les détails, on peut adapter l'algorithme de multiplication des polynômes vu précédemment en un algorithme de multiplication des entiers de complexité $O(N \log N \log\log N)$.

La complexité est meilleure que celle de l'algorithme naîf, en $O(N^2)$, et aussi que l'algorithme de Karatsuba, en $O(N^{1.59})$ (vu en Licence). Toutefois, il faut bien avoir à l'esprit qu'il n'est plus rapide que ces derniers que pour des grandes valeurs de N..

Chapter 7

Autres applications

Dans ce chapitre nous présentons deux très jolis résultats, que l'on peut voir comme des applications de la transformée de Fourier sur un groupe abélien.

7.1 La loi de réciprocité quadratique

Ce célèbre résultat d'arithmétique fut démontré par Gauss en 1798 (à l'age de 18 ans), après avoir été énoncé par Legendre. Il en existe plus d'une centaine de preuve; celle que nous présentons ici utilise les sommes de Gauss et fait intervenir les caractères des deux groupes $(\mathbb{F}_p, +)$ et $(\mathbb{F}_p^*, \times)$.

Introduisons d'abord le symbole de Legendre:

Définition 12 *Soit p un nombre premier impair et a un entier quelconque. Le symbole de Legendre $\left(\frac{a}{p}\right)$ est défini par:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } p \text{ divise } a \\ 1 \text{ si } a \text{ est un carré modulo } p \\ -1 \text{ si } a \text{ n'est pas un carré modulo } p \end{cases}$$

Théorème 10 *Le symbole de Legendre a les propriétés suivantes:*

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

2. $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$

3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ *et* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Preuve: L'application de $\mathbb{F}_p^*$ dans $\mathbb{F}_p^*$, qui à x associe x^2, est un homomorphisme de groupes. Son noyau est $\{x \in \mathbb{F}_p^* \mid x^2 = 1\} = \{\pm 1\}$ (car $\mathbb{F}_p$ est un corps..). Son image est donc un sous-groupe de $\mathbb{F}_p^*$ d'ordre $(p-1)/2$. Comme $\mathbb{F}_p^*$ est cyclique, c'est l'unique sous-groupe d'ordre $(p-1)/2$, et un élément $y \in \mathbb{F}_p^*$ appartient à ce sous-groupe si et seulement si $y^{\frac{p-1}{2}} = 1$. Remarquer que, comme $y^{p-1} = 1$, dans le cas contraire, on a $y^{\frac{p-1}{2}} = -1$. Cela démontre le point 2. et le point 1. Également, 3. résulte de 2.

Il reste le calcul de $\left(\frac{2}{p}\right)$. Soit α une racine primitive 8-ième de l'unité dans une clôture algébrique de $\mathbb{F}_p$. Soit $y := \alpha + \alpha^{-1}$. On a $y^2 = 2 + \alpha^2 + \alpha^{-2}$. Mais $\alpha^4 = -1$, donc $\alpha^2(\alpha^2 + \alpha^{-2}) = 0$, donc $y^2 = 2$. Il faut maintenant discuter si $\pm y$ appartient à $\mathbb{F}_p$. On a $y^p = \alpha^p + \alpha^{-p}$. Si $p \equiv \pm 1 \mod 8$, alors $y^p = y$, alors que, si $p \equiv \pm 5 \mod 8$, $y^p = -y$. D'où le résultat.

□

Le symbole de Legendre définit donc un *caractère quadratique* η sur $\mathbb{F}_p^*$: $\eta(x) = \left(\frac{x}{p}\right)$. Nous sommes maintenant en mesure d'énoncer la loi de réciprocité quadratique:

Théorème 11 *[Loi de réciprocité quadratique] Soit p, q deux nombres premiers impairs. Alors:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \tag{7.1}$$

Avant de nous lancer dans la démonstration, regardons comment on peut utiliser cette identité. Supposons que l'on veuille déterminer si 219 est un carré modulo 383. Suivant la formule, on calcule:

$$\begin{aligned}\left(\frac{219}{383}\right) &= \left(\frac{3}{383}\right)\left(\frac{73}{383}\right) = -\left(\frac{383}{3}\right)\left(\frac{383}{73}\right) \\ &= -\left(\frac{-1}{3}\right)\left(\frac{18}{73}\right) = -\left(\frac{-1}{3}\right)\left(\frac{2}{73}\right) = 1\end{aligned}$$

D'autre part, le symbole de Legendre se généralise au symbole de Jacobi $\left(\frac{a}{b}\right)$ pour des entiers a, b avec b impair. La formule (7.1) reste vraie lorsque a et b sont impairs et premiers entre eux. En particulier, cela permet d'éviter la factorisation des nombres apparaissant dans les calculs intermédiaires du symbole de Legendre!

