

ESTIA 2^e Année TRANSFORMEES
Edition 2006
Conforme au nouveau programme 2006
(version incomplète)

J.ESTERLE¹

7 septembre 2007

¹I.Harlouchet-en eskuhartzearekin

Remarque préliminaire

La version initiale de ce cours, enseigné à l'ESTIA depuis la rentrée 1998, se limitait aux quatre premiers chapitres. Suite à une demande de la Direction des Etudes de l'ESTIA, le Chapitre 5 (Transformée en Z) a été introduit à la rentrée 2005.

Le volume horaire du module "Transformées" ayant été doublé à la rentrée 2006, il a été décidé d'ajouter des versions discrètes de la transformée de Fourier et certaines de leur nombreuses applications. Le Chapitre concernant la transformée de Walsh a été ajouté dès la rentrée 2006 à ce support de cours, et une présentation de la transformée de Fourier discrète et de la transformée de Fourier dans le cas général a été ajoutée à l'automne 2006, ainsi qu'une présentation des algorithmes "rapides" de calcul de la transformée de Walsh et de la transformée de Fourier discrète (il s'agit de la "Fast Fourier Transform", connue sous le nom de FFT). Des applications de la FFT à la théorie du signal 1-D et à l'imagerie seront introduites dès que possible. L'introduction n'a pas été réactualisée et ne présente que les quatre premiers Chapitres.

Introduction

Le but de ce cours est de présenter les transformations de Fourier et de Laplace, qui ont de très nombreuses applications à la mécanique, à l'automatique, à l'électronique et à la théorie du signal (nous espérons être en mesure de présenter quelques unes de ces applications dans une prochaine édition). On a mis l'accent ici sur les applications de la transformée de Laplace aux équations et systèmes différentiels, en gardant en tête que le rôle d'un ingénieur n'est pas de résoudre de subtils problèmes de convergence, mais de savoir utiliser de manière efficace des outils puissants pour résoudre des problèmes concrets. Les transformations de Fourier et de Laplace permettent de ramener des équations compliquées (équations différentielles, équations de convolution) à des équations algébriques plus simples. Une fois ces dernières équations résolues il faut "inverser la transformation". On dispose certes dans un certain nombre de cas de formules mathématiques (formules d'inversion de Fourier et de Laplace) mais dans les applications pratiques **on utilise des tables, lues de gauche à droite pour traduire les équations au niveau des transformées et lues dans le sens inverse pour revenir au domaine de départ.**

Nous avons fait le choix de brièvement présenter l'intégrale de Lebesgue, car l'espace de fonctions intégrables sur \mathbb{R} et l'espace des fonctions de carré intégrable sur \mathbb{R} sont des domaines de définition naturels de la transformée de Fourier. Les théorèmes fondamentaux (théorèmes de convergence monotone et dominée, théorème de Fubini, formules d'inversion de Fourier et de Laplace, formules de Plancherel-Parseval) sont énoncés avec précision, mais la plupart des démonstrations sont omises. On notera que la transformée de Fourier des fonctions de carré intégrable peut être définie explicitement grâce à un très profond théorème de Carleson qui garantit l'existence "pour presque tout x " de la limite $\lim_{R \rightarrow +\infty} \int_{-R}^R f(t) e^{itx} dt$ si f^2 est intégrable. Un choix d'exemples et d'exercices souvent très concrets devrait permettre à tous les utilisateurs de ce cours de profiter des puissants outils que sont les transformations de Fourier et de Laplace.

Aitzin solasa

Ikastaro honen helburua mekanikan, automatikan, elektronikan eta seinalearen teorian aplikazio anitz dituzten Fourier-en eta Laplace-en transformazioak aurkeztea da (heldu den argitalpenean aplikazio horietarik zenbaiten aurkezteko neurrian izaitea espero dugu). Hemen azpimarratu ditugu

Laplace-en transformazioaren aplikazioak ekuazio eta sistema diferentzialetan, gogoan atxikiz injine-ruaren eginbearra ez dela konbergentzia arazo sotil batzuren ebaztea, baizik eta tresna ahaltu batzu modu eraginkorrean erabiltzen jakitea arazo konkretuen ebazteko. Fourier-en eta Laplace-en transformazioek ekuazio konplikatuak (ekuazio diferentzialak, konboluzio ekuazioak) ekuazio algebraiko sinpleagoetara eramaitea ahalbidetzen dute. Behin azken ekuazio horiek ebatzi eta, “transformazioa inbertitu” behar da. Zenbait kasutan, noski, formula matematikoak eskura ditugu (Fourier-en eta Laplace-en inbertsio formulak), baina aplikazio praktikoetan **taulak baliatzen ditugu, ezkerretik eskuinera irakurriz transformatuei dagozkien ekuazioen itzultzeko, eta alderantzizko zentzuan irakurriz hastapeneko eremura itzultzeko.**

Lebesgue-en integrala laburki aurkezteko hautua egin dugu, ezen \mathbb{R} gaineko funtzio integragarrien espazioa eta \mathbb{R} gaineko karratu integragarriko funtzioen espazioa Fourier-en transformazioaren definizio-eremu naturalak baitira. Oinarrizko teoremak (konbergentzia monotonoaren eta menperatuaren teoremak, Fubini-ren teorema, Fourier eta Laplace-en inbertitze formulak, Plancherel-Parseval-en formulak) zehazki adieraziak dira, baina frogapen gehienak baztertuak dira. “*Ia x guzientzat*” $\lim_{R \rightarrow +\infty} \int_{-R}^R f(t)e^{itx} dt$ limitearen izaitea bermatzen duen Carleson-en teorema arras barnari esker, ohartuko gara karratu integragarriko f funtzioen Fourier-en transformatua ezplizituki defini daitekeela. Adibide eta ariketa arrunt konkretuen bildumak erabiltzaile guzietan tresna ahaltuak diren Fourier-en eta Laplace-en transformazioei etekina ateratzen lagundu behar lieke.

Table des matières

1	L'intégrale de Lebesgue	1
1.1	Ensembles mesurables	1
1.2	Construction de l'intégrale de Lebesgue	5
1.3	Deux résultats fondamentaux	7
1.4	Exercices sur le Chapitre 1	9
2	La transformée de Fourier	13
2.1	Transformée de Fourier sur $L^1(\mathbb{R})$	13
2.2	Transformée de Fourier sur $L^2(\mathbb{R})$	16
2.3	Exercices sur le Chapitre 2	18
3	Intégration en plusieurs variables, théorème de Fubini	21
3.1	L'intégrale de Lebesgue en plusieurs variables	21
3.2	La transformée de Fourier en plusieurs variables	25
3.3	Le théorème de Fubini	28
3.4	Exercices sur le Chapitre 3	31
4	Transformée de Laplace et applications	35
4.1	Définition de la transformée de Laplace	35
4.2	Transformation de Laplace, convolution et dérivation	38
4.3	Applications de la transformation de Laplace	40
4.4	Exercices sur le Chapitre 4	47
5	Transformée en Z	51
5.1	Transformée en Z bilatérale	51
5.2	Transformée en Z unilatérale	55
5.3	Exercices sur le Chapitre 5	59
6	Transformée de Walsh	61
6.1	Matrices et transformée de Walsh	61
6.2	Transformée de Walsh rapide	62
6.3	Application aux fonctions booléennes	64

6.4	Applications de la transformée de Walsh à la compression de signaux 1-D	70
6.5	Applications de la transformée de Walsh à la compression des images	81
6.6	Exercices sur le Chapitre 6	83
7	Transformée de Fourier discrète	87
7.1	Définition de la transformée de Fourier discrète	87
7.2	Convolution cyclique et convolution acyclique	89
7.3	La FFT	91
7.4	Applications de la FFT au calcul de produits de polynômes	98
7.5	Applications de la FFT au traitement du signal et de l'image (en préparation)	101
7.6	Exercices sur le Chapitre 7	103
8	Etude générale de la transformée de Fourier	107
8.1	Groupe dual d'un groupe localement compact abélien	107
8.2	Mesure de Haar et transformée de Fourier, théorie générale	113
8.3	Formule de Plancherel-Parseval et formule d'inversion de Fourier	114
8.4	Séries de Fourier et transformation de Fourier sur le cercle	116
8.5	Transformée de Fourier sur les groupes abéliens finis	119
8.6	Transformée de Walsh, transformée de Fourier discrète, échantillonnage	122
8.7	Exercices sur le Chapitre 8	125

Chapitre 1

L'intégrale de Lebesgue

1.1 Ensembles mesurables

On rappelle brièvement la construction de l'intégrale de Riemann. Soit f une fonction bornée à valeurs réelles définie sur un intervalle fermé borné $[a, b]$ de \mathbb{R} , et soit \mathcal{P} l'ensemble des *partitions* de $[a, b]$, c'est à dire l'ensemble des suites finies $\sigma = (x_0, \dots, x_n)$ telles que $a = x_0 < x_1 < \dots < x_n = b$. Si σ est une partition de $[a, b]$ on pose

$$M_\sigma(f) = \sum_{i=0}^{n-1} (x_{i+1} - x_i) \sup_{x_i \leq x \leq x_{i+1}} f(x)$$
$$m_\sigma(f) = \sum_{i=0}^{n-1} (x_{i+1} - x_i) \inf_{x_i \leq x \leq x_{i+1}} f(x).$$

On vérifie que $m_\sigma(f) \leq M_\tau(f)$ pour $\sigma, \tau \in \mathcal{P}$. On dit que la fonction f est **intégrable au sens de Riemann** si $\sup_{\sigma \in \mathcal{P}} m_\sigma(f) = \inf_{\sigma \in \mathcal{P}} M_\sigma(f)$, et dans ce cas on pose

$$\int_a^b f(t) dt = \sup_{\sigma \in \mathcal{P}} m_\sigma(f) = \inf_{\sigma \in \mathcal{P}} M_\sigma(f)$$

Les fonctions continues sur $[a, b]$ et les fonctions bornées et monotones sur $[a, b]$ sont intégrables au sens de Riemann.

Si f est continue sur un intervalle I de \mathbb{R} et si $x_0 \in I$, alors la formule

$$F(x) = \int_{x_0}^x f(t) dt$$

définit une primitive de f sur I , c'est à dire que $F'(x) = f(x)$ pour tout x intérieur à I , que la dérivée à droite de F en a est égale à $f(a)$ si I possède un plus petit élément a , et que la dérivée à gauche de F en b est égale à $f(b)$ si I possède un plus grand élément b (et la fonction F est l'unique primitive de f sur I telle que $f(x_0) = 0$).

Rappelons également que si f est continue sur un intervalle fermé borné $[a, b]$, on peut utiliser les sommes de Riemann pour calculer $\int_a^b f(t)dt$ grâce à la formule suivante :

$$(1.1) \quad \lim_{n \rightarrow +\infty} \frac{b-a}{n} \sum_{k=0}^n f\left(a+k\frac{b-a}{n}\right) = \lim_{n \rightarrow +\infty} \frac{b-a}{n} \sum_{k=1}^n f\left(a+k\frac{b-a}{n}\right) = \int_a^b f(t)dt.$$

Cette formule, basée sur la définition de l'intégrale de Riemann, amène à la méthode des rectangles. Nous renvoyons au cours d'Analyse Numérique de X.Fischer[9] pour plus de détails sur les méthodes numériques de calcul d'intégrales (méthode des trapèzes, méthode de Simpson, etc...).

La théorie de l'intégrale de Riemann présente des inconvénients.

Premier inconvénient (pour Mathématiciens)

$$\text{Posons } \begin{cases} f(x) = 0 & \text{si } x \in \mathbb{Q}, \quad 0 \leq x \leq 1 \\ f(x) = 1 & \text{si } x \notin \mathbb{Q}, \quad 0 \leq x \leq 1 \end{cases}$$

La fonction f n'est pas intégrable sur $[0,1]$ car tout intervalle ouvert non vide de \mathbb{R} contient à la fois des rationnels et des irrationnels et avec les notations précédentes on a $m_\sigma(f) = 0$ et $M_\sigma(f) = 1$ pour toute partition σ de $[0, 1]$. Pourtant, intuitivement, l'ensemble des nombres rationnels est négligeable par rapport à l'ensemble des nombres irrationnels (les nombres rationnels sont ceux dont le développement décimal est périodique) et on a envie de dire que l'intégrale de cette fonction f sur $[0, 1]$ existe et est égale à 1.

Autres inconvénients (plus sérieux)

Pour travailler sur des intervalles non bornés ou avec des fonctions non bornées on est obligé de faire des passages à la limite (intégrales généralisées) souvent peu commodes, et il arrive dans les applications qu'on soit amené à intégrer des fonctions trop irrégulières pour être intégrables au sens de Riemann. C'est le cas pour certaines fonctions périodiques définies "presque partout" par la formule

$$f(t) = a_0 + \sum_{n=1}^{+\infty} a_n \cos(nt) + b_n \sin(nt),$$

où $(a_n)_{n \geq 0}$ et $(b_n)_{n \geq 0}$ sont deux suites de réels telles que les séries $\sum_{n \geq 0} |a_n|^2$ et $\sum_{n \geq 1} |b_n|^2$ soient convergentes.

Une réponse à ces questions a été donnée au tout début du siècle dernier par H.Lebesgue dans sa thèse : c'est l'intégrale de Lebesgue, qui permet d'intégrer une classe très vaste de fonctions.

Le point de départ consiste à "**mesurer les ensembles**", c'est à dire à définir la "longueur" de sous-ensembles très généraux de \mathbb{R} . La mesure d'un ensemble E sera notée $m(E)$. On commence par définir $m(E)$ pour les ensembles les plus simples (avec la convention $a + \infty = +\infty$ pour tout $a \in [0, +\infty]$).

- 1) Si E est fini ou vide, $m(E) = 0$.
- 2) Si E est un intervalle non borné, $m(E) = +\infty$.
- 3) Si E est un intervalle borné de la forme $[a, b]$, $[a, b[$, $]a, b]$ ou $]a, b[$, $m(E) = b - a$.
- 4) Si $E = \cup_{1 \leq n \leq k} I_n$ est une réunion finie d'intervalles disjoints, on pose $m(E) = \sum_{1 \leq n \leq k} m(I_n)$.
- 5) Si $E = \cup_{n \geq 1} I_n$ est une réunion d'une suite d'intervalles disjoints, on pose $m(E) = \sum_{n \geq 1} m(I_n)$, ce qui fait que $m(E) = +\infty$ si un des intervalles I_n est non borné, ou si tous les intervalles I_n sont bornés et si la série $\sum_{n \geq 1} m(I_n)$ est divergente.

Rappelons qu'un ensemble non vide $E \subset \mathbb{R}$ est dit **ouvert** si pour tout $x \in E$ il existe $\delta > 0$ tel que $]x - \delta, x + \delta[\subset E$. L'ensemble vide est ouvert par convention, et on dit qu'un ensemble $F \subset \mathbb{R}$ est **fermé** si son complémentaire est ouvert.

On peut montrer que tout ensemble ouvert non vide E peut s'écrire sous la forme $E = \cup_n I_n$, où $(I_n)_n$ est une suite finie ou infinie d'intervalles ouverts disjoints. Les formules 1), 4), et 5) permettent alors de définir $m(E)$ pour tout sous ensemble ouvert E de \mathbb{R} .

On dira qu'un sous-ensemble de \mathbb{R} est borné s'il est contenu dans un intervalle fermé borné de \mathbb{R} . Soit maintenant F un fermé borné de \mathbb{R} . Il existe $N \geq 1$ tel que $F \subset] - N, N[$. Soit E le complémentaire de F dans $] - N, N[$. Alors E est ouvert. On pose

$$m(F) = m(] - N, N[) - m(E) = 2N - m(E).$$

Définition 1.1.1

1) On dit qu'un ensemble borné $A \subset \mathbb{R}$ est mesurable au sens de Lebesgue s'il existe une suite $(E_n)_{n \geq 1}$ d'ouverts de \mathbb{R} contenant A et une suite $(F_n)_{n \geq 1}$ de fermés de \mathbb{R} contenus dans A tels que $\lim_{n \rightarrow +\infty} m(E_n) = \lim_{n \rightarrow +\infty} m(F_n)$, et dans ce cas on pose

$$m(A) = \lim_{n \rightarrow +\infty} m(E_n) = \lim_{n \rightarrow +\infty} m(F_n).$$

2) On dit qu'un ensemble non borné $B \subset \mathbb{R}$ est mesurable au sens de Lebesgue si $B \cap] - n, n[$ est mesurable au sens de Lebesgue pour $n \geq 1$, et dans ce cas on pose

$$m(B) = \lim_{n \rightarrow +\infty} m(B \cap] - n, n[).$$

Notons que dans la partie 2) de la définition on peut bien sûr obtenir $m(B) = +\infty$. Dans la partie 1) de la définition on peut supposer que la suite $(E_n)_{n \geq 1}$ est décroissante et que la suite $(F_n)_{n \geq 1}$ est croissante (il suffit pour cela de remplacer E_n par $\cap_{1 \leq m \leq n} E_m$ et F_n par $\cup_{1 \leq m \leq n} F_m$). On vérifie bien entendu que la valeur de $m(F)$ ne dépend pas du choix des suites $(E_n)_{n \geq 1}$ et $(F_n)_{n \geq 1}$.

On a les propriétés suivantes

(1.2) Si A est mesurable, alors le complémentaire de A est mesurable.

(1.3) Si $(A_n)_{n \geq 1}$ est une suite d'ensembles mesurables, alors $\cup_{n \geq 1} A_n$ et $\cap_{n \geq 1} A_n$ sont mesurables.

(1.4) Si $(A_n)_{n \geq 1}$ est une suite croissante d'ensembles mesurables, alors $m(\cup_{n \geq 1} A_n) = \lim_{n \rightarrow +\infty} m(A_n)$.

(1.5) Si $(A_n)_{n \geq 1}$ est une suite décroissante d'ensembles mesurables, et s'il existe $n_0 \geq 1$ tel que $m(A_{n_0}) < +\infty$, alors $m(\cap_{n \geq 1} A_n) = \lim_{n \rightarrow +\infty} m(A_n)$.

D'autre part la mesure de Lebesgue est **invariante par translation** : si $E \subset \mathbb{R}$ est mesurable, alors $m(E_a) = m(E)$ pour tout $a \in \mathbb{R}$, où $E_a := \{x - a\}_{x \in E}$.

On peut se demander si tous les sous-ensembles de \mathbb{R} sont mesurables. Le système d'axiomes usuel est appelé ZF, du nom de Zermelo et Fraenkel. On peut y adjoindre l'**axiome du choix**, qui s'énonce comme suit :

Soit X un ensemble quelconque, et soit $\mathcal{P}(X)$ l'ensemble des parties non vides de X . Alors il existe une application $\phi : \mathcal{P}(X) \rightarrow X$ telle que $\phi(A) \in A \quad \forall A \in \mathcal{P}(X)$.

Dans le système d'axiomes ZFC (axiomes de Zermelo-Fraenkel auquel on adjoint l'axiome du choix), on peut construire des parties de \mathbb{R} qui ne sont pas mesurables au sens de Lebesgue. C'est pourquoi Lebesgue n'aimait pas cet axiome, par contre fort apprécié à la même époque par le grand Mathématicien Emile Borel. En fait on peut faire ce qu'on veut en vertu d'un résultat du logicien R.Solovay, de l'Université de Berkeley.

Théorème 1.1.2 (Solovay, 1965) *L'axiome "Tout sous-ensemble de \mathbb{R} est mesurable au sens de Lebesgue" est consistant avec ZF.*

Ceci signifie qu'ajouter à ZF cet axiome ne mènera pas à une contradiction qui ne serait pas déjà dans ZF (le fait que ZF est non contradictoire est indémontrable...).

On retiendra de cette discussion qu'il n'y a aucun moyen explicite de construire des parties non mesurables de \mathbb{R} . Un ingénieur peut donc s'abriter derrière le théorème de Solovay et considérer que tout sous-ensemble de \mathbb{R} est mesurable au sens de Lebesgue.

1.2 Construction de l'intégrale de Lebesgue

Définition 1.2.1 On dit que $f : \mathbb{R} \rightarrow \mathbb{R}$ est mesurable si $f^{-1}(E) := \{x \in \mathbb{R} \mid f(x) \in E\}$ est mesurable pour tout ouvert E de \mathbb{R} . On définit de même les fonctions mesurables à valeurs dans \mathbb{C} .

La somme, le produit, le sup et l'inf de deux fonctions mesurables sont mesurables. On vérifie que toute limite simple d'une suite de fonctions mesurables est mesurable : si f_n est mesurable pour $n \geq 1$, et si $f(x) = \lim_{n \rightarrow +\infty} f_n(x)$ pour tout x , alors f est mesurable.

En fait il résulte des remarques précédentes qu'il est impossible de construire une fonction non mesurable de manière explicite, et **un ingénieur peut donc s'abriter derrière le théorème de Solovay et considérer que toute fonction à valeurs réelles ou complexes définie sur \mathbb{R} est mesurable.**

Si $E \subset \mathbb{R}$, on pose $\chi_E(x) = 1$ si $x \in E$, $\chi_E(x) = 0$ si $x \notin E$. On dit qu'une fonction f est une *fonction en escalier* s'il existe une famille finie E_1, \dots, E_p d'ensembles mesurables de mesure finie et une famille c_1, \dots, c_p de réels tels que l'on ait

$$f = \sum_{1 \leq k \leq p} c_k \chi_{E_k}.$$

Un calcul élémentaire montre que l'on peut toujours supposer que les ensembles E_1, \dots, E_p sont disjoints deux à deux. Si $f = \sum_{1 \leq k \leq p} c_k \chi_{E_k}$ est une fonction en escalier sur \mathbb{R} , on pose

$$\int_{\mathbb{R}} f(t) dt = \sum_{1 \leq k \leq p} c_k m(E_k).$$

Définition 1.2.2 Soit $f : \mathbb{R} \rightarrow [0, +\infty[$ une fonction mesurable positive, et soit $(f_n)_{n \geq 1}$ une suite croissante de fonctions positives en escalier telle que $f(x) = \lim_{n \rightarrow +\infty} f_n(x)$ pour tout $x \in \mathbb{R}$. On pose

$$\int_{\mathbb{R}} f(t) dt = \lim_{n \rightarrow +\infty} \int_{\mathbb{R}} f_n(t) dt \in [0, +\infty].$$

On dit que la fonction f est intégrable si $\int_{\mathbb{R}} f(t) dt < +\infty$.

Il faut évidemment vérifier qu'il existe bien une suite $(f_n)_{n \geq 1}$ de fonctions positives en escalier telle que $f(x) = \lim_{n \rightarrow +\infty} f_n(x)$ pour tout $x \in \mathbb{R}$, et que la valeur (finie ou infinie) de $\lim_{n \rightarrow +\infty} \int_{\mathbb{R}} f_n(t) dt$ est indépendante du choix de la suite $(f_n)_{n \geq 1}$. Nous admettrons ces résultats.

Définition 1.2.3

1) Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ une fonction mesurable. On dit que f est intégrable quand $|f|$ est intégrable, et dans ce cas on pose

$$\int_{\mathbb{R}} f(t)dt = \int_{\mathbb{R}} f^+(t)dt - \int_{\mathbb{R}} f_-(t)dt,$$

où $f^+(t) = \max(f(t), 0)$ et $f^-(t) = \max(-f(t), 0)$ pour $t \in \mathbb{R}$.

2) Soit $f : \mathbb{R} \rightarrow \mathbb{C}$ une fonction mesurable. On dit que f est intégrable quand $|f|$ est intégrable, et dans ce cas on pose

$$\int_{\mathbb{R}} f(t)dt = \int_{\mathbb{R}} \operatorname{Re}(f)(t)dt + i \int_{\mathbb{R}} \operatorname{Im}(f)(t)dt.$$

Remarquons que l'intégrale de Lebesgue est **invariante par translation** : si f est intégrable, on a pour tout $a \in \mathbb{R}$

$$\int_{\mathbb{R}} f(t-a)dt = \int_{\mathbb{R}} f(t)dt.$$

On va maintenant définir une notion d'intégration sur un ensemble mesurable .

Définition 1.2.4 Soit $E \subset \mathbb{R}$ un ensemble mesurable, soit $f : E \rightarrow \mathbb{C}$ une fonction et soit $\tilde{f} : \mathbb{R} \rightarrow \mathbb{C}$ l'extension de f à \mathbb{R} définie par les formules $\tilde{f}(x) = 0$ si $x \notin E$, $\tilde{f}(x) = f(x)$ si $x \in E$.

On dit que f est mesurable sur E si \tilde{f} est mesurable, et on dit que f est intégrable sur E si \tilde{f} est intégrable sur \mathbb{R} . Dans ce cas on pose

$$\int_E f(t)dt = \int_{\mathbb{R}} \tilde{f}(t)dt$$

On a des propriétés analogues à celles de l'intégrale de Riemann, par exemple la linéarité : si f et g sont intégrables sur E , alors $\lambda f + \mu g$ est intégrable sur E pour $\lambda, \mu \in \mathbb{C}$ et on a

$$(1.6) \quad \int_E (\lambda f(t) + \mu g(t))dt = \lambda \int_E f(t)dt + \mu \int_E g(t)dt.$$

On a également un analogue de l'inégalité de Cauchy-Schwartz : Si f et g sont mesurables sur E , et si $|f|^2$ et $|g|^2$ sont intégrables sur E , alors fg est intégrable sur E et on a

$$(1.7) \quad \left| \int_E f(t)g(t)dt \right| \leq \sqrt{\int_E |f(t)|^2 dt} \sqrt{\int_E |g(t)|^2 dt}.$$

On dira que deux fonctions f et g sont *égales presque partout* sur un ensemble mesurable E si on a la condition suivante

$$(1.8) \quad \text{L'ensemble } \{x \in E \mid f(x) \neq g(x)\} \text{ est de mesure nulle.}$$

Pus généralement on dira qu'une propriété est vraie *presque partout* si elle est vérifiée sur le complémentaire d'un ensemble de mesure nulle.

On déduit de la définition de l'intégrale de Lebesgue que l'on a la propriété suivante

Proposition 1.2.5 *Soit f une fonction intégrable sur un ensemble E . Si une fonction g est égale à f presque partout sur E , alors g est intégrable sur E et on a*

$$\int_E f(t)dt = \int_E g(t)dt.$$

Soit maintenant F un ensemble dénombrable, c'est à dire un ensemble de la forme $F = \{x_n\}_{n \geq 1}$, avec $x_n \neq x_m$ pour $n \neq m$. Alors E est la réunion de la suite disjointe formée des ensembles $\{x_n\}$, et il résulte de la formule (1.4) que $m(F) = \sum_{n \geq 1} m(\{x_n\}) = 0$. On peut montrer que l'ensemble \mathbb{Q} des nombres rationnels est dénombrable. Par conséquent $\mathbb{Q} \cap [0, 1]$ est dénombrable. Posons de nouveau $f(x) = 0$ si $x \in [0, 1] \cap \mathbb{Q}$, $f(x) = 1$ si $x \in [0, 1]$, $x \notin \mathbb{Q}$, de sorte que f n'est pas intégrable au sens de Riemann sur $[0, 1]$. Alors f est égale à 1 presque partout sur $[0, 1]$, donc f est intégrable au sens de Lebesgue sur $[0, 1]$ et $\int_0^1 f(t)dt = \int_0^1 dt = 1$.

1.3 Deux résultats fondamentaux

Nous concluons cette présentation en donnant sans démonstration deux résultats fondamentaux de la théorie de l'intégrale de Lebesgue.

Théorème 1.3.1 (*Théorème de convergence dominée*) *Soit $(f_n)_{n \geq 1}$ une suite de fonctions mesurables sur un ensemble mesurable E , et soit f une fonction définie sur E .*

On suppose que les deux conditions suivantes sont vérifiées :

(i) *$\lim_{n \rightarrow +\infty} f_n(t) = f(t)$ presque partout.*

(ii) *Il existe une fonction intégrable g sur E telle que $|f_n(t)| \leq g(t)$ presque partout pour tout $n \geq 1$.*

Alors f est intégrable sur E , et $\int_E f(t)dt = \lim_{n \rightarrow +\infty} \int_E f_n(t)dt$.

Corollaire 1.3.2 *Soit f une fonction intégrable sur \mathbb{R} . On pose $\hat{f}(x) = \int_{-\infty}^{+\infty} f(t)e^{-itx} dt$. Alors \hat{f} est continue sur \mathbb{R} .*

Démonstration : Pour montrer que \hat{f} est continue, il suffit de vérifier que $\hat{f}(x) = \lim_{n \rightarrow +\infty} \hat{f}(x_n)$ pour tout $x \in \mathbb{R}$ et pour toute suite $(x_n)_{n \geq 1}$ de réels qui converge vers x .

Soit $x \in \mathbb{R}$ et soit $(x_n)_{n \geq 1}$ une suite de réels tels que $x = \lim_{n \rightarrow +\infty} x_n$. Posons $h(t) = f(t)e^{-itx}$ et $h_n(t) = f(t)e^{-itx_n}$ pour $n \geq 1$. Comme l'exponentielle complexe est continue, on a

(i)

$$\lim_{n \rightarrow +\infty} h_n(t) = h(t) \text{ pour tout } t \in \mathbb{R},$$

et la première hypothèse du théorème de convergence dominée est vérifiée. D'autre part $|e^{itx}| = 1$ pour tout t , et on a

(ii)

$$|h_n(t)| = |f(t)| \text{ pour tout } t \in \mathbb{R} \text{ et tout } n \geq 1.$$

Comme f est intégrable sur \mathbb{R} , les deux hypothèses du théorème de convergence dominée sont vérifiées et on a

$$\begin{aligned} \hat{f}(x) &= \int_{-\infty}^{+\infty} f(t)e^{-itx} dt = \int_{-\infty}^{+\infty} h(t) dt = \lim_{n \rightarrow +\infty} \int_{-\infty}^{+\infty} h_n(t) dt \\ &= \lim_{n \rightarrow +\infty} \int_{-\infty}^{+\infty} f(t)e^{-itx_n} dt = \lim_{n \rightarrow +\infty} \hat{f}(x_n). \end{aligned}$$

Donc \hat{f} est continue sur \mathbb{R} . ♣

Théorème 1.3.3 (*Théorème de convergence monotone*) Soit $(f_n)_{n \geq 1}$ une suite croissante de fonctions positives intégrables telle que $f(t) := \lim_{n \rightarrow +\infty} f_n(t)$ soit finie pour presque tout $t \in E$. Alors on a

$$\int_E f(t) dt = \lim_{n \rightarrow +\infty} \int_E f_n(t) dt \in [0, +\infty].$$

Notons que dans le cas où $\lim_{n \rightarrow +\infty} \int_E f_n(t) dt = +\infty$, le théorème indique que f n'est pas intégrable sur E .

Rappelons que si f est continue sur $[a, +\infty[$, on dit que l'intégrale de Riemann généralisée $\int_a^{+\infty} f(t) dt$ est convergente si et seulement si $\int_a^L f(t) dt$ a une limite quand $L \rightarrow +\infty$, et dans ce cas on pose $\int_a^{+\infty} f(t) dt = \lim_{L \rightarrow +\infty} \int_a^L f(t) dt$. On va voir que si $f \geq 0$, l'intégrale de Riemann généralisée $\int_a^{+\infty} f(t) dt$ est convergente si et seulement

si f est intégrable au sens de Lebesgue sur $[a, +\infty[$ (attention, ce résultat n'est plus vrai en général pour les fonctions de signe non constant).

Corollaire 1.3.4 Soit $a \in \mathbb{R}$, et soit f une fonction continue sur $[a, +\infty[$ telle que $f(t) \geq 0$ pour $t \geq a$.

Alors l'intégrale de Riemann généralisée $\int_a^{+\infty} f(t)dt$ est convergente si et seulement si f est intégrable au sens de Lebesgue sur $[a, +\infty[$, et l'intégrale de Riemann généralisée $\int_a^{+\infty} f(t)dt$ et l'intégrale de Lebesgue $\int_{[a, +\infty[} f(t)dt$ sont égales.

Démonstration : Posons $F(L) = \int_a^L f(t)dt$. Comme $f \geq 0$, F est croissante sur $[a, +\infty[$, et $F(L)$ a une limite finie quand $L \rightarrow +\infty$ si et seulement si la suite $(F(n))_{n \geq 1}$ est convergente. Posons $f_n(t) = f(t)$ si $a \leq t \leq n$, $f_n(t) = 0$ si $t > n$. Alors f_n est intégrable pour $n \geq 1$, la suite f_n est croissante, et $f(t) = \lim_{n \rightarrow +\infty} f_n(t)$ pour $t \geq a$. On déduit du théorème de convergence monotone que f n'est pas intégrable au sens de Lebesgue sur $[a, +\infty[$ si $\lim_{n \rightarrow +\infty} \int_a^n f(t)dt = +\infty$, que f est intégrable au sens de Lebesgue sur $[a, +\infty[$ si la suite $(\lim_{n \rightarrow +\infty} \int_a^n f(t)dt)_{n \geq 1}$ est convergente, et que dans ce cas on a, avec les notations du Corollaire

$$\int_{[a, +\infty[} f(t)dt = \lim_{n \rightarrow +\infty} \int_{[a, +\infty[} f_n(t)dt = \lim_{n \rightarrow +\infty} \int_a^{+\infty} f(t)dt. \clubsuit$$

On verra en exercice qu'on a les mêmes propriétés pour les autres types d'intégrales de Riemann généralisées de fonctions continues positives.

1.4 Exercices sur le Chapitre 1

exercice 1

Calculer $\lim_{n \rightarrow +\infty} \sum_{1 \leq k \leq n} \frac{1}{n+k}$

exercice 2

Pour $\alpha > 0$ on pose $E_\alpha = \cup_{n \geq 1} [n, n + \frac{1}{n^\alpha}[$. Pour quelles valeurs de α la mesure de E_α est elle finie? En utilisant vos souvenirs sur les séries de Fourier, déterminer $m(E_2)$.

exercice 3 (Annales ESTIA, examens Transformées 2000 et 2001)

Soit $f \in L^1(\mathbb{R})$. On pose, pour $x \in \mathbb{R}$

$$F(x) = \int_{-\infty}^{+\infty} f(t) \sin^4(t^3 x^2 + tx) dt,$$

$$G(x) = \int_{-\infty}^{+\infty} f(t) \cos^2(1 + t^2 x^2) dt.$$

En utilisant le théorème de convergence dominée, montrer que F et G sont continues sur \mathbb{R} .

exercice 4(Annales ESTIA, examen Transformées 1998)

Soit $f \in L^1(\mathbb{R})$. On pose, pour $t \in \mathbb{R}$

$$F(t) = \int_{-\infty}^{+\infty} f(x) \cos(t^2 x) dx.$$

1) En utilisant le théorème de convergence dominée, montrer que f est continue sur \mathbb{R} .

2) On note \hat{f} la transformée de Fourier de f . Exprimer F à partir de \hat{f} . Retrouver ainsi le résultat du 1), et montrer que $\lim_{t \rightarrow +\infty} F(t) = 0$.

exercice 5(Annales ESTIA, examen Transformées 1999)

Soit $f \in L^1(\mathbb{R})$. On pose, pour $x \in \mathbb{R}$

$$G(x) = \int_{-\infty}^{+\infty} f(t) \sin(te^x) dt.$$

1) En utilisant le théorème de convergence dominée, montrer que G est continue sur \mathbb{R} .

2) Calculer G en fonction de \hat{f} . Retrouver ainsi le résultat ci-dessus, et montrer que $\lim_{x \rightarrow +\infty} G(x) = 0$.

3) Que peut-on dire du comportement de $G(x)$ quand $x \rightarrow -\infty$?

exercice 6(Annales ESTIA, examen transformées 2002)

Soit $f \in L^1(\mathbb{R})$ On pose, pour $x > 1$,

$$F(x) = \int_{-\infty}^{+\infty} f(t) \cos\left(\frac{tx}{(x-1)^2}\right) dt.$$

1) En utilisant le théorème de convergence dominée, montrer que F est continue sur $]1, +\infty[$.

2-a) Calculer F en fonction de la transformée de Fourier \hat{f} de f , et retrouver le résultat de la question précédente.

2-b) Déterminer $\lim_{x \rightarrow 1^+} F(x)$.

2-c) Déterminer $\lim_{x \rightarrow +\infty} F(x)$.

exercice 7

Soit f une fonction continue sur $]a, b]$. Montrer que si $f \geq 0$, l'intégrale de Riemann généralisée $\int_a^b f(t)dt$ est convergente si et seulement si f est intégrable au sens de Lebesgue sur $]a, b]$, et que dans ce cas l'intégrale de Riemann généralisée $\int_a^b f(t)dt$ et l'intégrale de Lebesgue $\int_{]a,b]} f(t)dt$ sont égales.

exercice 8

On pose $f(t) = \frac{\cos(t)}{t}$ pour $x \geq 1$. Montrer que l'intégrale de Riemann généralisée $\int_1^{+\infty} f(t)dt$ est convergente (on pourra intégrer par parties) mais que f n'est pas intégrable au sens de Lebesgue sur $[1, +\infty[$ (on pourra minorer $\int_{-\frac{\pi}{4}+2k\pi}^{\frac{\pi}{4}+2k\pi} |f(t)|dt$).

exercice 9

Soit $f \in L^1(\mathbb{R})$. Pour $x > 0$, on pose

$$F(x) = \int_{-\infty}^{+\infty} f(t)e^{-x|t|}dt.$$

1) Montrer que F est continue sur $[0 + \infty[$.

2) On suppose de plus que $\int_{-\infty}^{+\infty} |t||f(t)|dt < +\infty$.

Montrer que F est dérivable sur $[0, +\infty[$, et que $F'(x) = -\int_{-\infty}^{+\infty} |t||f(t)|e^{-x|t|}dt$ (on pourra revenir à la définition de la dérivée, et appliquer le théorème de convergence dominée).

exercice 10

Soit $(f_n)_{n \geq 1}$ une suite de fonctions continues et intégrables sur un sous-ensemble mesurable E de \mathbb{R} .

1) On suppose que $f_n(t) \geq 0$ et que la série $\sum_{n \geq 1} f_n(t)$ converge pour tout $t \in E$.

Montrer que si $\int_E [\sum_{n \geq 1} f_n(t)] dt = +\infty$, alors la série $\sum_{n \geq 1} [\int_E f_n(t)] dt$ est divergente, et que si

$\int_E [\sum_{n \geq 1} f_n(t)] dt < +\infty$, alors la série $\sum_{n \geq 1} [\int_E f_n(t)dt]$ est convergente, et que l'on a dans ce cas

$$\sum_{n \geq 1} \left[\int_E f_n(t)dt \right] = \int_E \left[\sum_{n \geq 1} f_n(t) \right] dt.$$

2) On suppose que la série $\sum_{n \geq 1} |f_n(t)|$ converge pour tout $t \in E$, et que la série $\sum_{n \geq 1} [\int_E |f_n(t)|dt]$ est convergente.

On pose $f(t) = \sum_{n \geq 1} f_n(t)$ pour $t \in E$.

Montrer que f est bien définie sur E et appartient à $L^1(E)$ et que l'on a

$$\sum_{n \geq 1} \left[\int_E f_n(t) dt \right] = \int_E \left[\sum_{n \geq 1} f_n(t) \right] dt.$$

Indication : On pourra appliquer le théorème de convergence monotone à la question 1 et le théorème de convergence dominée à la question 2.

Chapitre 2

La transformée de Fourier

2.1 Transformée de Fourier sur $L^1(\mathbb{R})$

On va introduire plusieurs espaces de fonctions.

1) $L^1(\mathbb{R})$ désigne l'espace vectoriel des fonctions intégrables sur \mathbb{R} , **où on identifie les fonctions égales presque partout**. Pour $f \in L^1(\mathbb{R})$ on pose

$$\|f\|_1 := \int_{-\infty}^{+\infty} |f(t)| dt.$$

2) $L^2(\mathbb{R})$ désigne l'espace vectoriel des fonctions mesurables sur \mathbb{R} telles que $|f|^2$ soit intégrable sur \mathbb{R} , **où on identifie les fonctions égales presque partout**. Pour $f \in L^2(\mathbb{R})$ on pose

$$\|f\|_2 := \sqrt{\int_{-\infty}^{+\infty} |f(t)|^2 dt}.$$

3) $L^\infty(\mathbb{R})$ désigne l'espace vectoriel des fonctions mesurables sur \mathbb{R} telles qu'il existe $m \geq 0$ vérifiant $|f(t)| \leq m$ presque partout, **où on identifie les fonctions égales presque partout**. Pour $f \in L^\infty(\mathbb{R})$ on pose

$$\|f\|_\infty = \inf\{m \geq 0 \mid |f(t)| \leq m \text{ presque partout}\}.$$

4) $\mathcal{C}_0(\mathbb{R})$ désigne l'ensemble des fonctions continues sur \mathbb{R} telles que $\lim_{|t| \rightarrow +\infty} f(t) = 0$. Pour $f \in \mathcal{C}_0(\mathbb{R})$, on pose

$$\|f\|_\infty = \sup_{t \in \mathbb{R}} |f(t)|.$$

5) $\mathcal{E}(\mathbb{R})$ désigne l'espace des fonctions f indéfiniment dérivables sur \mathbb{R} telles que l'on ait, avec la convention $f^{(0)} = f$,

$$\lim_{|t| \rightarrow +\infty} |t|^p |f^{(q)}(t)| = 0 \quad \forall p \geq 1, \forall q \geq 0.$$

Dans les quatre premiers cas on a affaire à des espaces **normés** : si $\|\cdot\|_i$, $i = 1, 2$ ou ∞ désigne une des quantités introduites ci-dessus, on a les propriétés suivantes

$$(2.1) \quad \|f + g\|_i \leq \|f\|_i + \|g\|_i \text{ pour tout couple } (f, g) \text{ de fonctions,}$$

$$(2.2) \quad \|\lambda f\|_i = |\lambda| \|f\|_i \text{ pour toute fonction } f \text{ et pour tout nombre complexe } \lambda,$$

$$(2.3) \quad \|f\|_i \geq 0 \text{ pour toute fonction } f, \text{ et } \|f\|_i \neq 0 \text{ si } f \neq 0.$$

Ces espaces normés sont **complets**, en ce sens que si une suite $(x_p)_{p \geq 1}$ de l'un de ces espaces vérifie $\lim_{n \rightarrow +\infty} \sup_{p \geq n, q \geq n} \|x_p - x_q\|_i = 0$, alors il existe un élément x de l'espace tel que $\lim_{n \rightarrow +\infty} \|x - x_n\|_i = 0$. De tels espaces sont appelés des **espaces de Banach**. L'espace $\mathcal{E}(\mathbb{R})$ n'est pas un espace de Banach. C'est en fait un **espace de Fréchet**, notion un peu plus compliquée que nous n'expliciterons pas ici.

On va admettre provisoirement le résultat suivant, qui sera démontré au Chapitre 3.

Théorème 2.1.1 *Soient $f, g \in L^1(\mathbb{R})$. Alors la fonction $t \mapsto f(x-t)g(t)$ est intégrable sur \mathbb{R} pour presque tout $x \in \mathbb{R}$. De plus si on définit presque partout le produit de convolution $f * g$ par la formule*

$$(f * g)(x) = \int_{-\infty}^{+\infty} f(x-t)g(t)dt,$$

alors $f * g \in L^1(\mathbb{R})$, et $\|f * g\|_1 \leq \|f\|_1 \|g\|_1$.

Le produit de convolution est **commutatif** et **associatif**, c'est à dire qu'on a les propriétés suivantes :

$$(2.4) \quad f * g = g * f \quad \forall f \in L^1(\mathbb{R}), \quad \forall g \in L^1(\mathbb{R}).$$

$$(2.5) \quad f * (g * h) = (f * g) * h \quad \forall f \in L^1(\mathbb{R}), \quad \forall g \in L^1(\mathbb{R}), \quad \forall h \in L^1(\mathbb{R}).$$

On va maintenant définir la transformation de Fourier, déjà entrevue au Chapitre précédent.

Définition 2.1.2 *Soit $f \in L^1(\mathbb{R})$. Pour $x \in \mathbb{R}$, on pose*

$$\hat{f}(x) = \int_{-\infty}^{+\infty} f(t)e^{-itx} dt$$

La fonction \hat{f} est appelée la transformée de Fourier de f , et l'application $\mathcal{F} : f \mapsto \hat{f}$ est appelée la transformation de Fourier.

Il est clair que la transformation de Fourier est une application linéaire, et on a déjà vu au Chapitre précédent que \hat{f} est continue sur \mathbb{R} pour $f \in L^1(\mathbb{R})$. Le théorème suivant résume les principales propriétés de la transformation de Fourier.