Pour démontrer ce théorème, nous introduisons les *sommes de Gauss*. Celles-ci relient les caractères additifs et multiplicatifs sur $\mathbb{F}_p$.

Définition 13 *Soit ψ un caractère de $(\mathbb{F}_p, +)$ et soit χ un caractère de $(\mathbb{F}_p^*, \times)$. La somme de Gauss associée à ψ et χ est:*

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

Remarquons que, en termes de transformée de Fourier, on peut interpréter $G(\chi, \psi)$ soit comme la transformée de Fourier sur le groupe $\mathbb{F}_p^*$ de $f := \tilde{\psi}$, où $\tilde{\psi}$ est la restriction de ψ à $\mathbb{F}_p^*$, soit comme la transformée de Fourier sur le groupe $\mathbb{F}_p$ de $f := \tilde{\chi}$, où $\tilde{\chi}$ est le prolongement de χ à $\mathbb{F}_p$, par $\tilde{\chi}(0) = 0$

Les caractères de $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ se décrivent comme d'habitude: on note ψ_m le caractère défini par $\psi_m(x) = w_p^{mx}$, où w_p est une racine primitive p-ième de 1 dans $\mathbb{C}$, par exemple $w_p = e^{2i\pi/p}$.

Parmi les (nombreuses) propriétés des sommes de Gauss, nous aurons besoin de:

Lemme 2 *Les sommes de Gauss ont les propriétés suivantes:*

1. $G(\chi, \psi_{mn}) = \overline{\chi(m)}G(\chi, \psi_n)$*, pour tout* $1 \leq m \leq p-1$.
2. $G(\chi, \psi)G(\overline{\chi}, \psi) = \chi(-1)p$*, pour tout* $\chi \neq 1$, $\psi \neq 1$.

Preuve: Calculons:

$$\begin{aligned} G(\chi, \psi_{mn}) &= \sum_{x \in \mathbb{F}_p^*} \chi(x) w_p^{mnx} = \sum_{x \in \mathbb{F}_p^*} \chi(x)\psi_n(mx) \\ &= \sum_{y \in \mathbb{F}_p^*} \chi(m^{-1}y)\psi_n(y) = \sum_{y \in \mathbb{F}_p^*} \chi(m^{-1})\chi(y)\psi_n(y) \\ &= \overline{\chi(m)} \sum_{y \in \mathbb{F}_p^*} \chi(y)\psi_n(y) = \overline{\chi(m)}G(\chi, \psi_n). \end{aligned}$$

d'où la première identité.

$$\begin{aligned} G(\chi,\psi)G(\overline{\chi},\psi) &= (\sum_{x\in\mathbb{F}_p^*}\chi(x)\psi(x))(\sum_{x\in\mathbb{F}_p^*}\overline{\chi(x)}\psi(x)) \\ &= \sum_{x,y\in\mathbb{F}_p^*}\chi(xy^{-1})\psi(x)\psi(y) \\ &= \sum_{z\in\mathbb{F}_p^*}\chi(z)(\sum_{y\in\mathbb{F}_p^*}\psi(zy)\psi(y)) \end{aligned}$$

L'application $\psi_z : y \to \psi(zy)$ est une caractère additif. On peut donc utiliser les relations d'orthogonalité entre ψ_z et $\overline{\psi}$. On voit facilement que, comme $\psi \neq 1$, $\psi_z = \overline{\psi} \Leftrightarrow z = -1$. Donc, en vertu de la Proposition 7:

$$\sum_{y\in\mathbb{F}_p}\psi(zy)\psi(y) = \begin{cases} p \text{ si } z=-1 \\ 0 \text{ sinon.} \end{cases}$$

donc

$$\sum_{y\in\mathbb{F}_p^*}\psi(zy)\psi(y) = \begin{cases} p-1 \text{ si } z=-1 \\ -1 \text{ sinon.} \end{cases}$$

et

$$G(\chi,\psi)G(\overline{\chi},\psi) = \chi(-1)(p-1) - \sum_{z\in\mathbb{F}_p^*, z\neq -1}\chi(z)$$

à nouveau, on applique les relations d'orthogonalité, cette fois-ci relatives au groupe $\mathbb{F}_p^*$, en tenant compte de l'hypothèse $\chi \neq 1$:

$$G(\chi,\psi)G(\overline{\chi},\psi) = \chi(-1)(p-1) - (-\chi(-1)) = \chi(-1)p.$$

□

Lemme 3 $G(\eta,\psi_1)^2 = (-1)^{\frac{p-1}{2}}p$.

Preuve: Le caractère multiplication η est réel, et $\eta(-1) = (-1)^{\frac{p-1}{2}}$, donc le résultat suit du lemme précédent. □

Nous sommes maintenant en mesure de démontrer le théorème 11. Pour cela, posons $G := G(\eta, \psi_1)$; on calcule G^q modulo q. Notons que G appartient à l'anneau $\mathbb{Z}[w_p] = \mathbb{Z} + \mathbb{Z}w_p + \mathbb{Z}w_p^2 + \cdots + \mathbb{Z}w_p^{p-2}$.

$$\begin{aligned} G^q &= (\sum_{x\in\mathbb{F}_p^*} \eta(x)\psi_1(x))^q = \sum_{x\in\mathbb{F}_p^*} \eta(x)^q\psi_1(x)^q \mod q \\ &= \sum_{x\in\mathbb{F}_p^*} \eta(x)\psi_q(x) = G(\eta,\psi_q) \mod q \\ &= \eta(q)G(\eta,\psi_1) = \eta(q)G \mod q \end{aligned}$$

où, dans la dernière ligne, on utilise le Lemme 2(1.). Ensuite, on écrit:

$$G^q = (G^2)^{\frac{q-1}{2}}G = ((-1)^{\frac{p-1}{2}}p)^{\frac{q-1}{2}}G$$

grâce au Lemme 3, et donc,

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}G = \eta(q)G \mod q$$

On peut multiplier par G pour à nouveau utiliser $G^2 = (-1)^{\frac{p-1}{2}}p$; comme p et q sont premiers entre eux, on peut diviser par $p \mod q$ pour obtenir:

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}} = \eta(q) \mod q.$$

Maintenant, les deux termes de l'égalité appartiennent à $\mathbb{Z}$; leur différence appartient donc à $q\mathbb{Z}[w_p]\cap\mathbb{Z} = q\mathbb{Z}$. Autrement dit, on a bien une relation de congruence dans $\mathbb{Z}$. En utilisant le Théorème 10(2.), on obtient:

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

et, comme chaque terme est maintenant un ± 1, on peut conclure:

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

7.2 La formule de Jessie MacWilliams

La formule de MacWilliams relie la distribution des poids d'un code et de son dual. Elle est à la base de l'étude des codes autoduaux, et aussi d'une très jolie méthode permettant d'obtenir des bornes pour le cardinal des codes à distance minimal donnée, et plus généralement pour des problèmes d'empilement de sphères..

On rappelle qu'un code linéaire C (sur $\mathbb{F}_q$, de longueur n), est un sous-espace vectoriel de $\mathbb{F}_q^n$. On note pour tout $u, v \in \mathbb{F}_q^n$,

$$u \cdot v = \sum_{i=1}^{n} u_i v_i.$$

Le code dual de C, noté $C^\perp$, est l'orthogonal de C pour ce produit scalaire:

$$C^\perp := \{v \in \mathbb{F}_q^n \mid u \cdot v = 0 \text{ pour tout } u \in C\}.$$

On rappelle que, si C est de dimension k, alors $C^\perp$ est de dimension $n - k$. D'autre part, le poids de Hamming $wt(u)$ d'un élément u de $\mathbb{F}_q^n$ est comme d'habitude le nombre de ses coordonées non nulles.

Définition 14 *La* distribution des poids *d'un code C linéaire est le n-uplet $(A_0, A_1, \ldots, A_n)$, où A_i est égal au nombre des mots de C de poids i.*

$$A_i = \text{card}\{u \in C \mid wt(u) = i\}.$$

En particulier, $A_0 = 1$ et $\sum_i A_i = q^k$, où k est la dimension de C.