Théorème 2.1.3

- 1) Si $f \in L^1(\mathbb{R})$, alors $\hat{f} \in \mathcal{C}_0(\mathbb{R})$, et $\|\hat{f}\|_\infty \leq \|f\|_1$.
- 2) On a $\mathcal{F}(f * g) = \mathcal{F}(f)\mathcal{F}(g)$ pour $f \in L^1(\mathbb{R})$, $g \in L^1(\mathbb{R})$.
- 3) Si f et \hat{f} appartiennent à $L^1(\mathbb{R})$, alors on a pour presque tout $t \in \mathbb{R}$,

$$f(t) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \hat{f}(x)e^{itx} dx.$$

4) (i) Si $f \in \mathcal{E}(\mathbb{R})$, alors $\hat{f} \in \mathcal{E}(\mathbb{R})$ et la transformation de Fourier $\mathcal{F} : \mathcal{E}(\mathbb{R}) \rightarrow \mathcal{E}(\mathbb{R})$ est bijective.

(ii) On a $\mathcal{F}^{-1}(f)(t) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} f(x)e^{itx} dx$ pour $f \in \mathcal{E}(\mathbb{R})$, $t \in \mathbb{R}$.

(iii) On a $\mathcal{F}(f^{(k)})(x) = (ix)^k \mathcal{F}(f)(x)$ pour $f \in \mathcal{E}(\mathbb{R})$, $x \in \mathbb{R}$, $k \geq 1$.

La formule 3) du théorème ci-dessus est appelée la **formule d'inversion de Fourier**. Elle montre en particulier que si $f \in L^1(\mathbb{R})$, et si $\hat{f} = 0$, alors $f = 0$, ou plus précisément f est nulle presque partout, ce qui veut dire que f est l'élément nul de $L^1(\mathbb{R})$. Ceci montre que $\mathcal{F} : L^1(\mathbb{R}) \rightarrow \mathcal{C}_0(\mathbb{R})$ est **injective**. Par contre on peut montrer que $\mathcal{F} : L^1(\mathbb{R}) \rightarrow \mathcal{C}_0(\mathbb{R})$ **n'est pas surjective** : il existe des fonctions $g \in \mathcal{C}_0(\mathbb{R})$ qui ne coïncident avec la transformée de Fourier d'aucune fonction $f \in L^1(\mathbb{R})$.

Le produit de convolution est l'expression mathématique de nombreux phénomènes de Physique (ceci sera illustré dans des versions ultérieures plus détaillées de ce cours). En tout état de cause les équations de convolution du type $f * g = h$, où f et g sont données et où h est à déterminer, ne peuvent se résoudre directement. La transformation de Fourier, d'après la formule 2) du théorème, ramène ce type d'équation à une équation du type $\hat{f} \cdot \hat{g} = \hat{h}$, ce qui donne, si le quotient \hat{h}/\hat{f} est bien défini, $\hat{g} = \hat{h}/\hat{f}$. Il peut arriver qu'il n'y ait pas de solution, ou qu'il y en ait une infinité, pour ce type d'équations dans $\mathcal{C}_0(\mathbb{R})$. De même considérons une équation différentielle du type

$$a_n f^{(n)} + \dots + a_1 f' + a_0 f = h,$$

avec $h \in \mathcal{E}(\mathbb{R})$ donnée, $f \in \mathcal{E}(\mathbb{R})$ inconnue.

Posons $p(x) = a_n x^n + \dots + a_1 x + a_0$ (ce polynôme est appelé le **polynôme caractéristique** de l'équation différentielle). La formule 4) (iii) du théorème donne

$$p(ix)\hat{f}(x) = \hat{h}(x) \quad \forall x \in \mathbb{R}.$$

Si le polynôme p n'a pas de racine imaginaire pure, on vérifie que la fonction $x \mapsto \frac{\hat{h}(x)}{p(ix)}$ appartient à $\mathcal{E}(\mathbb{R})$, et l'unique solution f de l'équation dans $\mathcal{E}(\mathbb{R})$, est donnée par la formule

$$f(x) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \frac{\hat{h}(t)e^{itx}}{p(it)} dt.$$

Supposons maintenant que p a des racines imaginaires pures distinctes $(i\alpha_1, \dots, i\alpha_k)$. Pour $1 \leq j \leq k$ soit m_j l'ordre de multiplicité de $i\alpha_j$, c'est à dire le plus petit entier $m \geq 1$ tel que $p^{(m)}(i\alpha_j) \neq 0$. Il résulte de la formule de Leibnitz que si l'équation a une solution h , avec la convention $\hat{h}^{(0)} = \hat{h}$,

$$\hat{h}^{(m)}(\alpha_j) = 0 \quad \forall m \leq m_j - 1, \quad \forall j \leq k.$$

Réciproquement si la condition ci-dessus est satisfaite, on peut vérifier que la fonction $t \mapsto \frac{\hat{h}(t)}{p(it)}$ se prolonge par continuité à \mathbb{R} et que ce prolongement appartient à $\mathcal{E}(\mathbb{R})$. L'équation différentielle admet donc une unique solution f dans $\mathcal{E}(\mathbb{R})$, donnée de nouveau par la formule

$$f(x) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \frac{\hat{h}(t)e^{itx}}{p(it)} dt.$$

Dans ces deux situations le passage à la transformée de Fourier a permis de ramener des équations assez compliquées à des équations algébriques beaucoup plus simples. On attend d'un ingénieur de savoir lire les tables de transformées de Fourier dans le sens direct, pour pouvoir expliciter les équations algébriques obtenues et leur solution(s), puis de savoir lire les tables de transformées de Fourier dans le sens inverse, pour pouvoir donner la ou les solutions des équations initiales dans l'espace de départ.

On explicitera un peu plus loin ce programme dans le cas voisin de la transformée de Laplace.

2.2 Transformée de Fourier sur $L^2(\mathbb{R})$

On va maintenant décrire la transformée de Fourier sur $L^2(\mathbb{R})$. La situation est en un certain sens très simple : la transformée de Fourier est une bijection de $L^2(\mathbb{R})$

sur $L^2(\mathbb{R})$. Vu sous un autre angle elle est très compliquée : la formule $\hat{f}(x) = \int_{-\infty}^{+\infty} f(t)e^{-itx} dt$, qui définit la transformée de Fourier pour $f \in L^1(\mathbb{R})$, fait intervenir une intégrale en général divergente si $f \in L^2(\mathbb{R})$. Par contre si $\alpha > 0$ et $f \in L^2(\mathbb{R})$ alors la fonction $t \mapsto f(t)e^{-\alpha|t|}$ est intégrable sur \mathbb{R} . D'autre part il résulte de l'inégalité de Cauchy-Schwartz que toute fonction $f \in L^2(\mathbb{R})$ est intégrable sur $[-R, R]$ pour $R > 0$. On a alors les résultats suivants.

Théorème 2.2.1 *Soit $f \in L^2(\mathbb{R})$. Alors les limites $\lim_{\alpha \rightarrow 0^+} \int_{-\infty}^{+\infty} f(t)e^{-itx-\alpha|t|} dt$ et $\lim_{R \rightarrow +\infty} \int_{-R}^R f(t)e^{-itx} dt$ existent et sont égales pour presque tout $x \in \mathbb{R}$.*

La première propriété est liée à un résultat concernant les limites radiales des fonctions holomorphes bornées dans le cercle unité démontré en 1907 par P. Fatou. La démonstration est du niveau du DEA de Mathématiques. Le deuxième résultat est un théorème célèbre de L.Carleson[?] (1967). Les autres démonstrations données par C.Fefferman[?] (1973) et par M.Lacey et C.Thiele[?] (2000) restent très difficiles.

On peut alors définir la transformée de Fourier sur $L^2(\mathbb{R})$, qui s'avère être une bijection de $L^2(\mathbb{R})$ sur lui-même.

Définition 2.2.2 *Pour $f \in L^2(\mathbb{R})$, on définit \hat{f} presque partout sur \mathbb{R} par la formule*

$$\hat{f}(x) = \lim_{\alpha \rightarrow 0^+} \int_{-\infty}^{+\infty} f(t)e^{-itx-\alpha|t|} dt = \lim_{R \rightarrow +\infty} \int_{-R}^R f(t)e^{-itx} dt$$

Théorème 2.2.3 *Pour $f \in L^2(\mathbb{R})$, on a $\hat{f} \in L^2(\mathbb{R})$ et*

(i) $f(t) = \lim_{\alpha \rightarrow 0^+} \frac{1}{2\pi} \int_{-\infty}^{+\infty} \hat{f}(x)e^{itx-\alpha|x|} dx = \lim_{R \rightarrow +\infty} \frac{1}{2\pi} \int_{-R}^R \hat{f}(x)e^{itx} dx$ pour presque tout $t \in \mathbb{R}$.

$$(ii) \int_{-\infty}^{+\infty} |f(t)|^2 dt = \frac{1}{2\pi} \int_{-\infty}^{+\infty} |\hat{f}(t)|^2 dt.$$

Plus généralement on a, pour $f \in L^2(\mathbb{R})$, $g \in L^2(\mathbb{R})$,

$$(iii) \int_{-\infty}^{+\infty} f(t)\bar{g}(t) dt = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \hat{f}(t)\bar{\hat{g}}(t) dt,$$

et la transformation de Fourier $\mathcal{F} : f \mapsto \hat{f}$ est une bijection de $L^2(\mathbb{R})$ sur lui-même.

La formule (i) est la formule d'inversion de Fourier pour $L^2(\mathbb{R})$, et peut s'écrire pour $f \in L^2(\mathbb{R})$ sous la forme

$$(2.6) \quad \mathcal{F}^{-1}(f)(t) = \frac{1}{2\pi} \mathcal{F}(f)(-t).$$

La formule (iii) est appelée *formule de Plancherel* et la formule (ii), qui est un cas particulier de (iii), est appelée *formule de Parseval*.

2.3 Exercices sur le Chapitre 2

exercice 1

On pose $H(t) = e^{-|t|}$ pour $t \in \mathbb{R}$. Calculer la transformée de Fourier de H .

exercice 2 (Annales Estia, Examen Transformées 2000)

1) On pose $f(t) = te^{-t}$ pour $t \geq 0$, $f(t) = 0$ pour $t < 0$. Vérifier que f est continue sur \mathbb{R} , et que $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$.

2) Par un calcul direct, montrer que $\hat{f}(x) = \frac{1}{(1+ix)^2}$.

3) Montrer que $\int_0^{+\infty} t^2 e^{-2t} dt = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \frac{dx}{(1+x^2)^2}$.

4) Calculer $\int_{-\infty}^{+\infty} \frac{e^{ixt}}{(1+ix)^2} dx$ pour $t \in \mathbb{R}$.

exercice 3 (Annales ESTIA, examen Transformées 2001)

1) Montrer que $\int_{-\infty}^{+\infty} |t|^n e^{-\frac{t^2}{2}} dt < +\infty$ pour n entier, $n \geq 0$.

2) Montrer que $\int_{-\infty}^{+\infty} t^n e^{-\frac{t^2}{2}} dt = 0$ si n est impair.

3) On pose $u_m = \int_{-\infty}^{+\infty} t^{2m} e^{-\frac{t^2}{2}} dt$ pour m entier, $m \geq 0$. En intégrant avec soin par parties, montrer que $u_m = \frac{1}{2m+1} u_{m+1}$.

4) Montrer par récurrence que $u_m = \frac{(2m)!}{2^m (m!)^2} u_0$ pour $m \geq 1$.

5) En utilisant l'exercice 5 du Chapitre 3, montrer que $u_0 = \sqrt{2\pi}$.

6) On pose $f(t) = e^{-\frac{t^2}{2}}$ pour $t \in \mathbb{R}$. Soit $p \geq 0$ un entier, et soit $x \in \mathbb{R}$. On pose, pour $t \in \mathbb{R}$

$$F_{p,x}(t) = \sum_{n=0}^p \frac{(-ix)^n}{n!} t^n.$$

En utilisant le théorème de convergence dominée, montrer que $\hat{f}(x) = \lim_{p \rightarrow +\infty} \int_{-\infty}^{+\infty} F_{p,x}(t) e^{-\frac{t^2}{2}} dt$.

En déduire que $\hat{f}(x) = \sqrt{2\pi} f(x)$ pour $x \in \mathbb{R}$.

7) En utilisant la formule d'inversion de Fourier, montrer que $(f \star f)(t) = \sqrt{\pi} e^{-\frac{t^2}{4}}$ pour $t \in \mathbb{R}$. Retrouver ce résultat par un calcul direct.

exercice 4 (Annales ESTIA, examen Transformées 2002)

1) Soit $f \in L^1(\mathbb{R})$, et soit \hat{f} la transformée de Fourier de f . Montrer que si f est paire, on a

$$\hat{f}(x) = \int_{-\infty}^{+\infty} f(t) \cos(xt) dt.$$

2) On pose $f(t) = 0$ pour $|t| > 1$, $f(t) = \frac{1-t^2}{4}$ pour $-1 \leq t \leq 1$. Esquisser le graphe de f , et calculer $\int_{-\infty}^{+\infty} |f(t)| dt = \int_{-\infty}^{+\infty} f(t) dt$ et $\int_{-\infty}^{+\infty} |f(t)|^2 dt$. En déduire la valeur de $\hat{f}(0)$.

3) Au moyen d'une double intégration par parties, calculer $\hat{f}(x)$ pour $x \neq 0$. Donner un développement en série entière de \hat{f} .

4) Expliciter la formule obtenue en appliquant à f la formule de Parseval.

5) A t'on $\hat{f} \in L^1(\mathbb{R})$? Si oui, expliciter la formule obtenue en appliquant à f la formule d'inversion de Fourier.

exercice 5

1) On pose $H_\lambda(t) = e^{-\lambda|t|}$ pour $\lambda > 0$, $t \in \mathbb{R}$, et on pose

$$h_\lambda(t) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} H_\lambda(x) e^{ixt} dx.$$

Calculer h_λ , et vérifier que $\int_{-\infty}^{+\infty} h_\lambda(x) dx = 1$.

2) En appliquant le théorème de Fubini, vérifier que si $f \in L^1(\mathbb{R})$, on a pour $t \in \mathbb{R}$

$$(f * h_\lambda)(t) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} H_\lambda(x) e^{ixt} dx.$$

3) On suppose maintenant que g est continue et bornée sur \mathbb{R} . Montrer que l'on a, pour $t \in \mathbb{R}$

$$g(t) = \lim_{\lambda \rightarrow 0^+} (g * h_\lambda)(t).$$

4) On suppose que f est continue, intégrable et bornée sur \mathbb{R} , et que \hat{f} est intégrable.

Déduire de ce qui précède que l'on a, pour $t \in \mathbb{R}$,

$$f(t) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \hat{f}(x) e^{ixt} dx.$$

(c'est un cas particulier de la formule d'inversion de Fourier).

exercice 6

Soit f une fonction continue sur \mathbb{R} . On suppose qu'il existe $L > 0$ tel que $f(t) = 0$ pour $t > L$, et on pose $\tilde{f}(t) = \bar{f}(-t)$ pour $t \in \mathbb{R}$.

1) On pose $g = f * \tilde{f}$. Vérifier que g est continue sur \mathbb{R} , que $|g(x)| \leq \|f\|_2$ pour $x \in \mathbb{R}$, et que $g(x) = 0$ pour $|x| \geq 2L$.

2) Les notations étant celles de l'exercice 5, déduire de la question 3 de l'exercice 5 que l'on a

$$\|f\|_2^2 = g(0) = \lim_{\lambda \rightarrow 0^+} (g * h_\lambda)(0).$$

3) Vérifier que l'on a, pour $x \in \mathbb{R}$,

$$\hat{g}(x) = |\hat{f}(x)|^2.$$

4) En utilisant la question 2 de l'exercice 5 et le théorème de convergence monotone, montrer que l'on a

$$\int_{-\infty}^{+\infty} |f(t)|^2 dt = \frac{1}{2\pi} \int_{-\infty}^{+\infty} |\hat{f}(x)|^2 dx.$$

(c'est un cas particulier de la formule de Parseval).

Chapitre 3

Intégration en plusieurs variables, théorème de Fubini

3.1 L'intégrale de Lebesgue en plusieurs variables

La construction de l'intégrale de Lebesgue en dimension $k \geq 2$ se fait selon une méthode analogue à la méthode utilisée dans le cas $k = 1$. Soit $P = [a_1, b_1] \times \dots \times [a_k, b_k]$ un "pavé". On pose

$$m_k(P) = (b_1 - a_1) \dots (b_k - a_k).$$

On reconnaît en dimension 2 l'aire du rectangle, et en dimension 3 le volume du parallélépipède rectangle. Pour $\mathbf{p} = (p_1, \dots, p_k) \in \mathbb{Z}^k$, $\epsilon > 0$, on pose $C_{\mathbf{p}, \epsilon} = [\epsilon p_1, \epsilon(p_1 + 1)] \times \dots \times [\epsilon p_k, \epsilon(p_k + 1)]$, de sorte que $m(C_{\mathbf{p}, \epsilon}) = \epsilon^k$. On note \mathcal{C} la famille des ensembles de la forme $C = \cup_{1 \leq i \leq q} C_{\mathbf{p}_i, \epsilon}$, avec $\mathbf{p}_1, \dots, \mathbf{p}_q$ distincts, $q \geq 1$, $\epsilon > 0$. Si $C = \cup_{1 \leq i \leq q} C_{\mathbf{p}_i, \epsilon} \in \mathcal{C}$, on pose

$$m_k(C) = q\epsilon^k = \sum_{1 \leq i \leq q} m_k(C_{\mathbf{p}_i, \epsilon}).$$

Pour $a = (a_1, \dots, a_k) \in \mathbb{R}^k$, $r > 0$ on pose $B(a, r) = \{x = (x_1, \dots, x_k) \in \mathbb{R}^k \mid x_1^2 + \dots + x_k^2 < r^2\}$. On dit que $U \subset \mathbb{R}^k$ est **ouvert** si pour tout $a \in U$ il existe $r > 0$ tel que $B(a, r) \subset U$, l'ensemble vide étant ouvert par convention, on dit que $V \subset \mathbb{R}^k$ est **fermé** si son complémentaire est ouvert, et on dit que $W \subset \mathbb{R}^k$ est **borné** s'il existe $R > 0$ tel que $W \subset B(0, R)$.

Si $U \subset \mathbb{R}^k$ est ouvert, on pose $m_k(U) = \sup_{C \in \mathcal{C}, C \subset U} m_k(C)$.

Soit maintenant F un fermé borné de \mathbb{R}^k , et soit U un ouvert borné de \mathbb{R}^k tel que $F \subset U$. Soit V le complémentaire de F dans U . Alors E est ouvert. On pose

$$(3.1) \quad m_k(F) = m_k(U) - m_k(V)$$

Définition 3.1.1

1) On dit qu'un ensemble borné $R \subset \mathbb{R}^k$ est mesurable au sens de Lebesgue s'il existe une suite $(U_n)_{n \geq 1}$ d'ouverts de \mathbb{R}^k contenant R et une suite $(F_n)_{n \geq 1}$ de fermés de \mathbb{R}^k contenus dans R tels que $\lim_{n \rightarrow +\infty} m_k(U_n) = \lim_{n \rightarrow +\infty} m_k(F_n)$, et dans ce cas on pose

$$m_k(R) = \lim_{n \rightarrow +\infty} m_k(U_n) = \lim_{n \rightarrow +\infty} m_k(F_n).$$

2) On dit qu'un ensemble non borné $S \subset \mathbb{R}^k$ est mesurable au sens de Lebesgue si $S \cap B(0, n)$ est mesurable au sens de Lebesgue pour $n \geq 1$, et dans ce cas on pose

$$m_k(S) = \lim_{n \rightarrow +\infty} m_k(S \cap B(0, n)).$$

De même que dans le cas $k = 1$, on a les propriétés suivantes :

(3.2) Si R est mesurable, alors le complémentaire de R est mesurable.

(3.3) Si $(R_n)_{n \geq 1}$ est une suite d'ensembles mesurables, alors $\cup_{n \geq 1} R_n$ et $\cap_{n \geq 1} R_n$ sont mesurables.

(3.4) Si $(R_n)_{n \geq 1}$ est une suite croissante d'ensembles mesurables, alors $m_k(\cup_{n \geq 1} R_n) = \lim_{n \rightarrow +\infty} m_k(R_n)$.

(3.5) Si $(R_n)_{n \geq 1}$ est une suite décroissante d'ensembles mesurables, et s'il existe $n_0 \geq 1$ tel que $m_k(R_{n_0}) < +\infty$, alors $m_k(\cap_{n \geq 1} R_n) = \lim_{n \rightarrow +\infty} m_k(R_n)$.

D'autre part la mesure de Lebesgue est de nouveau **invariante par translation** : si $E \in \mathbb{R}^k$ est mesurable, alors $m(E - a) = m(E)$ pour tout $a = (a_1, \dots, a_k) \in \mathbb{R}^k$, où $E - a = \{x - a\}_{x \in E}$.

Définition 3.1.2 On dit que $f : \mathbb{R}^k \rightarrow \mathbb{C}$ est mesurable si $f^{-1}(E) := \{x \in \mathbb{R}^k \mid f(x) \in E\}$ est mesurable pour tout ouvert E de \mathbb{C} .

La somme, le produit, le sup et l'inf de deux fonctions mesurables sont mesurables. On vérifie que toute limite simple d'une suite de fonctions mesurables est mesurable : si f_n est mesurable pour $n \geq 1$, et si $f(x) = \lim_{n \rightarrow +\infty} f_n(x)$ pour tout x , alors f est mesurable.

Si $E \subset \mathbb{R}^k$, on pose $\chi_E(x) = 1$ si $x \in E$, $\chi_E(x) = 0$ si $x \notin E$. On dit qu'une fonction f est une *fonction en escalier* s'il existe une famille finie E_1, \dots, E_p d'ensembles mesurables de mesure finie et une famille c_1, \dots, c_p de réels tels que l'on ait

$$f = \sum_{1 \leq i \leq p} c_i \chi_{E_i}.$$

On pose alors

$$\int \dots \int_{\mathbb{R}^k} f(x_1, \dots, x_k) dx_1 \dots dx_k = \sum_{1 \leq i \leq p} c_i m_k(E_i).$$

Définition 3.1.3 Soit $f : \mathbb{R}^k \rightarrow [0, +\infty[$ une fonction mesurable positive, et soit $(f_n)_{n \geq 1}$ une suite croissante de fonctions positives en escalier telle que $f(x) = \lim_{n \rightarrow +\infty} f_n(x)$ pour tout $x \in \mathbb{R}^k$. On pose

$$\int \dots \int_{\mathbb{R}^k} f(x_1, \dots, x_k) dx_1 \dots dx_k = \lim_{n \rightarrow +\infty} \int \dots \int_{\mathbb{R}^k} f_n(x_1, \dots, x_k) dx_1 \dots dx_k \in [0, +\infty].$$

On dit que la fonction f est intégrable si $\int \dots \int_{\mathbb{R}^k} |f(x_1, \dots, x_k)| dx_1 \dots dx_k < +\infty$.

Définition 3.1.4

1) Soit $f : \mathbb{R}^k \rightarrow \mathbb{C}$ une fonction mesurable. On dit que f est intégrable quand $|f|$ est intégrable, et dans ce cas on pose

$$\int \dots \int_{\mathbb{R}^k} f(x_1, \dots, x_k) dx_1 \dots dx_k = \int \dots \int_{\mathbb{R}^k} f^+(x_1, \dots, x_k) dx_1 \dots dx_k - \int \dots \int_{\mathbb{R}^k} f^-(x_1, \dots, x_k) dx_1 \dots dx_k,$$

où $f^+(x) = \max(f(x), 0)$ et $f^-(x) = \max(-f(x), 0)$ pour $x = (x_1, \dots, x_k) \in \mathbb{R}^k$.

2) Soit $f : \mathbb{R}^k \rightarrow \mathbb{C}$ une fonction mesurable. On dit que f est intégrable quand $|f|$ est intégrable, et dans ce cas on pose

$$\int \dots \int_{\mathbb{R}^k} f(x_1, \dots, x_k) dx_1 \dots dx_k = \int_{\mathbb{R}} \operatorname{Re} f(x_1, \dots, x_k) dx_1 \dots dx_k + i \int \dots \int_{\mathbb{R}^k} \operatorname{Im} f(x_1, \dots, x_k) dx_1 \dots dx_k.$$

On va maintenant définir une notion d'intégration sur un ensemble mesurable.

Définition 3.1.5 Soit $E \subset \mathbb{R}^k$ un ensemble mesurable, soit $f : E \rightarrow \mathbb{C}$ une fonction et soit $\tilde{f} : \mathbb{R}^k \rightarrow \mathbb{C}$ l'extension de f à \mathbb{R}^k définie par les formules $\tilde{f}(x) = f(x)$ si $x \in E$, $\tilde{f}(x) = 0$ si $x \notin E$. On dit que f est mesurable sur E si \tilde{f} est mesurable, et on dit que f est intégrable sur E si \tilde{f} est intégrable sur \mathbb{R}^k . Dans ce cas on pose

$$\int \dots \int_E f(x_1, \dots, x_k) dx_1 \dots dx_k = \int \dots \int_{\mathbb{R}^k} \tilde{f}(x_1, \dots, x_k) dx_1 \dots dx_k$$

On a des propriétés analogues à celles obtenues pour $k = 1$: si f et g sont intégrables sur E , alors $\lambda f + \mu g$ est intégrable sur E pour $\lambda, \mu \in \mathbb{C}$ et on a

$$(3.6) \int_E (\lambda f(x_1, \dots, x_k) + \mu g(x_1, \dots, x_k)) dx_1 \dots dx_k = \lambda \int_E f(x_1, \dots, x_k) dx_1 \dots dx_k + \mu \int_E g(x_1, \dots, x_k) dx_1 \dots dx_k.$$

Si $f : E \longrightarrow \mathbb{C}$ est intégrable sur un ensemble mesurable E , on a

$$(3.7) \quad \left| \int_E f(x_1, \dots, x_k) dx_1 \dots dx_k \right| \leq \int_E |f(x_1, \dots, x_k)| dx_1 \dots dx_k.$$

On a également un analogue de l'inégalité de Cauchy-Schwartz : Si f et g sont mesurables sur E , et si $|f|^2$ et $|g|^2$ sont intégrables sur E , alors fg est intégrable sur E et on a

$$(3.8) \quad \left| \int_E f(x_1, \dots, x_k) g(x_1, \dots, x_k) dx_1 \dots dx_k \right| \\ \leq \sqrt{\int_E |f(x_1, \dots, x_k)|^2 dx_1 \dots dx_k} \sqrt{\int_E |g(x_1, \dots, x_k)|^2 dx_1 \dots dx_k}.$$

On dira qu'une propriété est vraie *presque partout* si elle est vérifiée sur le complémentaire d'un ensemble de mesure nulle.

On déduit de la définition de l'intégrale de Lebesgue que l'on a la propriété suivante

Proposition 3.1.6 *Soit f une fonction intégrable sur un ensemble E . Si une fonction g est égale à f presque partout sur E , alors g est intégrable sur E et on a*

$$\int_E f(x_1, \dots, x_k) dx_1 \dots dx_k = \int_E g(x_1, \dots, x_k) dx_1 \dots dx_k.$$

On a les mêmes résultats fondamentaux que dans le cas $k = 1$.

Théorème 3.1.7 (*Théorème de convergence dominée*) *Soit $(f_n)_{n \geq 1}$ une suite de fonctions mesurables sur un ensemble mesurable $E \subset \mathbb{R}^k$ et soit f une fonction définie sur E .*

On suppose que les deux conditions suivantes sont vérifiées :

(i) *$\lim_{n \rightarrow +\infty} f_n(x_1, \dots, x_k) = f(x_1, \dots, x_k)$ presque partout sur E .*

(ii) *Il existe une fonction intégrable g sur E telle que $|f_n(x_1, \dots, x_k)| \leq g(x_1, \dots, x_k)$ presque partout pour tout $n \geq 1$.*

Alors f est intégrable sur E , et $\int_E f(x_1, \dots, x_k) dx_1 \dots dx_k = \lim_{n \rightarrow +\infty} \int_E f_n(x_1, \dots, x_k) dx_1 \dots dx_k$.

Théorème 3.1.8 (*Théorème de convergence monotone*) *Soit $(f_n)_{n \geq 1}$ une suite croissante de fonctions positives intégrables sur un ensemble mesurable E telle que $f(x_1, \dots, x_k) := \lim_{n \rightarrow +\infty} f_n(x_1, \dots, x_k)$ soit finie pour presque tout $x \in E$. Alors on a*

$$\int_E f(x_1, \dots, x_k) dx_1 \dots dx_k = \lim_{n \rightarrow +\infty} \int_E f_n(x_1, \dots, x_k) dx_1 \dots dx_k \in [0, +\infty].$$

Notons que dans le cas où $\lim_{n \rightarrow +\infty} \int_E f_n(x_1, \dots, x_k) dx_1 \dots dx_k = +\infty$, le théorème indique que f n'est pas intégrable sur E .

3.2 La transformée de Fourier en plusieurs variables

On va introduire des espaces de fonctions analogues à ceux introduits dans le cas $k = 1$.

1) $L^1(\mathbb{R}^k)$ désigne l'espace vectoriel des fonctions intégrables sur \mathbb{R}^k , **où on identifie les fonctions égales presque partout**. Pour $f \in L^1(\mathbb{R}^k)$ on pose

$$\|f\|_1 := \int_{-\infty}^{+\infty} |f(x_1, \dots, x_k)| dx_1 \dots dx_k.$$

2) $L^2(\mathbb{R}^k)$ désigne l'espace vectoriel des fonctions mesurables sur \mathbb{R}^k telles que $|f|^2$ soit intégrable sur \mathbb{R}^k , **où on identifie les fonctions égales presque partout**. Pour $f \in L^2(\mathbb{R}^k)$ on pose

$$\|f\|_2 := \sqrt{\int_{-\infty}^{+\infty} |f(x_1, \dots, x_k)|^2 dx_1 \dots dx_k}.$$

3) $L^\infty(\mathbb{R}^k)$ désigne l'espace vectoriel des fonctions mesurables sur \mathbb{R}^k telles qu'il existe $m \geq 0$ vérifiant $|f(x_1, \dots, x_k)| \leq m$ presque partout, **où on identifie les fonctions égales presque partout**. Pour $f \in L^\infty(\mathbb{R}^k)$ on pose

$$\|f\|_\infty = \inf\{m \geq 0 \mid |f(x_1, \dots, x_k)| \leq m \text{ presque partout}\}.$$

Pour $x = x_1, \dots, x_k \in \mathbb{R}^k$, on pose $|x| = \sqrt{x_1^2 + \dots + x_n^2}$. Ceci permet d'introduire les espaces suivants.

4) $\mathcal{C}_0(\mathbb{R}^k)$ désigne l'ensemble des fonctions continues sur \mathbb{R}^k telles que $\lim_{|x| \rightarrow +\infty} f(x) = 0$. Pour $f \in \mathcal{C}_0(\mathbb{R}^k)$, on pose

$$\|f\|_\infty = \sup_{x \in \mathbb{R}^k} |f(x)|.$$

5) $\mathcal{E}(\mathbb{R}^k)$ désigne l'espace des fonctions f ayant des dérivées partielles de tous ordres sur \mathbb{R}^k telles que l'on ait :

$$\lim_{|x| \rightarrow +\infty} |x|^p |f(t)| = 0 \quad \forall q \geq 0 \text{ et } \lim_{|t| \rightarrow +\infty} |x|^p \left| \frac{\partial^{\alpha_1 + \dots + \alpha_k} f}{\partial^{\alpha_1} x_1 \dots \partial^{\alpha_k} x_k}(x_1, \dots, x_k) \right| = 0$$

$$\forall \alpha_1 \geq 0, \dots, \forall \alpha_k \geq 0, \forall q \geq 0.$$

Dans les quatre premiers cas on a de nouveau affaire à des espaces de Banach, et $\mathcal{E}(\mathbb{R}^k)$ est un espace de Fréchet.

On a de nouveau un produit de convolution dans ce contexte.

Théorème 3.2.1 Soient $f, g \in L^1(\mathbb{R}^k)$. Alors la fonction $t \mapsto f(x - t)g(t)$ est intégrable sur \mathbb{R}^k pour presque tout $x \in \mathbb{R}^k$. De plus si on définit presque partout le produit de convolution $f * g$ par la formule

$$(f * g)(x_1, \dots, x_k) = \int_{-\infty}^{+\infty} f(x_1 - t_1, \dots, x_k - t_k) g(t_1, \dots, t_k) dt_1 \dots dt_k,$$

alors $f * g \in L^1(\mathbb{R}^k)$, et $\|f * g\|_1 \leq \|f\|_1 \|g\|_1$.

Le produit de convolution est **commutatif** et **associatif**, c'est à dire qu'on a les propriétés suivantes :

$$(3.9) \quad f * g = g * f \quad \forall f \in L^1(\mathbb{R}^k), \quad \forall g \in L^1(\mathbb{R}^k).$$

$$(3.10) \quad f * (g * h) = (f * g) * h \quad \forall f \in L^1(\mathbb{R}^k), \quad \forall g \in L^1(\mathbb{R}^k), \quad \forall h \in L^1(\mathbb{R}^k).$$

On va maintenant définir la transformation de Fourier.

Définition 3.2.2 Soit $f \in L^1(\mathbb{R}^k)$. Pour $x = (x_1, \dots, x_k) \in \mathbb{R}^k$, on pose

$$\hat{f}(x) = \int_{-\infty}^{+\infty} f(t_1, \dots, t_k) e^{-it_1 x_1 + \dots - it_k x_k} dt_1 \dots dt_k$$

La fonction \hat{f} est appelée la transformée de Fourier de f , et l'application $\mathcal{F} : f \mapsto \hat{f}$ est appelée la transformation de Fourier.

Il est clair que la transformation de Fourier est une application linéaire. Le théorème suivant résume les principales propriétés de la transformation de Fourier.

Théorème 3.2.3

1) Si $f \in L^1(\mathbb{R}^k)$, alors $\hat{f} \in C_0(\mathbb{R}^k)$, et $\|\hat{f}\|_\infty \leq \|f\|_1$.

2) On a $\mathcal{F}(f * g) = \mathcal{F}(f)\mathcal{F}(g)$ pour $f \in L^1(\mathbb{R}^k)$, $g \in L^1(\mathbb{R}^k)$.

3) Si f et \hat{f} appartiennent à $L^1(\mathbb{R}^k)$, alors on a pour presque tout $t = (t_1, \dots, t_k) \in \mathbb{R}^k$,

$$f(t_1, \dots, t_k) = \frac{1}{(2\pi)^k} \int \dots \int_{\mathbb{R}^k} \hat{f}(x_1, \dots, x_k) e^{it_1 x_1 + \dots + it_k x_k} dx_1 \dots dx_k.$$

4) (i) Si $f \in \mathcal{E}(\mathbb{R}^k)$, alors $\hat{f} \in \mathcal{E}(\mathbb{R}^k)$ et la transformation de Fourier $\mathcal{F} : \mathcal{E}(\mathbb{R}^k) \longrightarrow \mathcal{E}(\mathbb{R}^k)$ est bijective.

(ii) On a $\mathcal{F}^{-1}(f)(t_1, \dots, t_k) = \frac{1}{(2\pi)^k} \int \dots \int_{\mathbb{R}^k} f(x_1, \dots, x_k) e^{it_1 x_1 + \dots + it_k x_k} dx$ pour $f \in \mathcal{E}(\mathbb{R}^k)$, $t \in \mathbb{R}^k$.

(iii) Pour $f \in \mathcal{E}(\mathbb{R}^k)$, $x_1, \dots, x_k \in \mathbb{R}$, $p_1 \geq 0, \dots, p_k \geq 0$, on a

$$\mathcal{F}\left(\frac{\partial^{p_1 + \dots + p_k} f}{\partial^{p_1} x_1 \dots \partial^{p_k} x_k}\right)(x_1, \dots, x_k) = (ix_1)^{p_1} \dots (ix_k)^{p_k} \mathcal{F}(f)(x_1, \dots, x_k)$$

La formule 3) du théorème ci-dessus est appelée la **formule d'inversion de Fourier**. Elle montre en particulier que si $f \in L^1(\mathbb{R}^k)$, et si $\hat{f} = 0$, alors $f = 0$, ou plus précisément f est nulle presque partout, ce qui veut dire que f est l'élément nul de $L^1(\mathbb{R}^k)$. Ceci montre que $\mathcal{F} : L^1(\mathbb{R}^k) \longrightarrow \mathcal{C}_0(\mathbb{R}^k)$ est **injective**. Par contre, de même que dans le cas où $k = 1$, on peut montrer que $\mathcal{F} : L^1(\mathbb{R}^k) \longrightarrow \mathcal{C}_0(\mathbb{R}^k)$ **n'est pas surjective**.

De même que dans le cas $k = 1$, les formules 3) et 4)(iii) du théorème sont très utiles pour résoudre des équations de convolution ou des équations aux dérivées partielles en utilisant la transformation de Fourier.

On va maintenant décrire la transformée de Fourier sur $L^2(\mathbb{R}^k)$. On se contentera du résultat suivant, moins précis que celui donné dans le cas $k = 1$, qui utilise le fait que si $f \in L^2(\mathbb{R}^k)$ alors f est intégrable sur tout ensemble mesurable borné de \mathbb{R}^k .

Théorème 3.2.4 Soit $f \in L^2(\mathbb{R}^k)$, et pour $R > 0$ soit f_R la fonction définie par les formules $f_R(x) = f(x)$ si $|x| \leq R$, $f_R(x) = 0$ si $|x| > R$, de sorte que $f_R \in L^1(\mathbb{R}^k)$. Alors il existe une fonction $\hat{f} \in L^2(\mathbb{R}^k)$ telle que $\lim_{R \rightarrow +\infty} \|\hat{f} - \hat{f}_R\|_2 = 0$. Cette fonction est appelée la transformée de Fourier de f .

On a les propriétés suivantes.

Théorème 3.2.5 Pour $f \in L^2(\mathbb{R}^k)$, on a $\hat{f} \in L^2(\mathbb{R}^k)$ et

$$(i) \int_{-\infty}^{+\infty} |f(x_1, \dots, x_k)|^2 dx_1 \dots dx_k = \frac{1}{(2\pi)^k} \int_{-\infty}^{+\infty} |\hat{f}(x_1, \dots, x_k)|^2 dx_1 \dots dx_k.$$

Pus généralement on a, pour $f \in L^2(\mathbb{R}^k)$, $g \in L^2(\mathbb{R}^k)$,

$$(ii) \int_{-\infty}^{+\infty} f(x_1, \dots, x_k) \bar{g}(x_1, \dots, x_k) dx_1 \dots dx_k = \frac{1}{(2\pi)^k} \int_{-\infty}^{+\infty} \hat{f}(x_1, \dots, x_k) \bar{\hat{g}}(x_1, \dots, x_k) dx_1 \dots dx_k,$$

et la transformation de Fourier $\mathcal{F} : f \mapsto \hat{f}$ est une bijection de $L^2(\mathbb{R}^k)$ sur lui-même. La transformée de Fourier inverse est donnée par la formule

$$\mathcal{F}^{-1}(f)(x) = \frac{1}{(2\pi)^k} \mathcal{F}(f)(-x).$$

De même que dans le cas $k = 1$, la formule (i) est appelée formule de Parseval, la première formule de (ii) est appelée formule de Plancherel et la deuxième formule de (ii) est appelée formule d'inversion de Fourier.

3.3 Le théorème de Fubini

Soient p et q deux entiers positifs. On note $\pi_1 : (x, y) \mapsto x$ la projection de \mathbb{R}^{p+q} sur \mathbb{R}^p et $\pi_2 : (x, y) \mapsto y$ la projection de \mathbb{R}^{p+q} sur \mathbb{R}^q . On pose $dx := dx_1 \dots dx_p$, $dy := dy_1 \dots dy_q$.

Soit $E \subset \mathbb{R}^{p+q}$. Pour $x \in \mathbb{R}^p$, on pose

$$E_x = \{y \in \mathbb{R}^q \mid (x, y) \in E\}$$

De même, pour $y \in \mathbb{R}^q$, on pose

$$E^y = \{x \in \mathbb{R}^p \mid (x, y) \in E\}.$$

On a donc $\pi_1(E) = \{x \in \mathbb{R}^p \mid E_x \neq \emptyset\}$ et $\pi_2(E) = \{y \in \mathbb{R}^q \mid E^y \neq \emptyset\}$.

On peut maintenant énoncer le théorème de Fubini.

Théorème 3.3.1 *Soient p et q deux entiers positifs, et soit $E \subset \mathbb{R}^{p+q}$ un ensemble mesurable.*

1) *L'ensemble $E_x \subset \mathbb{R}^q$ est mesurable pour presque tout $x \in \pi_1(E)$, et l'ensemble $E^y \subset \mathbb{R}^p$ est mesurable pour presque tout $y \in \pi_2(E)$.*

2) *Soit $f : E \rightarrow [0, +\infty[$ une fonction mesurable. On a*

$$\int \dots \int_E f(x, y) dx dy = \int \dots \int_{\pi_1(E)} \left[\int \dots \int_{E_x} f(x, y) dy \right] dx = \int \dots \int_{\pi_2(E)} \left[\int \dots \int_{E^y} f(x, y) dx \right] dy \in [0, +\infty].$$

3) *Soit $g : E \rightarrow \mathbb{C}$ une fonction intégrable. Alors la restriction de g à E_x est intégrable pour presque tout $x \in \pi_1(E)$, la restriction de g à E^y est intégrable pour presque tout $y \in \pi_2(E)$, et on a :*

$$\int \dots \int_E g(x, y) dx dy = \int \dots \int_{\pi_1(E)} \left[\int \dots \int_{E_x} g(x, y) dy \right] dx = \int \dots \int_{\pi_2(E)} \left[\int \dots \int_{E^y} g(x, y) dx \right] dy.$$

Notons que la formule 2) s'applique aux fonctions positives mesurables non intégrables. Dans ce cas on a

$$\int \dots \int_E f(x, y) dx dy = \int \dots \int_{\pi_1(E)} \left[\int \dots \int_{E_x} f(x, y) dy \right] dx = \int \dots \int_{\pi_2(E)} \left[\int \dots \int_{E^y} f(x, y) dx \right] dy = +\infty.$$

En pratique **tous les ensembles et toutes les fonctions dont ont à s'occuper les ingénieurs sont mesurables.** Pour appliquer la formule 3) du théorème à une fonction g on procèdera donc de la manière suivante (notons que si E et g sont bornés on peut se dispenser de l'étape 1, et que si f est positive l'étape 1 donne directement le résultat).

1) On vérifie que $\int \dots \int_E |g(x, y)| dx dy < +\infty$ en calculant au choix $\int \dots \int_{\pi_1(E)} \left[\int \dots \int_{E_x} f(x, y) dy \right] dx$ ou $\int \dots \int_{\pi_2(E)} \left[\int \dots \int_{E^y} f(x, y) dx \right] dy$.

2) On obtient $\int \dots \int_E f(x, y) dx dy$ en calculant au choix $\int \dots \int_{\pi_1(E)} \left[\int \dots \int_{E_x} f(x, y) dy \right] dx$ ou $\int \dots \int_{\pi_2(E)} \left[\int \dots \int_{E^y} f(x, y) dx \right] dy$.

On va maintenant donner trois exemples d'applications de ce théorème, les deux premières très simples et la troisième plus sophistiquée.

Exemple 3.3.1 : Aire d'un disque.

Soit $D = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq R^2\}$ le disque fermé de rayon R centré à l'origine.

Pour $x \in \mathbb{R}$ on a $D_x = \{y \in \mathbb{R} \mid x^2 + y^2 \leq R^2\} = \{y \in \mathbb{R} \mid y^2 \leq R^2 - x^2\}$.

Si $|x| > R$ on a $D_x = \emptyset$, et si $|x| \leq R$ on a $D_x = [-\sqrt{R^2 - x^2}, \sqrt{R^2 - x^2}]$. Donc $\pi_1(D) = [-R, R]$.

D'après le théorème de Fubini on a

$$\text{Aire}(D) = \int_D dx dy = \int_{\pi_1(D)} \left[\int_{D_x} dy \right] dx = \int_{-R}^R \left[\int_{-\sqrt{R^2 - x^2}}^{\sqrt{R^2 - x^2}} dy \right] dx = \int_{-R}^R 2\sqrt{R^2 - x^2} dx.$$

Pour calculer cette intégrale on remarque que $\int_{-R}^R 2\sqrt{R^2 - x^2} dx = 4 \int_0^R \sqrt{R^2 - x^2} dx$.