La formule de MacWilliams est une formule qui relie la distribution des poids $(A_0, A_1, \ldots, A_n)$ de C et celle, notons-la $(B_0, B_1, \ldots, B_n)$, de $C^\perp$. En particulier, si on connait l'une alors on connait l'autre. Pour manipuler aisément cette distribution des poids, on définit le polynôme énumérateur des poids de C; c'est un polynôme homogène à deux variables.

Définition 15 *Le* polynôme énumérateur des poids *d'un code C de longueur n sur $\mathbb{F}_q$ est le polynôme homogène en deux variables x et y, de degré n, défini par:*

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)}.$$

Théorème 12 *(Formule de MacWilliams)*

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+(q-1)y, x-y).$$

Preuve: C'est une conséquence de la formule de Poisson! Pour simplifier la démonstration, on va supposer que $\mathbb{F}_q = \mathbb{F}_2$. Rappelons que les caractères de $\mathbb{F}_2^n$ sont les χ_y, définis par $\chi_y(x) = (-1)^{x\cdot y}$. pour $f : \mathbb{F}_2^n \to \mathbb{C}$, on a dfini $\hat{f}$ par

$$\hat{f}(x) = \sum_{y\in\mathbb{F}_2^n} f(y)(-1)^{x\cdot y}.$$

La formule de Poisson devient: pour tout sous-groupe (i.e. code!) $C \subset \mathbb{F}_2^n$,

$$\sum_{u\in C^\perp} f(u) = \frac{1}{|C|} \sum_{v\in C} \hat{f}(v).$$

On la généralise facilement au cas où f est à valeurs dans un $\mathbb{C}$-espace vectoriel E de dimension finie. En effet, il suffit de l'appliquer aux coordonnées de f sur une base fixée de E.

Dans notre situation, on prend pour E le $\mathbb{C}$-espace vectoriel des polynômes en x, y, homogènes de degré n. C'est un espace vectoriel de dimension $n+1$ (de base $x^n, x^{n-1}y, \ldots, y^n$). On pose $f(u) = x^{n-wt(u)}y^{wt(u)}$. Il faut calculer $\hat{f}$.

$$\begin{aligned}
\hat{f}(v) &= \sum_{u\in\mathbb{F}_2^n} x^{n-wt(u)}y^{wt(u)}(-1)^{v\cdot u} \\
&= \sum_{u\in\mathbb{F}_2^n} \prod_{i=1}^{n} (-1)^{v_i u_i} x^{1-wt(u_i)} y^{wt(u_i)} \\
&= \prod_{i=1}^{n} (x + (-1)^{v_i} y) \\
&= (x+y)^{n-wt(v)}(x-y)^{wt(v)}.
\end{aligned}$$

Alors, la formule de Poisson pour f devient exactement la formule de MacWilliams.

□

Exemple: On a vu dans le DM2 que le code $H(q,r)^\perp$ est un code dont tous les mots non nuls sont de poids q^{r-1}. Son polynôme énumérateur des poids est donc

$$W_{H(q,r)^\perp}(x,y) = x^n + (q^r-1)x^{n-q^{r-1}}y^{q^{r-1}}.$$

La formule de MacWilliams nous permet donc de calculer $W_H(q,r)$:

$$W_{H(q,r)}(x,y) = \frac{1}{q^r}\Big((x+(q-1)y)^n + (q^r-1)(x+(q-1)y)^{n-q^{r-1}}(x-y)^{q^{r-1}}\Big).$$

Pour $q=2$, on obtient:

$$W_{H(2,r)}(x,y) = \frac{1}{2^r}(x+y)^{2^{r-1}-1}\left((x+y)^{2^{r-1}} + (2^r-1)(x-y)^{2^{r-1}}\right)$$

et, pour $q=2$ et $r=3$,

$$W_{H(2,3)}(x,y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7.$$

Chapter 8

Représentations linéaires des groupes finis

8.1 Les représentations linéaires d'un groupe fini G

Soit G un groupe fini, non nécessairement commutatif. Les caractères de G au sens du Chapitre 3 peuvent être très rares. En effet, il y a toujours le caractère trivial, mais il peut être le seul, si par exemple G est simple, i.e. ne contient pas de sous-groupe distingué. (En effet, $\ker(\chi)$ est un sous-groupe distingué de G; par exemple, A_n est simple pour $n \geq 5$, ainsi que $PSL(n, \mathbb{F}_q)$, sauf exceptions..). Nous allons dans ce chapitre étendre la notion de caractère d'un groupe.