On pose $x = R \sin t$, soit $dx = R \cos t dt$, avec $t \in [0, \frac{\pi}{2}]$, et on obtient

$$\int_0^R \sqrt{R^2 - x^2} dx = \int_0^{\frac{\pi}{2}} \sqrt{R^2 - R^2 \sin^2 t} R \cos t dt = R^2 \int_0^{\frac{\pi}{2}} \sqrt{1 - \sin^2 t} \cos t dt = \int_0^{\frac{\pi}{2}} \cos^2 t dt = \frac{R^2}{2} \int_0^{\frac{\pi}{2}} (1 + \cos 2t) dt = \frac{R^2}{2} \left[t + \frac{\sin 2t}{2} \right]_0^{\frac{\pi}{2}} = \frac{R^2}{2} \left[\frac{\pi}{2} + \frac{\sin \pi}{2} \right] = \frac{R^2}{2} \cdot \frac{\pi}{2} = \frac{\pi R^2}{4}.$$

$$= \frac{\pi R^2}{4} + \left[\frac{\sin 2t}{2} \right]_0^{\frac{\pi}{2}} = \frac{\pi R^2}{4}.$$

Donc Aire(D) = πR^2 (ouf).

Exemple 3.3.2 : Volume d'une sphère.

Soit $S = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 \leq R^2\}$ la sphère fermée de rayon R centrée à l'origine.

Pour $x \in \mathbb{R}$ on a $D_x = \{(y, z) \in \mathbb{R}^2 \mid x^2 + y^2 + z^2 \leq R^2\} = \{(y, z) \in \mathbb{R}^2 \mid y^2 + z^2 \leq R^2 - x^2\}$. Si $|x| > R$ on a $S_x = \emptyset$, et si $|x| \leq R$ on a $S_x = D(0, \sqrt{R^2 - x^2})$, où $D(0, \sqrt{R^2 - x^2})$ désigne le disque fermé de rayon $\sqrt{R^2 - x^2}$ centré à l'origine. Donc $\pi_1(S) = [-R, R]$.

D'après le théorème de Fubini on a

$$\begin{aligned} \text{Vol}(S) &= \int \dots \int_S dx dy dz = \int_{\pi_1(S)} \left[\int \int_{S_x} dy dz \right] dx = \int_{-R}^R \left[\int \int_{D(0, \sqrt{R^2 - x^2})} dy dz \right] dx = \int_{-R}^R \pi(R^2 - x^2) dx \\ &= 2 \int_{-R}^R \pi(R^2 - x^2) dx = 2 \left[R^2 x - \frac{x^3}{3} \right]_{-R}^R. \end{aligned}$$

On obtient donc $\text{Vol}(S) = \frac{4\pi R^3}{3}$, et un grand bravo à Archimède, qui a obtenu ce résultat sans disposer de la théorie de l'intégration (on sait qu'Archimède était également un grand physicien, qui avait transformé sa Baignoire en Laboratoire [1]; spécialiste de l'optique aussi bien que de l'hydraulique, il avait trouvé le moyen d'incendier la flotte Romaine au moyen de miroirs reflétant le soleil. Ceci n'a malheureusement pas empêché les Romains de s'emparer de Syracuse en l'an -212, et Archimède figure parmi les nombreuses victimes du massacre qui s'ensuivit).

Exemple 3 : Démonstration du théorème 2.1.1.

Soient f et g deux fonctions intégrables sur \mathbb{R} . On vérifie que si $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}$ est continue, et si $h : \mathbb{R} \rightarrow \mathbb{C}$ est mesurable, alors $f \circ \phi : \mathbb{R}^2 \rightarrow \mathbb{C}$ est mesurable. Comme les applications $(x, t) \mapsto x - t$ et $(x, t) \mapsto t$ sont continues, l'application $h : (x, t) \mapsto f(x - t)g(t)$ est mesurable sur \mathbb{R}^2 .

On a d'après le théorème de Fubini,

$$\begin{aligned} \int \int_{\mathbb{R}^2} |f(x-t)g(t)| dt &= \int_{\mathbb{R}} \left[\int_{\mathbb{R}} |f(x-t)g(t)| dx \right] dt = \int_{\mathbb{R}} |g(t)| \left[\int_{\mathbb{R}} |f(x-t)| dx \right] dt = \int_{\mathbb{R}} |g(t)| \left[\int_{\mathbb{R}} |f(s)| ds \right] \\ &= \int_{\mathbb{R}} |f(s)| ds \int_{\mathbb{R}} |g(t)| dt = \|f\|_1 \|g\|_1 < +\infty. \end{aligned}$$

Donc h est intégrable sur R . D'après le théorème de Fubini, la fonction $t \rightarrow f(x-t)g(t)$ est intégrable sur \mathbb{R} pour presque tout $x \in \mathbb{R}$, et si on définit le produit de convolution $f * g$ presque partout sur \mathbb{R} par la formule

$$(f * g)(x) = \int_{\mathbb{R}} f(x-t)g(t)dt,$$

on obtient

$$\begin{aligned} \int_{\mathbb{R}} |(f * g)(x)|dx &= \int_{\mathbb{R}} \left| \int_{\mathbb{R}} f(x-t)g(t)dt \right| dx \leq \int_{\mathbb{R}} \left[\int_{\mathbb{R}} |f(x-t)g(t)|dt \right] dx \\ &= \int \int_{\mathbb{R}^2} |f(x-t)g(t)|dt = \|f\|_1 \|g\|_1. \end{aligned}$$

Donc $f * g \in L^1(\mathbb{R})$, et $\|f * g\|_1 \leq \|f\|_1 \|g\|_1$. ♣

3.4 Exercices sur le Chapitre 3

exercice 1

Soient $f_1, \dots, f_k \in L^1(\mathbb{R})$. On pose $g(t_1, \dots, t_k) = f_1(t_1) \dots f_k(t_k)$.

1) Montrer que $g \in L^1(\mathbb{R}^k)$ et que l'on a, pour $x = (x_1, \dots, x_k) \in \mathbb{R}^k$,

$$\hat{g}(x) = \hat{f}_1(x_1) \dots \hat{f}_k(x_k).$$

2) On pose $g(t_1, \dots, t_k) = e^{-|t_1| \dots - |t_k|}$. En utilisant l'exercice 1 du Chapitre 2, en déduire la valeur de $\hat{g}(x_1, \dots, x_k)$.

exercice 2

1) Soit f une fonction ayant des dérivées partielles d'ordre 1 continues sur \mathbb{R}^k . On suppose que $\lim_{\|x\|_2 \rightarrow +\infty} f(x) = 0$, et que $\frac{\partial f}{\partial x_j}$ est intégrable sur \mathbb{R}^k . En utilisant le théorème de Fubini et une intégration par parties, vérifier que l'on a

$$\mathcal{F}\left(\frac{\partial f}{\partial x_j}\right)(t_1, \dots, t_k) = it_j \mathcal{F}(f)(t_1, \dots, t_k).$$

2) Soit $r > 0$. On pose $u_r(x) = 1$ pour $0 \leq x \leq r^2$, $u_r(x) = 1 - \frac{(x-r^2)^2}{2r^2}$ pour $r^2 \leq x \leq 2r^2$, $u_r(x) = \frac{(x-3r^2)^2}{2r^2}$ pour $2r^2 < x \leq 3r^2$, $u_r(x) = 0$ pour $x > 3r^2$ et $u_r(x) = u_r(-x)$ pour $x < 0$. Esquisser le graphe de u_r et vérifier que u_r est continûment dérivable sur \mathbb{R} .

3) Soit f une fonction admettant des dérivées partielles d'ordre ≤ 2 continues sur un ouvert U de \mathbb{R}^k , soit $a = (a_1, \dots, a_k) \in U$ et soit $r > 0$ tel que tout $x \in \mathbb{R}^k$ vérifiant

$\|x - a\|_2 \leq 3r$ appartienne à U . On pose $g(x_1, \dots, x_k) = f(x_1, \dots, x_k)u((x_1 - a_1)^2 + \dots + (x_k - a_k)^2)$ pour $x = (x_1, \dots, x_k) \in \mathbb{R}^k$.

a) Vérifier que $\frac{\partial f}{\partial x_j}(x) = \frac{\partial g}{\partial x_j}(x)$ pour $\|x\|_2 < r$, $1 \leq j \leq k$.

b) En déduire que $\frac{\partial^2 f}{\partial x_j \partial x_l} = \frac{\partial^2 g}{\partial x_l \partial x_j}$ pour $1 \leq j \leq k, 1 \leq l \leq k$ (théorème de Schwarz).

exercice 3 On pose $A = \{(x, y) \in \mathbb{R}^2 \mid x^2 + 2y^2 \leq 1, x \geq 0\}$.

1) Dessiner A .

2) Calculer l'aire de A en utilisant le théorème de Fubini.

exercice 4 (Annales ESTIA, Examen Transformées 2002)

On pose $V = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 \leq z^2, 0 \leq z \leq 1\}$. Quelle est la nature géométrique de V ? Calculer le volume de V en utilisant le théorème de Fubini.

exercice 5

1) En passant en coordonnées polaires, calculer $\int \int_{D_R} e^{-x^2 - y^2} dx dy$, où $D_R = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq R^2\}$.

2) En déduire que $\int_0^{+\infty} e^{-x^2} dx = \frac{\sqrt{\pi}}{2}$.

exercice 6(Annales ESTIA, Examen Transformées 2001)

On rappelle que le volume de la sphère de rayon R dans \mathbb{R}^3 est égal à $\frac{4}{3}\pi R^3$. On considère dans \mathbb{R}^4 l'hypersphère $\mathcal{S}_R = \{(x, y, z, t) \in \mathbb{R}^4 \mid x^2 + y^2 + z^2 + t^2 \leq R^2\}$, et on définit le volume de l'hypersphère \mathcal{S}_R par la formule

$$V(\mathcal{S}_R) = \int \int \int \int_{\mathcal{S}_R} dx dy dz dt$$

Calculer $V(\mathcal{S}_R)$ en utilisant le théorème de Fubini.

exercice 7

- 1) Calculer $\int_0^{+\infty} \frac{dt}{1+t^2}$ et $\int_0^{+\infty} e^{-xt} dt$.
- 2) Montrer que $\lim_{L \rightarrow +\infty} \int_0^{+\infty} \frac{(\cos L + t \sin L) e^{-tL}}{1+t^2} dt = 0$.
- 3) Calculer $\int_0^A \sin(x) e^{-tx} dt$ (on pourra utiliser Mupad).
- 4) On pose $f(x, t) = \sin(x) e^{-xt}$. Montrer que f est intégrable sur $[0, L] \times [0, +\infty]$ pour $L > 0$.
- 5) En appliquant le théorème de Fubini à f , montrer que $\lim_{L \rightarrow +\infty} \int_0^L \frac{\sin x}{x} dx = \frac{\pi}{2}$.

Chapitre 4

Transformée de Laplace et applications

4.1 Définition de la transformée de Laplace

Définition 4.1.1 Soit f une fonction mesurable sur $[0, +\infty[$, et soit $z \in \mathbb{C}$. Si $\int_0^{+\infty} |f(t)|e^{-zt}|dt < +\infty$, on pose

$$\mathcal{L}(f)(z) = \int_0^{+\infty} f(t)e^{-zt}dt.$$

La fonction $\mathcal{L}(f)$ est appelée la **transformée de Laplace** de f et l'ensemble des nombres complexes z tels que $\int_0^{+\infty} |f(t)|e^{-zt}|dt < +\infty$ est appelé le **domaine de définition de $\mathcal{L}(f)$** . Il est clair que la transformation de Laplace est linéaire : si z appartient à l'intersection des domaines de définition des transformées de Laplace de f et g , on a pour $\lambda, \mu \in \mathbb{C}$

$$\mathcal{L}(\lambda f + \mu g)(z) = \lambda \mathcal{L}(f)(z) + \mu \mathcal{L}(g)(z).$$

Pour $a \in \mathbb{R}$ on pose $P_a := \{z \in \mathbb{C} \mid \operatorname{Re}(z) \geq a\}$ et $\mathring{P}_a := \{z \in \mathbb{C} \mid \operatorname{Re}(z) > a\}$.

Proposition 4.1.2 Soit f une fonction mesurable sur $[0, +\infty[$, et soit $\operatorname{Dom}(\mathcal{L}(f))$ le domaine de définition de $\mathcal{L}(f)$. Alors on a les quatre possibilités suivantes

(1) $\operatorname{Dom}(\mathcal{L}(f)) = \emptyset$,

(2) $\operatorname{Dom}(\mathcal{L}(f)) = \mathbb{C}$,

(3) Il existe $a \in \mathbb{R}$ tel que $\operatorname{Dom}(\mathcal{L}(f))$ soit égal au demi-plan fermé P_a ,

(4) Il existe $a \in \mathbb{R}$ tel que $\text{Dom}(\mathcal{L}(f))$ soit égal au demi-plan ouvert \mathring{P}_a .

Démonstration : Pour $z \in \mathbb{C}$, on a $|e^{zt}| = e^{\text{Re}(zt)} = e^{t\text{Re}(z)}$. Si $z \in \text{Dom}(\mathcal{L}(f))$, et si $\text{Re}(z') \geq \text{Re}(z)$, alors $e^{-t\text{Re}(z')} \leq e^{-t\text{Re}(z)}$ donc $\int_0^{+\infty} |f(t)|e^{-z't} dt \leq \int_0^{+\infty} |f(t)|e^{-zt} dt < +\infty$, et $z' \in \text{Dom}(\mathcal{L}(f))$. Si $\text{Dom}(\mathcal{L}(f))$ est non vide et distinct de \mathbb{C} , soit a la borne inférieure de $\text{Dom}(\mathcal{L}(f)) \cap \mathbb{R}$. Il résulte de ce qui précède que $\text{Dom}(\mathcal{L}(f)) = P_a$ si $a \in \text{Dom}(\mathcal{L}(f))$ et que $\text{Dom}(\mathcal{L}(f)) = \mathring{P}_a$ si $a \notin \text{Dom}(\mathcal{L}(f))$. ♣

On se souvient que $\int_1^{+\infty} \frac{dx}{x} = +\infty$ et que $\int_1^{+\infty} \frac{dx}{x^\alpha} < +\infty$ pour $\alpha > 1$. On en déduit le critère classique suivant

Proposition 4.1.3 (Critère de Riemann) Soit $a \in \mathbb{R}$, et soit $f \geq 0$ une fonction continue sur $[a, +\infty[$.

(i) Si $\lim_{x \rightarrow +\infty} x f(x) > 0$ alors f n'est pas intégrable sur $[a, +\infty[$.

(ii) S'il existe $\alpha > 1$ tel que $\lim_{x \rightarrow +\infty} x^\alpha f(x) < +\infty$, alors f est intégrable sur $[a, +\infty[$.

Ceci nous permet d'obtenir des exemples correspondant à chaque situation prévues ci-dessus pour le domaine de la transformée de Laplace.

Exemple 4.1.4

(1) Posons $f_1(x) = e^{x^2}$ pour $x > 0$. Alors $\text{Dom}(\mathcal{L}(f_1)) = \emptyset$.

(2) Posons $f_2(x) = e^{-x^2}$ pour $x > 0$. Alors $\text{Dom}(\mathcal{L}(f_2)) = \mathbb{C}$.

(3) Posons $f_3(x) = 1$ pour $x > 0$. Alors $\text{Dom}(\mathcal{L}(f_3)) = \mathring{P}_0$.

(4) Posons $f_4(x) = \frac{1}{1+x^2}$ pour $x > 0$. Alors $\text{Dom}(\mathcal{L}(f_4)) = P_0$.

En effet $\lim_{x \rightarrow +\infty} x^2 e^{x^2} e^{-ax} = +\infty$ pour tout $a \in \mathbb{R}$, ce qui prouve (1). D'autre part $\lim_{x \rightarrow +\infty} x e^{-x^2} e^{-ax} = 0$ pour tout $a \in \mathbb{R}$, ce qui prouve (2). On a $\lim_{x \rightarrow +\infty} x e^{-ax} = +\infty$ pour $a \leq 0$, $\lim_{x \rightarrow +\infty} x^2 e^{-ax} = 0$ pour $a > 0$, ce qui prouve (3). Enfin $\lim_{x \rightarrow +\infty} \frac{x}{1+x^2} e^{-ax} = +\infty$ pour $a < 0$, $\lim_{x \rightarrow +\infty} \frac{x^{3/2}}{1+x^2} e^{-ax} = 0$ pour $a \geq 0$, ce qui prouve (4) (tous ces calculs de limites sont basés sur le fait que l'exponentielle l'emporte sur les puissances, et on peut détailler ces calculs de limites en passant au logarithme).

Soit U un ouvert de \mathbb{C} . On dit qu'une fonction $F : U \rightarrow \mathbb{C}$ est **dérivable au sens complexe** en $u \in U$ si le quotient $\frac{F(u+h)-F(u)}{h}$ admet une limite quand h

tend vers 0 dans \mathbb{C} . Dans ce cas cette limite est notée $F'(u)$ (attention, c'est une condition beaucoup plus forte que la différentiabilité au sens réel : la fonction $z \mapsto \bar{z}$ n'est dérivable au sens complexe en aucun point de \mathbb{C}).

Théorème 4.1.5 *Soit f une fonction mesurable sur \mathbb{C} telle que $\text{Dom}(\mathcal{L}(f))$ soit non vide, et soit $a \in \mathbb{R}$.*

(i) *Si $\mathcal{L}(f)(z)$ est définie pour $\text{Re}(z) > a$, alors $\mathcal{L}(f)(z)$ est dérivable au sens complexe pour $\text{Re}(z) > a$, et on a pour $\text{Re}(z) > a$*

$$\mathcal{L}(f)'(z) = - \int_0^{+\infty} t f(t) e^{-zt} dt$$

(ii) *Si $\mathcal{L}(f)(z)$ est définie pour $\text{Re}(z) \geq a$, alors $\mathcal{L}(f)(z)$ est continue pour $\text{Re}(z) \geq a$.*

Le deuxième résultat est une conséquence simple du théorème de convergence dominée. Le premier résultat se déduit du théorème de convergence dominée et d'une version bidimensionnelle du théorème des accroissements finis.

On dispose dans certains cas d'une formule d'inversion pour la transformée de Laplace

Théorème 4.1.6 (*Formule d'inversion de Laplace*) *Soit f une fonction mesurable sur $[0, +\infty[$. Si $\mathcal{L}(f)$ est définie en $a \in \mathbb{R}$, et si on a*

$$\int_{-\infty}^{+\infty} |\mathcal{L}(f)(a + iy)| dy < +\infty$$

alors on a, pour presque tout $t \geq 0$,

$$f(t) = e^{at} \frac{1}{2\pi} \int_{-\infty}^{+\infty} \mathcal{L}(f)(a + iy) e^{ity} dy.$$

Démonstration : Posons $f_a(t) = 0$ pour $t < 0$, $f_a(t) = e^{-ta} f(t)$ pour $t > 0$. Puisque la transformée de Laplace de f est définie en a , la fonction f_a est intégrable sur \mathbb{R} , et on a pour $y \in \mathbb{R}$

$$(4.1) \quad \mathcal{L}(f)(a + iy) = \mathcal{F}(f_a)(y).$$

L'hypothèse du théorème montre alors que $\mathcal{F}(f_a) \in L^1(\mathbb{R})$. On peut alors appliquer la formule d'inversion de Fourier et on obtient pour presque tout $t \in [0, +\infty[$

$$f(t)e^{-at} = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \hat{f}_a(y) e^{ity} dy = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \mathcal{L}(f)(a + iy) e^{ity} dy. \clubsuit$$

4.2 Transformation de Laplace, convolution et dérivation

On se souvient que si $f, g \in L^1(\mathbb{R})$, alors on peut définir presque partout sur \mathbb{R} le produit de convolution $f * g \in L^1(\mathbb{R})$ par la formule

$$(f * g)(x) = \int_{-\infty}^{+\infty} f(x-t)g(t)dt.$$

Si f et g sont nulles presque partout sur $] -\infty, 0[$, la formule devient

$$(f * g)(x) = \int_0^x f(x-t)g(t)dt.$$

Ceci suggère le résultat suivant.

Théorème 4.2.1 *Soit $L_{loc}^1(\mathbb{R}^+)$ l'espace vectoriel des fonctions $f : [0, +\infty[\rightarrow \mathbb{C}$ dont la restriction à $[0, L[$ est intégrable pour tout $L > 0$, et soient $f, g \in L_{loc}^1(\mathbb{R}^+)$.*

*Alors la fonction $t \mapsto f(x-t)g(t)$ est intégrable sur $[0, x]$ pour presque tout $x > 0$. De plus si on définit presque partout sur $[0, +\infty[$ le produit de convolution $f * g$ par la formule*

$$(f * g)(x) = \int_0^x f(x-t)g(t)dt,$$

*alors $f * g \in L_{loc}^1(\mathbb{R}^+)$.*

Nous laissons en exercice la démonstration de ce résultat, (on peut se ramener au cas de $L^1(\mathbb{R})$). Notons que si le domaine de définition de la transformée de Laplace de f est non vide alors $f \in L_{loc}^1(\mathbb{R}^+)$ (ceci résulte du fait que $f(t) = e^{at}[e^{-at}f(t)]$ pour $t \geq 0$ et que $|f(t)| \leq e^{aL}[e^{-at}|f(t)|]$ pour $t \in [0, L]$, $L > 0$, $a \in \mathbb{R}$ désignant un élément du domaine de définition de $\mathcal{L}(f)$).

Ce produit de convolution est **commutatif** et **associatif**, c'est à dire qu'on a les propriétés suivantes :

$$(4.2) \quad f * g = g * f \quad \forall f \in L_{loc}^1(\mathbb{R}^+), \quad \forall g \in L_{loc}^1(\mathbb{R}^+).$$

$$(4.3) \quad f * (g * h) = (f * g) * h \quad \forall f \in L_{loc}^1(\mathbb{R}^+), \quad \forall g \in L_{loc}^1(\mathbb{R}^+), \quad \forall h \in L_{loc}^1(\mathbb{R}^+).$$

De même que la transformation de Fourier, la transformation de Laplace transforme le produit de convolution en produit usuel.

Théorème 4.2.2 *Soient $f, g \in L_{loc}^1(\mathbb{R}^+)$. Alors $\text{Dom}(\mathcal{L}(f)) \cap \text{Dom}(\mathcal{L}(g)) \subset \text{Dom}(\mathcal{L}(f * g))$, et pour $z \in \text{Dom}(\mathcal{L}(f)) \cap \text{Dom}(\mathcal{L}(g))$, on a*

$$\mathcal{L}(f * g)(z) = \mathcal{L}(f)(z)\mathcal{L}(g)(z).$$

Démonstration : Posons $h = f * g$, et soit $z = a + ib \in \text{Dom}(\mathcal{L}(f)) \cap \text{Dom}(\mathcal{L}(g))$. Posons, de même que plus haut

$f_a(t) = g_a(t) = 0$ pour $t < 0$, $f_a(t) = e^{-ta}f(t)$, $g_a(t) = e^{-ta}g(t)$, $h_a(t) = e^{-ta}h(t)$ pour $t \geq 0$.

On a $(f_a * g_a)(x) = 0 = h_a(x)$ pour $x < 0$, $(f_a * g_a)(x) = \int_0^x f_a(x-t)g_a(t)dt = \int_0^x e^{-ax+at}f(x-t)e^{-at}g(t)dt = e^{-ax} \int_0^x f(x-t)g(t)dt = h_a(x)$ pour $x \geq 0$. Donc $h_a = f_a * g_a \in L^1(\mathbb{R})$, et $\int_0^{+\infty} |(f * g)(t)|e^{-zt}dt = \int_0^{+\infty} |(f * g)(t)|e^{-at}dt = \|h_a\|_1 < +\infty$, ce qui prouve que $z \in \text{Dom}(\mathcal{L}(f * g))$. D'après la formule (4.1) et le théorème 1.2.1, on obtient

$$\mathcal{L}(f * g)(z) = \mathcal{L}(f * g)(a + ib) = \mathcal{F}(h_a)(b) = \mathcal{F}(f_a * g_a)(b) = \mathcal{F}(f_a)(b)\mathcal{F}(g_a)(b) = \mathcal{L}(f)(z)\mathcal{L}(g)(z). \clubsuit$$

On va maintenant étudier l'effet de la transformée de Laplace sur la dérivation.

Théorème 4.2.3 *Soit f une fonction continûment dérivable sur $[0, +\infty[$, et soit $z \in \text{Dom}(\mathcal{L}(f)) \cap \text{Dom}(\mathcal{L}(f'))$. On a alors*

$$\mathcal{L}(f')(z) = z\mathcal{L}(f)(z) - f(0).$$

Démonstration : Il s'agit en fait d'une intégration par parties. Pour $L > 0$, on a, en posant $u = e^{-zt}$, $dv = f'(t)dt$, soit $du = -ze^{-zt}$, $v = f(t)$,

$$\int_0^L e^{-zt}f'(t)dt = [f(t)e^{-zt}]_0^L + \int_0^L zf(t)e^{-zt}dt = f(L)e^{-zL} - f(0) + z \int_0^L f(t)e^{-zt}dt.$$

Comme $z \in \text{Dom}(\mathcal{L}(f))$, il existe une suite $(L_n)_{n \geq 1}$ de réels positifs telle que $\lim_{n \rightarrow +\infty} L_n = +\infty$ et $\lim_{n \rightarrow +\infty} |f(L_n)e^{-zL_n}| = 0$. On a alors

$$\mathcal{L}(f')(z) = \lim_{n \rightarrow +\infty} \int_0^{L_n} e^{-zt}f'(t)dt = \lim_{n \rightarrow +\infty} f(L_n)e^{-zL_n} - f(0) + z \int_0^{L_n} f(t)e^{-zt}dt = \mathcal{L}(f)(z) - f(0). \clubsuit$$

On peut construire des fonctions très oscillantes f sur $[0, +\infty[$ telles que le domaine de définition de $\mathcal{L}(f)$ soit égal à \mathbb{C} et tel que le domaine de définition de $\mathcal{L}(f')$ soit vide. C'est pourquoi le théorème ci-dessus a été énoncé pour $z \in \text{Dom}(\mathcal{L}(f)) \cap \text{Dom}(\mathcal{L}(f'))$. En pratique ce genre de phénomène se rencontre rarement et on pourra appliquer ce théorème pour $z \in \text{Dom}(\mathcal{L}(f))$, quitte à définir $\mathcal{L}(f')(z)$ par l'intégrale de Riemann généralisée $\int_0^{+\infty} f(t)e^{-zt}dt$, qui converge si $z \in \text{Dom}(\mathcal{L}(f))$ et si $\lim_{t \rightarrow +\infty} |f(t)|e^{-t\text{Re}(z)} = 0$ (on verra d'autre part en exercice que $\text{Dom}(\mathcal{L}(f')) \cap P_0 \subset \text{Dom}(\mathcal{L}(f))$).

4.3 Applications de la transformation de Laplace

Nous commençons par donner une table de transformées de Laplace.

$f(t)$	$\mathcal{L}(f)(z)$	$\text{Dom}(\mathcal{L}(f))$
1	$1/z$	$\text{Re}z > 0$
e^{at}	$1/(z-a)$	$\text{Re}z > a$
$\cos(at)$	$z/(z^2+a^2)$	$\text{Re}z > 0$
$\sin(at)$	$a/(z^2+a^2)$	$\text{Re}z > 0$
t^n	$n!/z^{n+1}$	$\text{Re}z > 0$
$t^n e^{at}$	$n!/(z-a)^{n+1}$	$\text{Re}z > a$
$g(t)e^{at}$	$\mathcal{L}(g)(z-a)$	$a + \text{Dom}(\mathcal{L}(g))$
$g(t\alpha), \alpha > 0$	$\alpha \mathcal{L}(g)(\alpha z)$	$\frac{1}{\alpha} \text{Dom}(\mathcal{L}(g))$
$g(t-\alpha), \alpha > 0$	$e^{-\alpha z} \mathcal{L}(g)(z)$	$\text{Dom}(\text{cal}L(g))$
$g^{(n)}(t)$	$z^n \mathcal{L}(g)(z) - z^{n-1}g(0) - z^{n-2}g'(0) - z g^{(n-2)}(0) - g^{(n-1)}(0)$	voir ci-dessous

L'avant-dernière ligne de la table concerne la fonction f définie sur $[0, +\infty[$ par la formule $f(t) = 0$ pour $0 \leq t < \alpha$, $f(t) = g(t - \alpha)$ pour $t \geq \alpha$, g désignant une fonction mesurable sur $[0, +\infty[$ dont le domaine de définition de la transformée de Laplace est non vide. La dernière formule est en toute rigueur valable pour $z \in \bigcap_{1 \leq i \leq n} \text{Dom}(\mathcal{L})(g^{(i)})$, mais de même que plus haut on pourra l'appliquer en pratique pour $z \in \text{Dom}(\mathcal{L})(g)$.

La transformée de Laplace permet de résoudre les équations différentielles linéaires à coefficients constants du type

$$a_n y^{(n)}(t) + \dots + a_1 y'(t) + a_0 y(t) = f(t)$$

en prenant directement en compte les conditions initiales. Le protocole est le suivant.

1) Si on pose $Y = \mathcal{L}(y)$, $F = \mathcal{L}(f)$ alors d'après la table des transformées de Laplace, on a $\mathcal{L}(y^k) = z^k Y(z) - z^{k-1}y(0) - \dots - zy^{k-2}(0) - y^{k-1}(0)$. En passant aux transformées de Laplace, on obtient une équation du type

$$p(z)Y(z) = q(z) + F(z)$$

où $p(z) := a_0 + a_1 z + \dots + a_n z^n$ est le **polynôme caractéristique de l'équation différentielle**, et où $q(z)$ est un polynôme **dépendant uniquement des conditions initiales**. En divisant par $p(z)$ on obtient $Y(z)$ (le fait que $p(z)$ ait des racines

$\alpha_1, \dots, \alpha_n$ n'est pas gênant, il signifie simplement que la transformée de Laplace de la solution n'est définie que pour $\text{Re}z$ assez grand).

2) On remonte de $Y = \mathcal{L}(y)$ à y en lisant de droite à gauche la table des transformées de Laplace.

On évoquera plus loin la résolution basée sur les exponentielles de matrice des systèmes différentiels linéaires à coefficients constants du type

$$\begin{bmatrix} x_1'(t) \\ \vdots \\ x_n'(t) \end{bmatrix} = A \begin{bmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{bmatrix} + b(t),$$

où A est une matrice carrée à n lignes et n colonnes et où la fonction $t \mapsto b(t)$ est à valeurs dans \mathbb{R}^n . Mais **on peut aussi résoudre ces systèmes en utilisant la transformée de Laplace**. Le protocole est le suivant.

1) En notant X_i la transformée de Laplace de x_i , et en notant B la transformée de Laplace de b (calculée composante par composante), on déduit de la table que $\mathcal{L}(x_i')(z) = zX_i(z) - x_i(0)$, et on aboutit au système

$$\begin{bmatrix} zX_1(z) \\ \vdots \\ zX_n(z) \end{bmatrix} - \begin{bmatrix} x_1(0) \\ \vdots \\ x_n(0) \end{bmatrix} = A \begin{bmatrix} X_1(z) \\ \vdots \\ X_n(z) \end{bmatrix} + B(z).$$

Soient $\lambda_1, \dots, \lambda_n$ les valeurs propres de A , répétées selon leur ordre de multiplicité, et soit $a = \max_{1 \leq i \leq n} \text{Re} \lambda_i$. On obtient, pour $\text{Re}z > a$, I désignant la matrice unité

$$(4.4) \quad \begin{bmatrix} X_1(z) \\ \vdots \\ X_n(z) \end{bmatrix} = (zI - A)^{-1} \left[B(z) + \begin{bmatrix} X_1(0) \\ \vdots \\ X_n(0) \end{bmatrix} \right].$$

2) On remonte de $X_1 = \mathcal{L}(x_1), \dots, X_n = \mathcal{L}(x_n)$ à x_1, \dots, x_n en lisant de droite à gauche la table des transformées de Laplace.

Exemple 4.3.1 *L'équation différentielle $y'' - y' - 2y = 0$, avec les conditions initiales $y(0) = 1, y'(0) = 0$.*

1) On pose $Y(z) = \mathcal{L}(y)(z)$. On a d'après la table

$$\mathcal{L}(y')(z) = zY(z) - y(0) = zY(z) - 1.$$

$$\mathcal{L}(y'')(z) = z^2Y(z) - zy(0) - y'(0) = z^2Y(z) - z.$$

L'équation devient

$$z^2Y(z) - z - zY(z) + 1 - 2Y(z) = 0 \iff (z^2 - z - 2)Y(z) = z - 1 \iff Y(z) = \frac{z - 1}{z^2 - z - 2}$$

On se souvient alors du Chapitre 4 du **Cours d'algèbre**[5], où on montre comment **décomposer une fraction rationnelle en éléments simples**. On a $z^2 - z - 2 = (z + 1)(z - 2)$, et on a affaire à une fraction rationnelle pour laquelle le degré du numérateur est inférieur au degré du dénominateur. On a donc une décomposition de la forme

$$\frac{z - 1}{z^2 - z - 2} = \frac{z - 1}{(z + 1)(z - 2)} = \frac{a}{z + 1} + \frac{b}{z - 2}$$

Pour trouver a on multiplie les deux membres par $z + 1$ et on fait $z = -1$. On trouve $a = \frac{2}{3}$.

Pour trouver b on multiplie les deux membres par $z - 2$ et on fait $z = 2$. On trouve $b = \frac{1}{3}$. Donc $Y(z) = \frac{2}{3(z+1)} + \frac{1}{3(z-2)}$.

On lit alors de droite à gauche la table des transformées de Laplace et on trouve

$$y(t) = \frac{2}{3}e^{-t} + \frac{1}{3}e^{2t}.$$

Notons qu'on peut résoudre cette équation en utilisant des formules vues en Terminale (voir également le Chapitre 4 du **bf Cours d'Analyse** [7] : le **polynôme caractéristique** de l'équation $y'' - y' - 2y$ est le polynôme $p(r) = r^2 - r - 2$, dont les racines sont -1 et 2 . Comme ces racines sont distinctes, on sait que la solution générale de l'équation différentielle est de la forme $y(t) = ae^{-t} + be^{2t}$, soit $y'(t) = -ae^{-t} + 2be^{2t}$. Pour trouver la solution vérifiant les conditions initiales $y(0) = 1$, $y'(0) = 0$, on aboutit au système

$$\begin{cases} a + b = 1 \\ -a + 2b = 0 \end{cases}, \text{ ce qui donne de nouveau } a = \frac{2}{3}, b = \frac{1}{3}, \text{ et on retrouve le fait que } y(t) = \frac{2}{3}e^{-t} + \frac{1}{3}e^{2t}.$$

On va également profiter de cet exemple pour réviser les systèmes différentiels linéaires. On pose

$$X(t) = \begin{bmatrix} y(t) \\ y'(t) \end{bmatrix}, \text{ de sorte que } X'(t) = \begin{bmatrix} y'(t) \\ y''(t) \end{bmatrix}.$$

L'équation différentielle $y'' - y' - 2y = 0$, avec les conditions initiales $y(0) = 1$, $y'(0) = 0$, donne

$$X'(t) = \begin{bmatrix} y'(t) \\ 2y(t) + y'(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} y(t) \\ y'(t) \end{bmatrix} = AX(t),$$

où $A := \begin{bmatrix} 0 & 1 \\ 2 & 1 \end{bmatrix}$, avec la condition initiale $X(0) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

On se souvient alors du **Cours d'algèbre linéaire**[6]. La solution de ce système est donnée par la formule

$$X(t) = e^{tA}X(0),$$

où $e^{tA} = \sum_{n=0}^{+\infty} \frac{A^n}{n!}$, avec la convention $A^0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Le polynôme caractéristique de A est le polynôme $p_A = x^2 - \text{Tr}(A)x + \text{Det}(A) = x^2 - x - 2$, (on retrouve le polynôme caractéristique de l'équation différentielle), dont les racines sont -1 et 2 . Comme ces racines sont distinctes, A est diagonalisable, et il existe une matrice inversible P telle que

$$P^{-1}AP = \begin{bmatrix} -1 & 0 \\ 0 & 2 \end{bmatrix},$$

d'où

$$A = P \begin{bmatrix} -1 & 0 \\ 0 & 2 \end{bmatrix} P^{-1}, \quad e^{tA} = P \begin{bmatrix} e^{-t} & 0 \\ 0 & e^{2t} \end{bmatrix} P^{-1}.$$

Pour trouver une matrice P ayant les propriétés ci-dessus on prend $P = [V_1, V_2]$, où $V_1 \in \mathbb{R}^2$ est un vecteur colonne non nul tel que $AV_1 = -V_1$, et où $V_2 \in \mathbb{R}^2$ est un vecteur colonne non nul tel que $AV_2 = 2V_2$, voir le Cours d'algèbre linéaire. [6] Nous laissons la fin du calcul en exercice, et nous allons conclure ici en faisant appel à Mupad.

```
M:= Dom::Matrix ();
A:=M([ [0,1],[2,1]]);
exp(A,t);
```

```
Dom::Matrix(Dom::ExpressionField(id, iszero))
```

```
+ -      - +
|  0, 1  |
|        |
|  2, 1  |
+ -      - +
```

```
+ -
```

```
- +
```


$$\frac{z^2 + 6}{(z^2 + 1)(z^2 + 4)} = \frac{(-z)^2 + 6}{(-z)^2 + 4} = \frac{-az + b}{z^2 + 1} + \frac{-cz + d}{z^2 + 4}$$

Par unicité de la décomposition en éléments simples, on obtient $a = c = 0$. En multipliant par $z^2 + 1$ et en faisant $z = i$, on obtient $b = 5/3$. En multipliant par $z^2 + 4$ et en faisant $z = 2i$, on obtient $d = -2/3$. Finalement

$$\mathcal{L}(y)(z) = \frac{z^2 + 6}{(z^2 + 1)(z^2 + 4)} = \frac{5}{3(z^2 + 1)} - \frac{2}{3(z^2 + 4)}.$$

En lisant de droite à gauche la table des transformées de Laplace, on obtient

$$y(t) = \frac{5}{3} \sin t - \frac{1}{3} \sin 2t.$$

Exemple 4.3.3 Le système différentiel $\begin{cases} x'(t) = y(t) \\ y'(t) = 2x(t) + y(t) \end{cases}$, avec les conditions initiales $x(0) = 1, y(0) = 0$.

On a déjà rencontré ce système plus haut, et on a vu comment le résoudre en utilisant les exponentielles de matrices. On va maintenant le résoudre en utilisant la transformation de Laplace. On pose $X = \mathcal{L}(x), Y = \mathcal{L}(y)$. D'après la table on a $\mathcal{L}(x')(z) = zX(z) - x(0) = zX(z) - 1$ et $\mathcal{L}(y')(z) = zY(z) - y(0) = zY(z)$.

Comme la transformation de Laplace est linéaire, on obtient

$$\begin{cases} zX(z) = Y(z) + 1 \\ zY(z) = 2X(z) + Y(z) \end{cases} \iff z \begin{bmatrix} X(z) \\ Y(z) \end{bmatrix} = A \begin{bmatrix} X(z) \\ Y(z) \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

avec $A = \begin{bmatrix} 0 & 1 \\ 2 & 1 \end{bmatrix}$. Les valeurs propres de A sont -1 et 2 , et on a, pour $\operatorname{Re} z > 2$,

$$\begin{bmatrix} X(z) \\ Y(z) \end{bmatrix} = (zI - A)^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

On a $\det(zI - A) = \begin{vmatrix} z & -1 \\ -2 & z - 1 \end{vmatrix} = z(z - 1) - 2 = z^2 - z - 2 = (z + 1)(z - 2)$. En

utilisant la formule $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, valable si $ad - bc \neq 0$, on obtient

$$\begin{bmatrix} X(z) \\ Y(z) \end{bmatrix} = \frac{1}{(z + 1)(z - 2)} \begin{bmatrix} z - 1 & 1 \\ 2 & z - 2 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{z-1}{(z+1)(z-2)} \\ \frac{2}{(z+1)(z-2)} \end{bmatrix}.$$

On a déjà vu que $\frac{z-1}{(z+1)(z-2)} = \frac{2}{3(z+1)} + \frac{1}{3(z+2)}$. On a de même une décomposition de la forme $\frac{2}{(z+1)(z-2)} = \frac{a}{z-1} + \frac{b}{z+2}$. En multipliant par $z + 1$ et en faisant $z = -1$, on

obtient $a = -\frac{2}{3}$, et en multipliant par $z - 2$ et en faisant $z = 2$, on obtient $b = \frac{2}{3}$.
Donc on a

$$X(z) = \frac{2}{3(z+1)} + \frac{1}{3(z-2)}, \quad Y(z) = -\frac{2}{3(z+1)} + \frac{2}{3(z-2)},$$

et en lisant de droite à gauche la table des transformées de Laplace, on trouve

$$x(t) = \frac{2}{3}e^{-t} + \frac{1}{3}e^{2t}, \quad y(t) = -\frac{2}{3}e^{-t} + \frac{2}{3}e^{2t}.$$

Exemple 4.3.4 Le système différentiel $\begin{cases} x' = 3x + y + e^{-t} \\ y' = -x + y + 1 \end{cases}$, avec les conditions initiales $x(0) = 1, y(0) = 0$.

Posons $X = \mathcal{L}(x), Y = \mathcal{L}(y)$. On applique directement la formule 4.4 et on trouve, avec $A = \begin{bmatrix} 3 & 1 \\ -1 & 1 \end{bmatrix}$,

$$\begin{bmatrix} X \\ Y \end{bmatrix} = (zI - A)^{-1} \begin{bmatrix} \frac{1}{z+1} + 1 \\ \frac{1}{z} \end{bmatrix}.$$

On a $\det(zI - A) = \begin{vmatrix} z-3 & -1 \\ 1 & z-1 \end{vmatrix} = (z-3)(z-1) + 1 = z^2 - 4z + 4 = (z-2)^2$.

En utilisant la formule $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ pour $ad-bc \neq 0$, on obtient

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \frac{1}{(z-2)^2} \begin{bmatrix} z-1 & 1 \\ -1 & z-3 \end{bmatrix} \begin{bmatrix} \frac{z+2}{z+1} \\ \frac{1}{z} \end{bmatrix}.$$

On a alors

$$\begin{aligned} X(z) &= \frac{1}{(z-2)^2} \left[\frac{(z-1)(z+2)}{z+1} + \frac{1}{z} \right] = \frac{z(z-1)(z+2) + z + 1}{z(z+1)(z-2)^2} \\ &= \frac{z^3 + z^2 - z + 1}{z(z+1)(z-2)^2} \end{aligned}$$

$$\begin{aligned} Y(z) &= \frac{1}{(z-2)^2} \left[-\frac{z+2}{z+1} + \frac{z-3}{z} \right] = \frac{-z(z+2) + (z+1)(z-3)}{z(z+1)(z-2)^2} \\ &= \frac{-4z-3}{z(z+1)(z-2)^2} \end{aligned}$$

La première fraction rationnelle admet une décomposition de la forme

$$\frac{z^3 + z^2 - z + 1}{z(z+1)(z-2)^2} = \frac{a_1}{z} + \frac{b_1}{z+1} + \frac{c_1}{(z-2)^2} + \frac{d_1}{z-2}.$$

En multipliant par z les deux membres et en faisant $z = 0$ on obtient $a_1 = \frac{1}{4}$. En multipliant par $z + 1$ les deux membres et en faisant $z = -1$ on obtient $b_1 = -\frac{2}{9}$. En multipliant par $(z - 2)^2$ les deux membres et en faisant $z = 2$ on obtient $c_1 = \frac{11}{6}$. En faisant $z = 1$ on obtient $\frac{2}{2} = \frac{1}{4} - \frac{1}{9} + \frac{11}{6} - d_1$, soit $d_1 = \frac{1}{4} - \frac{1}{9} + \frac{11}{6} - 1 = \frac{9-4+66-36}{36} = \frac{35}{36}$.

La deuxième fraction rationnelle admet une décomposition de la forme

$$\frac{-4z - 3}{z(z + 1)(z - 2)^2} = \frac{a_2}{z} + \frac{b_2}{z + 1} + \frac{c_2}{(z - 2)^2} + \frac{d_2}{z - 2}.$$

En multipliant par z les deux membres et en faisant $z = 0$ on obtient $a_2 = -\frac{3}{4}$. En multipliant par $z + 1$ les deux membres et en faisant $z = -1$ on obtient $b_2 = -\frac{1}{9}$. En multipliant par $(z - 2)^2$ les deux membres et en faisant $z = 2$ on obtient $c_2 = -\frac{11}{6}$. En faisant $z = 1$ on obtient $-\frac{7}{2} = -\frac{3}{4} - \frac{1}{18} - \frac{11}{6} - d_2$, soit $d_2 = -\frac{3}{4} - \frac{1}{18} - \frac{11}{6} + \frac{7}{2} = \frac{-27-2-66+126}{36} = \frac{31}{36}$.

Finalement on a

$$X(z) = \frac{1}{4z} - \frac{2}{9(z + 1)} + \frac{11}{6(z - 2)^2} + \frac{35}{36(z - 2)}, \quad Y(z) = -\frac{3}{4z} - \frac{1}{9(z + 1)} - \frac{11}{6(z - 2)^2} + \frac{31}{36(z - 2)}.$$

En lisant de droite à gauche la table des transformées de Laplace, on obtient

$$x(t) = \frac{1}{4} - \frac{2}{9}e^{-t} + \frac{11}{6}te^{2t} + \frac{35}{36}e^{2t}, \quad y(t) = -\frac{3}{4} - \frac{1}{9}e^{-t} - \frac{11}{6}te^{2t} + \frac{31}{36}e^{2t}.$$

4.4 Exercices sur le Chapitre 4

exercice 1 (Annales ESTIA, examens Transformées 1998, 1999, 2000)

Calculer les transformées de Laplace des fonctions définies pour $x \geq 0$ par les formules suivantes

$$f(x) = \int_0^x (x - t)^2 \cos(2t) dt,$$

$$g(x) = \int_0^x (x - t)^6 \cos(4t) dt,$$

$$h(x) = \int_0^x (x - t)^8 \sin(3t) dt.$$

exercice 2 (Annales ESTIA, Examen Transformées 2001)

1) On pose $h(x) = \sin^2 2x$ pour $x \geq 0$. Calculer la transformée de Laplace de h .

2) On pose $f(x) = \int_0^x (x-t)^5 \sin(2t) dt$ pour $x \geq 0$. Calculer la transformée de Laplace de f .

exercice 3 (Annales ESTIA, examen Transformées 2002)

1) Pour $t \geq 0$, on pose $g(t) = \sin^2(6t)$ et $h(t) = t^3 e^t$. En utilisant la table des transformées de Laplace et un peu de trigonométrie, déterminer les transformées de Laplace de g et h .

2) On pose $f(x) = \int_0^x \sin^2(6t)(x-t)^3 e^{x-t} dt$ pour $x \geq 0$. Calculer la transformée de Laplace de f .

exercice 4

Pour $n \geq 1$, $t \geq 0$, on pose $e_n(t) = \frac{t^{n-1} e^{-t}}{(n-1)!}$.

1) Donner la transformée de Laplace de e_n (on pourra utiliser la table).

2) Comparer e_{m+n} et $e_m * e_n$ pour $m \geq 1$, $n \geq 1$.

Exercice 5 (Annales ESTIA, examen transformées 2002)

1) On pose $f(t) = 1 - 6t$ pour $t \geq 0$. Déterminer la transformée de Laplace de f .

2) Trouver un réel a tel que $z^3 - 7z^2 + 36 = (z+2)(z-3)(z+a)$.

3) En utilisant la transformation de Laplace, résoudre l'équation différentielle

$$y''(t) - y'(t) - 6y(t) = 36t,$$

avec les conditions initiales $y(0) = 1$, $y'(0) = -6$.

exercice 6 (Annales ESTIA, examen Transformées 2001)

1) Trouver trois constantes a , b , c telles que $\frac{z^2-3z-3}{(z+1)(z-1)(z-4)} = \frac{a}{z+1} + \frac{b}{z-1} + \frac{c}{z-4}$.

2) Soit y la fonction vérifiant $y(0) = y'(0) = 1$ et $y''(x) - 5y'(x) + 4y(x) = e^{-x}$ pour $x \geq 0$.

On note Y la transformée de Laplace de y . Calculer $Y(z)$ pour $\operatorname{Re}(z) > 4$. En déduire la valeur de $y(x)$.

exercice 7

1) On pose $f(t) = te^t$ pour $t \geq 0$. Calculer la transformée de Laplace de f .

2) On considère l'équation différentielle

$$y''(t) - 6y'(t) + 9y(t) = te^t,$$

avec la condition initiale $y(0) = 0$, $y'(0) = 1$.

a) Résoudre cette équation en utilisant la transformation de Laplace.

b) En posant $X(t) = \begin{bmatrix} y(t) \\ y'(t) \end{bmatrix}$, ramener l'équation ci-dessus à un système différentiel.

c) Résoudre ce système différentiel en utilisant la transformation de Laplace.

d) Résoudre ce système en utilisant les exponentielles de matrices (on pourra effectuer les calculs sous Mupad).

exercice 8(Annales ESTIA, examen Transformées 2002)

En utilisant la transformation de Laplace, résoudre le système différentiel

$$\begin{cases} x'(t) = x(t) - y(t) + e^t \\ y'(t) = x(t) + 3y(t) - 4 \end{cases}$$

avec la condition initiale $x(0) = y(0) = 0$.

exercice 9

On considère le système différentiel

$$\begin{cases} x'(t) = 4x(t) + y(t) + e^t \\ y'(t) = -x(t) + 2y(t) + 1 \end{cases}, \text{ avec la condition initiale } x(0) = y(0) = 0.$$

a) Résoudre ce système en utilisant la transformation de Laplace.

b) Résoudre ce système en utilisant les exponentielles de matrices (on pourra effectuer les calculs sous Mupad).

Chapitre 5

Transformée en Z

5.1 Transformée en Z bilatérale

Définition 5.1.1 Soit $u : \mathbb{Z} \rightarrow \mathbb{C}$ une application de \mathbb{Z} dans \mathbb{C} . On définit la transformée en Z de u par la formule

$$\mathcal{Z}(u)(z) = \sum_{n=-\infty}^{+\infty} u[n]z^{-n}.$$

On définit le domaine de convergence $\mathcal{D}(\mathcal{Z}(u))$ et le domaine de convergence absolue $\mathcal{D}_{abs}(\mathcal{Z}(u))$ par les formules

$$\mathcal{D}(\mathcal{Z}(u)) = \{z \in \mathbb{C} \setminus \{0\} \mid \text{les séries } \sum_{n=0}^{+\infty} u[-n]z^n \text{ et } \sum_{n=0}^{+\infty} u[n]z^{-n} \text{ sont convergentes}\}, \quad (5.1)$$

$$\mathcal{D}_{abs}(\mathcal{Z}(u)) = \{z \in \mathbb{C} \setminus \{0\} \mid \sum_{n=-\infty}^{+\infty} |u[n]||z^{-n}| < +\infty\}. \quad (5.2)$$

Rappelons qu'une série numérique $\sum_{n=0}^{+\infty} a_n$ est dite *absolument convergente* quand $\sum_{n=0}^{+\infty} |a_n| < +\infty$. Autrement dit $\mathcal{D}_{abs}(\mathcal{Z}(u))$ est l'ensemble des nombres complexes z tels que les séries $\sum_{n=0}^{+\infty} u[-n]z^n$ et $\sum_{n=0}^{+\infty} u[n]z^{-n}$ sont absolument convergentes. On sait que si une série entière $\sum_{n=0}^{+\infty} a_n z^n$ est convergente pour $z = u$, alors cette série entière est absolument convergente pour $|z| < |u|$, voir le Chapitre 4 de [?]. Ceci permet de définir le *rayon de convergence* $R \in [0, +\infty]$ d'une série entière, caractérisé par le fait que la série entière est absolument convergente pour $|z| < R$ et est divergente pour $|z| > R$. Avec les conventions $\frac{1}{0} = +\infty$ et $\frac{1}{+\infty} = 0$, le rayon de convergence R d'une série entière $\sum_{n=0}^{+\infty} a_n z^n$ est donné par la formule (voir également le Chapitre 4 de [?])

$$R = \frac{1}{\limsup_{n \rightarrow +\infty} |a_n|^{1/n}}. \quad (5.3)$$

Pour $0 \leq a \leq b \leq +\infty$, on pose $\Omega_{a,b} = \{z \in \mathbb{C} \mid a < |z| < b\}$, avec la convention $\Omega_{a,b} = \emptyset$ si $a \geq b$, et on pose $\bar{\Omega}_{a,b} = \{z \in \mathbb{C} \mid a \leq |z| \leq b\}$, avec la convention $\bar{\Omega}_{a,b} = \emptyset$ si $a > b$. On obtient alors les résultats suivants

Proposition 5.1.2 *Soit $u : \mathbb{Z} \rightarrow \mathbb{C}$, et soient $r(u) = \limsup_{n \rightarrow +\infty} |u[n]|^{1/n}$, $R(u) = \frac{1}{\limsup_{n \rightarrow +\infty} |u[-n]|^{1/n}}$.*

(i) *Le domaine de convergence absolue (qui peut être vide) $\mathcal{D}_{abs}(\mathcal{Z}(u))$ de $\mathcal{Z}(u)$ est égal à $\Omega_{r(u), R(u)}$,*

(ii) *Le domaine de convergence (qui peut être vide) de $\mathcal{D}(\mathcal{Z}(u))$ de $\mathcal{Z}(u)$ vérifie $\Omega_{r(u), R(u)} \subset \mathcal{D}(\mathcal{Z}(u)) \subset \bar{\Omega}_{r(u), R(u)}$.*

Démonstration : Il est clair que $\frac{1}{r(u)}$ est le rayon de convergence de la série entière $\sum_{n=0}^{+\infty} u[n]z^n$, donc la série $\sum_{n=0}^{+\infty} u[n]z^{-n}$ est absolument convergente si et seulement si $|z| > r(u)$. De même $R(u)$ est le rayon de convergence de la série entière $\sum_{n=0}^{+\infty} u[-n]z^n$, donc le série $\sum_{n=0}^{+\infty} u[-n]z^{-n}$, est absolument convergente si et seulement si $|z| < R(u)$, ce qui prouve (i). D'autre part la série $\sum_{n=0}^{+\infty} u[n]z^{-n}$ diverge pour $|z| > r(u)$, et la série $\sum_{n=0}^{+\infty} u[-n]z^n$ diverge pour $|z| < R(u)$. Par conséquent $\mathcal{D}(\mathcal{Z}(u)) \subset \bar{\Omega}_{r(u), R(u)}$. Comme $\mathcal{D}_{abs}(\mathcal{Z}(u)) \subset \mathcal{D}(\mathcal{Z}(u))$, on obtient (ii). ♣

Il est évident que la transformée en Z est linéaire. Supposons maintenant que l'intersection des domaines de convergence absolues de $\mathcal{Z}(u)$ et $\mathcal{Z}(v)$ est non vide, et soit $z \in \mathcal{D}_{abs}(\mathcal{Z}(u)) \cap \mathcal{D}_{abs}(\mathcal{Z}(v))$. On a, pour $n \in \mathbb{Z}$, en utilisant une version discrète du théorème de Fubini,

$$\begin{aligned} \sum_{p=-\infty}^{+\infty} |u[p]||v[n-p]| &= |z|^n \left[\sum_{p=-\infty}^{+\infty} |u[p]||z|^{-p}|v[n-p]||z|^{-n+p} \right] \\ &= |z|^n \left[\sum_{p=-\infty}^{+\infty} |u[p]||z|^{-p} \right] \left[\sum_{q=-\infty}^{+\infty} |v[q]||z|^{-q} \right] < +\infty. \end{aligned}$$

On peut alors définir $u * v : \mathbb{Z} \rightarrow \mathbb{C}$ par la formule

$$(u * v)[n] = \sum_{p=-\infty}^{+\infty} u[p]v[n-p]. \quad (5.4)$$

On obtient, en utilisant de nouveau une version discrète du théorème de Fubini, pour $z \in \mathcal{D}_{abs}(\mathcal{Z}(u)) \cap \mathcal{D}_{abs}(\mathcal{Z}(v))$,

$$\begin{aligned} \sum_{n=-\infty}^{+\infty} \left[\sum_{p=-\infty}^{+\infty} |u[p]||v[n-p]| \right] |z|^{-n} \\ = \left[\sum_{p,q \in \mathbb{Z}} |u[p]||z|^{-p}|v[q]||z|^{-q} \right] \end{aligned}$$

$$= \left[\sum_{p=-\infty}^{+\infty} |u[p]||z|^{-p} \right] \left[\sum_{q=-\infty}^{+\infty} |v[q]||z|^{-q} \right] < +\infty.$$

Ceci montre que $\mathcal{D}_{abs}(\mathcal{Z}(u)) \cap \mathcal{D}_{abs}(\mathcal{Z}(v)) \subset \mathcal{D}_{abs}(\mathcal{Z}(u * v))$, et on a, pour $z \in \mathcal{D}_{abs}(\mathcal{Z}(u)) \cap \mathcal{D}_{abs}(\mathcal{Z}(v))$,

$$\begin{aligned} \mathcal{Z}(u * v)(z) &= \sum_{n=-\infty}^{+\infty} \left[\sum_{p=-\infty}^{+\infty} u[p]v[n-p] \right] z^{-n} \\ &= \left[\sum_{p,q \in \mathbb{Z}} u[p]z^{-p}v[q]z^{-q} \right] \\ &= \left[\sum_{p=-\infty}^{+\infty} u[p]z^{-p} \right] \left[\sum_{q=-\infty}^{+\infty} v[q]z^{-q} \right] \\ &= \mathcal{Z}(u)(z)\mathcal{Z}(v)(z). \end{aligned}$$

On obtient donc le résultat suivant.

Théorème 5.1.3 *Soient $u : \mathbb{Z} \rightarrow \mathbb{C}$ et $v : \mathbb{Z} \rightarrow \mathbb{C}$. Si $\mathcal{D}_{abs}(u) \cap \mathcal{D}_{abs}(v) \neq \emptyset$, alors $u * v$ est bien défini, $\mathcal{D}_{abs}(u) \cap \mathcal{D}_{abs}(v) \subset \mathcal{D}_{abs}(u * v)$, et on a, pour $z \in \mathcal{D}_{abs}(u) \cap \mathcal{D}_{abs}(v)$,*

$$\mathcal{Z}(u * v)(z) = \mathcal{Z}(u)(z)\mathcal{Z}(v)(z). \quad (5.5)$$

Exemple 5.1.4 *On pose $u[n] = \frac{1}{n!}$ pour $n \geq 0$, $u[n] = 0$ pour $n < 0$, $v[n] = 0$ pour $n > 0$, $v[n] = \frac{1}{|n|!}$ pour $n \leq 0$. Alors $u * v$ est bien défini, et $\mathcal{Z}(u * v)(z) = e^{\frac{z^2+1}{z}}$.*

En effet on sait que le rayon de convergence de la série entière $\sum_{n=0}^{+\infty} \frac{z^n}{n!}$ est égal à $+\infty$, et que la somme de cette série est égale à e^z . On a donc $\mathcal{D}_{abs}(u) = \mathcal{D}_{abs}(v) = \mathbb{C} \setminus \{0\}$, $\mathcal{Z}(u)(z) = e^{1/z}$, $\mathcal{Z}(v)(z) = e^z$, et $\mathcal{Z}(u * v)(z) = \mathcal{Z}(u)(z)\mathcal{Z}(v)(z) = e^{\frac{z^2+1}{z}}$.

Un résultat standard d'Analyse complexe montre que la somme d'une série entière de rayon de convergence R est indéfiniment dérivable au sens complexe pour $|z| < R$, et que sa dérivée s'obtient comme somme de la série entière obtenue en dérivant terme à terme cette série entière. On en déduit immédiatement que si $\mathcal{D}(u) = \Omega_{a,b}$, alors $\mathcal{Z}(u)$ est indéfiniment dérivable au sens complexe sur $\Omega_{a,b}$, et que l'on a, pour $a < |z| < b$, $n \geq 0$,

$$\begin{aligned} f^{(p)}(z) &= \sum_{n=-\infty}^{+\infty} (-n)(-n-1)(-n-p+1)u[n]z^{-n-p} \\ &= \sum_{n=-\infty}^{-p} (-n)(-n-1)(-n-p+1)u[n]z^{-n-p} + \sum_{n=1}^{+\infty} u[n]z^{-n}. \end{aligned} \quad (5.6)$$

On voit donc que si on pose $U(r, \theta) = \mathcal{Z}(u)(re^{i\theta})$, alors U admet des dérivées partielles continues de tous ordres pour $a < r < b$, $\theta \in \mathbb{R}$. On a, pour $a < r < b$, $U(r, \theta) = \sum_{n=-\infty}^{+\infty} u[n]r^n e^{-in\theta}$.

Comme $\sum_{n=-\infty}^{+\infty} |u[n]| < +\infty$, la série $\sum_{n=-\infty}^{+\infty} u[n]r^n e^{-in\theta} e^{ip\theta}$ est normalement convergente, donc uniformément convergente, sur $[0, 2\pi]$, et d'après un résultat classique rappelé dans le Chapitre 4 de [?], (on peut aussi faire appel à la théorie des séries de Fourier) on a

$$\frac{1}{2\pi} \int_0^{2\pi} \sum_{n=-\infty}^{+\infty} u[n]r^n e^{-in\theta} e^{ip\theta} d\theta = \sum_{n=-\infty}^{+\infty} \frac{1}{2\pi} \int_0^{2\pi} u[n]r^n e^{-in\theta} e^{ip\theta} d\theta.$$

On a $\int_0^{2\pi} e^{i(p-n)\theta} d\theta = \left[\frac{e^{i(p-n)\theta}}{i(p-n)} \right]_0^{2\pi} = 0$ pour $n \neq p$, et $\int_0^{2\pi} e^{i(n-n)\theta} d\theta = 1$. On obtient, pour $a < r < b$, $p \in \mathbb{Z}$, la *formule d'inversion pour la transformée en Z bilatérale*

$$u[p] = \frac{r^{-p}}{2\pi} \int_0^{2\pi} \mathcal{Z}(u)(re^{i\theta}) e^{ip\theta} d\theta, \quad (5.7)$$

formule qui traduit le fait que au sens complexe le *coefficient de Fourier* d'indice p de la fonction $\theta \mapsto \mathcal{Z}(u)(re^{i\theta})$ est égal à $u[-p]r^p$.

Nous concluons ce paragraphe par un exemple simple qui montre que la transformée en Z bilatérale peut avoir une extension holomorphe, c'est à dire dérivable au sens complexe qui va bien au delà du domaine de convergence $\mathcal{D}(\mathcal{Z}(u))$ défini plus haut.

Exemple 5.1.5 On pose $u[n] = a^n$ pour $n \geq 0$, $u[n] = b^n$ pour $n < 0$. Alors $\mathcal{Z}(u)(z) = \frac{z}{z-a} + \frac{z}{b-z}$.

En effet pour $|z| > |a|$ on a $\sum_{n=0}^{+\infty} u[n]z^{-n} = \sum_{n=0}^{+\infty} a^n z^{-n} = \frac{1}{1-a/z} = \frac{z}{z-a}$ et pour $|z| < |b|$ on a $\sum_{n=-\infty}^{-1} u[n]z^{-n} = \sum_{n=-\infty}^{-1} b^n z^{-n} - 1 = \sum_{n=0}^{+\infty} b^{-n} z^n - 1 = \frac{1}{1-z/b} - 1 = \frac{b}{b-z} - 1$, donc $\mathcal{Z}(u)(z) = \sum_{n=-\infty}^{+\infty} u[n]z^{-n} = \frac{z}{z-a} + \frac{b}{b-z} - 1 = \frac{z}{z-a} + \frac{z}{b-z}$ pour $z \in \Omega_{|a|,|b|} = \mathcal{D}_{abs}(\mathcal{Z})(u)$. On obtient donc une fonction holomorphe sur $\mathbb{C} \setminus \{a, b\}$, et on notera que ce calcul reste formellement valable même quand le domaine de convergence de $\mathcal{Z}(u)$ est vide, ce qui correspond au cas où $|a| \geq |b|$. Ceci permet dans beaucoup de situations d'utiliser des formules d'inversion de la transformée en Z beaucoup plus subtiles que la formule 1.7, qui sont basées sur des intégrales curvilignes sur des contours situés dans le domaine d'holomorphic de $\mathcal{Z}(u)$.

La transformée en Z bilatérale permet d'étudier le filtrage de signaux théoriques infinis. Ceci correspond à des applications du type $x \mapsto y = x * g$, avec $x = (x[n])_{n \in \mathbb{Z}}$, $g = (g[n])_{n \in \mathbb{Z}}$, $y = (y[n])_{n \in \mathbb{Z}}$. Il n'y a pas de problèmes de convergence si $x[n]$ et $g[n]$ sont nuls pour $|n|$ assez grand, et on a $\mathcal{Z}(x)(z) = \frac{\mathcal{Z}(y)(z)}{\mathcal{Z}(g)(z)}$, ce qui permet de reconstituer quand les points d'annulation de $\mathcal{Z}(g)$ sont compensés par ceux de $\mathcal{Z}(y)$ la suite $x = (x[n])_{n \in \mathbb{Z}}$ (input) à partir de la suite $y = (y[n])_{n \in \mathbb{Z}}$ (l'output), en lisant de gauche à droite puis de droite à gauche les tables de transformée en z.

Nous expliciterons cette approche dans le paragraphe suivant dans le cas "causal", qui correspond à des signaux discrets définis pour $n \geq 0$.

5.2 Transformée en Z unilatérale

On s'intéresse ici aux applications $u : \mathbb{N} \rightarrow \mathbb{C}$, où $\mathbb{N} = \mathbb{Z}^+$ désigne l'ensemble des entiers positifs ou nuls. Dans ce contexte la définition de la convolution ne pose aucun problème

Définition 5.2.1 Soient $u : \mathbb{N} \rightarrow \mathbb{C}$ et $v : \mathbb{N} \rightarrow \mathbb{C}$. On pose, pour $n \geq 0$,

$$(u * v)[n] = \sum_{p=0}^n u[p]v[n-p]. \quad (5.8)$$

Notons $\mathbb{C}^{\mathbb{N}}$ l'ensemble des applications de \mathbb{N} dans \mathbb{C} , c'est à dire l'ensemble des suites $(u[n])_{n \geq 0}$. On a les propriétés suivantes

$$\text{L'application } u \rightarrow u * v \text{ est linéaire } \forall v \in \mathbb{C}^{\mathbb{N}}. \quad (5.9)$$

$$u * v = v * u \quad \forall u \in \mathbb{C}^{\mathbb{N}}, \forall v \in \mathbb{C}^{\mathbb{N}}. \quad (5.10)$$

$$(u * v) * w = u * (v * w) \quad \forall u \in \mathbb{C}^{\mathbb{N}}, \forall v \in \mathbb{C}^{\mathbb{N}}, \forall w \in \mathbb{C}^{\mathbb{N}}. \quad (5.11)$$

$$e_0 * u = u \quad \forall u \in \mathbb{C}^{\mathbb{N}}, \text{ où } e_0[0] = 1, e_0[n] = 1 \text{ pour } n \geq 1 \quad (5.12)$$

On peut maintenant définir de manière très simple la transformée en Z unilatérale.

Définition 5.2.2 Soit $u : \mathbb{N} \rightarrow \mathbb{C} \in \mathbb{C}^{\mathbb{N}}$. On définit la transformée en Z de u par la formule

$$\mathcal{Z}(u)(z) = \sum_{n=0}^{+\infty} u[n]z^{-n}.$$

On définit le domaine de convergence $\mathcal{D}(\mathcal{Z}(u))$ et le domaine de convergence absolue $\mathcal{D}_{abs}(\mathcal{Z}(u))$ par les formules

$$\mathcal{D}(\mathcal{Z}(u)) = \{z \in \mathbb{C} \setminus \{0\} \mid \sum_{n=0}^{+\infty} u[n]z^{-n} \text{ est convergente}\},$$

$$\mathcal{D}_{abs}(\mathcal{Z}(u)) = \{z \in \mathbb{C} \setminus \{0\} \mid \sum_{n=0}^{+\infty} |u[n]||z|^{-n} < +\infty\}.$$

De même que plus haut on voit que si on pose $r(u) = \limsup_{n \rightarrow +\infty} |u[n]|^{1/n}$, de sorte que $r(u)^{-1}$ est le rayon de convergence de la série entière $\sum_{n=0}^{+\infty} u[n]z^n$, on a

$$\mathcal{D}_{abs}(\mathcal{Z}(u)) = \Omega_{r(u), +\infty} = \{z \in \mathbb{C} \mid |z| > r(u)\}, \quad (5.13)$$

$$\Omega_{r(u), +\infty} \subset \mathcal{D}(\mathcal{Z}(u)) \subset \bar{\Omega}_{r(u), +\infty} = \{z \in \mathbb{C} \mid |z| \geq r(u)\}. \quad (5.14)$$

On a également une *formule d'inversion*, qui est un cas particulier de la formule d'inversion vue plus haut.

Théorème 5.2.3 *Soit $u \in \mathbb{C}^{\mathbb{N}}$, et soit $r > r(u)$. On a alors, pour $p \geq 0$,*

$$u[p] = \frac{r^{-p}}{2\pi} \int_0^{2\pi} \mathcal{Z}(u)(re^{i\theta}) e^{ip\theta} d\theta, \quad (5.15)$$

De même que plus haut, il arrive souvent que $\mathcal{Z}(u)$ se prolonge naturellement en une fonction holomorphe sur un domaine plus grand que son domaine de convergence, ce qui permet d'obtenir des formules d'inversion plus subtiles, basées sur d'autres intégrales curvilignes.. Nous n'aborderons pas ce sujet ici.

Si $\sum_{n=0}^{+\infty} a_n$ et $\sum_{n=0}^{+\infty} b_n$ sont deux séries numériques, on définit la "série produit" $\sum_{n=0}^{+\infty} c_n$ par la formule $c_n = \sum_{p=0}^n a_p b_{n-p}$. On sait (voir le Chapitre 2 de [?]) que si la série $\sum_{n=0}^{+\infty} a_n$ est absolument convergente, et si la série $\sum_{n=0}^{+\infty} b_n$ est convergente (resp. absolument convergente), alors la série produit $\sum_{n=0}^{+\infty} c_n$ est convergente (resp. absolument convergente), et on a

$$\sum_{n=0}^{+\infty} \left(\sum_{p=0}^{+\infty} a_p b_{n-p} \right) = \left(\sum_{n=0}^{+\infty} a_n \right) \left(\sum_{n=0}^{+\infty} b_n \right).$$

On en déduit immédiatement le résultat suivant.

Théorème 5.2.4 *Soient $u, v \in \mathbb{C}^{\mathbb{N}}$. Alors $\mathcal{D}_{abs}(\mathcal{Z})(u) \cap \mathcal{D}_{abs}(\mathcal{Z})(v) \subset \mathcal{D}_{abs}(\mathcal{Z})(u * v)$, $\mathcal{D}_{abs}(\mathcal{Z})(u) \cap (\mathcal{D}(\mathcal{Z})(v)) \subset \mathcal{D}(\mathcal{Z})(u * v)$, et on a, pour $z \in \mathcal{D}_{abs}(\mathcal{Z})(u) \cap \mathcal{D}(\mathcal{Z})(v)$,*

$$\mathcal{Z}(u * v)(z) = \mathcal{Z}(u)(z) \mathcal{Z}(v)(z). \quad (5.16)$$

On va maintenant donner une table des transformées en Z unilatérales (on trouvera une table beaucoup plus détaillée dans [10]). On pose selon l'usage $\delta_{n,m} = 0$ si $n \neq m$, $\delta_{n,n} = 1$ (le symbole $\delta_{n,m}$ est appelé le *symbole de Kronecker*). Dans la table ci-dessous, p désigne un entier ≥ 0 , et on pose par convention $u[n] = 0$ pour $n < 0$ si $u \in \mathbb{C}^{\mathbb{N}}$.

$u[n]$	$\mathcal{Z}(u)(z)$	$\mathcal{D}(\mathcal{Z}(u))$
$\delta_{p,n}$	z^{-p}	$\mathbb{C} \setminus \{0\}$
1	$\frac{z}{z-1}$	$ z > 1$
n	$\frac{z}{(z-1)^2}$	$ z > 1 $
n^2	$\frac{z(z+1)}{(z-1)^3}$	$ z > 1 $
n^3	$\frac{z(z^2+4z+1)}{(z-1)^4}$	$ z > 1 $
$n(n-1)$	$\frac{2z}{(z-1)^3}$	$ z > 1 $
$n(n-1)\dots(n-k+1)$	$\frac{k!z}{(z-1)^{k+1}}$	$ z > 1 $
a^n	$\frac{z}{z-a}$	$ z > a $
$\frac{a^n}{n!}$	$e^{a/z}$	$\mathbb{C} \setminus \{0\}$
$a^n u[n]$	$\mathcal{Z}(u)(z/a)$	$a\mathcal{D}(\mathcal{Z}(u))$
na^n	$\frac{az}{(z-a)^2}$	$ z > 1 $
$n(n-1)a^n$	$\frac{2az}{(z-a)^2}$	$ z > a $
$n(n-1)\dots(n-p+1)a^n$	$\frac{k!a^k z}{(z-a)^{k+1}}$	$ z > 1 $
$nu[n]$	$-z \frac{d\mathcal{Z}(u)}{dz}(z)$	contains $\mathcal{D}_{abs}(\mathcal{Z}(u))$
$u[n-p]$	$z^{-p} \mathcal{Z}(u)(z)$	$\mathcal{D}(\mathcal{Z}(u))$
$u[n+p]$	$z^p \mathcal{Z}(u)(z) - u[0]z^p \dots - u[p-2]z^2 - u[p-1]z$	$\mathcal{D}(\mathcal{Z}(u))$

On va maintenant donner un exemple d'application de la transformée en Z . On considère un *filtre récursif causal* qui à un signal discret $x = (x[n])_{n \geq 0}$ associe le signal discret $y = (y[n])_{n \geq 0}$ défini pour $n \geq 0$ par la formule

$$y[n] = a_0 x[n] + a_1 x[n-1] + \dots + a_p x[n-p] + b_1 y[n-1] + \dots + b_q y[n-q] \quad (5.17)$$

avec les conventions $x[n] = y[n] = 0$ pour $n < 0$.

Posons $X(z) = \mathcal{Z}(x)(z)$, $Y(z) = \mathcal{Z}(y)(z)$. On a d'après la table

$$(1 - b_1 z^{-1} \dots - b_q z^{-q}) Y(z) = (a_0 + a_1 z^{-1} + \dots + a_p z^{-p}) X(z), \quad Y(z) = \frac{a_0 + a_1 z^{-1} + \dots + a_p z^{-p}}{1 - b_1 z^{-1} \dots - b_q z^{-q}} X(z).$$

La fraction rationnelle $R = \frac{a_0 + a_1 z^{-1} + \dots + a_p z^{-p}}{1 - b_1 z^{-1} \dots - b_q z^{-q}}$ est appelée *fonction de transfert* du filtre récursif causal considéré. On voit donc que le filtre se traduit par l'équation

$$Y = G * X \quad (5.18)$$

où $G \in \mathbb{C}^{\mathbb{N}}$ est quand elle existe la suite telle que $\mathcal{Z}(G) = R$. Pour obtenir G on décompose en éléments simples la fraction rationnelle $\frac{R(z)}{z}$, ce qui permet en multipliant par z décrire R sous la forme

$$R(z) = U(z) + \sum_j 1^k \left(\sum_{i=1}^{n(j)} \frac{b_{i,j} z}{(z - a_{i,j})^i} \right).$$

où U est un polynôme. Quand le polynôme U est constant, on peut déterminer G en lisant de droite à gauche la table des transformées en Z .

Exemple 5.2.5 On pose $y[n] = x[n] - 2x[n-1] - y[n-1]$ pour $n \geq 0$, avec les conventions $x[n] = y[n] = 0$ pour $n < 0$. Alors

Posons $X(z) = \mathcal{Z}(x)(z)$, $Y(z) = \mathcal{Z}(y)(z)$. Si on pose $x_{(1)}[n] = x[n-1]$, $y_1[n] = y[n-1]$ pour $n \geq 0$, On a d'après la table $\mathcal{Z}(x_1)(z) = z^{-1}X(z)$, $\mathcal{Z}(y_1)(z) = z^{-1}Y(z)$, et on obtient

$$Y(z) = X(z) - 2z^{-1}X(z) - z^{-1}Y(z), \quad (1+z^{-1})Y(z) = (1-2z^{-1})X(z), \quad Y(z) = \frac{(z-2)X(z)}{z+1}.$$

On obtient

$$\frac{z-2}{z(z+1)} = \frac{a}{z} + \frac{b}{z+1}.$$

En multipliant par z et en faisant $z = 0$, puis en multipliant par z et en faisant $z = -1$, on obtient

$$\frac{z-2}{z(z+1)} = -\frac{2}{z} + \frac{3}{z+1}, \quad \frac{z-2}{z+1} = -2 + \frac{3z}{z+1}.$$

Posons $e_0[0] = 1$, $e_0[n] = 0$ pour $n \geq 1$. En utilisant la table, et en posant $u[n] = (-1)^n$ pour $n \geq 0$, on obtient $\mathcal{Z}(-2e_0 + 3u)(z) = \frac{(z-2)}{z+1}$, ce qui donne

$$y = (-2e_0 + 3u) * x = -2x + 3u * x,$$

$$y[n] = -2x[n] + 3(-1)^n \sum_{p=0}^n (-1)^p x[p] \quad \forall n \geq 0.$$

Dans le cas d'un signal d'entrée constant tel que $x[n] = 1$ pour tout $n \geq 0$, on obtient $y[n] = -2 + 3(-1)^n \sum_{p=0}^n (-1)^p$. Il est clair que $\sum_{p=0}^n (-1)^p = 1$ si n est pair, $\sum_{p=0}^n (-1)^p = 0$ si n est impair, ce qui donne $y[n] = 1$ si n est pair, $y[n] = -2$ si n est impair. On peut également par ces méthodes calculer le signal d'entrée $x = (x[n])_{n \geq 0}$ à partir du signal de sortie $y = (y[n])_{n \geq 0}$, voir les exercices 2 et 3.

Dans la pratique on applique souvent la transformée en Z à des fonctions continues f : on choisit un "pas" T , une origine a , un entier N et on pose $f[n] = f(a + nT)$ pour $0 \leq n \leq N$, $f[n] = 0$ sinon. Ceci revient à procéder à un *échantillonnage* de la fonction f . Ce point de vue est en particulier développé dans le cours de *Théorie du signal* donné à l'ESTIA par F. Luthon [12].

5.3 Exercices sur le Chapitre 5

Exercice 1

Justifier par le calcul les résultats donnés dans la table des transformées en Z .

Exercice 2

On reprend l'étude du filtre récursif causal donné pour $n \geq 0$ par la formule

$$y[n] = x[n] - 2x[n-1] - y[n-1].$$

Calculer le signal d'entrée $x = (x[n])_{n \geq 0}$ en fonction du signal de sortie $y = (y[n])_{n \geq 0}$. Peut-on obtenir $y[n] = 1$ pour tout $n \geq 0$?

Exercice 3

On considère le filtre récursif causal donné pour $n \geq 0$ par la formule

$$y[n] = x[n] - x[n-1] - y[n-1].$$

1) Calculer le signal de sortie $y = (y[n])_{n \geq 0}$ en fonction du signal d'entrée $x = (x[n])_{n \geq 0}$. Que trouve-t'on si $x[n] = 1$ pour tout $n \geq 0$?

2) Calculer le signal d'entrée $x = (x[n])_{n \geq 0}$ en fonction du signal de sortie $y = (y[n])_{n \geq 0}$. Peut-on obtenir $y[n] = 2^n$ pour tout $n \geq 0$?

Chapitre 6

Transformée de Walsh

6.1 Matrices et transformée de Walsh

La matrice de Walsh W_k est une matrice carrée à 2^k lignes et 2^k colonnes. Ces matrices se définissent par récurrence. On a $W_0 = [1]$. On définit ensuite W_{k+1} à partir de W_k pour $k \geq 0$ en utilisant la formule

$$W_{k+1} = \begin{bmatrix} W_k & W_k \\ W_k & -W_k \end{bmatrix}. \quad (6.1)$$

On obtient

$$W_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad W_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \quad W_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix},$$

et ainsi de suite.

Posons $W_k = [w_{i,j}]_{\substack{0 \leq i \leq 2^k - 1 \\ 0 \leq j \leq 2^k - 1}}$, de sorte que $w_{i,j} \in \{-1, 1\}$.

On va maintenant définir la transformée de Walsh $\mathcal{W}_k : \mathbb{C}^{2^k} \rightarrow \mathbb{C}^{2^k}$.

Définition 6.1.1 Soit $f = \{f[0], f[1], \dots, f[2^k - 1]\}$ un vecteur complexe de taille 2^k . La transformée de Walsh $\mathcal{W}_k(f)$ est le vecteur complexe de taille 2^k défini pour $0 \leq i \leq 2^k - 1$ par la formule

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

En d'autres termes on a ${}^t\mathcal{W}_k(f) = W_k {}^t f$, c'est à dire

$$\begin{bmatrix} \mathcal{W}_k(f)[0] \\ \vdots \\ \mathcal{W}_k(f)[2^k - 1] \end{bmatrix} = W_k \begin{bmatrix} f[0] \\ \vdots \\ f[2^k - 1] \end{bmatrix} \quad (6.2)$$

Pour $0 \leq j \leq 2^k - 1$, notons $\delta_j \in \mathbb{C}^{2^k}$ la "fonction de Dirac" définie par la formule $\delta_j[i] = 0$ si $0 \leq i \leq 2^k - 1, i \neq j$, et $\delta_j[j] = 1$ (en d'autres termes $\delta_j = \{\delta_{i,j}\}_{1 \leq i \leq 2^k - 1}$, où $\delta_{i,j}$ désigne le symbole de Kronecker). La famille $\mathcal{B} := \{\delta_0, \dots, \delta_{2^k - 1}\}$ n'est autre que la "base canonique" de \mathbb{C}^{2^k} introduite dans le *Cours d'algèbre linéaire* [6]. On voit donc que la transformée de Walsh \mathcal{W}_k est l'application linéaire de \mathbb{C}^{2^k} dans lui-même dont la matrice par rapport à la base canonique \mathcal{B} de \mathbb{C}^{2^k} est égale à W_k . Autrement dit, avec les notations du Chapitre 2 de [6], on a

$$\mathcal{M}_{\mathcal{W}_k, \mathcal{B}, \mathcal{B}} = W_k. \quad (6.3)$$

On a, pour $k \geq 0$,

$${}^tW_{k+1} = \begin{bmatrix} {}^tW_k & {}^tW_k \\ {}^tW_k & -{}^tW_k \end{bmatrix}, W_{k+1}^2 = \begin{bmatrix} W_k & W_k \\ W_k & -W_k \end{bmatrix} \begin{bmatrix} W_k & W_k \\ W_k & -W_k \end{bmatrix} = \begin{bmatrix} 2W_k^2 & 0 \\ 0 & 2W_k^2 \end{bmatrix}.$$

Comme W_1 est symétrique, et comme $W_1^2 = 2I_2$, on voit par une récurrence immédiate que W_k est symétrique et que $W_k^2 = 2^k I_{2^k}$ pour $k \geq 1$, où I_{2^k} désigne la matrice carrée unité à 2^k lignes et 2^k colonnes. Par conséquent W_k est inversible, et $W_k^{-1} = \frac{1}{2^k} W_k$. Donc la transformée de Walsh est inversible, et on a

$$\mathcal{W}_k^{-1} = \frac{1}{2^k} \mathcal{W}_k. \quad (6.4)$$

Remarquons également que, puisque la matrice de Walsh est symétrique, on a $\mathcal{W}_k(f) = fW_k$, soit

$$[\mathcal{W}_k(f)[0], \dots, \mathcal{W}_k(f)[2^k - 1]] = [f[0], \dots, f[2^k - 1]] W_k \quad (6.5)$$

En fait, la transformée de Walsh peut être interprétée comme une *transformée de Fourier*, et la formule ci-dessus devient alors un cas particulier de la *formule d'inversion de Fourier*, comme on le verra plus tard.

6.2 Transformée de Walsh rapide

Comme la matrice de Walsh d'ordre k possède 2^{2k} coefficients, le calcul direct de la transformée de Walsh utilisant cette matrice nécessite 2^{2k} opérations. On va maintenant donner un procédé beaucoup plus rapide, puisqu'il ne nécessite que $k2^k$ opérations. Ce procédé est basé sur l'observation suivante.

Proposition 6.2.1 Soit $k \geq 1$ un entier. Pour $f \in \mathbb{C}^{2^k}$, $0 \leq j \leq 2^{k-1} - 1$, posons

$$\pi_0(f)[j] = f[j], \quad \pi_1(f)[j] = f[2^{k-1} + j] \quad (6.6)$$

On a alors, pour $0 \leq j \leq 2^{k-1} - 1$

$$\pi_0(\mathcal{W}_k(f)) = \mathcal{W}_{k-1}(\pi_0(f)) + \mathcal{W}_{k-1}(\pi_1(f)), \quad \pi_1(\mathcal{W}_k(f)) = \mathcal{W}_{k-1}(\pi_0(f)) - \mathcal{W}_{k-1}(\pi_1(f)) \quad (6.7)$$

Démonstration : On a

$$W_k = \begin{bmatrix} W_{k-1} & W_{k-1} \\ W_{k-1} & -W_{k-1} \end{bmatrix}.$$

Posons $f_0 := \pi_0(f)$, $f_1 := \pi_1(f)$, $g := \mathcal{W}_k(f)$, $g_0 := \pi_0(g)$, $g_1 := \pi_1(g)$. On obtient $g = fW_k$, soit

$$g_0 = f_0W_{k-1} + f_1W_{k-1}, \quad g_1 = f_0W_{k-1} - f_1W_{k-1}.$$

Donc $g_0 = \mathcal{W}_{k-1}(f_0) + \mathcal{W}_{k-1}(f_1)$, $g_1 = \mathcal{W}_{k-1}(f_0) - \mathcal{W}_{k-1}(f_1)$, ce qui démontre la proposition. ♣

Ceci permet d'obtenir un algorithme effectif pour calculer la transformée de Walsh. Notons $P(k)$ le nombre d'opérations nécessaires pour calculer une transformée de Walsh d'ordre k en utilisant la proposition ci-dessus. On a $P(k) = 2^k + 2P(k-1)$, car il faut $2 \times 2^{k-1} = 2^k$ opérations pour faire apparaître $\pi_0(f)$ et $\pi_1(f)$, et ensuite calculer deux transformées de Walsh d'ordre $k-1$, ce qui nécessite $2P(k-1)$ opérations. Une transformée de Walsh d'ordre 0 ne nécessite aucun calcul, donc $P(0) = 0$, et on a $P(1) = 1$. Une récurrence évidente montre alors que $P(k) = k2^k$. Pour $k = 10$ ceci correspond à $10 \times 2^{10} = 10240$ opérations au lieu des $10^{20} = 1048576$ opérations nécessaires en utilisant directement la matrice de Walsh.

On va maintenant décrire en détail l'algorithme. On commence par remplacer $f = \{f[0], f[1], \dots, f[2^k - 1]\}$ par $f^{(1)}$, où $f^{(1)}[2p] = f[2p] + f[2p + 1]$, $f^{(1)}[2p + 1] = f[2p] - f[2p + 1]$ pour $0 \leq p \leq 2^{k-1} - 1$. La n^e -étape, pour $1 \leq n \leq k$, consiste à remplacer $f^{(n-1)}$ par $f^{(n)}$, où on pose, pour $0 \leq p \leq 2^{k-n} - 1$, $0 \leq q \leq 2^n - 1$,
 $f^{(n)}[2^n p + q] = f^{(n-1)}[2^n p + q] + f^{(n-1)}[2^n p + q + 2^{n-1}]$,
 $f^{(n)}[2^n p + q + 2^{n-1}] = f^{(n-1)}[2^n p + q] - f^{(n-1)}[2^n p + q + 2^{n-1}]$.

On a alors $f^{(k)} = \mathcal{W}_k(f)$. On appelle ceci *l'effet papillon* (l'aile du "papillon" double à chaque étape), ou la méthode consistant à *diviser pour régner*.

Le fait que $f^{(k)} = \mathcal{W}_k(f)$ est évident par récurrence. Il est clair que cet algorithme est valide à l'ordre 1. D'autre part dire qu'il est valide à l'ordre $k-1$ indique que si $f \in \mathbb{C}^{2^k}$ alors $\pi_0(f^{(k-1)}) = \mathcal{W}_{k-1}(\pi_0(f))$ et $\pi_1(f^{(k-1)}) = \mathcal{W}_{k-1}(\pi_1(f))$, et il résulte alors de la proposition que $f^{(k)} = \mathcal{W}_k(f)$.

On va maintenant illustrer cet algorithme par un exemple.

Exemple 6.2.2 Calcul de la transformée de Walsh de $f = \{1, 2, -1, -3, 6, -1, 2, 0\}$.

On détaille les calculs sous forme d'un tableau, en respectant les notations ci-dessus.