Définition 16 *Une représentation d'un groupe G est la donnée d'un $\mathbb{C}$-espace vectoriel V et d'un homomorphisme ρ:*

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

On dit que la représentation est fidèle si ρ est injective. La dimension de V s'appelle le degré de ρ.

Exemple: $V = \mathbb{C}$; $GL(V) = \mathbb{C}^*$ et $\rho = \chi$ un caractère de G au sens du Chapitre 3. Ainsi, les représentations de degré 1 sont les caractères (on dira désormais multiplicatifs) de G.

Exemple: $G = S_3$. La signature fournit un caractère multiplicatif, i.e. une représentation de degré 1 de S_3. Il y a aussi une représentation de degré 2 donnée par le groupe des isométries du triangle.

Remarquer que, si on choisit une base de V, cela revient à "voir" G comme un sous-groupe de matrices complexes. Si on change de bases, on va changer les matrices - en fait on va toutes les conjuguer par la matrice de changement de base - mais on dira que les représentations sont équivalentes.

Définition 17 *Deux représentations $\rho : G \to GL(V)$ et $\rho' : G \to GL(V')$ sont dites équivalentes (ou isomorphes) s'il existe un isomorphisme de $\mathbb{C}$-espaces vectoriels $f : V \to V'$ tel que, pour tout $g \in G$, $\rho'(g) \circ f = f \circ \rho(g)$.*

On va chercher à classifier les représentations d'un même groupe G; nous allons voir qu'elles sont fabriquées à partir de briques élémentaires qui sont les représentations irréductibles.

Le point de vue algèbre de groupe: on a déjà parlé de l'algèbre de groupes $\mathbb{C}[G]$. C'est l'algèbre des fonctions de G dans $\mathbb{C}$, muni de l'addition et de la convolution des fonctions. Comme $\delta_g * \delta_h = \delta_{gh}$, on notera désormais un élément $f = \sum_{g\in G} f(g)\delta_g = \sum_{g\in G} f(g)g$.

Se donner une représentation (ρ, V) de G, c'est la même chose que de se donner un $\mathbb{C}[G]$-module V. En effet, on peut définir à partir de (ρ, V), une structure de $\mathbb{C}[G]$-module sur V par : $f.v := \sum_{g\in G} f(g)\rho(g)(v)$. Réciproquement, si V est un $\mathbb{C}[G]$-module, on peut définir une représentation ρ de G par: $\rho(g)(v) = g.v$. Pour alléger les notations, on remplacera souvent $\rho(g)(v)$ par la notation $g.v$; il faut alors faire attention à savoir de quelle représentation on parle. Remarquons que la notion de représentations équivalentes correspond à des structures de $\mathbb{C}[G]$-modules isomorphes.

Exemple: $V = \mathbb{C}[G]$ définit lui-même une représentation de G, de degré $|G|$, en associant à $g \in G$ la multiplication par g, vue comme une transformation linéaire de V. C'est la représentation régulière de G. Remarquons que, dans la base usuelle des g, les matrices associées aux éléments de G sont des matrices de permutation.

Définition 18 *La somme de deux représentations $\rho : G \to GL(V)$ et $\rho' : G \to GL(V')$ est la représentation ρ'' sur l'espace $V \oplus V'$ définie par $\rho''(g)(v, v') = (\rho(g)(v), \rho'(g)(v'))$.*

Un sous-espace W de V est appelé une sous-représentation de (ρ, V), si, pour tout $g \in G$, $\rho(g)(W) \subset W$. Alors W définit une représentation de G par restriction.

On dit que la représentation (ρ, V) est irréductible (ou indécomposable) si elle n'a pas de sous-représentation autre que $\{0\}$ et elle-même.

Théorème 13 *Si (ρ, V) est réductible, i.e. si elle contient une sous-représentation W non triviale, alors il existe un supplémentaire W' de W qui est une sous-représentation de la représentation (ρ, V). La représentation (ρ, V) est alors la somme des deux représentations de G définies par W et W'.*

Toute représentation se décompose en une somme directe de représentations irréductibles.

Preuve: Pour construire un supplémentaire de W stable, il nous faut un produit hermitien G-stable. On pourra alors prendre pour W' le supplémentaire orthogonal de W.