	0	1	2	3	4	5	6	7
f	1	2	-1	-3	6	-1	2	0
$f^{(1)}$	3	-1	-4	2	5	7	2	2
$f^{(2)}$	-1	1	7	-3	7	9	3	5
$\mathcal{W}_3(f) = f^{(3)}$	6	10	10	2	-8	-8	4	-8

On retrouve le même résultat par un calcul direct, qui est déjà sensiblement plus long que l'algorithme rapide pour $k = 3$.

$$\begin{aligned}
 & \begin{bmatrix} \mathcal{W}_3(f)[0] \\ \mathcal{W}_3(f)[1] \\ \mathcal{W}_3(f)[2] \\ \mathcal{W}_3(f)[3] \\ \mathcal{W}_3(f)[4] \\ \mathcal{W}_3(f)[5] \\ \mathcal{W}_3(f)[6] \\ \mathcal{W}_3(f)[7] \end{bmatrix} = W_3 \begin{bmatrix} f[0] \\ f[1] \\ f[2] \\ f[3] \\ f[4] \\ f[5] \\ f[6] \\ f[7] \end{bmatrix} \\
 & = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ -1 \\ -3 \\ 6 \\ -1 \\ 2 \\ 0 \end{bmatrix} \\
 & = \begin{bmatrix} 6 \\ 10 \\ 10 \\ 2 \\ -8 \\ -8 \\ 4 \\ -8 \end{bmatrix}
 \end{aligned}$$

6.3 Application aux fonctions booléennes

Soit $p \geq 2$ un entier. On note \mathbb{F}_p l'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ introduit dans le *cours d'algèbre* [5]. Formellement, les éléments de $\mathbb{Z}/p\mathbb{Z}$ sont les parties de \mathbb{Z} de la forme

$\bar{m} := m + p\mathbb{Z}$, de sorte que $\bar{m} = \bar{n}$ si et seulement si $m \equiv n \pmod{p}$, c'est à dire si et seulement si $m - n$ est divisible par p . On munit $\mathbb{Z}/p\mathbb{Z}$ des opérations suivantes, m et n désignant deux entiers relatifs quelconques.

$$\bar{m} + \bar{n} = \overline{m + n}, \quad \bar{m} \cdot \bar{n} = \overline{mn} \quad (6.8)$$

En pratique $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \dots, \overline{p-1}\}$, $\bar{m} + \bar{n} = \overline{r_{m+n}}$, où r_{m+n} , désigne le reste de la division de $m + n$ par p , et $\bar{m} \cdot \bar{n} = \overline{r_{mn}}$, où r_{mn} , désigne le reste de la division de mn par p . Muni de ces deux opérations, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ est un anneau, voir le Chapitre 1 de [5]. Notons également que si p est premier, alors \mathbb{F}_p est un corps, ce qui permet de munir \mathbb{F}_p^k d'une structure d'espace vectoriel sur \mathbb{F}_p pour $k \geq 1$.

On va maintenant restreindre l'attention à \mathbb{F}_2 . Notons que si $m, n \in \mathbb{Z}$, et si $m - n$ est divisible par 2, alors $(-1)^m = (-1)^n$. On peut donc poser $(-1)^{\bar{m}} = -1^m$ pour $m \in \mathbb{Z}$, et on a $(-1)^{a+b} = (-1)^a(-1)^b$ pour $a, b \in \mathbb{F}_2$.

Définition 6.3.1 Une fonction booléenne d'ordre k est une application $f : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$. L'ensemble des fonctions booléennes d'ordre k sera noté \mathcal{B}_k . Pour $f, g \in \mathcal{B}_k, u \in \mathbb{F}_2$, on définit $uf, f + g$ et fg par les formules

$$(uf)(x) = uf(x), \quad (f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x) \quad \forall x \in \mathbb{F}_2^k.$$

D'autre part on pose $X_i(x) = x_i$, pour $x = [x_0, \dots, x_{k-1}] \in \mathbb{F}_2^k$, $0 \leq i \leq k - 1$. Les fonctions de la forme $X_S := \prod_{i \in S} X_i$, où $S \subset \{0, \dots, k - 1\}$ sont appelées des **monômes** (on pose par convention $X_\emptyset(x) = \bar{1}$, avec la notation usuelle $u(x) = u$ pour tout $x \in \mathbb{F}_2^k$ si $u \in \mathbb{F}_2$).

Il est clair que, muni des opérations ci-dessus, \mathcal{B}_k est un anneau, et que $X_i^2 = X_i$ pour $0 \leq i \leq k - 1$. C'est également un espace vectoriel sur \mathbb{F}_2 . Notons que le produit de deux monômes est également un monôme.

Proposition 6.3.2 La dimension de \mathcal{B}_k est égale à 2^k , et l'ensemble \mathcal{M}_k des monômes est une base de \mathcal{B}_k .

Démonstration : Il est clair que \mathbb{F}_2^k possède 2^k éléments, donc \mathcal{B}_k est isomorphe à $\mathbb{F}_2^{2^k}$ et $\dim(\mathcal{B}_k) = 2^k$ (une base "canonique" de \mathcal{B}_k est donnée par la famille $\{\delta_x\}_{x \in \mathbb{F}_2^k}$, où $\delta_x(x) = \bar{1}$ et $\delta_x(y) = \bar{0}$ pour $x \neq y$). On considère bien entendu la fonction $X_\emptyset = \bar{1}$ comme un monôme, de sorte que la famille $\mathcal{M}_k = \{X_S\}_{S \subset \mathbb{F}_2^k}$ des monômes possède 2^k éléments.

Soit $\{\lambda_S\}_{S \subset \mathbb{F}_2^k}$ une famille d'éléments de \mathbb{F}_2 , et supposons qu'il existe $S_0 \subset \mathbb{F}_2^k$ tel que $\lambda_{S_0} \neq \bar{0}$. Comme S_0 est fini il existe un sous-ensemble S_1 de S_0 tel que $\lambda_{S_1} \neq \bar{0}$ et tel que $\lambda_S = \bar{0}$ pour tout sous-ensemble S de \mathbb{F}_2^k strictement inclus dans S_1 . Posons $f(x) = \bar{1}$ si $x \in S_1$ et $f(x) = \bar{0}$ si $x \notin S_1$ (de sorte que $f = \bar{0}$ si $S_1 = \emptyset$ et $f = \bar{1}$ si $S_1 = \mathbb{F}_2^k$). Il est clair que $X_S(f) = \bar{0}$ si S n'est pas inclus dans S_1 , et il résulte du choix de S_1 que $X_S(f) = \bar{0}$ si S est strictement inclus dans S_1 . Comme $X_{S_1}(f) = \bar{1}$

on a $\left(\sum_{S \subset \mathbb{F}_2^k} \lambda_S X_S \right) (f) = \lambda_{S_1} \neq \bar{0}$, et $\sum_{S \subset \mathbb{F}_2^k} \lambda_S X_S \neq \bar{0}$. Ceci montre que \mathcal{M}_k est libre. Comme le nombre d'éléments de \mathcal{M}_k est égal à la dimension de \mathcal{B}_k , on voit que \mathcal{M}_k est une base de de \mathcal{B}_k . ♣

Définition 6.3.3 (i) On dit que $f \in \mathcal{B}_k$ est une **fonction affine d'ordre k** s'il existe $a = (a_0, \dots, a_{k-1}) \in \mathbb{F}_2^k$ et $b \in \mathbb{F}_2$ tels que l'on ait

$$f(x) = \sum_{j=0}^{k-1} a_j x_j + b \quad \forall x = (x_0, \dots, x_{k-1}) \in \mathcal{B}_k, \quad (6.9)$$

et dans ce cas on pose $f = f_{a,b}$.

(ii) Pour $g, h \in \mathcal{B}_k$, on pose

$$d(g, h) = \text{Card} [\{x \in \mathbb{F}_2^k \mid g(x) \neq h(x)\}].$$

(iii) Pour $g \in \mathcal{B}_k$, on pose

$$d(g, \mathcal{A}_k) = \min\{d(f, g) \mid f \in \mathcal{A}_k\},$$

où \mathcal{A}_k désigne l'ensemble des fonctions affines d'ordre k .

Les fonctions booléennes jouent un rôle important en cryptographie, et il est important de pouvoir utiliser dans ce domaine des fonctions booléennes aussi éloignées que possible des fonctions affines. On va établir une formule qui permet d'évaluer la "distance" d'une fonction booléenne aux fonctions affines au moyen de la transformée de Walsh. On va commencer par établir deux résultats techniques concernant la transformée de Walsh.

Lemme 6.3.4 On a, pour $f \in \mathbb{C}^{2^k}$

$$\sum_{p=0}^{2^k-1} |\mathcal{W}_k(f)(p)|^2 = 2^k \sum_{p=0}^{2^k-1} |f(p)|^2 \quad (6.10)$$

Démonstration : On verra plus loin qu'il s'agit en fait d'un cas particulier de la formule de Parseval, mais on va donner une démonstration directe. La formule est évidente pour $k = 0$. Supposons qu'elle est vérifiée pour $k - 1$, avec $k \geq 1$, et soit $f \in \mathbb{C}^{2^k}$. Il résulte de la formule 6.6 que l'on a, en posant $g = \mathcal{W}_k(f)$, $f_0 = \pi_0(f)$, $f_1 = \pi_1(f)$, $g_0 = \pi_0(g)$, $g_1 = \pi_1(g)$,

$$\sum_{p=0}^{2^k-1} |\mathcal{W}_k(f)(p)|^2 = \sum_{p=0}^{2^{k-1}-1} |g_0(p)|^2 + \sum_{p=0}^{2^{k-1}-1} |g_1(p)|^2$$

$$\begin{aligned}
&= \sum_{p=0}^{2^{k-1}-1} |\mathcal{W}_{k-1}(f_0)(p) + \mathcal{W}_{k-1}(f_1)(p)|^2 + \sum_{p=0}^{2^{k-1}-1} |\mathcal{W}_{k-1}(f_0)(p) - \mathcal{W}_{k-1}(f_1)(p)|^2 \\
&\quad 2 \sum_{k=0}^{2^{k-1}-1} |\mathcal{W}_{k-1}(f_0)(p)|^2 + 2 \sum_{k=0}^{2^{k-1}-1} |\mathcal{W}_{k-1}(f_1)(p)|^2 \\
&= 2^k \sum_{k=0}^{2^{k-1}-1} |f_0(p)|^2 + 2^k \sum_{k=0}^{2^{k-1}-1} |f_1(p)|^2 = 2^k \sum_{p=0}^{2^k-1} |f(p)|^2,
\end{aligned}$$

et le résultat est démontré par récurrence. ♣

Pour $x = (x_0, \dots, x_{k-1}) \in \mathbb{F}_2^k, y = (y_0, \dots, y_{k-1}) \in \mathbb{F}_2^k$, on pose

$$x.y := \sum_{j=0}^{k-1} x_j y_j \quad (6.11)$$

Lemme 6.3.5 *Pour $0 \leq p \leq 2^k - 1$, soit $p = \sum_{j=0}^{k-1} p_j 2^j$, avec $p_j \in \{0, 1\}$, la décomposition dyadique de p , et soit $p^* := (\bar{p}_0, \dots, \bar{p}_{k-1})$. Soit $W_k = (w_{p,q})_{\substack{0 \leq p \leq k-1 \\ 0 \leq q \leq k-1}}$ la matrice de Walsh d'ordre k . On a, pour $0 \leq p, q \leq k-1$,*

$$w_{p,q} = (-1)^{p^*.q^*} = (-1)^{\sum_{0 \leq j \leq k-1} p_j q_j} \quad (6.12)$$

Démonstration : La propriété est vérifiée pour $p = 0$. Avec les notations ci-dessus posons $\tilde{w}_{p,q} = (-1)^{p^*.q^*}$, $\tilde{W}_k = (\tilde{w}_{p,q})_{\substack{0 \leq p \leq k-1 \\ 0 \leq q \leq k-1}}$. D'autre part pour $0 \leq p \leq 2^{k-1} - 1, 0 \leq q \leq 2^{k-1} - 1$, posons $p' = p + 2^{k-1}, q' = q + 2^{k-1}$. Dans ce cas $p_{k-1} = q_{k-1} = 0, p'_j = p_j, q'_j = q_j$ pour $0 \leq j \leq k-2$, et $p'_{k-1} = q'_{k-1} = 1$. On déduit de la première équation que l'on a

$$\tilde{W}_{k-1} = (\tilde{w}_{p,q})_{\substack{0 \leq p \leq 2^{k-1}-1 \\ 0 \leq q \leq 2^{k-1}-1}}$$

On déduit des autres équations que l'on a, pour $0 \leq p \leq 2^{k-1} - 1, 0 \leq q \leq 2^{k-1} - 1$,

$$\tilde{w}_{p',q} = \tilde{w}_{p,q'} = \tilde{w}_{p,q}, \quad \tilde{w}_{p',q'} = -\tilde{w}_{p,q},$$

et on obtient

$$\tilde{W}_k = \begin{bmatrix} \tilde{W}_{k-1} & \tilde{W}_{k-1} \\ \tilde{W}_{k-1} & -\tilde{W}_{k-1} \end{bmatrix}.$$

On voit donc par récurrence que $W_k = \tilde{W}_k$ pour tout $k \geq 0$. ♣

Définition 6.3.6 Pour $f \in \mathcal{B}_k$, $0 \leq p \leq 2^k - 1$, on pose $f^*(p) = (-1)^{f(p^*)}$. Autrement dit si $p_j \in \{0, 1\}$ pour $0 \leq j \leq 2^k - 1$, on a

$$f^* \left(\sum_{j=0}^{2^k-1} p_j 2^j \right) = (-1)^{f(\bar{p}_0, \dots, \bar{p}_{k-1})}. \quad (6.13)$$

On peut alors exprimer simplement la distance d'une fonction booléenne à une fonction affine sans terme constant.

Lemme 6.3.7 Soit $f \in \mathcal{B}_k$, soit $a = (\bar{a}_0, \dots, \bar{a}_{k-1}) \in \mathbb{F}_2^k$, avec $a_j \in \{0, 1\}$, soit $\tilde{a} = \sum_{j=0}^{k-1} a_j 2^j \in \{0, \dots, 2^k - 1\}$ l'entier associé à a et soit $f_a := f_{a, \bar{0}} : x \rightarrow a \cdot x$ la fonction affine sans terme constant associée à a . Alors on a

$$d(f, f_a) = 2^{k-1} - \frac{1}{2} \mathcal{W}_k(f^*)(\tilde{a}). \quad (6.14)$$

Démonstration : On a $f^*(\tilde{a}) = f((\tilde{a})^*) = f(a)$. On obtient

$$\begin{aligned} \mathcal{W}_k(f^*)(\tilde{a}) &= \sum_{q=0}^{2^k-1} w_{\tilde{a}, q} f^*(q) = \sum_{q=0}^{2^k-1} (-1)^{a \cdot q^* + f(q^*)} \\ &= \sum_{q=0}^{2^k-1} (-1)^{f_a(q^*) + f(q^*)} = \sum_{x \in \mathbb{F}_2^k} (-1)^{f_a(x) + f(x)} = \end{aligned}$$

$$\text{Card}(\{x \in \mathbb{F}_2^k \mid f(x) = f_a(x)\}) - \text{Card}(\{x \in \mathbb{F}_2^k \mid f(x) \neq f_a(x)\}).$$

Comme $\text{Card}(\{x \in \mathbb{F}_2^k \mid f(x) = f_a(x)\}) + \text{Card}(\{x \in \mathbb{F}_2^k \mid f(x) \neq f_a(x)\}) = \text{Card}(\mathbb{F}_2^k) = 2^k$, et comme $d(f, f_a) = \text{card}(\{x \in \mathbb{F}_2^k \mid f(x) \neq f_a(x)\})$, on obtient la formule du lemme. ♣

On peut alors exprimer simplement la distance d'une fonction booléenne aux fonctions affines.

Théorème 6.3.8 (i) Soit $f \in \mathcal{B}_k$ une fonction booléenne. On a

$$d(f, \mathcal{A}_k) = 2^{k-1} - \frac{1}{2} \max_{0 \leq p \leq 2^k-1} |\mathcal{W}_k(f^*)(p)| \leq 2^{k-1} - 2^{\frac{k}{2}-1}, \quad (6.15)$$

et l'inégalité ci-dessus est toujours stricte si k est impair.

(ii) Si k est pair, posons $f_{(k)} = \sum_{j=0}^{\frac{k}{2}-1} X_{2j} X_{2j+1}$. On a alors

$$d(f_{(k)}, \mathcal{A}_k) = 2^{k-1} - 2^{\frac{k}{2}-1}.$$

Démonstration : Le fait que $d(f, \mathcal{A}_k) = 2^{k-1} - \frac{1}{2} \max_{0 \leq p \leq 2^k-1} |\mathcal{W}_k(f^*)(p)|$ résulte du lemme 6.3.7. D'autre part il résulte de la formule de Parseval (lemme 6.3.4) que l'on a

$$2^k \max_{0 \leq p \leq 2^k-1} |\mathcal{W}_k(f^*)(p)|^2 \geq \sum_{p=0}^{2^k-1} |\mathcal{W}_k(f^*)(p)|^2 = 2^k \sum_{p=0}^{2^k-1} |f^*(p)|^2 = 2^{2k}.$$

Donc $\max_{0 \leq p \leq 2^k-1} |\mathcal{W}_k(f^*)(p)| \geq 2^{\frac{k}{2}}$. Comme $f^*(p) \in \{-1, 1\}$ pour $0 \leq p \leq 2^k-1$, la transformée de Walsh de f^* est à valeurs entières ainsi que $\max_{0 \leq p \leq 2^k-1} |\mathcal{W}_k(f^*)(p)|$, et l'inégalité de (i) est stricte si k est impair.

On va maintenant construire par récurrence sur m une fonction $h_m \in \mathbb{C}^{2^{2m}}$, prenant ses valeurs dans $\{-1, 1\}$, telle que $\mathcal{W}_{2m}(h_m) = 2^m h_m$, de sorte que

$$\max_{0 \leq p \leq 2^{2m}-1} |\mathcal{W}_{2m}(h_m)(p)| = 2^m.$$

Le polynôme minimal de W_{2m} est égal à $x^2 - 2^{2m} = (x - 2^m)(x + 2^m)$. On sait alors d'après le Chapitre 5 du *Cours d'algèbre linéaire* [6] que le sous-espace propre de W_{2m} associé à la valeur propre 2^m est engendré par les colonnes de $W_{2m} - 2^m I_{2^{2m}}$, $I_{2^{2m}}$ désignant la matrice unité d'ordre $2m$. On a

$$W_2 - 2I_4 = \begin{bmatrix} 3 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 3 \end{bmatrix}.$$

On peut donc prendre $h_1 = [1, 1, 1, -1]$.

On définit alors la suite $(h_m)_{m \geq 1}$ par récurrence en posant, pour $m \geq 2$,

$$h_m = [h_{m-1}, h_{m-1}, h_{m-1}, -h_{m-1}].$$

Supposons que $\mathcal{W}_{2(m-1)}(h_{m-1}) = 2^{m-1} h_{m-1}$. On a alors, d'après la formule 6.5,

$$\begin{aligned} h_m W_{2m} &= [h_{m-1}, h_{m-1}, h_{m-1}, h_{m-1}] \begin{bmatrix} W_{2m-2} & W_{2m-2} & W_{2m-2} & W_{2m-2} \\ W_{2m-2} & -W_{2m-2} & W_{2m-2} & -W_{2m-2} \\ W_{2m-2} & W_{2m-2} & -W_{2m-2} & -W_{2m-2} \\ W_{2m-2} & -W_{2m-2} & -W_{2m-2} & W_{2m-2} \end{bmatrix} \\ &= [2h_{m-1}W_{2m-2}, 2h_{m-1}W_{2m-2}, 2h_{m-1}W_{2m-2}, 2h_{m-1}W_{2m-2}] \\ &= [2^m h_{m-1}, 2^m h_{m-1}, 2^m h_{m-1}, 2^m h_{m-1}] = 2^m h_m, \end{aligned}$$

de sorte que $\mathcal{W}_{2m}(h_m) = 2^m h_m$. On voit donc par récurrence que $\mathcal{W}_{2m}(h_m) = 2^m h_m$ pour tout $m \geq 1$.

Posons maintenant $H_m = f_{(2m)}^* = (\sum_{j=0}^{m-1} X_{2j} X_{2j+1})^*$. Soit $p = \sum_{j=0}^{2m-1} p_j 2^j$, avec $p_j \in \{0, 1\}$, le développement en base 2 d'un entier $p \in \{0, \dots, 2^{2m} - 1\}$. On a

$$H_m(p) = (-1)^{\sum_{j=0}^{m-1} p_{2j} p_{2j+1}}. \quad (6.16)$$

Posons $p^{(1)} = p$, $p^{(2)} = p + 2^{2m}$, $p^{(3)} = p + 2^{2m+1}$, $p^{(4)} = p + 2^{2m} + 2^{2m+1}$. On a $p_j^{(1)} = p_j^{(2)} = p_j^{(3)} = p_j^{(4)} = p_j$ pour $0 \leq j \leq 2m - 1$, $p_{2m}^{(1)} = p_{2m+1}^{(1)} = p_{2m+1}^{(2)} = p_{2m}^{(3)} = 0$, $p_{2m}^{(2)} = p_{2m+1}^{(3)} = p_{2m}^{(4)} = p_{2m+1}^{(4)} = 1$. Il résulte alors de la formule 6.16 appliquée à l'ordre $m + 1$ que l'on a, pour $m \geq 1$,

$$H_{m+1} = [H_m, H_m, H_m, -H_m].$$

D'autre part, en appliquant la formule 6.16 à l'ordre 1, on trouve $H_1(0) = H_1(1) = H_2(1) = 1$, $H_3(1) = -1$, donc $H_1 = [1, 1, 1, -1] = h_1$. Une récurrence immédiate montre alors que $h_m = H_m = f_{(2m)}^*$ pour tout $m \geq 1$. Comme h_m est à valeurs dans $\{-1, 1\}$, et comme $\mathcal{W}_{2m}(h_m) = 2^m h_m$, on a $|\mathcal{W}_{2m}(f_{(2m)}(p))| = 2^m$ pour $0 \leq p \leq 2^{2m} - 1$, et $d(f_{(2m)}, \mathcal{A}_{2m}) = 2^{2m-1} - 2^{m-1}$. ♣

On dit qu'une fonction booléenne $f \in \mathcal{A}_k$ est une *fonction courbe* si sa distance aux fonctions affines est maximale. Le théorème précédent montre que la fonction $f_k = \sum_{j=0}^{k/2-1} X_{2j} X_{2j+1}$ est une fonction courbe si k est pair. Les fonctions courbes restent mal connues quand k est impair.

6.4 Applications de la transformée de Walsh à la compression de signaux 1-D

Dans les applications de la transformée de Walsh la notion de **nombre de changements de signes** joue un rôle important

Définition 6.4.1 Soit $k \geq 1$ un entier, soit $W_k = (w_{i,j})_{\substack{1 \leq j \leq 2^k - 1 \\ 1 \leq i \leq 2^k - 1}}$ la matrice de Walsh d'ordre k . On pose, pour $1 \leq j \leq 2^k - 1$,

$$cs_k(i) = \frac{1}{2} \sum_{j=1}^{2^k-1} |w_{i,j-1} - w_{i,j}|. \quad (6.17)$$

Le **réarrangement par changement de signes** $\mathcal{R}_k(i)$ de la suite $\{0, \dots, 2^k - 1\}$ est la suite $\{cs_k^{-1}(0), \dots, cs_k^{-1}(2^k - 1)\}$.

En d'autres termes le nombre $cs_k(i)$ est le nombre de changements de signes dans la i^e ligne de la matrice de Walsh W_k , et on peut écrire $\mathcal{R}_k(i) = \{u_0, \dots, u_{2^k-1}\} \subset \{0, \dots, 2^k - 1\}$, avec $cs(u_j) > cs(u_{j-1})$ pour $1 \leq j \leq 2^k - 1$.

On va maintenant illustrer ces notions pour $k = 1$ et $k = 2$ (il faut bien évidemment faire appel à l'ordinateur pour les grandes valeurs de k).

On a

$$W_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad cs_1(0) = 0, cs_1(1) = 1, \quad \mathcal{R}_1 = \{0, 1\},$$

$$W_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \quad cs_1(0) = 0, \quad cs_1(1) = 3, \quad cs_1(2) = 1, \quad cs_1(3) = 2,$$

$$\mathcal{R}_2 = \{0, 2, 3, 1\}.$$

On remarque que l'application $j \rightarrow cs_1(j)$ prend les valeurs 0 et 1 sur l'ensemble $\{0, 1\}$, et que l'application $j \rightarrow cs_1(j)$ prend les valeurs 0, 1, 2 et 3 sur l'ensemble $\{0, 1, 2, 3\}$. On a en fait le résultat général suivant, qui montre bien que la suite \mathcal{R}_k est bien un réarrangement de la suite $\{0, \dots, 2^k - 1\}$.

Théorème 6.4.2 *Pour $k \geq 1$, l'application $j \rightarrow cs_k(j)$ est une bijection de l'ensemble $\{0, \dots, 2^k - 1\}$ sur lui-même.*

Démonstration : Il est clair que $cs_k(j)$ est un nombre entier, et on a, pour $0 \leq j \leq k - 1$,

$$0 \leq cs_k(j) = \frac{1}{2} \sum_{j=1}^{2^k-1} |w_{k,j} - w_{k,j-1}| \leq 2^k - 1,$$

donc il suffit de vérifier que $cs_k : \{0, \dots, 2^k - 1\} \rightarrow \{0, \dots, 2^k - 1\}$ est surjective, puisque toute application surjective d'un ensemble fini sur lui-même est bijective. C'est vrai si $k = 1$.

Notons $L_{i,k} = [w_{0,1}, \dots, w_{0,2^k-1}]$ la i^e ligne de W_k . Comme $W_k = \begin{bmatrix} W_k & W_k \\ W_k & -W_k \end{bmatrix}$, on a, pour $0 \leq i \leq 2^k - 1$

$$L_{i,k+1} = [L_{i,k}, L_{i,k}], \quad L_{i+2^k,k+1} = [L_{i,k}, -L_{i,k}].$$

Comme $w_{0,i} = 1$, on voit que $cs_{k+1}(i) = 2cs_k(i)$ et $cs_{k+1}(i + 2^k) = 2cs_k(i) + 1$ si $w_{i,2^k} = 1$, alors que $cs_{k+1}(i) = 2cs_k(i) + 1$ et $cs_{k+1}(i + 2^k) = cs_k(i)$ si $w_{i,2^k} = -1$.

Supposons maintenant que pour tout $p \in \{0, \dots, 2^k - 1\}$ il existe $i \in \{0, \dots, 2^k - 1\}$ tel que $cs_k(i) = p$, et soit $p \in \{0, \dots, 2^{k+1} - 1\}$. Si p est pair il est de la forme $p = 2q$, et si p est impair il est de la forme $p = 2q + 1$, avec q entier, $0 \leq q \leq 2^k - 1$. On a alors soit $cs_{k+1}(i) = p$, soit $cs_{k+1}(i + 2^k) = p$, où $i \in \{0, \dots, 2^k - 1\}$ est choisi de sorte que $cs_k(i) = q$. Comme $0 \leq i < i + 2^k \leq 2^{k+1} - 1$, on voit par récurrence que l'application $i \rightarrow cs_k(i)$ est bien une application surjective, donc bijective, de l'ensemble $\{0, \dots, 2^k - 1\}$ sur lui-même pour tout $k \geq 1$. ♣

Définition 6.4.3 *Soit $f = \{f[0], f[1], \dots, f[2^k - 1]\} \in \mathbb{C}^{2^k}$, soit $p \in \{0, 2^k - 1\}$, et soit $c = \frac{p}{2^k}$. Posons $\mathcal{W}_{c,k}(f)[i] = \mathcal{W}_k(f)[i]$ si $cs_k(i) \leq c2^k - 1$, $\mathcal{W}_{c,k}(f)[i] = 0$ si $c2^k - 1 < cs_k(i) \leq 2^k - 1$. La **compression d'ordre c de f** est la suite $Comp_c(f) \in \mathbb{C}^{2^k}$ définie par la formule*

$$\text{Comp}_c(f) = (\mathcal{W}_k^{-1} \circ \mathcal{W}_{c,k})(f). \quad (6.18)$$

Soit $D_c = (d_{i,j})_{\substack{0 \leq i \leq 2^k-1 \\ 0 \leq j \leq 2^k-1}}$ la matrice diagonale définie par les formules $d_{i,j} = 0$ si $i \neq j$, $d_{i,i} = 0$ si $c2^k - 1 < cs_k(i) \leq 2^k - 1$, $d_{i,i} = 1$ si $cs_k(i) \leq c2^k - 1 - 1$. On a

$${}^t(\mathcal{W}_{c,k}(f)) = D_c^t(\mathcal{W}_k(f)) = D_c \mathcal{W}_k^t f, \quad \text{Comp}_c(f) = \frac{1}{2^k} \mathcal{W}_k D_c \mathcal{W}_k^t f.$$

Si on préfère faire les calculs avec les matrices lignes f et $f^{(c)}$, on obtient

$$f^{(c)} = \frac{1}{2^k} f \mathcal{W}_k D_c \mathcal{W}_k. \quad (6.19)$$

Pour $k = 2$, $c = 50\%$, on obtient

$$\begin{aligned} W_2 &= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \quad D_c = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \\ \frac{1}{4} W_2 D_c W_2 &= \frac{1}{4} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1/2 & 1/2 & 0 & 0 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 1/2 & 1/2 \end{bmatrix}. \end{aligned}$$

Donc si $f = \{f[0], f[1], f[2], f[3]\}$, $f^{(c)} = \left\{ \frac{f[0]+f[1]}{2}, \frac{f[0]+f[1]}{2}, \frac{f[3]+f[4]}{2}, \frac{f[3]+f[4]}{2} \right\}$.

On a vu au début de ce chapitre, en utilisant la transformée de Walsh rapide, que si $f = \{1, 2, -1, -3, 6, -1, 2, 0\}$, alors $\mathcal{W}_3(f) = \{6, 10, 10, 2, -8, -8, 4, -8\}$.

On a

$$W_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

On obtient

$$c_3(0) = 0, \quad c_3(1) = 7, \quad c_3(2) = 3, \quad c_3(3) = 4, \quad c_3(4) = 1, \quad c_3(5) = 6, \quad c_3(6) = 2, \quad c_3(7) = 5.$$

On pose $c = 37,5\%$, donc $\mathcal{W}_{3,c}(f) = \{6, 0, 0, 0, -8, 0, 4, 0\}$. On termine le calcul de $f^{(c)}$ en utilisant la transformée de Walsh rapide (ne pas oublier de diviser par 8 le résultat obtenu en appliquant la transformée de Walsh à $\mathcal{W}_{3,c}(f)$ pour obtenir sa transformée de Walsh inverse.

	0	1	2	3	4	5	6	7
$g = \mathcal{W}_{3,c}(f)$	6	0	0	0	-8	0	4	0
$g^{(1)}$	6	6	0	0	-8	-8	4	4
$g^{(2)}$	6	6	6	6	-4	-4	-12	-12
$8f^{(c)} = g^{(3)}$	2	2	-6	-6	10	10	18	18
$f^{(c)}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{3}{4}$	$-\frac{3}{4}$	$\frac{5}{4}$	$\frac{5}{4}$	$\frac{9}{4}$	$\frac{9}{4}$

Ce calcul est confirmé sous Mupad, voir la feuille de calcul jointe.

Cette méthode de compression est en général efficace, mais elle ne peut pas donner toujours de bon résultats : il suffit pour la mettre en défaut avec un taux de compression c de considérer une suite non nulle $f \in \mathbb{C}^{2^k}$ telle que $\mathcal{W}_k(f)[j] = 0$ pour tout $j \geq c(2^k - 1)$. On peut évidemment construire des exemples de ce type, en prenant k assez grand, pour $c > 99,99\%$, et plus généralement pour des taux de compression arbitrairement proches de 1.

On va maintenant mettre en place une procédure sous Matlab pour appliquer cette méthode à des signaux 1-D. En pratique on a une fonction $f : [a, b] \rightarrow \mathbb{R}$. on fixe un entier $k \geq 1$, et on pose, pour $0 \leq j \leq 2^k - 1$,

$$\tilde{f}[j] = f\left(a + j \frac{b-a}{2^k - 1}\right).$$

On applique la procédure ci-dessus à \tilde{f} , ce qui donne $\tilde{f}^{(c)} \in \mathbb{C}^{2^k}$, et on construit la compression $f^{(c)}$ de f associée à cet échantillonnage, qui est la fonction affine sur les intervalles $[a + j \frac{b-a}{2^k - 1}, a + (j+1) \frac{b-a}{2^k - 1}]$, $0 \leq j \leq 2^k - 2$ vérifiant $f^{(c)}(a + j \frac{b-a}{2^k - 1}) = \tilde{f}^{(c)}[j]$ pour $0 \leq j \leq 2^k - 1$. On donne ensuite les représentations de f et $f^{(c)}$ sous Matlab associées à ces échantillonnages.

Nous décrivons maintenant en détail une implémentation sous Matlab de cette méthode de compression des signaux 1-D. Ce procédé est décrit par G.Peyré dans [13]. Nous donnons la version obtenue par G.Fenez et S. Ismais en 2006 à Bordeaux dans leur mémoire de master1-crypto [9]. On commence par écrire un programme pour le réarrangement par changements de signes.

On écrit

```
edit ncs
```

Matlab ouvre un fichier (une m-file).

```
M:=Dom::Matrix();
```

```
Dom::Matrix()
```

```
W0:=M([[1]]);
```

```
W1:=
```

```
linalg::stackMatrix(linalg::concatMatrix(W0,W0),linalg::concatMatrix(W0,-W0));
```

```
W2:=
```

```
linalg::stackMatrix(linalg::concatMatrix(W1,W1),linalg::concatMatrix(W1,-W1));
```

```
W3:=
```

```
linalg::stackMatrix(linalg::concatMatrix(W2,W2),linalg::concatMatrix(W2,-W2));
```

(1)

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

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

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

```
DC:=
```

```
M([[1,0,0,0,0,0,0,0],[0,0,0,0,0,0,0,0],[0,0,0,0,0,0,0,0],[0,0,0,0,0,0,0,0],[0,0,0,0,1,0,0,0],[0,0,0,0,0,0,1,0],[0,0,0,0,0,0,0,1],[0,0,0,0,0,0,0,0]]);
```


6.4. APPLICATIONS DE LA TRANSFORMÉE DE WALSH À LA COMPRESSION DE SIGNAUX 1-D 75

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$f := ([1, 2, -1, -3, 6, -1, 2, 0]); g := f * W3; gc := g * DC; fc = (1/8) * gc * W3;$

$[[1, 2, -1, -3, 6, -1, 2, 0]]$

$(6 \ 10 \ 10 \ 2 \ -8 \ -8 \ 4 \ -8)$

$(6 \ 0 \ 0 \ 0 \ -8 \ 0 \ 4 \ 0)$

$fc = \left(\frac{1}{4} \ \frac{1}{4} \ -\frac{3}{4} \ -\frac{3}{4} \ \frac{5}{4} \ \frac{5}{4} \ \frac{9}{4} \ \frac{9}{4}\right)$

```
function nk = ncs(n)
p = log2(n); nk = 0; ek = 0;

for k=1:p
    ek = [ek;1-ek];
    nk = 2*[nk;nk]+ek;
end
```

Pour réorganiser par changements de signe les nombres entiers entre 0 et $n - 1$, n désignant une puissance de 2, il suffit d'utiliser la commande `ncs(n)`.

On obtient par exemple

```
>> ncs(32)
```

```
ans =
```

```
0
31
15
16
7
24
8
23
3
28
12
19
4
27
11
20
1
30
14
17
6
25
9
22
2
```

6.4. APPLICATIONS DE LA TRANSFORMÉE DE WALSH À LA COMPRESSION DE SIGNAUX 1-D 77

29
13
18
5
26
10
21

Ce programme fonctionne à l'échelle industrielle : il faut à peine quelques secondes à Matlab pour dérouler la liste des nombres de 0 à $10^{20} - 1$, reclassés par changements de signe.

On implémente ensuite la transformée de Walsh rapide. On introduit sous Matlab une deuxième m-file, notée `fw`.

```
% Transformée de Walsh rapide
function res = fwt(a)
% N doit être une puissance de 2
[NN,N] = size(a);
res = zeros(N,1);
if N==1
    % fin de l'algorithme
    res = a;
    return;
end
% appels récursifs
P = N/2;
a(1:P) = fwt(a(1:P));
a((P+1):N) = fwt(a((P+1):N));
for i=1:P
    tmp = a(i);
    a(i) = tmp + a(i+P);
    a(i+P) = tmp - a(i+P);
end;
res = a;
```

On vérifie l'algorithme en l'appliquant à la suite $a = [12 - 1 - 36 - 120]$. On retrouve bien le résultat vu plus haut.

```
a=[ 1 2 -1 -3 6 -1 2 0];
>> b=fwt(a)
```

b =

6 10 10 2 -8 -8 4 -8

On teste maintenant cette machine sur un signal à 1024 entées. Le résultat est obtenu instantanément, et on vérifie que la transformée de Walsh inverse de la transformée du signal b est nulle aux erreurs d'arrondi près (le résultat, qui consiste en une liste de nombres de l'ordre de 10^{-14} , n'est pas affiché).

```
>> a=[0:1:1023];
>> b=sin(a);
>> c=fwt(b);
>> d=b-(1/1024)*fwt(c)
```

On va maintenant mettre en place la procédure de compression proprement dite, qui fait appel aux deux programmes précédents. On ouvre une m-file nommée `compr1d`, dont les entrées sont un signal `1d` et un taux de compression. On représente graphiquement ensuite le résultat obtenu.

```
function res = compr1d(entree,fact_red)

walsh = fwt(entree);
[a,b] = size (entree);
tab_chgt = ncs(b);

for k=1:b
    if tab_chgt(k) >= fact_red
        walsh(k) = 0;
    end
end

res = fwt(walsh)/b;
```

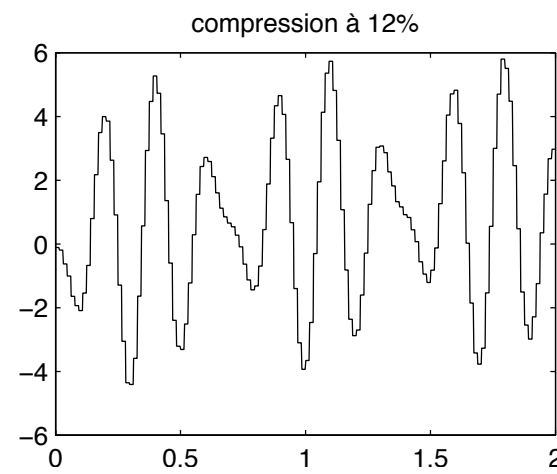
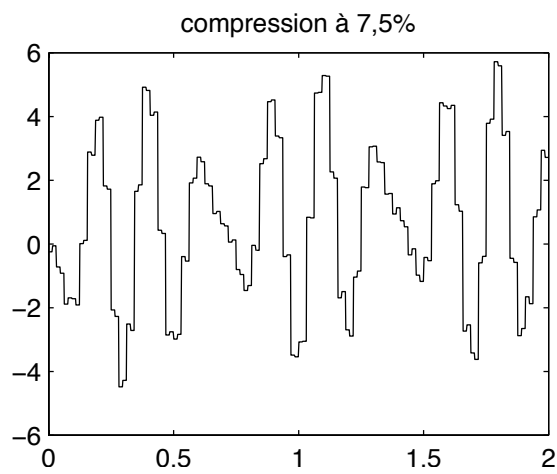
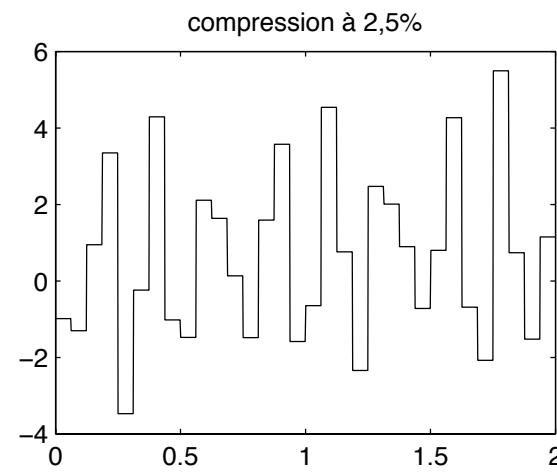
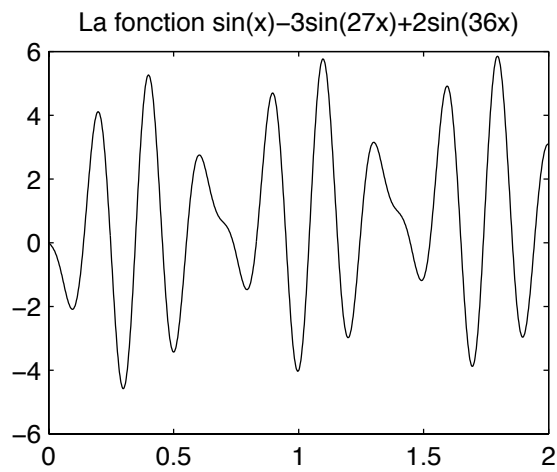
On notera que le taux de compression à rentrer dans la commande `compr1d` est en fait le produit du taux de compression cherché par la longueur du signal. On applique ceci au signal obtenu à partir de la fonction $x \rightarrow \sin(x) - 3 * \sin(x/27) + 2\sin(x/36)$, avec des taux de compression de 10%, 30% et 75%.

```
x=[0:2/1023:2];
```

6.4. APPLICATIONS DE LA TRANSFORMÉE DE WALSH À LA COMPRESSION DE SIGNAUX 1-D 79

```
y1=sin(x)-3*sin(x*27)+2*sin(x*36);  
z11=compr1d(y1,25);  
z12=compr1d(y1,76);  
z13=compr1d(y1,123);  
>> subplot(221);plot(x,y1);  
>> subplot(222);plot(x,z11);  
>> subplot(223);plot(x,z12);  
>> subplot(224);plot(x,z13);
```

On obtient un fichier eps avec la commande matlab "print -depsc compld" que l'on insère dans le support de cours.



6.5 Applications de la transformée de Walsh à la compression des images

On aborde maintenant le traitement des images. Une image en noir et blanc peut être considérée comme une matrice carrée dont les coefficients, communément appelés **pixels**, sont des réels mesurant toutes les variantes de gris entre le blanc et le noir. Pour les images en couleur à chaque pixel seront associés trois nombres permettant de reconstituer la couleur du pixel à partir de trois couleurs fondamentales. Le principe de la compression est le même dans les deux cas, et nous allons décrire en détail comment compresser les images en noir et blanc en utilisant la transformée de Walsh.

Dans toute la suite on notera $L_i(M)$ la i^e ligne et $C_j(M)$ la j^e colonne d'une matrice $M = (m_{i,j})_{\substack{0 \leq i \leq p-1 \\ 0 \leq j \leq q-1}}$.

Définition 6.5.1 Soit $k \geq 1$. Une **image numérisée** à 2^{2k} pixels est une matrice $\Omega = (\Omega_{i,j})_{\substack{0 \leq j \leq 2^{k-1} \\ 0 \leq i \leq 2^{k-1}}}$ à coefficients réels.

La transformée de Walsh horizontale $\mathcal{W}^{(k,hor)}(\Omega)$ d'une image numérisée Ω à 2^{2k} pixels Ω est par définition la matrice obtenue en appliquant la transformée de Walsh \mathcal{W}_k à toutes les lignes de Ω , la transformée de Walsh verticale $\mathcal{W}^{(k,vert)}(\Omega)$ de Ω est par définition la matrice obtenue en appliquant la transformée de Walsh \mathcal{W}_k à toutes les colonnes de Ω , et on définit la transformée de Walsh $\mathcal{W}^{(k)}$ de Ω par la formule

$$\mathcal{W}^{(k)}(\Omega) = (\mathcal{W}^{(k,vert)} \circ \mathcal{W}^{(k,hor)})(\Omega).$$

Notons que comme d'après les formules 6.2 et 6.5, on a $L_i(\mathcal{W}^{(k,hor)}(\Omega)) = L_i(\omega)W_k$ et $C_j(\mathcal{W}^{(k,vert)}(\Omega)) = W_k C_j(\Omega)$, et on obtient les formules

$$\begin{aligned} \mathcal{W}^{(k,hor)}(\Omega) &= W_k \Omega, \quad \mathcal{W}^{(k,vert)}(\Omega) = \Omega W_k, \\ \mathcal{W}^{(k)}(\Omega) &= (\mathcal{W}^{(k,vert)} \circ \mathcal{W}^{(k,hor)})(\Omega) = W_k \Omega W_k = (\mathcal{W}^{(k,hor)} \circ \mathcal{W}^{(k,vert)})(\Omega). \end{aligned} \quad (6.20)$$

On a alors

$$(\mathcal{W}^{(k)})^{-1}(\Omega) = \frac{1}{2^{2k}} (\mathcal{W}^{(k)})(\Omega) = \frac{1}{2^{2k}} W_k \Omega W_k. \quad (6.21)$$

Par exemple considérons l'image numérisée à 4 pixels $\Omega = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. On a

$$\begin{aligned} \mathcal{W}_1(\Omega) &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} a+b & a-b \\ c+d & c-d \end{bmatrix} \\ &= \begin{bmatrix} a+b+c+d & a-b+c-d \\ a+b-c-d & a-b-c+d \end{bmatrix}. \end{aligned}$$

Bien entendu dans la pratique on ne saurait travailler à moins de 1 million de pixels, ce qui donne au moins $k = 10$, car $10^{20} = 1048576$, et les calculs se font sur ordinateur à l'aide de la transformée de Walsh rapide, comme on le verra plus loin.

On va maintenant procéder à un "réarrangement selon les changements de signes" des couples (i, j) pour $0 \leq i \leq 2^k - 1, 0 \leq j \leq 2^k - 1$. Comme l'application $i \rightarrow cs_k(i)$ est une bijection de l'ensemble $\{0, \dots, 2^k - 1\}$ sur lui-même, l'application $(i, j) \rightarrow cs_k(i) + cs_k(j)$ est une application surjective de l'ensemble $\{0, \dots, 2^k - 1\} \times \{0, \dots, 2^k - 1\}$ sur l'ensemble $\{0, 2^{k+1} - 2\}$. On va alors définir un ordre total sur les (doubles) indices des pixels, ce qui va permettre de les réarranger par ordre croissant et d'appliquer la transformée de Walsh à la compression d'images.

Définition 6.5.2 Soient (i_1, j_1) et (i_2, j_2) deux éléments de l'ensemble $E_k := \{0, \dots, 2^k - 1\} \times \{0, \dots, 2^k - 1\}$. On dit par définition que (i_1, j_1) est strictement inférieur à (i_2, j_2) si $cs_k(i_1) + cs_k(j_1) < cs_k(i_2) + cs_k(j_2)$, ou si $cs_k(i_1) + cs_k(j_1) = cs_k(i_2) + cs_k(j_2)$ avec $cs_k(i_1) < cs_k(i_2)$.

On adopte la convention évidente $(i_1, j_1) \leq (i_2, j_2)$ si $(i_1, j_1) < (i_2, j_2)$, ou si $(i_1, j_1) = (i_2, j_2)$, et on obtient un ordre total sur E_k . On pose, pour $(i, j) \in E_k$,

$$\theta_k(i, j) = \text{Card}(\{(\alpha, \beta) \in E_k \mid (\alpha, \beta) \leq (i, j)\}). \quad (6.22)$$

Ceci permet de définir avec précision une procédure de compression d'images.

Définition 6.5.3 Soit $\Omega = (\omega_{i,j})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq k}}$ une image numérisée à 2^k pixels. Pour $c \in [0, 1]$, on pose

$$\mathcal{W}^{(k,c)}(\Omega)[i, j] = \mathcal{W}^{(k)}(\Omega)[i, j] \text{ si } \theta_k(i, j) \leq c2^{2k}, \quad \mathcal{W}^{(k,c)}(\Omega)[i, j] = 0 \text{ si } \theta_k(i, j) > c2^{2k},$$

et on définit la compression d'ordre c de Ω par la formule

$$\Omega^{(c)} = ([\mathcal{W}^{(k)}]^{-1} \circ \mathcal{W}^{(k,c)})(\Omega) = \frac{1}{2^{2k}} \mathcal{W}^{(k)}(\mathcal{W}^{(k)}(\Omega)\mathcal{W}^{(k)}).$$

Revenons à notre image numérisée $\Omega = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ à 4 pixels. Une compression à 0% donne $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, et une compression à 100% ; redonne Ω .

On a

$$(0, 0) < (0, 1) < (1, 0) < (1, 1),$$

et on obtient

$$\mathcal{W}^{(1,1/4)}(\Omega) = \begin{bmatrix} a + b + c + d & 0 \\ 0 & 0 \end{bmatrix}, \quad \mathcal{W}^{(1,1/2)}(\Omega) = \begin{bmatrix} a + b + c + d & a - b + c - d \\ 0 & 0 \end{bmatrix},$$

$$\mathcal{W}^{(1,3/4)}(\Omega) = \begin{bmatrix} a+b+c+d & a-b+c-d \\ a+b-c-d & 0 \end{bmatrix},$$

$$\Omega^{(1/4)} = \frac{1}{4} \begin{bmatrix} a+b+c+d & a+b+c+d \\ a+b+c+d & a+b+c+d \end{bmatrix}, \Omega^{(1/2)} = \frac{1}{2} \begin{bmatrix} a+c & b+d \\ a+c & b+d \end{bmatrix},$$

$$\Omega^{(3/4)} = \frac{1}{4} \begin{bmatrix} 3a+b+c-d & 3b+a-c+d \\ 3c+a-b+d & 3d-a+b+c \end{bmatrix}.$$

Des implémentations sous Matlab de cette méthode ont été réalisées par Fenez-Ismaïl et Le Moal-Ponsonnet dans leurs mémoires de Master 1 à Bordeaux [9] [11]. Nous n'avons hélas pas eu le temps de les faire figurer ici.

6.6 Exercices sur le Chapitre 6

exercice 1

- 1) Ecrire les matrices de Walsh W_2 , W_4 , W_8 et W_{16} et leurs inverses.
- 2) Calculer les transformées de Walsh des fonctions $[0, 1]$, $[0, 1, 0, 0]$, $[0, 1, 1, 1, 1, 1, 2, 3]$ et $[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]$.
 - a) En utilisant les matrices de Walsh
 - b) En utilisant la transformée de Walsh rapide.
- 3) Vérifier sous Mupad les résultats de la question précédente.

exercice 2

Soient S et T deux sous-ensembles de $\{0, \dots, k-1\}$. Montrer que l'on a

$$(i) X_S \cdot X_T = X_{S \cap T}.$$

$$(ii) X_{S \cup T} = X_S + X_T + X_S \cdot X_T.$$

exercice 3

En utilisant le *Cours d'algèbre linéaire* [6], montrer que le polynôme caractéristique de la matrice de Walsh W_k est égal à $(x^2 - 2^k)^{2^{k-1}}$. En déduire qu'il existe une matrice orthogonale $P \in \mathcal{M}_{2^k}(\mathbb{R})$ telle que l'on ait

$${}^t P W_k P = P^{-1} W_k P = 2^{\frac{k}{2}} \begin{bmatrix} I_{2^{k-1}} & 0 \\ 0 & -I_{2^{k-1}} \end{bmatrix},$$

où $I_{2^{k-1}}$ désigne la matrice unité à 2^{k-1} lignes et 2^{k-1} colonnes.

exercice 4

Exprimer toutes les fonctions booléennes sur \mathbb{F}^2 comme somme de monômes.

exercice 5

Déterminer le nombre de fonctions courbes et les expliciter toutes dans les cas $k = 2$, $k = 3$ et $k = 4$.

exercice 6

Soit $a \in \mathcal{B}_k$, et posons $\delta_a(x) = \bar{0}$ si $x \neq a$, $\delta_a(x) = \bar{1}$ si $x = a$.

1) Vérifier que $f = \sum_{a \in \mathbb{F}_2^k} f(a) \delta_a$ pour toute fonction $f \in \mathcal{B}_k$.

2) Montrer que l'on a, pour $a = [a_1, \dots, a_{k-1}] \in \mathbb{F}_2^k$

$$\delta_a = \prod_{j=0}^{k-1} (X_j + a_j + \bar{1}).$$

3) On énumère les éléments de \mathbb{F}_2^k en posant $a_{(p)} = [\bar{p}_0, \dots, \bar{p}_{k-1}]$ pour $0 \leq p \leq 2^k - 1$, où $p = \sum_{j=0}^{k-1} p_j 2^j$, avec $p_j \in \{-1, 1\}$, désigne la décomposition de p en base 2. De même on énumère les sous-ensembles S de $\{0, \dots, k-1\}$ en posant $S_p := \{j \in \{0, \dots, k-1\} \mid p_j = \bar{1}\}$.

Donner la matrice de passage de la base $\{a_{(0)}, \dots, a_{(2^k-1)}\}$ à la base $\{X_{S_0}, \dots, X_{S_{2^k-1}}\}$ et la matrice de passage de la base $\{X_{S_0}, \dots, X_{S_{2^k-1}}\}$ à la base $\{a_0, \dots, a_{2^k-1}\}$. Quel est le lien entre ces deux matrices ?

4) En utilisant ce qui précède, donner une formule permettant de calculer la décomposition d'une fonction booléenne en somme de monômes $f \in \mathcal{B}_k$ à partir du tableau des valeurs de f^* .

exercice 7

Soit $f \in \mathcal{B}_3$ la fonction booléenne vérifiant $f^*(x_p) = 1$ si $0 \leq p \leq 3$, $f^*(x_p) = -1$ si $4 \leq p \leq 7$.

1) Donner la table des valeurs de f , et exprimer f comme somme de monômes (on pourra utiliser l'exercice précédent).

2) Calculer transformée de Walsh de f^* en utilisant l'algorithme rapide du cours (donner le détail des calculs).

2) Quelles sont les fonctions booléennes affines les plus proches de f au sens de la distance du cours, et quelle est la valeur de $d(f, \mathcal{A}_3)$?

3) Même questions avec la fonction g vérifiant $g^*(p) = 1$ pour p impair, $g^*(p) = -1$ pour p pair quand $0 \leq p \leq 7$.

exercice 8 (usage de Mupad recommandé)

1) Trouver par le calcul matriciel la formule donnant la transformée de Walsh d'une image numérisée à 16 pixels.

2) Réarranger par ordre croissant les couples $(i, j)_{\substack{0 \leq i < 3 \\ 0 \leq j < 3}}$ en suivant la procédure du cours.

3) Trouver la formule permettant de calculer la compression à 75% d'une image numérisée à 16 pixels.

exercice 9

Donner un programme permettant de calculer par récurrence sous Mupad les matrices de Walsh.

Chapitre 7

Transformée de Fourier discrète

7.1 Définition de la transformée de Fourier discrète

On va définir la transformée de Fourier discrète sur \mathbb{C}^N .

Définition 7.1.1 Soit $N \geq 1$ un entier et soit $\omega_N = e^{\frac{2i\pi}{N}}$. On définit la **transformée de Fourier discrète** \hat{f} de $f = (f[0], \dots, f[N-1])$ par la formule

$$\hat{f}[m] = \sum_{n=0}^{N-1} f[n] \omega_N^{-nm}, \quad m \in \{0, \dots, N-1\}. \quad (7.1)$$

L'application $= \mathcal{F}_N(f) : f \rightarrow \hat{f}$ est appelée la *transformation de Fourier discrète* sur \mathbb{C}^N .

La matrice de Fourier A_N est définie par la formule

$$A_N = (\omega_N^{-mn})_{\substack{0 \leq m \leq N-1 \\ 0 \leq n \leq N-1}}.$$

Il est clair que la matrice de Fourier est symétrique, et que A_N est la matrice représentant $\mathcal{F}_N(f) : \mathbb{C}^N \rightarrow \mathbb{C}^N$ dans la base canonique $\{\delta_0, \dots, \delta_{N-1}\}$ de \mathbb{C}^N . On a alors les formules

$$\hat{f} = f A_N, \quad {}^t \hat{f} = A_N {}^t f. \quad (7.2)$$

On définit la matrice conjuguée \bar{B} d'une matrice $B = (b_{m,n})_{\substack{0 \leq i \leq p \\ 0 \leq j \leq q}}$ par la formule

$$\bar{B} := (\bar{b}_{m,n})_{\substack{0 \leq i \leq p \\ 0 \leq j \leq q}}.$$

On a

$$\sum_{k=0}^{N-1} \omega_N^{mk} \omega_N^{-nk} = \sum_{k=0}^{N-1} (\omega_N^{m-n})^k.$$

Comme $\omega_N^N = 1$, on obtient, pour $0 \leq m \leq N-1$, $0 \leq n \leq N-1$,

$$\sum_{k=0}^{N-1} \omega_N^{mk} \omega_N^{-nk} = N \text{ si } m = n,$$

$$\sum_{k=0}^{N-1} \omega_N^{mk} \omega_N^{-nk} = \frac{1 - \omega^{(m-n)N}}{1 - \omega^{m-n}} = 0 \text{ si } m \neq n.$$

On voit donc que, I_N désignant la matrice unité à N ligne et N colonnes, on a $\overline{A_N} A_N = \frac{1}{N} I_N$, donc A_N est inversible et on a

$$A_N^{-1} = \frac{1}{N} \overline{A_N}. \quad (7.3)$$

On obtient alors la "**formule d'inversion de Fourier**" et les **formules de Plancherel-Parseval** dans le cas discret.

Proposition 7.1.2 *On a pour $f \in \mathbb{C}^N$ la formule d'inversion*

$$f[m] = \frac{1}{N} \sum_{n=0}^{N-1} \hat{f}[n] \omega_N^{mn}, \quad 0 \leq m \leq N-1. \quad (7.4)$$

On a également pour $f, g \in \mathbb{C}^N$ la "formule de Plancherel"

$$\sum_{m=0}^{N-1} f[m] \hat{g}[m] = \frac{1}{N} \sum_{m=0}^{N-1} \hat{f}[m] \overline{\hat{g}[m]}. \quad (7.5)$$

En particulier on a pour $f \in \mathbb{C}^N$ la "formule de Parseval"

$$\sum_{m=0}^{N-1} |f[m]|^2 = \frac{1}{N} \sum_{m=0}^{N-1} |\hat{f}[m]|^2. \quad (7.6)$$

Démonstration : La formule d'inversion résulte du fait que $A_N^{-1} = \frac{1}{N} \overline{A_N}$. D'autre part on a

$$\sum_{m=0}^{N-1} \hat{f}[m] \overline{\hat{g}[m]} = \widehat{f \overline{g}} = f A_N \overline{A_N^t g} = N f^t g = N \sum_{m=0}^{N-1} f[m] \overline{\hat{g}[m]},$$

ce qui prouve la formule de Plancherel, et la formule de Parseval est un cas particulier de la formule de Plancherel. ♣

On va maintenant donner trois exemples en basses dimensions. Pour $N = 2$, on a $\omega_2 = -1$, et $A_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = W_2$, et la transformée de Fourier \mathcal{F}_2 correspond à la transformée de Walsh \mathcal{W}_1 . Pour $N = 3$, on a $\omega_3 = e^{\frac{2i\pi}{3}}$, et en posant $j = e^{\frac{2i\pi}{3}}$, et en remarquant que $j^3 = 1$ et $j^{-1} = j^2$, on obtient

$$A_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & j^2 & j \\ 1 & j & j^2 \end{bmatrix}.$$

Le lecteur remarquera que nous avons adopté la convention $j = e^{\frac{2i\pi}{3}}$, ce qui est l'usage en Mathématiques. Par contre pour les physiciens le nombre j représente le nombre "imaginaire pur", c'est à dire que le nombre j des physiciens est en fait le nombre i des mathématiciens.

Pour $N = 4$, on a $\omega_4 = e^{\frac{2i\pi}{4}} = i$, et on obtient

$$A_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}.$$

Posons $f = (f[0], f[1], f[2]) := (1, 0, 1)$, $g = (g[0], g[1], g[2], g[3]) := (1, 0, 0, i)$. Par calcul direct, on obtient

$$(\hat{f}[0], \hat{f}[1], \hat{f}[2]) = \hat{f} = fA_2 = (1, 0, 1) \begin{bmatrix} 1 & 1 & 1 \\ 1 & j^2 & j \\ 1 & j & j^2 \end{bmatrix} = (3, 0, 0),$$

$$\begin{aligned} (\hat{g}[0], \hat{g}[1], \hat{g}[2], \hat{g}[3]) &= gA_3 = (1, 0, 0, i) \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \\ &= (1 + i, 0, 1 - i, 2). \end{aligned}$$

Notons que dans le calcul de \hat{f} on a utilisé le fait que $1 + j + j^2 = \frac{1-j^3}{1-j} = 0$.

7.2 Convolution cyclique et convolution acyclique

Soient $u = (u[n])_{n \geq 0} \in \mathbb{C}^{\mathbb{N}}$ et $v = (v[n])_{n \geq 0} \in \mathbb{C}^{\mathbb{N}}$ deux signaux causaux. On a défini plus haut le produit de convolution $u * v = ((u * v)[n])_{n \geq 0}$ par la formule (formule 5.4 du Chapitre 5)

$$(u * v)[n] = \sum_{p=0}^n u[p]v[n-p].$$

Considérons maintenant $f = (f[n])_{0 \leq n \leq N-1} \in \mathbb{C}^N$ et $g = (g[n])_{0 \leq n \leq N-1} \in \mathbb{C}^N$.

On définit le **produit de convolution cyclique** $f \overset{(N)}{*} g$ de f et g par la formule

$$(f \stackrel{(N)}{*} g)[n] = \sum_{p=0}^n f[p]g[n-p] + \sum_{p=n+1}^{N-1} f(p)g(n+N-p), \quad 0 \leq n \leq N-1, \quad (7.7)$$

avec la convention évidente $\sum_{p=n+1}^{N-1} f(p)g(n+N-p) = 0$ si $n = N-1$.

On pourrait vérifier directement que la convolution cyclique, qui est une loi de composition interne sur \mathbb{C}^N , est commutative et associative, mais ces propriétés sont des conséquences immédiates de la propriété fondamentale suivante.

Théorème 7.2.1 *Soit $N \geq 1$. On a, pour $f = (f[n])_{0 \leq n \leq N-1} \in \mathbb{C}^N, g = (g[n])_{0 \leq n \leq N-1} \in \mathbb{C}^N$,*

$$\mathcal{F}_N \left(f \stackrel{(N)}{*} g \right) = \mathcal{F}_N(f) \mathcal{F}_N(g). \quad (7.8)$$

Démonstration : Soit $n \in \{0, \dots, N-1\}$, et posons $u[m] = f[m]$ pour $0 \leq m \leq N-1$, $u[m] = 0$ pour $m \geq N$, $v[m] = 0$ pour $0 \leq m \leq n-1$, $v[m] = g[m]$ pour $n \leq m \leq N-1$, $v[m] = g[m-N]$ pour $N \leq m \leq N+n-1$, et $v[m] = 0$ pour $m \geq N+n$, avec les conventions évidentes pour $n = 0$. On a

$$(u * v)[m] = 0 \quad \text{pour } 0 \leq m \leq n-1, \quad (u * v)[m] = (f \stackrel{(N)}{*} g)[m] \quad \text{pour } n \leq m \leq N-1,$$

$$(u * v)[m] = (f \stackrel{(N)}{*} g)(m-N) \quad \text{pour } N \leq m \leq n+N-1, \quad (u * v)[m] = 0 \quad \text{pour } m \geq n+N.$$

Avec les notations du Chapitre 5, et compte tenu du fait que $\omega^{-nN} = 1$, on a

$$\begin{aligned} \mathcal{Z}(u * v)(\omega^n) &= \sum_{m=0}^{+\infty} (u * v)[m] \omega^{-nm} = \sum_{m=n}^{N-1} (u * v)[m] \omega^{-nm} + \sum_{m=N}^{n+N-1} (u * v)[m] \omega^{-(m-N)n} \\ &= \sum_{m=n}^{N-1} (f \stackrel{(N)}{*} g)[m] \omega^{-nm} + \sum_{n=0}^{n-1} (f \stackrel{(N)}{*} g)[m] \omega^{-mn} = \mathcal{F}_N \left(f \stackrel{(N)}{*} g \right) [n]. \end{aligned}$$

Il est clair que $\mathcal{Z}(u)(\omega^n) = \mathcal{F}(f)[n]$. D'autre part on a

$$\begin{aligned} \mathcal{Z}(v)(\omega^n) &= \sum_{m=0}^{+\infty} v[m] \omega^{-mn} = \sum_{m=n}^{N-1} g[m] \omega^{-mn} + \sum_{m=n}^{n+N-1} g(m-N) \omega^{(m-N)n} \\ &= \sum_{m=n}^{N-1} g[m] \omega^{-mn} + \sum_{m=0}^{n-1} g[m] \omega^{-mn} = \mathcal{F}_N(g)[n]. \end{aligned}$$

On a alors, d'après le théorème 5.4

$$\mathcal{F}_N \left(f \overset{(N)}{*} g \right) [n] = \mathcal{Z}(u * v)(\omega^n) = \mathcal{Z}(u)(\omega^n) \mathcal{Z}(v)(\omega^n) = \mathcal{F}_N(f)[n] \mathcal{F}_N(g)[n].$$



Corollaire 7.2.2 *L'application $(f, g) \rightarrow f \overset{(N)}{*} g$ est une loi de composition commutative et associative sur \mathbb{C}^N .*

Notons que si on pose, de même que plus haut, $\delta_0[0] = 1$ et $\delta_0[n] = 0$ pour $1 \leq n \leq N - 1$, alors on a, pour $f \in \mathbb{C}^N$,

$$f \overset{(N)}{*} \delta_0 = \delta_0 \overset{(N)}{*} f = f, \quad (7.9)$$

de sorte que δ_0 est l'élément unité de \mathbb{C}^N pour la loi de composition interne $\overset{(N)}{*}$.

On va voir un peu plus loin que la FFT ("fast Fourier transform") fournit un algorithme performant pour calculer les transformées de Fourier discrètes, ce qui permet de calculer rapidement les produits de convolution cycliques en utilisant la formule

$$f \overset{(N)}{*} g = \mathcal{F}_N^{-1} (\mathcal{F}_N(f) \mathcal{F}_N(g)). \quad (7.10)$$

7.3 La FFT

On va maintenant donner un algorithme rapide (en fait deux versions, la version décimation temporelle et la version décimation séquentielle d'un algorithme rapide) permettant de calculer la transformée de Fourier sur le groupe $\mathbb{Z}/N\mathbb{Z}$ dans le cas où $N = 2^k$, $k \geq 1$. On peut toujours dans les applications se ramener à ce cas, en identifiant $f = (f[0], \dots, f[p]) \in \mathbb{C}(\mathbb{Z}/p\mathbb{Z})$ à la fonction $\tilde{f} \in \mathbb{C}(\mathbb{Z}/2^k\mathbb{Z})$ définie par les formules $\tilde{f}[\bar{j}] = f[\bar{j}]$ pour $0 \leq j \leq p - 1$, $\tilde{f}[\bar{j}] = 0$ pour $p \leq j \leq 2^k - 1$, $k \geq 1$ désignant le plus petit entier tel que $p \leq 2^k$. Cette méthode, inventée par Cooley et Tukey en 1965 et connue sous le nom de FFT (Fast Fourier Transform) a révolutionné le calcul sur ordinateur, en permettant d'effectuer en trente secondes des calculs qui nécessitaient auparavant deux bonnes semaines. Cet algorithme a connu depuis de nombreuses variantes, souvent adaptées à des situations spécifiques. Nous nous contenterons ici de donner les versions de base de cet algorithme, en renvoyant à *Numerical Recipes* [14] pour la version décimation temporelle, et à l'article de Brigham [3] pour la version décimation fréquentielle. On trouvera des détails historiques sur l'invention de la FFT et ses conséquences dans l'article de Rockmore [15].

On identifie dans la suite $[\mathbb{Z}/p\mathbb{Z}]$ à $\{0, \dots, p - 1\}$ en écrivant j au lieu de \bar{j} , et on pose de nouveau $\omega_p = e^{\frac{2i\pi}{p}}$. La version décimation fréquentielle de la FFT est basée sur l'observation suivante.

Proposition 7.3.1 Soit $N \geq 1$ un entier, et soit $f \in \mathbb{C}^{2N}$. Posons $f^{(0)}[j] = f[2j]$ et $f^{(1)}[j] = f[2j+1]$ pour $0 \leq j \leq N-1$. On a

$$\begin{aligned}\mathcal{F}_{2N}(f)[j] &= \mathcal{F}_N(f^{(0)})[j] + \omega_{2N}^{-j} \mathcal{F}_N(f^{(1)})[j] \text{ pour } 0 \leq j \leq N-1, \\ \mathcal{F}_{2N}(f)[j] &= \mathcal{F}_N(f^{(0)})[j-N] - \omega_{2N}^{-j} \mathcal{F}_N(f^{(1)})[j-N] \text{ pour } N \leq j \leq 2N-1. \quad (7.11)\end{aligned}$$

Démonstration : Il s'agit d'un simple calcul. Comme $\omega_N = \omega_{2N}^2$, on a, pour $0 \leq j \leq N-1$,

$$\begin{aligned}\mathcal{F}_{2N}[j] &= \sum_{m=0}^{N-1} f[2m] \omega_{2N}^{-2mj} + \sum_{m=0}^{N-1} f[2m+1] \omega_{2N}^{-(2m+1)j} \\ &= \sum_{m=0}^{N-1} f[2m] \omega_N^{-mj} + \omega_{2N}^{-j} \sum_{m=0}^{N-1} f[2m+1] \omega_N^{-mj} \\ &= \mathcal{F}_N(f^{(0)})[j] + \omega_{2N}^{-j} \mathcal{F}_N(f^{(1)})[j].\end{aligned}$$

Notons que $\omega_{2N}^N = -1$. On obtient, pour $N \leq j \leq 2N-1$,

$$\begin{aligned}\mathcal{F}_{2N}[j] &= \omega_{2N}^{-2mN} \sum_{m=0}^{N-1} f[2m] \omega_{2N}^{-2m(j-N)} + \omega_{2N}^{-(2m+1)N} \sum_{m=0}^{N-1} f[2m+1] \omega_{2N}^{-(2m+1)(j-N)} \\ &= \sum_{m=0}^{N-1} f[2m] \omega_{2N}^{-2m(j-N)} - \sum_{m=0}^{N-1} f[2m+1] \omega_{2N}^{-(2m+1)(j-N)} \\ &= \sum_{m=0}^{N-1} f[2m] \omega_{2N}^{-2m(j-N)} - \omega_{2N}^{-(j-N)} \sum_{m=0}^{N-1} f[2m+1] \omega_{2N}^{-2m(j-N)} \\ &= \sum_{m=0}^{N-1} f[2m] \omega_N^{-m(j-N)} - \omega_{2N}^{-(j-N)} \sum_{m=0}^{N-1} f[2m+1] \omega_N^{-m(j-N)} \\ &= \mathcal{F}_N(f^{(0)})[j-N] - \omega_{2N}^{-(j-N)} \mathcal{F}_N(f^{(1)})[j-N].\end{aligned}$$



On peut déduire directement une implémentation récursive de la transformée de Fourier discrète \mathcal{F}_n quand $N = 2^k$, mais celle-ci présente l'inconvénient d'avoir à séparer les termes pairs et impairs à chaque étape du calcul, alors que pour la transformée de Walsh rapide on associe à $f \in \mathbb{C}^{2^m}$ les fonctions $f_0 = (f[0], \dots, f[2^{m-1}-1]) \in \mathbb{C}^{2^{m-1}}$ et $f_1 = (f[2^{m-1}], \dots, f[2^m-1]) \in \mathbb{C}^{2^{m-1}}$ dans les calculs intermédiaires. On peut remédier à cet inconvénient par une procédure de "renversement de bits".

Définition 7.3.2 Pour $a \in \{0, \dots, 2^k - 1\}$ on note $a = [a_{k-1} \dots a_0]$ l'écriture dyadique de a , de sorte que $a = \sum_{j=0}^{k-1} a_j 2^j$, avec $a_j \in \{0, 1\}$ pour $0 \leq j \leq k - 1$. On pose

$$\text{rev}_k(a) = [a_0 \dots a_{k-1}]. \quad (7.12)$$

De même pour $f \in \mathbb{C}^{2^k}$, on pose

$$\sigma_k(f) = f \circ \text{rev}_k. \quad (7.13)$$

Il est clair que rev_k est une application de l'ensemble $\{0, \dots, 2^k - 1\}$ dans lui-même, et que $(\text{rev}_k \circ \text{rev}_k)(a) = a$ pour tout $a \in \{0, \dots, 2^k - 1\}$. Par conséquent les applications rev_k et σ_k sont bijectives et coïncident avec leurs applications réciproques. On va expliciter l'application rev_k pour $k = 3$.

Exemple 7.3.3 Les valeurs de l'application rev_3 sont données par le tableau suivant

j	0	1	2	3	4	5	6	7
j dyadique	000	001	010	011	100	101	110	111
$\text{rev}_3(j)$ dyadique	000	100	010	110	001	101	011	111
$\text{rev}_3(j)$	0	4	2	6	1	5	3	7

On va maintenant donner l'algorithme de la FFT dans la version décimation temporelle

Théorème 7.3.4 Soit $k \geq 1$, et soit $f \in \mathbb{C}^{2^k}$. On pose $(g_{0,0}, \dots, g_{0,2^k-1}) = g_0 := \sigma_k(f) \in \mathbb{C}^{2^k}$, et pour $1 \leq n \leq k$ on définit $g_n = (g_{n,0}, \dots, g_{n,2^k-n-1}) \in \mathbb{C}^{2^k}$, avec $g_{n,m} \in \mathbb{C}^{2^n}$ par la formule de récurrence suivante, où $0 \leq q \leq 2^{n-1} - 1$,

$$g_{n,m}[q] = g_{n-1,2m}[q] + \omega_{2^n}^q g_{n-1,2m+1}[q + 2^{n-1}],$$

$$g_{n,2m+1}[q + 2^{n-1}] = g_{n-1,2m}[q] - \omega_{2^n}^q g_{n-1,2m+1}[q + 2^{n-1}]. \quad (7.14)$$

Alors $g_k = \mathcal{F}_{2^k}(f)$.

Démonstration : Pour $k = 1$ ce résultat est une conséquence immédiate de la proposition 7.3.1. Supposons maintenant que l'algorithme fonctionne pour tout $f \in \mathbb{C}^{2^k}$, avec $k \geq 1$, et soit $f \in \mathbb{C}^{2^{k+1}}$. Posons $g = \sigma_{k+1}(f)$, et posons également, de même que plus haut, pour $0 \leq m \leq 2^k$,

$$f^{(0)}[m] = f[2m], \quad f^{(1)}[m] = f[2m + 1], \quad g_0[m] = g[m], \quad g_1[m] = g[2^k + m].$$

En écriture dyadique, un nombre de la forme $a = 2m$, avec $0 \leq m \leq 2^k - 1$, s'écrit $a = [a_k \dots a_1 0]$. Donc $m = [a_k \dots a_1]$, et $\text{rev}_{k+1}(a) = [0 a_1 \dots a_k] = \text{rev}_k(m)$. De même si $b = 2m + 1$, avec $0 \leq m \leq 2^k - 1$, b s'écrit $b = [b_k \dots b_1 1]$. Donc $m = [b_k \dots b_1]$, et $\text{rev}_{k+1}(1) = [0 b_1 \dots b_k] = 2^k + \text{rev}_k(m)$. On obtient, pour $0 \leq m \leq 2^k - 1$,

$$\text{rev}_{k+1}(2m) = \text{rev}_k(m), \text{rev}_{k+1}(2m+1) = 2^k + \text{rev}_k(m). \quad (7.15)$$

On en déduit que $g_0 = f^{(0)}$ et que $g_1 = f^{(1)}$. Il résulte alors de l'hypothèse de récurrence que $g_{2^k}(m) = \mathcal{F}_{2^k}(f^{(0)})(m)$ et que $g_{2^k}(2^k + m) = \mathcal{F}_{2^k}(f^{(1)})(m)$ pour $0 \leq m \leq 2^k - 1$. Il résulte alors de la proposition 7.3.1 que $g_{2^{k+1}} = \mathcal{F}_{2^{k+1}}(f)$, et la validité de l'algorithme proposé est vérifiée par récurrence. ♣

Exemple 7.3.5 On pose $f = [1, -1, -1, 0, 0, 1, 1, 0]$. Calculer la transformée de Fourier discrète de f en utilisant la FFT, version décimation temporelle.

On applique l'algorithme ci-dessus, en remarquant que $\omega_2 = -1$ et $\omega_4 = i$.

m	0	1	2	3	4	5	6	7
$f[m]$	1	-1	-1	0	0	1	1	0
$g_0[m]$	1	0	-1	1	-1	1	0	0
$n = 1, 2^n = 2, q = 0$	$g_{1,0}[0]$	$g_{1,0}[1]$	$g_{1,1}[0]$	$g_{1,1}[1]$	$g_{1,2}[0]$	$g_{1,2}[1]$	$g_{1,3}[0]$	$g_{1,3}[1]$
	1	1	0	-2	0	-2	0	0
$n = 2, 2^n = 4, q = 0$ ou 1	$g_{2,0}[0]$	$g_{2,0}[1]$	$g_{2,0}[2]$	$g_{2,0}[3]$	$g_{2,1}[0]$	$g_{2,1}[1]$	$g_{2,1}[2]$	$g_{2,1}[3]$
	1	$1+2i$	1	$1-2i$	0	-2	0	-2
$n = 3, 2^3 = 8, q = 0, 1, 2$ ou 3	$\hat{f}[0]$	$\hat{f}[1]$	$\hat{f}[2]$	$\hat{f}[3]$	$\hat{f}[4]$	$\hat{f}[5]$	$\hat{f}[6]$	$\hat{f}[7]$
	1	$1+2i$ $-2\omega_8^{-1}$	1	$1-2i$ $-2\omega_8^{-3}$	1	$1+2i$ $+2\omega_8^{-1}$	1	$1-2i$ $+2\omega_8^{-3}$

Puisque $\omega_8 = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}$, on a $\omega_8^{-1} = \frac{1-i}{\sqrt{2}}$, $\omega_8^{-3} = e^{-3i\pi/4} = -\frac{1+i}{\sqrt{2}}$. On obtient

$$1 + 2i - 2\omega_8^{-1} = 1 + 2i - \sqrt{2} + \sqrt{2}i = 1 - \sqrt{2} + (2 + \sqrt{2})i,$$

$$1 - 2i - 2\omega_8^{-3} = 1 - 2i + \sqrt{2} + i\sqrt{2} = 1 + \sqrt{2} - (2 - \sqrt{2})i,$$

$$1 + 2i + 2\omega_8^{-1} = 1 + \sqrt{2} + (2 - \sqrt{2})i,$$

$$1 - 2i + 2\omega_8^{-3} = 1 - \sqrt{2} - (2 + \sqrt{2})i,$$

ce que l'on peut résumer dans le tableau suivant

m	0	1	2	3	4	5	6	7
$f[m]$	1	-1	-1	0	0	1	1	0
$\hat{f}[m]$	1	$1 - \sqrt{2}$ $+(2 + \sqrt{2})i$	1	$1 + \sqrt{2}$ $-(2 - \sqrt{2})i$	1	$1 + \sqrt{2}$ $+(2 - \sqrt{2})i$	1	$1 - \sqrt{2}$ $-(2 + \sqrt{2})i$

Dans la suite les fonctions $f_0, f_1, f^{(0)}$ et $f^{(1)}$ sont définies de même que plus haut pour $f \in \mathbb{C}^{2^N}$, $n \geq 1$. Pour $g \in \mathbb{C}^N$, on définit $S_N(g) \in \mathbb{C}^N$ par la formule suivante, où $0 \leq j \leq N$,

$$S_N(g)[j] = \omega_{2^N}^{-j} g[j]. \quad (7.16)$$

On va maintenant aborder la version décimation fréquentielle de la FFT. Cet algorithme est basé sur le résultat suivant.

Proposition 7.3.6 Soit $N \geq 1$ un entier, et soit $f \in \mathbb{C}^{2N}$. On a

$$[\mathcal{F}_{2N}(f)]^{(0)} = \mathcal{F}_N(f_0 + f_1), [\mathcal{F}_{2N}(f)]^{(1)} = \mathcal{F}_N(S_N(f_0 - f_1)). \quad (7.17)$$

Démonstration : Il s'agit de nouveau d'un simple calcul. Pour $0 \leq j \leq N$, on a

$$\begin{aligned} [\mathcal{F}_{2N}(f)]^{(0)}[j] &= \mathcal{F}_{2N}(2j) = \sum_{m=0}^{2N-1} \omega_{2N}^{-2mj} f[m] = \sum_{m=0}^{2N-1} \omega_N^{-mj} f[m] \\ &= \sum_{m=0}^{N-1} \omega_N^{-mj} f[m] + \sum_{m=0}^{N-1} \omega_N^{-mN} \omega_N^{-mj} f[N+m] \\ &= \sum_{m=0}^{N-1} \omega_N^{-mj} f[m] + \sum_{m=0}^{N-1} \omega_N^{-mj} f[N+m], \end{aligned}$$

donc $[\mathcal{F}_{2N}(f)]^{(0)} = \mathcal{F}_N(f_0 + f_1)$.

De même on a, pour $0 \leq j \leq N$,

$$\begin{aligned} [\mathcal{F}_{2N}(f)]^{(1)}[j] &= \mathcal{F}_{2N}(2j+1) = \sum_{m=0}^{2N-1} \omega_{2N}^{-m(2j+1)} f[m] = \sum_{m=0}^{2N-1} \omega_{2N}^{-m} \omega_N^{-mj} f[m] \\ &= \sum_{m=0}^{N-1} \omega_N^{-mj} \omega_{2N}^{-m} f[m] + \sum_{m=0}^{N-1} \omega_N^{-mN} \omega_N^{-mj} \omega_{2N}^{-m} \omega_{2N}^{-N} f[N+m] \\ &= \sum_{m=0}^{N-1} \omega_N^{-mj} \omega_{2N}^{-m} f[m] - \sum_{m=0}^{N-1} \omega_N^{-mj} \omega_{2N}^{-m} f[N+m], \end{aligned}$$

donc $[\mathcal{F}_{2N}(f)]^{(1)} = \mathcal{F}_N(S_N(f_0 - f_1))$. ♣

On va maintenant donner l'algorithme de la FFT dans sa version décimation fréquentielle

Théorème 7.3.7 Soit $k \geq 1$, et soit $f \in \mathbb{C}^{2^k}$. On pose $h_0 = h_{0,0} = f$, et pour $1 \leq n \leq k$ on définit $h_n = (h_{n,0}, \dots, h_{n,2^n-1}) \in \mathbb{C}^{2^k}$, avec $h_{n,m} \in \mathbb{C}^{2^{k-n}}$ par la formule de récurrence suivante, où $0 \leq q \leq 2^{k-n-1} - 1$,

$$h_{n,2m}[q] = h_{n-1,m}[q] + h_{n-1,m}[q + 2^{k-n-1}],$$

$$h_{n,2m+1}[q] = \omega_{2^{k-n+1}}^{-q} (h_{n-1,m}[q] - h_{n-1,m}[q + 2^{k-n-1}]). \quad (7.18)$$

Alors $\sigma_k(h_k) = \mathcal{F}_{2^k}(f)$.

Démonstration : Pour $k = 1$, $f \in \mathbb{C}^2$, on a $h_1[0] = h_{1,0}[0] = h_{0,0}[0] + h_{0,0}[1] = f[0] + f[1]$, $h_1[1] = h_{1,1}[1] = \omega_1(h_{0,0}[0] - h_{0,0}[1]) = f[0] - f[1]$, donc $h_1 = \mathcal{F}_2(f)$. Donc le résultat est vrai pour $k = 1$.

Supposons maintenant que l'algorithme fonctionne pour $k \geq 1$, et soit $f \in \mathbb{C}^{2^{k+1}}$. D'après l'hypothèse de récurrence et la formule 7.15, on a, pour $0 \leq m \leq 2^k - 1$,

$$\begin{aligned}\mathcal{F}_{2^k}([h_1]_0)[m] &= h_{k+1}[\text{rev}_k(m)] = h_{k+1}[\text{rev}_{k+1}(2m)], \\ \mathcal{F}_{2^k}([h_1]_1)[m] &= h_{k+1}[2^k + \text{rev}_k(m)] = h_{k+1}[\text{rev}_{k+1}(2m + 1)].\end{aligned}$$

Il résulte de la formule 7.18 que $[h_1]_0 = f_0 + f_1$ et que $[h_1]_1 = S_N(f_0 - f_1)$. On obtient

$$[\sigma_{k+1}(h_{k+1})]^{(0)} = \mathcal{F}_{2^k}(f_0 - f_1), \quad [\sigma_{k+1}(h_{k+1})]^{(1)} = \mathcal{F}_{2^k}(S_N(f_0 - f_1)),$$

et il résulte alors de la proposition 7.3.6 que $\sigma_{k+1}(h_{k+1}) = \mathcal{F}_{2^k}(f)$. On a donc vérifié par récurrence que l'algorithme proposé est valable pour tout $k \geq 1$. ♣

Exemple 7.3.8 On pose $f = [1, -1, -1, 0, 0, 1, 1, 0]$. Calculer la transformée de Fourier discrète de f en utilisant la FFT, version décimation fréquentielle.

On applique l'algorithme ci-dessus, en remarquant que $\omega_2 = -1$, $\omega_4 = i$ et $\omega_8 = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$.

$h_0 = f$	$f[0]$	$f[1]$	$f[2]$	$f[3]$	$f[4]$	$f[5]$	$f[6]$	$f[7]$
	1	-1	-1	0	0	1	1	0
$N = 8, q = 0, 1, 2$ ou 3	$h_{1,0}[0]$	$h_{1,0}[1]$	$h_{1,0}[2]$	$h_{1,0}[3]$	$h_{1,1}[0]$	$h_{1,1}[1]$	$h_{1,1}[2]$	$h_{1,1}[3]$
$\omega_8 = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$	1	0	0	0	1	$-2\omega_8^{-1}$	$2i$	0
$N = 4, q = 0$ ou 1	$h_{2,0}[0]$	$h_{2,0}[1]$	$h_{2,1}[0]$	$h_{2,1}[1]$	$h_{2,2}[0]$	$h_{2,2}[1]$	$h_{2,3}[0]$	$h_{2,3}[1]$
$\omega_4 = i$	1	0	1	0	$1 + 2i$	$-2\omega_8^{-1}$	$1 - 2i$	$2i\omega_8^{-1}$
$N = 2, q = 0$	$h_{3,0}[0]$	$h_{3,1}[0]$	$h_{3,2}[0]$	$h_{3,3}[0]$	$h_{3,4}[0]$	$h_{3,5}[0]$	$h_{3,6}[0]$	$h_{3,7}[0]$
$\omega_2 = -1$	1	1	1	1	$1 + 2i$ $-2\omega_8^{-1}$ $= 1 - \sqrt{2}$ $+(2 + \sqrt{2})i$	$1 + 2i$ $+2\omega_8^{-1}$ $= 1 + \sqrt{2}$ $+(2 - \sqrt{2})i$	$1 - 2i$ $+2i\omega_8^{-1}$ $= 1 + \sqrt{2}$ $-(2 - \sqrt{2})i$	$1 - 2i$ $-2i\omega_8^{-1}$ $= 1 - \sqrt{2}$ $-(2 + \sqrt{2})i$
<i>revbits</i>	$\hat{f}[0]$	$\hat{f}[1]$	$\hat{f}[2]$	$\hat{f}[3]$	$\hat{f}[4]$	$\hat{f}[5]$	$\hat{f}[6]$	$\hat{f}[7]$
$\hat{f} = \sigma_3(h_3)$	1	$1 - \sqrt{2}$ $+(2 + \sqrt{2})i$	1	$1 + \sqrt{2}$ $-(2 - \sqrt{2})i$	1	$1 + \sqrt{2}$ $+(2 - \sqrt{2})i$	1	$1 - \sqrt{2}$ $-(2 + \sqrt{2})i$

La méthode de décimation fréquentielle donne évidemment les mêmes résultats que la méthode de décimation temporelle (à condition d'éviter les erreurs de calcul...).

Pour calculer la transformée de Fourier inverse, il suffit d'appliquer l'un ou l'autre des algorithmes ci-dessus sur \mathbb{C}^{2^k} en remplaçant à chaque étape ω_N par ω_N^{-1} et en divisant le résultat obtenu à la dernière étape par 2^k .

Exemple 7.3.9 Calcul de la transformée de Fourier discrète de $f = [1, -1, -1, 0]$ et calcul de la transformée de Fourier inverse de \hat{f} par FFT, version décimation temporelle.