On choisit arbitrairement un produit hermitien $h_0(x, y)$ sur V; puis on pose

$$h(x, y) := \frac{1}{|G|} \sum_{g \in G} h_0(g.x, g.y).$$

Clairement, h est une forme hermitienne, définie positive, et invariante par $\rho(G)$. Le groupe G agit donc via ρ par des transformations unitaires, et stabilise $W^{\perp}$.

Le fait que toute représentation se décompose en une somme directe de représentations irréductibles se démontre facilement par récurrence, compte tenu de ce qui précède. □

Les opérateurs d'entrelacement entre deux espaces de représentations sont les transformations linéaires qui commutent à l'action de G.

Théorème 14 *(Lemme de Schur) Soit $\mathrm{Hom}_G(V, W)$ le $\mathbb{C}$-espace vectoriel des applications linéaires $f : V \to W$ qui commutent aux actions de G, i.e. vérifient: $f(g.v) = g.f(v)$ (attention à l'interprétation des .: l'un correspnd à la représentation V l'autre à W). Supposons V et W irréductibles. Alors, si elles ne sont pas isomorphes, $\mathrm{Hom}_G(V, W) = \{0\}$, et si elles sont isomorphes, $\mathrm{Hom}_G(V, W)$ est de dimension* 1.

Preuve: Soit $f \in \mathrm{Hom}_G(V, W)$. Son noyau $\ker f$ est un sous-espace de V, stable par G (i.e. une sous-représentation de V). Donc, si V est irréductible, il n'y a que deux possibilités: $\ker f = V$ ou $\ker f = \{0\}$. Dans ce dernier cas, $\mathrm{Im}\, f$ est une sous-représentation de W, isomorphe à V. Si W est irréductible, ce n'est possible que si $V \simeq W$.

Supposons maintenant que $V \simeq W$. On peut donc supposer $V = W$. Soit $f : V \to V$; par les mêmes arguments, f est injective si non nulle. Comme le corps de base est $\mathbb{C}$, f possède une valeur propre λ; l'espace propre associé $\ker(f - \lambda \operatorname{Id})$ est non réduit à 0, et G-stable. Donc, si V est irréductible, c'est V tout entier. Donc $f = \lambda \operatorname{Id}$ et $\operatorname{Hom}_G(V, V)$ est de dimension 1.

□

8.2 Les caractères d'un groupe fini G

Pour étudier les représentations irréductibles d'un groupe fini, et plus généralement la décomposition d'une représentation donnée, on se ramène en fait à des fonctions à valeurs dans $\mathbb{C}$: les caractères.

Définition 19 *Le caractère χ, ou χ_ρ d'une représentation $\rho : G \to GL(V)$ est la fonction*

$$\begin{aligned} \chi : G &\longrightarrow \mathbb{C} \\ g &\longmapsto \chi(g) := \operatorname{trace}(\rho(g)) \end{aligned}$$

Exemple: Le caractère d'une représentation de degré 1 est elle-même. Attention, en général, le caractère d'une représentation de degré plus grand que 1 n'est pas une application multiplicative, car en général $\operatorname{trace}(AB) \neq \operatorname{trace}(A)\operatorname{trace}(B)$!

Le caractère de la représentation régulière, notée r_G, est donné par:

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

En effet, la multiplication par $g \neq 1$ est une permutation sans point fixe de G.

Proposition 13 *Les propriétés suivantes sont vraies pour tout caractère χ de G:*

1. $\chi(1) = \deg(\rho)$.
2. $\chi(g^{-1}) = \overline{\chi(g)}$ *pour tout* $g \in G$.
3. $\chi(hgh^{-1}) = \chi(g)$ *pour tout* $g, h \in G$ *(on dit que χ est une fonction centrale).*

4. $\chi_{\rho\oplus\rho'} = \chi_\rho + \chi_{\rho'}$.

5. *Deux représentations équivalentes ont même caractère.*

Preuve:

1. $\chi(1) = \mathrm{trace}(\mathrm{Id}_V) = \dim(V)$.

2. Il existe une forme hermitienne sur V invariante par G; dans une base orthonormée les matrices donnant l'action de G sont unitaires donc vérifient $M^{-1} = \overline{M}^t$. Donc $\mathrm{trace}(M^{-1}) = \mathrm{trace}(\overline{M})$.