On reprend les notations précédentes, en utilisant la notation \tilde{g} au lieu de g pour le calcul de la transformée de Fourier inverse de \hat{f} .

m	0	1	2	3
bits	00	01	10	11
revbits	00	10	01	11
$g_0[m] = f[m]$	1	-1	-1	0
$g[m] = \sigma_2(f)[m]$	1	-1	-1	0
$N = 2, q = 0, \omega_2 = -1$	$g_{1,0}[0]$	$g_{1,0}[1]$	$g_{1,1}[0]$	$g_{1,1}[1]$
	0	2	-1	-1
$N = 4, q = 0$ ou $1, \omega_4 = i$	$g_{2,0}[0]$	$g_{2,0}[1]$	$g_{2,0}[2]$	$g_{2,0}[3]$
$\hat{f}[m] = g_2[m]$	-1	$2 + i$	1	$2 - i$
$\tilde{g}[m] = \sigma_2(\hat{f})$	-1	1	$2 + i$	$2 - i$
$N = 2, q = 0, \omega_2 = -1$	$\tilde{g}_{1,0}[0]$	$\tilde{g}_{1,0}[1]$	$\tilde{g}_{1,1}[0]$	$\tilde{g}_{1,1}[1]$
	0	-2	4	$2i$
$N = 4, q = 0$ ou $1, \omega_4 = i$	$\tilde{g}_{2,0}[0]$	$\tilde{g}_{2,0}[1]$	$\tilde{g}_{2,0}[2]$	$\tilde{g}_{2,0}[3]$
$4\mathcal{F}_2^{-1}(\hat{f})[m] = \tilde{g}_2[m]$	4	-4	-4	0
$\mathcal{F}_2^{-1}(\hat{f})[m]$	1	-1	-1	0

Exemple 7.3.10 *Calcul de la transformée de Fourier discrète de $f = [1, -1, -1, 0]$ et calcul de la transformée de Fourier inverse de \hat{f} par FFT, version décimation fréquentielle.*

On reprend les notations précédentes, en utilisant la notation \tilde{h} au lieu de h pour le calcul de la transformée de Fourier inverse de \hat{f} . L'opération d' "inversion des bits" se fait cette fois à la fin des calculs de la transformée de Fourier et de la transformée de Fourier inverse.

m	0	1	2	3
bits	00	01	10	11
revbits	00	10	01	11
$f[m] = h_0[m]$	1	-1	-1	0
$N = 4, q = 0$ ou $1, \omega_2 = -1$	$h_{1,0}[0]$	$h_{1,0}[1]$	$h_{1,1}[0]$	$h_{1,1}[1]$
	0	-1	2	i
$N = 2, q = 0, \omega_2 = -1$	$h_{2,0}[0]$	$h_{2,1}[0]$	$h_{2,2}[0]$	$h_{2,3}[0]$
	-1	1	$2 + i$	$2 - i$
$\hat{f} = \sigma_2(h_2)$	-1	$2 + i$	1	$2 - i$
$\tilde{h}_0[m] = \hat{f}[m]$	-1	$2+i$	1	$2-i$
$N = 4, q = 0$ ou $1, \omega_2 = -1$	$\tilde{h}_{1,0}[0]$	$\tilde{h}_{1,0}[1]$	$\tilde{h}_{1,1}[0]$	$\tilde{h}_{1,1}[1]$
	0	4	-2	$2i \times i = -2$
$N = 2, q = 0, \omega_2 = -1$	$\tilde{h}_{2,0}[0]$	$\tilde{h}_{2,1}[0]$	$\tilde{h}_{2,2}[0]$	$\tilde{h}_{2,3}[0]$
$\tilde{h}_2[m]$	4	-4	-4	0
$4\mathcal{F}_2^{-1}(\hat{f})[m] = \sigma_2(\tilde{h}_2)[m]$	4	-4	-4	0
$\mathcal{F}_2^{-1}(\hat{f})[m]$	1	-1	-1	0

On vérifie donc dans ce cas particulier en utilisant les deux versions de la FFT que la transformée de Fourier inverse de \hat{f} est bien égale à f .

7.4 Applications de la FFT au calcul de produits de polynômes

Soient $p = a_0 + a_1x + \dots + a_mx^m$ et $q = b_0 + b_1x + \dots + b_nx^n$ deux polynômes à coefficients complexes. Soient $\tilde{a} = (\tilde{a}_j)_{j \geq 0}$ et $\tilde{b} = (\tilde{b}_j)_{j \geq 0}$ les suites définies par les formules $\tilde{a}_j = a_j$ pour $0 \leq j \leq m$, $\tilde{b}_j = b_j$ pour $0 \leq j \leq n$, $\tilde{a}_j = 0$ pour $j \geq m + 1$ et $\tilde{b}_j = 0$ pour $j \geq n + 1$. Si on pose

$$(\tilde{a} * \tilde{b})_j = \sum_{s=0}^j \tilde{a}_s \tilde{b}_{j-s}$$

on a

$$pq = \sum_{r=0}^{+\infty} (\tilde{a} * \tilde{b})_r x^r = \sum_{r=0}^{n+m} (\tilde{a} * \tilde{b})_r x^r.$$

A priori, les calculs dans $\mathbb{Z}/N\mathbb{Z}$ sont effectués modulo N , mais ceci ne change rien pour le calcul de $\tilde{a} * \tilde{b}$ si $N \geq m + n + 1$, il suffit d'identifier j avec \bar{j} et de considérer comme nuls les coefficients d'indice supérieur à $m + n$. On peut donc utiliser la FFT pour effectuer les calculs dans \mathbb{C}^{2^k} , pourvu que $2^k \geq m + n + 1$. Ceci s'applique également à des produits de nombres puisque un nombre α écrit en base d s'écrit sous la forme $\alpha = p(d)$, où p est un polynôme dont les coefficients appartiennent à l'ensemble $\{0, \dots, d - 1\}$ (ceci ne présente) d'intérêt pratique que pour les très grands nombres. Nous illustrons ceci par un exemple.

Exemple 7.4.1 Effectuer le produit des polynômes $x^4 + x + 1$ et $x^3 - 2$ en utilisant la FFT (décimation temporelle) et la FFT inverse (décimation fréquentielle) sur \mathbb{C}^8 . En déduire un moyen de calculer le produit 10011×998 , (on travaille en base 10) et effectuer les calculs correspondants.

Posons $p = x^4 + x + 1 = 1 + x + 0.x^2 + 0.x^3 + x^4$, $q = x^3 - 2 = -2 + 0.x + 0.x^2 + x^3$.

On va calculer en FFT décimation temporelle les transformées de Fourier de $[1, 1, 0, 0, 1, 0, 0, 0]$ et $[-2, 0, 0, 1, 0, 0, 0, 0]$, en effectuant les calculs dans \mathbb{C}^8 .

Renversement binaire

0	1	2	3	4	5	6	7
000	001	010	011	100	101	110	111
000	100	010	110	001	101	011	111
0	4	2	6	1	5	3	7

Décimation temporelle, $f_1 = [1, 1, 0, 0, 1, 0, 0, 0]$

m	0	1	2	3	4	5	6	7
$f_1[m]$	1	1	0	0	1	0	0	0
$g_0[m] = \sigma_3(f_1)[m]$	1	1	0	0	1	0	0	0
$N = 2, q = 0$ $\omega_2 = -1$	$g_{1,0}[0]$	$g_{1,0}[1]$	$g_{1,1}[0]$	$g_{1,1}[1]$	$g_{1,2}[0]$	$g_{1,2}[1]$	$g_{1,3}[0]$	$g_{1,3}[1]$
$g_1[m]$	2	0	0	0	1	1	0	0
$N = 4, q = 0$ ou 1, $\omega_4 = i$	$g_{2,0}[0]$	$g_{2,0}[1]$	$g_{2,0}[2]$	$g_{2,0}[3]$	$g_{2,1}[0]$	$g_{2,1}[1]$	$g_{2,1}[2]$	$g_{2,1}[3]$
$g_2[m]$	2	0	2	0	1	1	1	1
$N = 8, q = 0, 1$ 2 ou 3, $\omega_8 = e^{i\frac{\pi}{4}}$	$g_{3,0}[0]$	$g_{3,0}[1]$	$g_{3,0}[2]$	$g_{3,0}[3]$	$g_{3,0}[4]$	$g_{3,0}[5]$	$g_{3,0}[6]$	$g_{3,0}[7]$
$\hat{f}_1[m] = g_3[m]$	3	$e^{-\frac{i\pi}{4}}$	2-i	$e^{-\frac{3i\pi}{4}}$	1	$-e^{-\frac{i\pi}{4}}$	2+i	$-e^{-\frac{3i\pi}{4}}$

Décimation temporelle, $f_2 = [-2, 0, 0, 1, 0, 0, 0, 0]$

m	0	1	2	3	4	5	6	7
$f_2[m]$	-2	0	0	1	0	0	0	0
$g_0[m] = \sigma_3(f)[m]$	-2	0	0	0	0	0	1	0
$N = 2, q = 0$ $\omega_2 = -1$	$g_{1,0}[0]$	$g_{1,0}[1]$	$g_{1,1}[0]$	$g_{1,1}[1]$	$g_{1,2}[0]$	$g_{1,2}[1]$	$g_{1,3}[0]$	$g_{1,3}[1]$
$g_1[m]$	-2	-2	0	0	0	0	1	1
$N = 4, q = 0$ ou 1, $\omega_4 = i$	$g_{2,0}[0]$	$g_{2,0}[1]$	$g_{2,0}[2]$	$g_{2,0}[3]$	$g_{2,1}[0]$	$g_{2,1}[1]$	$g_{2,1}[2]$	$g_{2,1}[3]$
$g_2[m]$	-2	-2	-2	-2	1	$-i$	-1	i
$N = 8, q = 0, 1$ 2 ou 3, $\omega_8 = e^{i\frac{\pi}{4}}$	$g_{3,0}[0]$	$g_{3,0}[1]$	$g_{3,0}[2]$	$g_{3,0}[3]$	$g_{3,0}[4]$	$g_{3,0}[5]$	$g_{3,0}[6]$	$g_{3,0}[7]$
$\hat{f}_2[m] = g_3[m]$	-1	$-2 - e^{i\frac{\pi}{4}}$	$-2 + i$	$-2 + e^{-i\frac{\pi}{4}}$	-3	$-2 + e^{i\frac{\pi}{4}}$	$-2 - i$	$-2 - e^{-i\frac{\pi}{4}}$

Posons $u = \widehat{f_1 * f_2} = \hat{f}_1 \hat{f}_2$. On obtient

m	0	1	2	3	4	5	6	7
$u[m]$	-3	$-1 - 2e^{-i\frac{\pi}{4}}$ $= -1 - \sqrt{2} + i\sqrt{2}$	$-3 + 4i$	$-1 - 2e^{-\frac{3i\pi}{4}}$ $= -1 + \sqrt{2} + i\sqrt{2}$	-3	$-1 + 2e^{-i\frac{\pi}{4}}$ $= -1 + \sqrt{2} - i\sqrt{2}$	$-3 - 4i$	$-1 + 2e^{-\frac{3i\pi}{4}}$ $= -1 - \sqrt{2} - i\sqrt{2}$

On peut alors calculer la transformée de Fourier inverse de h par décimation fréquentielle. La méthode consiste à écrire au départ $h_0 = [h_{0,0}] := u$, et ensuite à associer à $\tilde{h}_{n,j} \in \mathbb{C}^{8/N}$, avec $N = 2^{3-n}$, $0 \leq n \leq 2$, $0 \leq j \leq 2^n - 1$, deux fonctions $\tilde{h}_{n+1,j} \in \mathbb{C}^{8/2N}$ et $\tilde{h}_{n+1,j+N/2} \in \mathbb{C}^{8/2N}$ en utilisant pour $0 \leq j \leq N/2 - 1$ les formules

$$\begin{cases} \tilde{h}_{n+1,j}[q] = \tilde{h}_{n,j}[q] + \tilde{h}_{n,j}[q + N/2] \\ \tilde{h}_{n,j}[q] = \omega_N^q \left(\tilde{h}_{n,j}[q] - \tilde{h}_{n,j}[q + N/2] \right) \end{cases}$$

On effectue les calculs selon le schéma papillon (en réduisant de moitié à chaque étape les ailes du papillon). Rendu à $n = 3$, on obtient avec $\tilde{h}_3 = [\tilde{h}_{3,0} \dots \tilde{h}_{3,7}]$ une fonction égale à $8\mathcal{F}_3^{-1}(u)$ "dans l'ordre binaire inversé" avec , et il suffit de "renverser les bits" pour obtenir $8\mathcal{F}_3^{-1}(u)$. La transformée de Fourier inverse de u s'obtient alors en divisant par 8 le résultat obtenu.

m	0	1	2	3	4	5	6	7
$\tilde{h}_0[m] = u[m]$	-3	$-1 - 2e^{-i\frac{\pi}{4}}$	$-3 + 4i$	$-1 - 2e^{-\frac{3i\pi}{4}}$	-3	$-1 + 2e^{-i\frac{\pi}{4}}$	$-3 - 4i$	$-1 + 2e^{-\frac{3i\pi}{4}}$
$N = 8, q = 0, 1, 2$ ou 3, $\omega_8 = e^{i\pi/4}$	$\tilde{h}_{1,0}[0]$	$\tilde{h}_{1,0}[1]$	$\tilde{h}_{1,0}[2]$	$\tilde{h}_{1,0}[3]$	$\tilde{h}_{1,1}[0]$	$\tilde{h}_{1,1}[1]$	$\tilde{h}_{1,1}[2]$	$\tilde{h}_{1,1}[3]$
$\tilde{h}_1[m]$	-6	-2	-6	-2	0	-4	-8	-4
$N = 4, q = 0$ ou 1, $\omega_4 = i$	$\tilde{h}_{2,0}[0]$	$\tilde{h}_{2,0}[1]$	$\tilde{h}_{2,1}[0]$	$\tilde{h}_{2,1}[1]$	$\tilde{h}_{2,2}[0]$	$\tilde{h}_{2,2}[1]$	$\tilde{h}_{2,3}[0]$	$\tilde{h}_{2,3}[1]$
$\tilde{h}_2[m]$	-12	-4	0	0	-8	-8	8	0
$N = 2, q = 0, \omega_2 = -1$	$\tilde{h}_{3,0}[0]$	$\tilde{h}_{3,1}[0]$	$\tilde{h}_{3,2}[0]$	$\tilde{h}_{3,3}[0]$	$\tilde{h}_{3,4}[0]$	$\tilde{h}_{3,5}[0]$	$\tilde{h}_{3,6}[0]$	$\tilde{h}_{3,7}[0]$
$\tilde{h}_3[m]$	-16	-8	0	0	-16	0	8	8
$\sigma_3(\tilde{h}_3)[m] = 8\mathcal{F}_3^{-1}(u)[m]$	-16	-16	0	8	-8	0	0	8
$\mathcal{F}_3^{-1}(u)[m]$	-2	-2	0	1	-1	0	0	1

On obtient ici $(x^4 + x + 1)(x^3 - 2) = -2 - 2x + x^3 - x^4 + x^7$, ce qui correspond au résultat obtenu par un calcul direct.

En appliquant cette formule avec $x = 10$, on obtient

$$10011 \times 998 = p(10)q(10) = 10^3 + 10^7 - 2 - 20 - 10000 = 10\,001\,000 - 10\,022 = 9\,990\,978.$$

7.5 Applications de la FFT au traitement du signal et de l'image (en préparation)

On peut régulariser des signaux 1-D ou des images en effectuant des convolutions avec des fonctions concentrées près de l'origine, et la FFT est un outil très utile pour implémenter ce procédé. Nous renvoyons au traité de G.Peyré pour plus d'information. L'implémentation de ces méthodes sous Matlab effectué par Le Moal et Ponsonnet dans leur mémoire de master 1 sera ajoutée à la prochaine édition de ce support de cours.

On va commencer par implanter la FFT sous Matlab. Ceci est réalisé dans le livre de G.Peyré, mais nous allons ici suivre pas à pas l'implémentation proposée par Le Moal et Ponsonnet dans leur mémoire de Master 1 [11].

On commence par calculer sous Matlab le reclassement d'un nombre $t \in \{0, \dots, 2^k - 1\}$ par "changements de bits". On introduit une m-file appelée `renvbits`. La commande est "`renvbits(k,t)`".

```
function res = rev_index(t,index)
res = 0;
tmp = index;
for i=0:t-1
    bit = mod(tmp,2);
    tmp = floor(tmp/2);
    res = res*2 + bit;
end
```

Par exemple on peut prendre $k = 4$, soit $2^k - 1 = 15$, et $t = 3$. En base 2 on a $3 = 0011$, donc après le renversement de bits on obtient $1100 = 8 + 4 = 12$. C'est bien ce que donne Matlab.

```
renvbits(4,3)
```

```
ans =
```

12

La réponse est aussi instantanée pour des renversements portant sur 20 bits.

```
>> renvbits(20,265431)

ans =

    963330
```

On va maintenant introduire une m-file nommée `reclass`, qui va reclasser un vecteur de taille 2^n par changement de signes sur les indices. Autrement dit si $x = (x_i)_{0 \leq i \leq 2^n - 1}$, $reclass(x)$ est le vecteur $(x_{renvbits(n,i)})_{0 \leq i \leq 2^n - 1}$.

```
function y = reclass(x)
n = length(x);
t = floor(log2(n));
y = zeros(n,1);
for i=0:n-1
    j = renvbits(t,i);
    y(j+1) = x(i+1);
end
```

On l'applique à deux vecteurs

```
>> x=[4 5 -1 4];

reclass(x)

ans =

     4
    -1
     5
     4
```

```

>> x=[-12 3 8 7 9 8 0 35 65 12 5.6 8.3 6.4 45 67 0.1],

reclass(x)

ans =

-12.0000
 65.0000
   9.0000
   6.4000
   8.0000
   5.6000
    0
 67.0000
   3.0000
 12.0000
   8.0000
 45.0000
   7.0000
   8.3000
 35.0000
   0.1000

```

Une expérience montre qu'il faut environ 1mn à Matlab pour reclasser un vecteur de $\mathbb{C}^{2^{20}}$ (on ne reproduit pas le résultat du reclassement).

```

>> x=[0:0.001:2^(20)/1000];

reclass(x);

```

7.6 Exercices sur le Chapitre 7

Exercice 1

- 1) Ecrire les matrices de Fourier A_1 , A_2 et A_3 .
- 2) On pose $f[0] = 1$, $f[1] = -1$, $f[2] = -1$, $f[3] = 0$. Calculer \hat{f} par les méthodes suivantes
 - a) En utilisant la matrice A_2 .
 - b) En utilisant l'algorithme FFT (version décimation temporelle).

- c) En utilisant l'algorithme FFT (version décimation spatiale).
- 3) On pose $g[0] = 1, g[1] = -1, g[2] = -1, g[3] = 0, g[4] = 0, g[5] = 1, g[6] = 1, g[7] = 0$. Calculer de même \hat{g} par les 3 méthodes données ci-dessus.
- 4) Calculer les produits de convolution cycliques $f * f$ et $g * g$
- a) En appliquant la définition.
- b) En calculant les transformées de Fourier de $f * f$ et $g * g$ et en appliquant la transformée de Fourier inverse.

Exercice 2

On se propose de calculer $(1 + x)^2$ en utilisant la transformée de Fourier discrète.

- 1) Donner le développement de $(1 + x)^2$.
- 2) Déterminer le plus petit entier p tel que le calcul par transformée de Fourier dans $\mathbb{Z}/2^p\mathbb{Z}$ donne le résultat exact.
- 3) On pose $f[0] = 1, f[1] = 1, f[2] = 0, f[3] = 0$. Calculer \hat{f} et \hat{f}^2 . En calculant la transformée de Fourier inverse de \hat{f}^2 , retrouver le résultat de la question 1.

Exercice 3

- 1) Effectuer le produit des polynômes $x^2 + 2x + 5$ et $3x + 2$ en utilisant la FFT et la FFT inverse sur \mathbb{C}^4 .
- 2) En déduire un moyen de calculer le produit 125×32 , et effectuer les calculs correspondants.

Exercice 4

On considère l'équation $f * f = f$, où $f : \{0, \dots, 2^{k-1}\} \rightarrow \mathbb{C}$.

- 1) Déterminer le nombre de solutions de cette équation.
- 2) Expliciter toutes les solutions de l'équation dans les cas $k = 1, k = 2, k = 3$.

Exercice 5

On se propose ici de décrire l'algorithme de Good-Thomas, qui fait intervenir le théorème chinois

- 1) On suppose que $N = pq$, où p et q sont des entiers premiers entre eux. On note $\pi_N : \mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$, $\pi_p : \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$, et $\pi_q : \mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ les surjections canoniques. Rappeler pourquoi l'application

$$\begin{aligned} \phi : \mathbb{Z}/N\mathbb{Z} &\rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ \pi_N(n) &\longmapsto (\bar{\pi}_p(n), \bar{\pi}_q(n)) \end{aligned}$$

est un isomorphisme d'anneaux de $\mathbb{Z}/N\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, et expliciter l'isomorphisme inverse ψ .

2) Soit $f \in \mathbb{C}^N$. On définit un signal $2D$ par la formule

$$\forall k_1 \in \{0, \dots, p-1\}, \quad \forall k_2 \in \{0, \dots, q-1\}, \quad F(k_1, k_2) = f(\psi(k_1, k_2)).$$

Montrer que si $s_1 \in \{0, \dots, p-1\}$ et $s_2 \in \{0, \dots, q-1\}$, on a

$$\hat{f}[r(s_1p + s_2q)] = \hat{F}(s_1, s_2),$$

où $r(s_1p + s_2q)$ désigne le reste de la division de $s_1p + s_2q$ par N .

3) Montrer que lorsque s_1 parcourt $\{0, \dots, p-1\}$ et s_2 parcourt $\{0, \dots, q-1\}$, alors $r(s_1p + s_2q)$ parcourt $\{0, \dots, N-1\}$. En déduire comment on peut calculer la transformée de Fourier de f à partir de celle de F , en explicitant le changement d'indice. Expliciter cette procédure quand $p = 2$ et $q = 3$.

Exercice 6

On note A_N la matrice de la transformée de Fourier discrète sur $\{0, \dots, N\}$. A $f \in \mathbb{C}^N$ on associe $\tilde{f} \in \mathbb{C}^N$ défini par la formule $\tilde{f}[0] = f[0], \tilde{f}[p] = f(N-p)$ pour $1 \leq p \leq n-1$. On dit que f est symétrique si $\tilde{f} = f$, antisymétrique si $\tilde{f} = -f$. On pose d'autre part $\mathcal{F}(f) = \hat{f}$.

1) Montrer que f s'écrit $f = f_s + f_a$ avec f_s symétrique et f_a antisymétrique. Cette décomposition est elle unique ?

2) Montrer que si f est symétrique, alors $\mathcal{F}(f)^2 = Nf$ et que si f est antisymétrique, alors $\mathcal{F}(f)^2 = -Nf$. En déduire que $A_N^2 = N^2 I_N$.

3) Pour $f \in C^N$ on pose $U^+(f) = \sqrt{N}f_s + \hat{f}, V^+(f) = \sqrt{N}f_a + i\hat{f}_a, U^-(f) = \sqrt{N}f_s - \hat{f}_s, V^-(f) = \sqrt{N}f_a - i\hat{f}_a$. Vérifier que $f = U^+(f) + V^+(f) + U^-(f) + V^-(f)$, que $U^+(f), V^+(f), U^-(f)$ et $V^-(f)$ sont des vecteurs propres de Ω_N , et déterminer les valeurs propres associées.

4) On considère la matrice $S = \begin{bmatrix} C_0 & 1 & 0 & \dots & \dots & 1 \\ 1 & C_1 & 1 & 0 & \dots & 0 \\ 0 & 1 & C_2 & 1 & 0 & \dots & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 0 & 0 & \dots & 1 & C_N - 1 \end{bmatrix}$, avec $C_k =$

$2 \left(\cos \left(\frac{2k\pi}{N} \right) - 2 \right)$ pour $0 < k \leq N-1$.

a) Expliquer pourquoi il existe une matrice orthogonale réelle U telle que $U^{-1} S U$ est diagonale, et que $S A_N = A_N S$. En déduire que les vecteurs propres de S sont aussi des vecteurs propres de A_N .

b) Pour $f \in C^N$ on pose $P(f)[0] = f[0], P(f)[n] = \frac{f[n] + f[N-n]}{\sqrt{2}}$ pour $1 \leq n \leq \frac{N-1}{2}$, $P(f)[n] = \frac{f[n] - f[N-n]}{\sqrt{2}}$ pour $\frac{N+1}{2} \leq n \leq N-1$, et si N est pair on pose $P(f)[N/2] =$

$f[N/2]$. Vérifier que P est symétrique et orthogonal, et que PSP^{-1} est une matrice tridiagonale symétrique.

c) Vérifier quand $N = 2, 3, 4, 5$ que les valeurs propres de S sont distinctes, ce qui donne un moyen canonique de trouver une BON de \mathbb{R}^N formée de vecteurs propres de A_N . En explorant la littérature sur le calcul des valeurs propres des matrices symétriques, montrer que ce résultat reste vrai pour tout $N \geq 2$.

Exercice 7

On présente ici l'algorithme de Karatsuba, qui permet de multiplier les polynômes en appliquant la technique consistant à "diviser pour régner". Soit K un corps, et soient $P, Q \in K[x]$ deux polynômes de degré n . On note k la partie entière de $\frac{n+1}{2}$.

1) On écrit les polynômes sous la forme

$$P = x^k P_1 + P_0, \quad Q = x^k Q_1 + Q_0, \quad d^\circ(P_0) < k, \quad d^\circ(Q_0) < k.$$

Discuter selon la parité de n les degrés de P_1 et Q_1 et écrire PQ sous la forme

$$PQ = R_0 + x^k R_1 + x^{2k} R_2,$$

avec $d^\circ(R_1) \leq k - 2$, et montrer que le calcul de R_1 fait intervenir une multiplication, mais par contre 4 additions.

2) Implémenter un algorithme récursif pour le calcul de PQ en implémentant à chaque étape la décomposition ci-dessus. Montrer que la complexité dudit algorithme est $O(n^{\log_3(2)})$. Pour quelles valeurs de n préférera-t-on cet algorithme à l'utilisation de la FFT ?

Chapitre 8

Etude générale de la transformée de Fourier

8.1 Groupe dual d'un groupe localement compact abélien

On va maintenant présenter la transformée de Fourier dans un cadre général qui unifie les différents chapitres de ce support de cours. Soit E un ensemble. Une topologie τ sur E est la donnée d'une famille \mathcal{U}_τ de parties de E possédant les propriétés suivantes

- (i) $E \in \mathcal{U}_\tau$ et $\emptyset \in \mathcal{U}_\tau$.
- (ii) La réunion d'une famille quelconque d'éléments de \mathcal{U}_τ appartient à \mathcal{U}_τ .
- (iii) L'intersection de toute famille finie d'éléments de \mathcal{U}_τ appartient à \mathcal{U}_τ .
- (iv) Pour tout couple (x, y) d'éléments distincts de E il existe $U, V \in \mathcal{U}_\tau$ tels que $x \in U$, $y \in V$ et $U \cap V = \emptyset$.

On dit alors que (E, τ) est un espace topologique. Dans ce cas on dit qu'un sous-ensemble U de E est ouvert si $U \in \mathcal{U}_\tau$, et on dit qu'un sous-ensemble F de E est fermé si son complémentaire est ouvert.

Rappelons que si E_1 et E_2 sont deux ensembles et si $f : E_1 \rightarrow E_2$ est une application, on pose, pour $A \subset E_2$,

$$f^{-1}(A) = \{x \in E_1 \mid f(x) \in A\}.$$

L'ensemble $f^{-1}(A)$ est appelé l'image réciproque de A par l'application f .

Définition 8.1.1 Soient (E_1, τ_1) et (E_2, τ_2) deux espaces topologiques.

1) On dit qu'une application $f : E_1 \rightarrow E_2$ est continue si et seulement si $f^{-1}(U) \in \mathcal{U}_{\tau_1}$ pour tout $U \in \mathcal{U}_{\tau_2}$.

2) On note $\mathcal{U}_{\tau_1 \times \tau_2}$ l'ensemble des parties de l'ensemble produit cartésien $E_1 \times E_2$ qui peuvent s'écrire comme réunion d'ensembles de la forme $U \times V$ avec $U \in \mathcal{U}_{\tau_1}$ et $V \in \mathcal{U}_{\tau_2}$.

On vérifie facilement que la définition ci-dessus permet d'obtenir une topologie $\tau_1 \times \tau_2$ sur le produit cartésien $E_1 \times E_2$, appelée topologie produit des topologies τ_1 et τ_2 . D'autre part il est clair que si (E_1, τ_1) , (E_2, τ_2) et (E_3, τ_3) sont trois espaces topologiques, et si $f : E_1 \rightarrow E_2$ et $g : E_2 \rightarrow E_3$ sont continues, alors l'application composée $g \circ f : E_1 \rightarrow E_3$ est continue. On retrouve la notion d'ouvert, de fermé sur \mathbb{R}^p et la notion de continuité usuelle pour les applications de \mathbb{R}^p dans \mathbb{R}^q , voir par exemple le chapitre 1 de [8].

Remarquons également que si A est un sous-ensemble d'un espace topologique (E, τ) on obtient une topologie τ_A sur A en posant $\mathcal{U}_{\tau_A} = \{U \cap A\}_{U \in \mathcal{U}_\tau}$. Cette topologie est appelée la topologie induite sur A par la topologie de E . Il est clair que si (E_1, τ_1) et (E_2, τ_2) sont des espaces topologiques, si $A \subset E_2$, si $f : E_1 \rightarrow E_2$ est une application et si $f(E_1) \subset A$, alors f est une application continue de (E_1, τ_1) dans (E_2, τ_2) si et seulement si f , considérée comme une application de E_1 dans A , est une application continue de (E_1, τ_1) dans A muni de la topologie induite sur A par τ_2 .

Soit maintenant (E, τ) un espace topologique, et soit F un sous-ensemble non vide de E . On dit qu'une famille $(U_\lambda)_{\lambda \in \Lambda}$ est un recouvrement ouvert de F si U_λ est ouvert pour tout $\lambda \in \Lambda$ et si $F \subset \cup_{\lambda \in \Lambda} U_\lambda$. On dit que $(U_{\lambda_j})_{1 \leq j \leq m}$ est un sous-recouvrement fini du recouvrement ouvert $(U_\lambda)_{\lambda \in \Lambda}$ de F si $F = \cup_{1 \leq j \leq m} U_{\lambda_j}$, avec $\lambda_j \in \Lambda$ pour $1 \leq j \leq m$, m désignant un entier positif quelconque. Ceci permet d'introduire la notion suivante.

Définition 8.1.2 Soit (E, τ) un espace topologique, et soit F une partie non vide de E . On dit que F est compacte si de tout recouvrement ouvert de F on peut extraire un sous recouvrement fini.

L'ensemble vide est compact par convention, et on vérifie que toute partie compacte d'un espace topologique est fermée. D'autre part les parties compactes d'un espace vectoriel normé de dimension finie coïncident avec les parties fermées bornées de E , voir par exemple le Chapitre 1 du support de cours de Calcul différentiel [8].

On a introduit au Chapitre 1 du Cours d'algèbre [5] la notion de groupe. On va maintenant introduire la notion de groupe localement compact.

Définition 8.1.3 Soit (G, \circ) un groupe et soit τ une topologie sur G . On dit que (G, \circ, τ) est un groupe topologique quand les deux conditions suivantes sont vérifiées

(i) L'application $(x, y) \rightarrow x \circ y$ est une application continue de $(G \times G, \tau \times \tau)$ dans (G, τ) .

(ii) L'application $x \rightarrow x^{-1}$ est une application continue de (G, τ) dans lui-même.

On dit qu'un groupe topologique (G, \circ, τ) est localement compact s'il existe une partie ouverte U et une partie compacte F de (G, τ) telles que $e \in U \subset F$, e désignant l'élément neutre de G .

Rappelons qu'un groupe (G, \circ) est dit abélien si $x \circ y = y \circ x$ pour tout couple (x, y) éléments de G . On va maintenant introduire en toute généralité la notion de groupe dual d'un groupe abélien localement compact.

Définition 8.1.4 Soit (G, \circ, τ) un groupe abélien localement compact et soit $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$. On appelle caractères de G l'ensemble des applications continues $\phi : G \rightarrow \mathbb{T}$ vérifiant

$$\phi(x \circ y) = \phi(x)\phi(y)$$

pour tout couple (x, y) d'éléments de G .

On note \hat{G} l'ensemble des caractères de G , et pour $\phi, \psi \in \hat{G}$, on définit $\phi \cdot \psi : G \rightarrow \mathbb{T}$ par la formule

$$(\phi \cdot \psi)(x) = \phi(x)\psi(x) \quad \forall x \in G.$$

D'autre part si $\phi \in \hat{G}$, et si $K \subset G$ est compact on pose, pour $\epsilon > 0$,

$$U_{\phi, K, \epsilon} = \{\psi \in \hat{G} \mid \sup_{x \in K} |\phi(x) - \psi(x)| < \epsilon\},$$

et on note $\mathcal{U}_{\hat{\tau}}$ la famille des sous-ensembles de \hat{G} qui sont soit vides, soit réunion d'une famille quelconque de sous-ensembles du type $U_{\phi, K, \epsilon}$ introduit ci-dessus.

Soient (G_1, \circ, τ_1) et (G_2, \circ, τ_2) deux groupes topologiques. On dira qu'une application $\theta : G_1 \rightarrow G_2$ est un isomorphisme de groupes topologiques quand les trois conditions suivantes sont vérifiées

- (i) L'application θ est une bijection de G_1 sur G_2 .
- (ii) On a $\theta(x \circ y) = \theta(x)\theta(y)$ pour tout couple (x, y) d'éléments de G_1 .
- (iii) L'application $\theta : G_1 \rightarrow G_2$ est une application continue de (G_1, τ_1) dans (G_2, τ_2) et l'application $\theta^{-1} : G_2 \rightarrow G_1$ est une application continue de (G_2, τ_2) dans (G_1, τ_1) .

On a alors le résultat très général suivant, connu sous le nom de théorème de dualité de Pontryagin.

Théorème 8.1.5 Soit (G, \circ, τ) un groupe abélien localement compact. Alors $\phi \cdot \psi \in \hat{G}$ pour $\phi \in \hat{G}, \psi \in \hat{G}$, la famille $\mathcal{U}_{\hat{\tau}}$ est la famille des sous-ensembles ouverts de \hat{G} pour une topologie $\hat{\tau}$ sur \hat{G} et $(\hat{G}, \cdot, \hat{\tau})$ est un groupe topologique localement compact abélien. De plus si on pose, pour $x \in G, \psi \in \hat{G}$

$$\tilde{x}(\psi) = \psi(x) \tag{8.1}$$

alors $\tilde{x} \in \hat{G}$ pour tout $x \in G$, et l'application $x \rightarrow \tilde{x}$ est un isomorphisme de groupes topologiques de (G, \circ, τ) sur $(\hat{G}, \cdot, \hat{\tau})$.

Démonstration : Le fait que $(\hat{G}, \cdot, \hat{\tau})$ est un groupe topologique abélien se démontre par une suite de vérifications de routine. Le fait que ce groupe topologique est localement compact est plus délicat, et le fait que l'application $x \rightarrow \tilde{x}$ est un isomorphisme de groupes topologiques de (G, \circ, τ) sur $(\hat{G}, \cdot, \hat{\tau})$ est un résultat profond et difficile.

Nous renvoyons à l'ouvrage classique de W. Rudin [16] pour des démonstrations détaillées. ♣

Notons que l'élément unité de \hat{G} est le caractère 1_G défini par la formule $1_G(x) = 1$ pour tout $x \in G$. Si $(G, +, \tau)$ est un groupe topologique localement compact abélien noté additivement, la condition

$\phi(x \circ y) = \phi(x)\phi(y)$ doit être remplacée par la condition $\phi(x + y) = \phi(x)\phi(y)$ pour $x, y \in G$, etc...

L'exemple le plus simple de groupe localement compact abélien est celui des groupes abéliens finis, que l'on munit de la topologie discrète, qui est la topologie pour laquelle tout ensemble est ouvert.

On peut décrire concrètement les caractères de $\mathbb{Z}/N\mathbb{Z}$.

Exemple 8.1.6 Soit $N \geq 1$, et soit $\omega_N = e^{\frac{2i\pi}{N}}$. On pose, pour $0 \leq p \leq N - 1$, $0 \leq q \leq N - 1$,

$$\phi_p(\bar{q}) = \omega^{pq}. \quad (8.2)$$

Alors l'application $p \rightarrow \phi_p$ est une bijection de l'ensemble $\{0, \dots, N - 1\}$ sur le dual de $\mathbb{Z}/N\mathbb{Z}$.

Nous laissons en exercice la vérification des détails de cet exemple.

En ce qui concerne le groupe $\mathbb{F}_2^k = (\mathbb{Z}/2\mathbb{Z})^k$, on a posé à la formule 6.11

$$x \cdot y = \sum_{j=0}^{k-1} x_j y_j$$

pour $x = (x_0, \dots, x_{k-1}) \in \mathbb{F}_2^k$, $y = (y_0, \dots, y_{k-1}) \in \mathbb{F}_2^k$. Avec la convention $(-1)^{\bar{n}} = (-1)^n$ pour $n \in \mathbb{Z}$, où $\bar{n} = n + 2\mathbb{Z}$ désigne la classe de n dans $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, posons, pour $x \in \mathbb{F}_2^k$, $y \in \mathbb{F}_2^k$,

$$\phi_y(x) = (-1)^{x \cdot y}. \quad (8.3)$$

On peut alors décrire les caractères de \mathbb{F}_2^k .

Exemple 8.1.7 L'application $x \rightarrow \phi_y(x)$ est un caractère de \mathbb{F}_2^k pour tout $y \in \mathbb{F}_2^k$, et l'application $y \rightarrow \phi_y$ est un isomorphisme de groupes de $(\mathbb{F}_2^k, +)$ sur $(\hat{\mathbb{F}}_2^k, \cdot)$.

Nous laissons également en exercice la vérification des détails de cet exemple.

On va maintenant identifier les caractères de $(\mathbb{R}, +)$. On a le résultat suivant.

Lemme 8.1.8 Soit $\phi : \mathbb{R} \rightarrow \mathbb{C} \setminus \{0\}$ une application continue vérifiant, pour tout couple (s, t) d'éléments de \mathbb{R} ,

$$\phi(s + t) = \phi(s)\phi(t).$$

Alors il existe $z \in \mathbb{C}$ tel que $\phi(s) = e^{sz}$ pour tout $s \in \mathbb{R}$.

Démonstration : Posons $\psi(s) = \int_0^s \phi(t)dt$. On a $\psi' = \phi$, et il existe $\alpha > 0$ tel que $\psi(\alpha) \neq 0$. On a, pour $h \neq 0$,

$$\begin{aligned}\psi(\alpha)\phi(h) &= \int_0^\alpha \phi(t)\phi(h)dt = \int_0^\alpha \phi(t+h)dt = \int_h^{\alpha+h} \phi(t)dt \\ &= \psi(\alpha+h) - \psi(h).\end{aligned}$$

On obtient

$$\psi(\alpha)\frac{\phi(h) - 1}{h} = \frac{\psi(\alpha+h) - \psi(\alpha)}{h} - \frac{\psi(h) - \psi(0)}{h},$$

$$\lim_{h \rightarrow 0} \psi(\alpha)\frac{\phi(h) - 1}{h} = \psi'(\alpha) - \psi'(0) = \phi(\alpha) - 1.$$

Comme $\phi(0) = 1$, et comme $\psi(\alpha) \neq 0$, on voit que ϕ est dérivable en 0. Soit maintenant $s \in \mathbb{R}$. On a, pour $h \neq 0$,

$$\frac{\phi(s+h) - \phi(s)}{h} = \phi(s)\frac{\phi(h) - 1}{h}.$$

On voit donc que ϕ est dérivable sur \mathbb{R} , et que $\phi'(s) = \phi'(0)\phi(s)$ pour $s \in \mathbb{R}$. Posons $z := \phi'(0)$ et $\theta(s) = e^{-sz}\phi(s)$. On a $\theta'(s) = -ze^{-sz}\phi(s) + ze^{-sz}\phi(s) = 0$, donc θ est constante. On obtient $\theta(s) = \theta(0) = 1$, et $\phi(s) = e^{sz}$ pour $s \in \mathbb{R}$. ♣

Proposition 8.1.9 Posons $\phi_t(s) = e^{ist}$ pour $s \in \mathbb{R}, t \in \mathbb{R}$, de sorte que ϕ_t est un caractère de $(\mathbb{R}, +)$. Alors l'application $\theta_1 : t \rightarrow \phi_t$ est un isomorphisme de groupes topologiques de $(\mathbb{R}, +)$ sur $(\hat{\mathbb{R}}, \cdot)$.

Démonstration : On a $\phi_t'(0) = it$, donc θ_1 est une application injective de \mathbb{R} dans $\hat{\mathbb{R}}$. Soit maintenant ϕ un caractère de \mathbb{R} . Il existe $z \in \mathbb{C}$ tel que $\phi(s) = e^{sz}$ pour tout $s \in \mathbb{R}$. On a $1 = |\phi(s)| = e^{s\operatorname{Re}(z)}$ pour tout s , donc $\operatorname{Re}(z) = 0$ et $\phi = \phi_t$ avec $t = \operatorname{Im}(z) = i^{-1}z$. Il est clair que $\phi_{t_1+t_2} = \phi_{t_1}\phi_{t_2}$, donc l'application $t\theta_1$ est au sens algébrique un isomorphisme de groupe de $(\mathbb{R}, +)$ sur $(\hat{\mathbb{R}}, \cdot)$. Le fait que θ_1 et θ_1^{-1} sont continues résulte de considérations assez techniques que nous omettrons (voir l'exercice 3). ♣

Pour $x = (x_1, \dots, x_p), y = (y_1, \dots, y_p) \in \mathbb{R}^p$, on note $\langle x, y \rangle = x_1y_1 + \dots + x_py_p$ le produit scalaire de x et y . On a alors le corollaire suivant.

Corollaire 8.1.10 Posons $\phi_y(x) = e^{i\langle x, y \rangle}$ pour $x, y \in \mathbb{R}^p$. Alors l'application $\theta_p : y \rightarrow \phi_y$ est un isomorphisme de groupes topologiques de $(\mathbb{R}^p, +)$ sur $(\hat{\mathbb{R}}^p, \cdot)$.

Démonstration : Pour $k \in \{1, \dots, p\}$, posons $\delta_k(k) = 1$ et $\delta_j(k) = 0$ pour $1 \leq j \leq p, j \neq k$. Soit $\phi \in \hat{\mathbb{R}}^p$. Les applications $s \rightarrow \phi(\delta_k s)$ sont des caractères de \mathbb{R} , donc il existe $y = (y_1, \dots, y_p) \in \mathbb{R}^p$ tel que $\phi(\delta_k s) = e^{isy_k}$ pour $s \in \mathbb{R}, 1 \leq k \leq p$. On a alors, pour $x = (x_1, \dots, x_k) \in \mathbb{R}^p$,

$$\phi(x) = \phi\left(\sum_{k=1}^p \delta_k x_k\right) = \prod_{k=1}^p \phi(\delta_k x_k) = \prod_{k=1}^p e^{ix_k y_k} = e^{i\langle x, y \rangle}.$$

Donc l'application θ_p est une application surjective de \mathbb{R}^p sur $\hat{\mathbb{R}}^p$. Soient maintenant $y = (y_1, \dots, y_p)$ et $y' = (y'_1, \dots, y'_p) \in \mathbb{R}^p$. Si $\phi_y = \phi_{y'}$, alors $e^{isy_k} = \phi_y(\delta_k s) = \phi_{y'}(\delta_k s) = e^{isy'_k}$ pour tout $s \in \mathbb{R}$, donc $y_k = y'_k$ pour $1 \leq k \leq p$, et $y = y'$. On voit donc que θ_p est un isomorphisme de groupes au sens algébrique de \mathbb{R}^p sur $\hat{\mathbb{R}}^p$. Le fait que θ_p et θ_p^{-1} soient continues se déduit de la continuité de θ_1 et θ_1^{-1} . ♣

La topologie discrète sur un ensemble E est la topologie pour laquelle tout sous-ensemble de E est ouvert. Toute application d'un espace topologique discret dans un espace topologique quelconque est continue, et tout groupe devient un groupe topologique localement compact quand on le munit de la topologie discrète. On peut montrer qu'un groupe topologique abélien G est discret si et seulement si son groupe dual est compact, ce qui implique d'après le théorème de dualité de Pontryagin qu'un groupe localement compact abélien est compact si et seulement si son groupe dual est discret. Nous nous contenterons ici de discuter le cas du groupe discret \mathbb{Z} et du groupe compact \mathbb{T} .