3. Résulte de la propriété $\mathrm{trace}(AB) = \mathrm{trace}(BA)$.

4. Dans une base adaptée, les matrices donnant l'action de G sur $V \oplus V'$ sont "par blocs" $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$ et la trace est la somme des traces des blocs.

5. C'est la même chose que 3.

□

On va voir que la propriété 5. a une réciproque: deux représentations qui ont même caractère sont isomorphes. C'est l'un des résultats les plus importants de ce chapitre.

Comme dans les chapitres précédents, on munit l'espace $\mathbb{C}[G]$ des fonctions $f : G \to \mathbb{C}$ d'un produit hermitien $< f_1, f_2 >$ défini par:

$$< f_1, f_2 >= \frac{1}{|G|} \sum_{g\in G} f_1(g)\overline{f_2(g)}.$$

Dans le cas des groupes commutatifs, les caractères (multiplicatifs) de G formaient une base orthonormée de cet espace hermitien. Nous allons voir que, dans le cas général, les caractères des représentations irréductibles de G forment une base orthonormée du sous-espace des fonctions centrales.

Définition 20 *On dit que $f : G \to \mathbb{C}$ est une fonction centrale, si $f(hgh^{-1}) = f(g)$ pour tout $g, h \in G$. En d'autre termes, f est constante sur les classes de conjugaison de G.*

Théorème 15 *(Relations d'orthogonalité des caractères irréductibles) Soit χ et χ' les caractères associés à deux représentations ρ, ρ' irréductibles de G. On a:*

$$< \chi, \chi' >= \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi'(g)} = \begin{cases} 1 \textit{ si } \rho \textit{ et } \rho' \textit{ sont isomorphes} \\ 0 \textit{ sinon} \end{cases}$$

Preuve: Soit V et V' les espaces des représentations ρ et ρ'. Nous allons utiliser le Lemme de Schur, et pour cela interpréter $< \chi, \chi' >$ comme la dimension de l'espace $\mathrm{Hom}_G(V, V')$.

L'espace $\mathrm{Hom}(V, V')$ est aussi une représentation de G. En effet, si $\phi \in \mathrm{Hom}(V, V')$, on définit $g.\phi$ par: $(g.\phi)(v) = g.\phi(g^{-1}.v)$ (qui signifie plus précisément $\rho'(g)(\phi(\rho(g^{-1})(v)))$). Notons ψ son caractère. Remarquons que $g.\phi = \phi$ signifie que $\phi \in \mathrm{Hom}_G(V, V')$.

Étant donnée une représentation W quelconque de G, on voit facilement que le sous-espace $W^G := \{x \in W \mid g.x = x \text{ pour tout } g \in G\}$ vérifie

$$W^G = P(W),$$

où P est l'endomorphisme $P = \frac{1}{|G|} \sum_{g \in G} g$ opérant sur W. Celui-ci est une projection car $P^2 = P$. Comme toutes les projections, $\mathrm{trace}(P) = \dim(\mathrm{Im}(P)) = \dim(W^G)$.

Revenons à la représentation de G définie sur $\mathrm{Hom}(V, V')$. D'après ce qui précède,

$$\dim \mathrm{Hom}_G(V, V') = \frac{1}{|G|} \sum_{g \in G} \psi(g).$$

Il nous reste à montrer que $\psi(g) = \overline{\chi(g)}\chi'(g)$. Le plus facile est de faire un calcul matriciel. Notons $e_1, \ldots, e_n$ une base de V orthonormée, dans laquelle $\rho(g)$ a pour matrice $A = (a_{i,j})_{1 \leq i,j \leq n}$. Notons $f_1, \ldots, f_m$ une base de V' orthonormée, dans laquelle $\rho'(g)$ a pour matrice $B = (b_{k,l})_{1 \leq k,l \leq m}$. Alors on obtient une base naturelle de $\mathrm{Hom}(V, V')$, indexée sur $I := \{(i, k) \mid 1 \leq i \leq n, 1 \leq k \leq m\}$, en posant: $E_{(i,k)}(v) = v_i f_k$ (avec les notations usuelles: $v = \sum_{i=1}^n v_i e_i$). On vérifie que, dans la base des $E_{(i,k)}$, l'action de g sur $\mathrm{Hom}(V, V')$ a pour matrice:

$$(\overline{a_{j,i}} b_{k,l})_{(i,k),(j,l) \in I}.$$

La trace de cette matrice, obtenue en sommant les termes diagonaux, i.e. ceux des coefficients associés à $(i, k) = (j, l)$, est:

$$\psi(g) = \sum_{(i,k)\in I} \overline{a_{i,i}} b_{k,k} = (\sum_{1\le i\le n} \overline{a_{i,i}})(\sum_{1\le k\le m} b_{k,k}) = \overline{\chi(g)}\chi'(g).$$

□

Corollaire 2 *On a:*

1. *Si $V = \oplus_i V_i^{n_i}$ avec V_i irréductible, de caractère χ_i, et les représentations V_i sont deux à deux non isomorphes, alors*
$$\chi = \sum_i n_i\chi_i,\ n_i =< \chi, \chi_i >,\ \textit{et}\ < \chi, \chi >= \sum n_i^2.$$
2. *La représentation de caractère χ est irréductible, si et seulement si $< \chi, \chi >= 1$. De plus, si deux représentations ont le même caractère alors elles sont isomorphes.*
3. *Le caractère r_G de la représentation régulière se décompose suivant:*
$$r_G = \sum \dim(\chi)\chi$$
où la somme porte sur l'ensemble des caractères des représentations irréductibles de G. En particulier,
$$|G| = \sum \dim(\chi)^2.$$

Preuve: Si $V = \oplus_i V_i^{n_i}$, il est clair que $\chi = \sum_i n_i\chi_i$. Si les V_i sont irréductibles et deux à deux non isomorphes, on a $< \chi_i, \chi_j >= \delta_{i,j}$, d'où $n_i =< \chi, \chi_i >$. Il suit que $< \chi, \chi >= \sum n_i^2$.

De la relation $< \chi, \chi >= \sum n_i^2$ on déduit que, si $< \chi, \chi >= 1$, alors un seul des n_i est non nul et vaut 1. Donc V est irréductible.

Si $\chi = \chi'$, alors $< \chi, \chi_i >=< \chi', \chi_i >$ donc, d'après ce qui précéde, $n_i = n_i'$ et les représentations associées sont équivalentes.

On applique ce qui précède à r_G; mais
$$< r_G, \chi >= \frac{1}{|G|}\sum_{g\in G} r_G(g)\overline{\chi(g)} = \overline{\chi(1)} = \dim(\chi).$$

En comparant les dimensions, on obtient
$$|G| = \sum \dim(\chi)^2.$$

□

Remarque 4 *La dernière formule, pour un groupe G abélien, exprime que G a exactement $|G|$ caractères multiplicatifs ($|G| = 1^2 + 1^2 + \cdots + 1^2$).*

Exemple: S_3: on connait deux représentations de degré 1, la triviale et la signature. On a aussi une représentation, clairement irréductible, de degré 2, donnée par le groupe des isométries du triangle. Comme $6 = 2^2 + 1^2 + 1^2$, le groupe S_3 n'a pas d'autres représentations irréductibles.

A_4: Le groupe A_4 a un sous-groupe distingué K d'ordre 4:
$K = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Les trois représentations de degré 1 de $A_4/K \simeq \mathbb{Z}/3\mathbb{Z}$ se relèvent en trois représentations de degré 1 de A_4. Le groupe des isométries positives du tétraèdre régulier fournit une représentation irréductible de degré 3 de A_4. Comme $12 = 3^2 + 1^2 + 1^2 + 1^2$, on les a toutes.

S_4: Ce groupe a un seul sous-groupe distingué K. Le quotient S_4/K est isomorphe à S_3. On peut ainsi relever la représentation de degré 2 de S_3. Outre la représentation triviale et la signature qui sont de degré 1, S_4 a deux représentations irréductibles de degré 3, qui sont données par le groupe des isométries du tétraèdre régulier (opérant sur ses sommets) et le groupe des isométries positives du cube, opérant sur les quatre diagonales.

On peut montrer que les caractères des représentations irréductibles de G forment une base de l'espace des fonctions centrales. Celui-ci a une base naturelle, bijectivement associée à l'ensemble des classes de conjugaison de G. Un groupe G a donc autant de représentations irréductibles que de classes de conjugaison, sans qu'il y ait une correspondance naturelle entre ces deux ensembles. Sauf pour le groupe symétrique..