Théorème 8.1.11 *Posons $\phi_z(n) = \psi_n(z) = z^n$ pour $n \in \mathbb{Z}$, $z \in \mathbb{T}$. Alors l'application $z \rightarrow \phi_z$ est un isomorphisme de groupes topologiques de (\mathbb{T}, \cdot) sur $(\hat{\mathbb{Z}}, +)$, et l'application $n \rightarrow \psi_n$ est un isomorphisme de groupes topologiques de $(\mathbb{Z}, +)$ sur $(\hat{\mathbb{T}}, \cdot)$.*

Démonstration : Il est clair que ϕ_z est un caractère de \mathbb{Z} pour tout $z \in \mathbb{T}$. D'autre part si $\phi \in \hat{\mathbb{T}}$ soit $z = \phi(1)$. Alors $\phi(n) = \phi(1)^n = z^n$ et $\phi(-n) = \phi(n)^{-1} = z^{-n}$ pour $n \geq 0$, donc $\phi = \phi_z$. Si $\lim_{p \rightarrow +\infty} z_p = z$, alors $\lim_{p \rightarrow \infty} \phi_{z_p}(n) = \lim_{p \rightarrow \infty} z_p^n = z^n$ pour tout $n \in \mathbb{Z}$. Comme les sous-ensembles compacts de \mathbb{Z} se réduisent aux sous-ensembles finis, on en déduit que la suite $(\phi_{z_p})_{p \geq 1}$ converge vers ϕ_z dans $\hat{\mathbb{Z}}$, et l'application $z \rightarrow \phi_z$ est une application continue de \mathbb{T} dans $\hat{\mathbb{Z}}$. Réciproquement si une suite $(\phi_{z_p})_{p \geq 1}$ converge vers ϕ_z dans $\hat{\mathbb{Z}}$, alors $\lim_{p \rightarrow +\infty} z_p = \lim_{p \rightarrow \infty} \phi_{z_p}(1) = \phi_z(1) = z$, et on en déduit que l'application $z \rightarrow \phi_z$ est un isomorphisme de groupes topologiques de (\mathbb{T}, \cdot) sur $(\hat{\mathbb{Z}}, +)$.

Il est clair que ψ_n est un caractère de \mathbb{T} pour tout $n \in \mathbb{Z}$. Soit maintenant ψ un caractère de \mathbb{T} . L'application $x \rightarrow \psi(ix)$ est un caractère de \mathbb{R} , et il existe $y \in \mathbb{R}$ tel que $\psi(ix) = e^{ixy}$ pour $x \in \mathbb{R}$. On a alors $1 = \psi(e^{2i\pi} e^{2i\pi y})$, donc $y \in \mathbb{Z}$ et l'application $n \rightarrow \psi_n$ est surjective. Si $\psi_n = \psi_m$, avec $n, m \in \mathbb{Z}$, $m \geq n$, on a $z^{m-n} = \psi_{m-n}(z) = 1$ pour tout $z \in \mathbb{T}$, et par conséquent $m = n$ puisque l'équation $z^k = 1$ n'admet que k solutions pour $k \neq 0$.

Soit maintenant $\psi_{n_0} \in \hat{\mathbb{T}}$. Pour $n \neq n_0$, on a $\sup_{z \in \mathbb{T}} |\psi_n(z) - \psi_{n_0}(z)| = \sup_{z \in \mathbb{T}} |1 - \psi_{n_0}(z)| = 2$. Donc $\{\psi_{n_0}\} = \{\psi \in \hat{\mathbb{T}} \mid \sup_{z \in \mathbb{T}} |\psi_n(z) - \psi_{n_0}(z)| < 2\}$ est un ouvert de $\hat{\mathbb{T}}$, et on voit que $\hat{\mathbb{T}}$ est un espace discret. Comme \mathbb{Z} est un groupe discret, on voit

que l'application $n \rightarrow \psi_n$ est un isomorphisme de groupes topologiques de $(\mathbb{Z}, +)$ sur $(\hat{\mathbb{T}}, \cdot)$. ♣

8.2 Mesure de Haar et transformée de Fourier, théorie générale

On va maintenant décrire un résultat très général, la construction de Haar qui permet de munir tout groupe topologique localement compact abélien (G, o, τ) d'une mesure positive invariante par translation. On dira qu'un sous-ensemble de G est borné s'il est contenu dans un compact de G , et on pose $xoA := \{xoa\}_{a \in A}$ pour $A \subset G, x \in G$. On peut définir $m_G(U) > 0$ pour tout ouvert non vide U contenu dans un compact de G , avec la propriété que $m_G(xoU) = m_G(U)$ pour tout ouvert U de G et pour tout $x \in G$, puis $m(K) \in [0, +\infty[$ pour tout compact K de G . On développe alors pour G et m_G une théorie des ensembles mesurables et une théorie de l'intégration analogue à la théorie de l'intégrale de Lebesgue (avec de sérieuses complications si le groupe ne peut pas s'écrire comme réunion d'une suite de sous-ensembles compacts). On peut démontrer que m_G , que l'on appelle la mesure de Haar sur G , est unique à une constante près : toute autre "mesure invariante par translation" sur G est de la forme λm_G , avec $\lambda > 0$.

Dans le cas de \mathbb{R} ou \mathbb{R}^n , on retrouve la mesure de Lebesgue. Dans le cas du cercle unité on a la "mesure de Lebesgue normalisée" : tout sous-ensemble mesurable A du cercle s'écrit sous la forme $A = \{e^{ix}\}_{x \in \tilde{A}}$, avec $\tilde{A} \subset [0, 2\pi[$, \tilde{A} mesurable, et on a $m_{\mathbb{T}}(A) = \frac{1}{2\pi} \int_{\tilde{A}} dx$, de sorte que $m_{\mathbb{T}}(\mathbb{T}) = 1$. Plus généralement si G est un groupe abélien compact on "normalise" la mesure de Haar en posant par convention $m_G(G) = 1$. Un exemple évident de mesure de Haar est la "mesure de comptage" pour les groupes discrets ; on note $Card(A)$ le cardinal d'un ensemble A , ce qui signifie que $Card(A)$ est égal au nombre d'éléments de A si A est fini et que $Card(A) = +\infty$ si A possède une infinité d'éléments.

Exemple 8.2.1 Soit (G, o) un groupe discret. Alors $Card(xoA) = Card(A)$ pour tout sous-ensemble A de G , et on peut poser $m_G(A) = Card(A)$ pour $A \subset G$.

Dans la suite on munit un groupe localement compact abélien (G, o, τ) de la mesure de Haar m_G . On note $\int_E f(x)dx$ l'intégrale sur un ensemble mesurable $E \subset G$ d'une fonction intégrable f intégrable sur E , les notions de mesurabilité et d'intégrabilité étant celles relatives à la mesure de Haar.

Définition 8.2.2 On note $L^1(G)$ l'ensemble des fonctions intégrables sur G et $L^2(G)$ l'ensemble des fonctions mesurables et de carré intégrable sur G pour la mesure de Haar. D'autre part on note $\mathbb{C}(G)$ l'ensemble des fonctions continues sur G , et on note $\mathbb{C}_0(G)$ l'ensemble des fonctions f continues sur G telles que pour tout $\epsilon > 0$ il existe un sous-ensemble compact K_ϵ de G pour lequel $\sup_{x \in G \setminus K} |f(x)| < \epsilon$. L'ensemble des

fonctions continues f sur G nulles en dehors d'un compact de G , appelées fonctions continues à support compact sur G , est noté $\mathcal{C}_c(G)$.

Pour $f \in L^1(G)$, on pose $\|f\|_1 = \int_G |f(x)| dx$. De même pour $f \in L^2(G)$, on pose $\|f\|_2 = \sqrt{\int_G |f(x)|^2 dx}$. Enfin on pose, pour $f \in \mathcal{C}_0(G)$, $\|f\|_\infty = \max_{x \in G} |f(x)|$.

Notons que, de même que sur \mathbb{R} , on identifie les fonctions mesurables sur G qui sont égales "presque partout", c'est à dire les fonctions mesurables égales en dehors d'un ensemble de mesure nulle. On notera que si G est discret, le seul sous-ensemble de mesure nulle de G est l'ensemble vide, et deux fonctions sur G égales presque partout sur G sont en fait égales sur G .

On peut alors définir la transformée de Fourier sur $L^1(G)$.

Définition 8.2.3 Soit (G, o, τ) un groupe localement compact abélien. Pour $f \in L^1(G)$, on définit la transformée de Fourier $\hat{f} = \mathcal{F}(f) : \hat{G} \rightarrow \mathbb{C}$ par la formule

$$\forall \chi \in \hat{G}, \quad \hat{f}(\chi) = \int_G f(x) \bar{\chi}(x) dx. \quad (8.4)$$

On obtient pour la transformée de Fourier sur $L^1(G)$ des résultats analogues aux résultats obtenus pour la transformée de Fourier sur $L^1(\mathbb{R}^p)$.

Théorème 8.2.4 (i) On a $\hat{f} \in C_0(\hat{G})$ pour $f \in L^1(G)$.

(ii) Soient $f, g \in L^1(G)$. Alors la fonction $s \rightarrow f(s)g(t-s)$ est intégrable pour presque tout $t \in G$, et si on définit $f * g$ presque partout sur G par la formule

$$(f * g)(t) = \int_G f(s)g(t-s) ds,$$

alors $f * g \in L^1(G)$ et on a, pour tout $\chi \in \hat{G}$,

$$\mathcal{F}(f * g)(\chi) = \mathcal{F}(f)(\chi)\mathcal{F}(g)(\chi). \quad (8.5)$$

Démonstration : La première propriété résulte d'une version adéquate du théorème de convergence dominée et du fait que pour toute fonction $f \in L^1(G)$ il existe une suite $(f_n)_{n \geq 1}$ de fonctions continues à support compact telles que $\lim_{n \rightarrow \infty} \|f - f_n\|_1 = 0$. La seconde fait appel à une version générale du théorème de Fubini. Nous renvoyons à l'ouvrage de Rudin [16] pour plus de détails. ♣

8.3 Formule de Plancherel-Parseval et formule d'inversion de Fourier

On va maintenant décrire la version générale de la formule de Plancherel-Parseval. Nous admettrons les lemmes suivants.

Lemme 8.3.1 Soit (G, o, τ) un groupe localement compact abélien. Il existe un réel $m > 0$ tel que l'on ait, pour toute fonction $f \in \mathcal{C}_c(G)$,

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

Lemme 8.3.2 Soit (G, o, τ) un groupe localement compact abélien. Il existe pour toute fonction $f \in L^2(G)$ une suite (f_n) de fonctions continues à support compact sur G telle que $\lim_{n \rightarrow \infty} \|f - f_n\|_2 = 0$, et il existe une fonction $h \in L^2(\hat{G})$ telle que $\lim_{n \rightarrow \infty} \|h - \hat{f}_n\|_2 = 0$.

En fait la fonction h ci-dessus est indépendante du choix de la suite $(f_n)_{n \geq 0}$. En effet supposons que $\lim_{n \rightarrow \infty} \|f - g_n\|_2 = 0$, avec $g_n \in \mathcal{C}_c(G)$ pour $n \geq 1$. On a alors

$$\begin{aligned} \|h - \hat{g}_n\|_2 &\leq \|h - \hat{f}_n\|_2 + \|\hat{f}_n - \hat{g}_n\|_2 = \|h - \hat{f}_n\|_2 + \frac{1}{m} \|f_n - g_n\|_2 \\ &\leq \|h - \hat{f}_n\|_2 + \frac{1}{m} \|f_n - f\|_2 + \frac{1}{m} \|f - g_n\|_2, \end{aligned}$$

et par conséquent $\lim_{n \rightarrow \infty} \|h - \hat{g}_n\|_2 = 0$. Ceci permet d'introduire la définition suivante.

Définition 8.3.3 Pour $f \in L^2(G)$, on définit $\hat{f} = \mathcal{F}(f) \in L^2(\hat{G})$ par la formule

$$\lim_{n \rightarrow \infty} \|f - f_n\|_2 = 0, \quad (8.6)$$

où $(f_n)_{n \geq 0}$ est une suite quelconque de fonctions continues sur G à support compact vérifiant $\lim_{n \rightarrow \infty} \|f - f_n\|_2 = 0$.

On obtient alors une version très générale des formules de Plancherel -Parseval.

Théorème 8.3.4 La transformée de Fourier $\mathcal{F} : f \rightarrow \hat{f}$ est une application linéaire bijective de $L^2(G)$ sur $L^2(\hat{G})$ et on a, pour $f, g \in L^2(G)$, la formule de Plancherel

$$\int_G f(x)\bar{g}(x)dx = m^2 \int_{\hat{G}} \hat{f}(\chi)\bar{\hat{g}}(\chi)d\chi. \quad (8.7)$$

En particulier les fonctions $f \in L^2(G)$ vérifient la formule de Parseval.

$$\int_G |f(x)|^2 dx = m^2 \int_{\hat{G}} |\hat{f}(\chi)|^2 d\chi. \quad (8.8)$$

On va maintenant donner une version générale de la formule d'inversion de Fourier.

Théorème 8.3.5 Soit $f \in L^1(G)$. Si $\hat{f} \in L^1(\hat{G})$, on a, pour presque tout $x \in G$,

$$f(x) = m^2 \int_{\hat{G}} \hat{f}(\chi)\chi(x)d\chi. \quad (8.9)$$

Notons que si $f \in L^2(G)$, et si $\hat{f} \in \mathcal{C}_c(\hat{G})$, on peut montrer que l'on a, pour presque tout $x \in G$,

$$f(x) = m^2 \int_{\hat{G}} \hat{f}(\chi) \chi(x) d\chi.$$

On peut alors poser $\mathcal{F}^{-1}(g)(x) = m^2 \int_{\hat{G}} g(\chi) \chi(x) d\chi$ pour $g \in \mathcal{C}_c(\hat{G})$, et définir $\mathcal{F}^{-1} : L^2(\hat{G}) \rightarrow L^2(G)$ pour $g \in L^2(\hat{G})$ par la formule

$$\lim_{n \rightarrow \infty} \|\mathcal{F}^{-1}(h) - \mathcal{F}^{-1}(g_n)\|_2 = 0,$$

où $(g_n)_{n \geq 1}$ est une suite d'éléments de $\mathcal{C}_c(\hat{G})$ telle que $\lim_{n \rightarrow \infty} \|g - g_n\|_2 = 0$. De même que plus haut, on vérifie que cette définition est indépendante du choix de la suite $(g_n)_{n \geq 1}$, et que l'application ainsi définie est bien l'application réciproque de la transformée de Fourier $\mathcal{F} : L^2(G) \rightarrow L^2(\hat{G})$.

Il serait tentant d'essayer de déduire de la définition ci-dessus que $\mathcal{F}^{-1}(g)(x) = \lim_{n \rightarrow \infty} \mathcal{F}^{-1}(g_n)(x) = \lim_{n \rightarrow \infty} m^2 \int_{\hat{G}} g_n(\chi) \chi(x) d\chi$ presque partout sur G . Malheureusement la réalité est plus compliquée, et il faut en général remplacer la suite $(g_n)_{n \geq 1}$ par une de ses sous-suites pour obtenir une telle limite ponctuelle presque partout.

On notera que la constante m qui intervient dans la formule de Plancherel-Parseval dépend du choix des mesures de Haar sur G et \hat{G} , et on peut toujours une fois fixée la mesure de Haar sur G "normaliser" la mesure de Haar sur \hat{G} de façon que cette constante m soit égale à 1. C'est ainsi que certains auteurs définissent la transformée de Fourier sur \mathbb{R} par la formule $\hat{f}(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} f(t) e^{-ixt} dt$, ce qui supprime le facteur $\frac{1}{2\pi}$ dans la formule de Parseval. Nous avons préféré nous en tenir aux définitions des chapitres 2 et 3 en prenant comme mesure de Haar sur \mathbb{R}^p la mesure de Lebesgue usuelle, ce qui introduit un facteur $m = \frac{1}{(2\pi)^{p/2}}$ dans la formule de Parseval telle qu'elle est énoncée ci-dessus.

On va maintenant expliciter cette théorie générale dans plusieurs cas particuliers importants.

8.4 Séries de Fourier et transformation de Fourier sur le cercle

Soit $T > 0$, et soit $f : \mathbb{R} \rightarrow \mathbb{C}$ une fonction mesurable de période T . Pour $z = e^{ix} \in \mathbb{T}$, posons $\tilde{f}(z) = f(\frac{xT}{2\pi})$. Notons que $f(\frac{(x+2k\pi)T}{2\pi}) = f(\frac{xT}{2\pi} + kT) = f(\frac{xT}{2\pi})$, et cette définition ne dépend pas du choix de l'argument x de z . Il est clair que f est mesurable, que \tilde{f} est continue sur \mathbb{T} si f est continue sur \mathbb{R} , et que \tilde{f} est intégrable sur \mathbb{T} si f est intégrable sur $[0, T]$.

Pour $n \in \mathbb{Z}$, $z \in \mathbb{T}$, posons de même que plus haut $\chi_n(z) = z^n$. Si f est mesurable sur \mathbb{R} , périodique de période T , et intégrable sur $[0, T]$, on définit le coefficient de Fourier d'ordre n de la fonction f par la formule

$$\hat{f}(n) = \tilde{f}(\chi_n) = \frac{1}{2\pi} \int_0^{2\pi} \tilde{f}(e^{ix}) \bar{\chi}_n(x) dx = \frac{1}{2\pi} \int_0^{2\pi} \tilde{f}\left(\frac{xT}{2\pi}\right) e^{-inx} dx.$$

On obtient, en posant $s = \frac{2\pi}{T}$,

$$\hat{f}(n) = \frac{1}{T} \int_0^T f(s) e^{-\frac{2in\pi s}{T}} ds. \quad (8.10)$$

On note $l^1(\mathbb{Z})$ l'ensemble des applications $u : \mathbb{Z} \rightarrow \mathbb{C}$ telles que $\|u\|_1 := \sum_{n \in \mathbb{Z}} |u(n)| < +\infty$, qui est l'espace L^1 associé à la mesure de Haar sur \mathbb{Z} muni de la topologie discrète, et on note $c_0(\mathbb{Z})$ l'ensemble des applications $u : \mathbb{Z} \rightarrow \mathbb{C}$ telles que $\lim_{|n| \rightarrow +\infty} u(n) = 0$, que l'on munit de la norme $\|u\|_\infty = \max_{n \in \mathbb{Z}} |u_n|$. Si $g \in L^1(\mathbb{T})$, on a $\hat{g} \in \mathcal{C}_0(\hat{\mathbb{T}})$, ce qui signifie que $\lim_{|n| \rightarrow \infty} \hat{g}(\chi_n) = 0$. On obtient donc le résultat suivant

Proposition 8.4.1 *Soit f une fonction périodique de période T , intégrable sur $[0, T]$. On a alors*

$$\lim_{|n| \rightarrow \infty} \hat{f}(n) = 0.$$

On sait qu'il existe une constante $m > 0$ telle que l'on ait, pour $g \in L^2(\mathbb{T})$

$$\frac{1}{2\pi} \int_0^{2\pi} |g(e^{is})|^2 ds = m^2 \sum_{n \in \mathbb{Z}} |\hat{g}(\chi_n)|^2.$$

En posant $g(e^{is}) = 1$ pour $s \in \mathbb{R}$, on obtient $\hat{g}(\chi_0) = 1$, $\hat{g}(\chi_n) = 0$ pour $n \neq 0$, donc $m = 1$, ce qui donne

$$\frac{1}{2\pi} \int_0^{2\pi} |g(e^{is})|^2 ds = \sum_{n \in \mathbb{Z}} |\hat{g}(\chi_n)|^2. \quad (8.11)$$

Supposons maintenant que f est mesurable sur \mathbb{R} et de carré intégrable sur $[0, T]$. Par changement de variables, on obtient

$$\frac{1}{2\pi} \int_0^{2\pi} |\tilde{f}(e^{is})|^2 ds = \frac{1}{2\pi} \int_0^{2\pi} \left| f\left(\frac{sT}{2\pi}\right) \right|^2 ds = \frac{1}{T} \int_0^T |f(x)|^2 dx.$$

On obtient ainsi la version "séries de Fourier" de la formule de Parseval, ainsi que la version "séries de Fourier" de la formule de Plancherel, qui se déduit de la même façon de la formule de Plancherel sur $L^2(\mathbb{T})$.

Théorème 8.4.2 (i) *Soit f mesurable sur \mathbb{R} , périodique de période T , de carré intégrable sur $[0, T]$. On a alors*

$$\frac{1}{T} \int_0^T |f(x)|^2 dx = \sum_{n \in \mathbb{Z}} |\hat{f}(n)|^2.$$

(ii) Soient f et g mesurables sur \mathbb{R} , périodiques de période T , de carré intégrable sur $[0, T]$. On a alors

$$\frac{1}{T} \int_0^T f(x)\bar{g}(x)dx = \sum_{n \in \mathbb{Z}} \hat{f}(n)\bar{\hat{g}}(n).$$

La formule d'inversion de Fourier pour $L^1(\mathbb{T})$ montre que si $g \in L^1(\mathbb{T})$, et si $\hat{g} \in l^1(\mathbb{Z})$, on a, pour presque tout $x \in [0, 2\pi]$,

$$g(e^{it}) = \int_{\hat{\mathbb{T}}} \hat{g}(\chi)\chi(e^{it})d\chi = \sum_{n \in \mathbb{Z}} \hat{g}(n)e^{int}.$$

Par changement de variables, on voit que si f est périodique de période T , intégrable sur $[0, T]$, et si $\sum_{n \in \mathbb{Z}} |\hat{f}(n)| < +\infty$, on a pour presque tout $x \in \mathbb{R}$,

$$f(x) = \sum_{n \in \mathbb{Z}} \hat{f}(n)e^{\frac{2i\pi nx}{T}}. \quad (8.12)$$

La série de Fourier est la série

$$S(f)(s) = \sum_{n \in \mathbb{Z}} \hat{f}(n)e^{\frac{2i\pi ns}{T}}.$$

Par intégration par parties on voit que si f est deux fois continûment dérivable sur \mathbb{R} , périodique de période T alors il existe $M > 0$ tel que $\hat{f}(n) \leq \frac{M}{n^2}$ pour $n \neq 0$, ce qui implique que $\sum_{n \in \mathbb{Z}} |\hat{f}(n)|^2 < +\infty$, et dans ce cas la fonction f coïncide pour tout x avec la somme de sa série de Fourier d'après la formule 8.2. On a des résultats plus fins, que nous mentionnons pour mémoire (voir par exemple le support de cours d'analyse [7]).

Théorème 8.4.3 Soit f périodique de période T , intégrable sur $[0, T]$. Posons, pour $N > 0$,

$$S_N(f)(x) = \sum_{-N}^N \hat{f}(n)e^{\frac{2i\pi nx}{T}}, \quad \sigma_N(f)(x) = \frac{1}{N+1} \sum_{n=0}^N s_n(x). \quad (8.13)$$

(i) Si f est continue sur \mathbb{R} , alors $\lim_{N \rightarrow \infty} \sigma_N(f)(x) = f(x)$ pour tout $x \in \mathbb{R}$, et la convergence est uniforme sur \mathbb{R} .

(ii) Si f est de classe C^1 par morceaux sur \mathbb{R} alors $\lim_{N \rightarrow \infty} S_N(x) = \frac{1}{2}(f^+(x) + f^-(x))$ pour tout $x \in \mathbb{R}$, où $f^+(x) = \lim_{h \rightarrow 0^+} f(x+h)$, et $f^-(x) = \lim_{h \rightarrow 0^-} f(x+h)$.

Le premier résultat est le théorème de Féjer, et le fait que la convergence est uniforme sur \mathbb{R} signifie que $\lim_{N \rightarrow \infty} \sup_{x \in \mathbb{R}} |f(x) - \sigma_N(f)(x)| = 0$. Dire qu'une fonction f est de classe C^1 sur un intervalle ou une réunion d'intervalles U d'intérieurs non vides veut dire qu'elle est continûment dérivable sur U . Dire qu'une fonction périodique de

période T est de classe C^1 par morceaux sur \mathbb{R} veut dire qu'elle est de classe C_1 sur $\mathbb{R} \setminus (F + T\mathbb{Z})$, où $F \subset [0, T]$ est un ensemble fini, et où $F + T\mathbb{Z} = \{u + nT\}_{u \in F, n \in \mathbb{Z}}$, et que f et sa dérivée ont des limites à droite et à gauche en tout $x \in F + T\mathbb{Z}$. En fait la convergence de $S_N(f)(x)$ vers $f(x)$ est uniforme sur tout intervalle fermé borné $[a, b]$ tel que $[a, b] \cap (F + T\mathbb{Z}) = \emptyset$. On trouvera les détails des démonstrations dans [7].

Pour conclure ce bref rappel sur les séries de Fourier notons que puisque $e^{inx} = \cos(nx) + i\sin(nx)$ pour $n \in \mathbb{Z}$, on peut réécrire la série de Fourier de f sous la forme

$$S(f)(x) = \hat{f}(0) + \sum_{n=0}^{+\infty} \left(a_n(f) \cos\left(\frac{2\pi nx}{T}\right) + b_n(f) \sin\left(\frac{2\pi nx}{T}\right) \right),$$

avec $a_0(f) = \hat{f}(0)$, $a_n(f) = \hat{f}(-n) + \hat{f}(n)$, $b_n(f) = i(\hat{f}(n) - \hat{f}(-n))$ pour $n \geq 1$.

On obtient $a_0 = \frac{1}{T} \int_0^T f(x) dx$, et, pour $n \geq 1$,

$$a_n(f) = \frac{2}{T} \int_0^T f(x) \cos\left(\frac{2\pi nx}{T}\right) dx, \quad b_n(f) = \frac{2}{T} \int_0^T f(x) \sin\left(\frac{2\pi nx}{T}\right) dx.$$

On obtient

$$S_N(f)(x) = a_0(f) + \sum_{n=1}^N \left(a_n(f) \cos\left(\frac{2\pi nx}{T}\right) + b_n(f) \sin\left(\frac{2\pi nx}{T}\right) \right).$$

On peut donc exprimer tous les résultats de convergence rappelés ci dessus en utilisant la version trigonométrique de la série de Fourier. D'autre part $\hat{f}(-n) = \frac{a_n(f) + ib_n(f)}{2}$ et $\hat{f}(n) = \frac{a_n(f) - ib_n(f)}{2}$, de sorte que $|\hat{f}(-n)|^2 + |\hat{f}(n)|^2 = \frac{|a_n(f)|^2 + |b_n(f)|^2}{2}$ pour $n \geq 1$. Si f est périodique de période T , et de carré intégrable sur $[0, T]$, la formule de Parseval peut donc s'écrire sous la forme

$$\frac{1}{T} \int_0^T |f(x)|^2 dx = |a_0(f)|^2 + \sum_{n=1}^{+\infty} \frac{|a_n(f)|^2 + |b_n(f)|^2}{2}.$$

8.5 Transformée de Fourier sur les groupes abéliens finis

Toute la théorie décrite plus haut s'applique en particulier aux groupes abéliens finis.

Pour $A \subset G$, notons $|A|$ le cardinal de A , c'est à dire le nombre d'éléments de A . On peut alors définir la mesure de Haar m_G par la formule $m_G(A) = |A|$, qui n'est autre que la "mesure de comptage" sur G . L'espace $L^1(G, m_G)$ coïncide alors avec l'espace $\mathbb{C}(G)$ de toutes les fonctions $f : G \rightarrow \mathbb{C}$. Pour $f \in \mathbb{C}[G]$, $A \in G$, on a alors

$$\int_A f(x) dx = \frac{1}{|G|} \sum_{x \in A} f(x).$$

L'espace vectoriel $\mathbb{C}(G)$ est de dimension égale au cardinal de G , car une base évidente de $\mathbb{C}(G)$ est fournie par la famille $(\delta_u)_{u \in G}$, où $\delta(u)(x) = 0$ pour $x \neq u$, $\delta_u(u) = 1$. En effet étant donnée $f \in \mathbb{C}(G)$ l'équation $f = \sum_{u \in G} \lambda_u \delta_u$ admet pour unique solution $\lambda_u = f(u)$ pour tout $u \in G$.

Si la loi du groupe abélien fini G est notée additivement, on obtient, pour $f, g \in \mathbb{C}(G)$, $x \in G$,

$$(f * g)(x) = \sum_{t \in G} f(t)g(x - t).$$

On munit $\mathbb{C}[G]$ du "produit hermitien" défini par la formule

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\bar{g}(x).$$

L'unité de \hat{G} est le caractère 1_G , défini par la formule $1_G(x) = 1$ pour tout $x \in G$. Soient maintenant $\chi \in \hat{G} \setminus \{1_G\}$, et soit $u \in G$ tel que $\chi(u) \neq 1$. Comme l'application $x \rightarrow ux$ est une bijection de G sur lui-même, on a

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(ux) = \chi(u) \sum_{x \in G} \chi(x).$$

Comme $\chi(u) \neq 1$, on a $\sum_{x \in G} \chi(x) = 0$. Soient maintenant ϕ et ψ deux caractères distincts sur G . Comme $\phi\bar{\psi}$ est un caractère sur G distinct de χ_0 , on a $\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{x \in G} \phi(x)\bar{\psi}(x) = 0$. On obtient, pour $\phi, \psi \in \hat{G}$,

$$\begin{cases} \langle \phi, \psi \rangle = 0 & \text{si } \psi \neq \phi \\ \langle \phi, \psi \rangle = 1 & \text{si } \phi = \psi \end{cases}$$

Il est clair que l'ensemble des caractères d'un groupe fini est fini, car si $\phi \in \hat{G}$ on a $\phi(x)^{|G|} = 1$, et \hat{G} est inclus dans l'ensemble des applications de G dans le groupe fini $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ formé des racines n^e de l'unité, où $n = |G|$.

Supposons maintenant qu'une famille $(\lambda_\phi)_{\phi \in \hat{G}}$ de nombres complexes vérifie $\sum_{\phi \in \hat{G}} \lambda_\phi \phi = 0$. On a alors $0 = \langle \sum_{\phi \in \hat{G}} \lambda_\phi \phi, \psi \rangle = \lambda_\psi$ pour tout $\psi \in \hat{G}$, donc \hat{G} est une famille libre d'éléments de $\mathbb{C}(G)$ et $|\hat{G}| \leq |G|$. Comme il existe une bijection du dual de \hat{G} sur G , d'après le théorème de dualité de Pontryagin, on a $|\hat{G}| = |G|$, et on obtient le résultat suivant

Théorème 8.5.1 *Soit G un groupe abélien fini. Alors \hat{G} est une base de $\mathbb{C}(G)$ (qui est orthonormale pour le "produit hermitien" de $\mathbb{C}(G)$).*

Il existe bien sûr des démonstrations du fait que $|\hat{G}| = |G|$ pour tout groupe abélien fini G qui ne font pas appel au théorème de Pontryagin. Nous en proposons une à l'exercice 5.

Nous explicitons maintenant les principaux résultats concernant la transformée de Fourier appliquée aux groupes abéliens finis. Comme la mesure de Haar sur un groupe abélien fini coïncide avec la mesure de comptage, la transformée de Fourier $\mathcal{F}_G : \mathbb{C}(G) \rightarrow \mathbb{C}(G)$ associée à toute fonction $f \in \mathbb{C}(G)$ sa transformée de Fourier $\hat{f} \in \mathbb{C}(\hat{G})$ définie pour $\chi \in \hat{G}$ par la formule

$$\hat{f}(\chi) = \sum_{x \in G} f(x) \bar{\chi}(x). \quad (8.14)$$

On a alors les résultats suivants

Théorème 8.5.2 *Soit G un groupe abélien fini.*

(i) *Pour $f, g \in \mathbb{C}(G)$, on a*

$$f \hat{*} g = \hat{f} \hat{g},$$

et ("formule de Plancherel")

$$\sum_{x \in G} f(x) \bar{g}(x) = \sum_{\chi \in \hat{G}} \hat{f}(\chi) \bar{\hat{g}}(\chi).$$

(ii) *Pour $f \in \mathbb{C}(G)$, on a ("formule d'inversion de Fourier")*

$$\forall x \in G, f(x) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(x).$$

et (formule de Parseval)

$$\sum_{x \in G} |\hat{f}(x)|^2 = \frac{1}{|G|} \sum_{\chi \in \hat{G}} |\hat{f}(\chi)|^2.$$

Tous ces résultats sont des cas particuliers de la théorie générale de l'intégration sur les groupes localement compacts abéliens (le fait que la constante intervenant dans la formule de Parseval est égale à $\frac{1}{|G|}$ provient du fait que si e est l'unité de G on a $\hat{e}(\chi) = 1$ pour tout $\chi \in \hat{G}$). On peut aussi les démontrer directement, voir l'exercice 6.

On va conclure ce chapitre en donnant une version matricielle de la transformée de Fourier sur un groupe abélien fini G possédant n éléments. On notera que la formule obtenue dépend de l'énumération choisie pour G et son groupe dual \hat{G} .

Proposition 8.5.3 *Soit $G = \{x_0, \dots, x_{n-1}\}$ un groupe abélien fini possédant n éléments et soit $\hat{G} = \{\chi_0, \dots, \chi_{n-1}\}$ son groupe dual. Soit $A_G := (a_{i,j})_{\substack{0 \leq i \leq n-1 \\ 0 \leq j \leq n-1}}$ la "matrice de Fourier" de G définie pour $0 \leq i \leq n-1, 0 \leq j \leq n-1$ par la formule*

$$a_{i,j} = \bar{\chi}_i(x_j).$$

On a, pour $f = (f[x_0], \dots, f[x_{n-1}]) \in \mathbb{C}(G)$,

$$\begin{bmatrix} \hat{f}[\chi_0] \\ \vdots \\ \hat{f}[\chi_{n-1}] \end{bmatrix} = A_G \begin{bmatrix} f[x_0] \\ \vdots \\ f[x_{n-1}] \end{bmatrix}$$

Démonstration : On munit $\mathbb{C}(G)$ de la base $\mathcal{B} := \{\delta_{x_0} \dots \delta_{x_{n-1}}\}$, et on munit $\mathbb{C}(G)$ de la base $\hat{\mathcal{B}} := \{\delta_{\chi_0} \dots \delta_{\chi_{n-1}}\}$. Soit $\mathcal{M} := \mathcal{M}_{\mathcal{F}_G, \mathcal{B}, \hat{\mathcal{B}}}$ la matrice représentant la transformée de Fourier $\mathcal{F}_G : \mathbb{C}(G) \rightarrow \mathbb{C}(\hat{G})$ par rapport aux bases \mathcal{B} et $\hat{\mathcal{B}}$ (voir le *Cours d'algèbre linéaire* [6]). La colonne d'indice j de \mathcal{M} est formée des coordonnées de $\mathcal{F}_G(\delta_{x_j})$ dans la base $\hat{\mathcal{B}}$. Comme $\hat{\delta}_{x_j} = \sum_{i=0}^{n-1} \hat{\delta}_{x_j}(\chi_i) \delta_{\chi_i}$, et comme $\hat{\delta}_{x_j}(\chi_i) = \sum_{k=0}^{n-1} \bar{\chi}_i(x_k) \delta_{x_j}(x_k) = \bar{\chi}_i(x_j)$, on voit que \mathcal{M} coïncide avec la matrice de Fourier A_G , ce qui implique immédiatement la formule ci-dessus. ♣

On peut utiliser la matrice de Fourier pour démontrer la formule d'inversion de Fourier, voir l'exercice 6.

8.6 Transformée de Walsh, transformée de Fourier discrète, échantillonnage

Considérons le groupe additif $\mathbb{F}_2^k = (\mathbb{Z}/2\mathbb{Z})^k$. On peut associer à tout élément $x = (\bar{x}_0, \dots, \bar{x}_{k-1})$ de \mathbb{F}_2^k , avec $x_j \in \{0, 1\}$ pour $0 \leq j \leq k$, l'entier $n(x) = \sum_{j=0}^{k-1} x_j 2^j$. On peut ainsi énumérer \mathbb{F}_2^k : à tout entier $j \in \{0, \dots, 2^k - 1\}$, écrit en base 2 sous la forme $j = j_{k-1} \dots j_0 := \sum_{i=0}^{k-1} j_i 2^i$, on associe $x_j = (\bar{j}_0, \dots, \bar{j}_{k-1}) \in \mathbb{F}_2^k$.

Rappelons que pour $x = (\bar{x}_0, \dots, \bar{x}_{k-1})$, $y = (\bar{y}_0, \dots, \bar{y}_{k-1}) \in \mathbb{F}_2^k$, on pose

$$x.y = \sum_{j=0}^{k-1} \bar{x}_j \bar{y}_j, \quad \phi_y(x) = (-1)^{\sum_{j=0}^{k-1} x_j y_j}.$$

Nous laissons au lecteur le soin de vérifier (voir l'exercice 2) que l'application ϕ_y est un caractère de \mathbb{F}_2^k pour tout $y \in \mathbb{F}_2^k$, et que l'application $y \rightarrow \phi_y$ est une bijection du groupe \mathbb{F}_2^k sur son groupe dual. On déduit alors du lemme 6.3.5 que pour $0 \leq i \leq k-1, 0 \leq j \leq k-1$, on a

$$\chi_i(y_j) = w_{i,j},$$

où $(w_{i,j})_{\substack{1 \leq i \leq k-1 \\ 1 \leq j \leq k-1}} = W_k$ est la matrice de Walsh d'ordre k . On voit donc que la transformée de Walsh n'est autre que la transformée de Fourier sur \mathbb{F}_2^k , réécrite en utilisant pour $f \in \mathbb{C}^{2^k}$, $0 \leq j \leq k$, la formule

$$\mathcal{W}_k(f)[j] = \mathcal{F}_{\mathbb{F}_2^k}(\tilde{f})[x_j],$$

où $\tilde{f}[x_i] = f[i]$ pour $0 \leq i \leq 2^k - 1$.

On voit donc que la formule d'inversion pour la transformée de Walsh est un cas particulier de la formule d'inversion de Fourier. La formule de Parseval donne, pour $f \in \mathbb{C}^{2^k}$,

$$\sum_{j=0}^{2^k-1} |f[j]|^2 = \sum_{j=0}^{2^k-1} |\tilde{f}[x_j]|^2 = \frac{1}{2^k} \sum_{j=0}^{2^k-1} |\mathcal{F}_{\mathbb{F}_2^k}(\tilde{f})[x_j]|^2 = \frac{1}{2^k} \sum_{j=0}^{2^k-1} |\mathcal{W}_k(f)[j]|^2,$$

et on retrouve la formule 6.10, qui avait été démontrée directement au Chapitre 6.

Soit $N \geq 2$. Posons $\omega_N = e^{2i\pi/N}$. On a également laissé au lecteur le soin de vérifier à l'exercice 1 que l'application $\phi_p : \bar{q} \rightarrow \omega_N^{pq}$ est un caractère de $\mathbb{Z}/N\mathbb{Z}$ pour $p \in \mathbb{Z}$, et que le dual de $\mathbb{Z}/N\mathbb{Z}$ est égal à l'ensemble $\{\phi_0, \dots, \phi_{N-1}\}$. On munit $\mathbb{C}(\mathbb{Z}/N\mathbb{Z})$ de la base $\mathcal{B} := \{\delta_{\bar{0}}, \dots, \delta_{\bar{N-1}}\}$, et on munit $\mathbb{C}(\mathbb{Z}/\hat{N}\mathbb{Z})$ de la base $\hat{\mathcal{B}} := \{\delta_{\phi_0}, \dots, \delta_{\phi_{N-1}}\}$. La colonne d'indice $j \in \{0, \dots, N-1\}$ de la matrice $\mathcal{M} := \mathcal{M}_{\mathcal{F}_{\mathbb{Z}/N\mathbb{Z}}, \mathcal{B}, \hat{\mathcal{B}}}$ représentant la transformation de Fourier $\mathcal{F}_{\mathbb{Z}/N\mathbb{Z}} : \mathbb{C}(\mathbb{Z}/N\mathbb{Z}) \rightarrow \mathbb{C}(\mathbb{Z}/\hat{N}\mathbb{Z})$ par rapport aux bases \mathcal{B} et $\hat{\mathcal{B}}$ est formée pour $0 \leq n \leq N-1$ des coordonnées de $\hat{\delta}_{\bar{n}}$ dans la base $\hat{\mathcal{B}}$.

On a pour $0 \leq m \leq N-1$,

$$\hat{\delta}_{\bar{n}}(\chi_m) = \sum_{p=0}^{N-1} \delta_{\bar{n}}(\bar{p}) \bar{\chi}_m(\bar{p}) = e^{-\frac{2\pi i m n}{N}} = \omega_N^{-mn}.$$

Donc la matrice de Fourier $A_{\mathbb{Z}/N\mathbb{Z}} = M$ associée à ces énumérations de $\mathbb{Z}/N\mathbb{Z}$ et de son groupe dual coïncide avec la matrice de Fourier A_N introduite au Chapitre 6, et la transformée de Fourier discrète n'est autre que la transformée de Fourier sur $\mathbb{Z}/N\mathbb{Z}$, réécrite en utilisant pour $0 \leq n \leq N-1$ la formule

$$\hat{f}[m] = \mathcal{F}_{\mathbb{Z}/N\mathbb{Z}}(\tilde{f})(\chi_m),$$

où $\tilde{f}[\bar{n}] = f[n]$ pour $0 \leq n \leq N-1$. On voit donc que tous les résultats obtenus au Chapitre 7 sont un cas particulier des propriétés de la transformée de Fourier sur un groupe abélien fini.

Pour conclure ce Chapitre on va faire apparaître le lien entre transformée de Fourier discrète, coefficients de Fourier d'une fonction périodique de période T et transformée de Fourier sur \mathbb{R} , ce qui nous renvoie aux sommes de Riemann dont les propriétés sont rappelées au tout début de ce support de cours.

Considérons tout d'abord une fonction continue sur \mathbb{R} , périodique de période 1. Pour $N \geq 2$, $0 \leq m \leq N-1$, posons

$$f_N[m] = f\left(\frac{n}{N}\right).$$

Notons \hat{f}_N la transformée de Fourier discrète de f_N . On a, pour $0 \leq p \leq N-1$, avec les notations du Chapitre 7,

$$\hat{f}_N[p] = \sum_{n=0}^{N-1} f_N[n] e^{-\frac{2i\pi pn}{N}} = \sum_{n=0}^{N-1} f\left(\frac{n}{N}\right) e^{-\frac{2i\pi pn}{N}}.$$

D'autre part le coefficient de Fourier $\hat{f}(p)$ peut s'obtenir comme limite de sommes de Riemann. En effet on a, pour $p \geq 0$,

$$\hat{f}(p) = \int_0^1 f(x) e^{-2i\pi px} dx = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} f\left(\frac{n}{N}\right) e^{-\frac{2i\pi pn}{N}}.$$

On obtient, pour $p \geq 0$,

$$\hat{f}(p) = \lim_{N \rightarrow \infty} \frac{\hat{f}_N[p]}{N}. \quad (8.15)$$

Un calcul analogue permet d'obtenir les coefficients de Fourier d'indice négatif de f en introduisant la fonction $f_1 : x \rightarrow f(-x)$, voir l'exercice 8.

On s'intéresse maintenant au cas d'une fonction g continue et intégrable sur \mathbb{R} . Pour $A > 0$, posons $g^{(A)}(x) = g(x)$ pour $x \in [-A, A]$, et posons $g^{(A)}(x) = 0$ pour $|x| > A$.

Pour $u \in \mathbb{R}$, on a

$$|\hat{g}(u) - \hat{g}^{(A)}(u)| = \left| \int_{-\infty}^{-A} g(u) e^{-ixu} dx + \int_A^{+\infty} g(u) e^{-ixu} dx \right| \leq \int_{-\infty}^{-A} |f(x)| dx + \int_A^{+\infty} |f(x)| dx.$$

On voit donc que $\hat{g}^{(A)}(u)$ converge uniformément sur \mathbb{R} vers $\hat{g}(u)$ quand $A \rightarrow +\infty$. On peut alors obtenir $\hat{g}^{(A)}(u)$ comme limite de transformées de Fourier discrètes pour certaines valeurs de u . Pour $N \geq 1$, $0 \leq m \leq 2N-1$, on pose

$$g_{2N}^{(A)}[m] = g\left(-A + \frac{mA}{N}\right).$$

On calcule maintenant la transformée de Fourier discrète de $g_{2N}^{(A)}$. On obtient, pour $0 \leq p \leq 2N-1$,

$$\hat{g}_{2N}^{(A)}[p] = \sum_{m=0}^{2N-1} g\left(-A + \frac{mA}{N}\right) e^{-\frac{ipm\pi}{N}}.$$

Soit $u \in \mathbb{R}$. On a $\hat{g}^{(A)}(u) = \int_{-A}^A g^{(A)}(x)e^{-ixu}dx$. La somme de Riemann $S_{2N}(u)$ associée à cette intégrale pour l'échantillonnage ci-dessus est donnée par la formule

$$S_{2N}(u) = \frac{2A}{2N} \sum_{m=0}^{2N-1} g\left(-A + \frac{mA}{N}\right) e^{-i(-A + \frac{mA}{N})u} = \frac{Ae^{iuA}}{N} \sum_{m=0}^{2N-1} g\left(-A + \frac{mA}{N}\right) e^{-\frac{imuA}{N}}.$$

La fonction $\hat{g}_{2N}^{(A)}$ peut être en fait considérée comme une fonction définie sur \mathbb{Z} , périodique de période $2N$. Posons $u_p = \frac{p\pi}{A}$ pour $-N+1 \leq p \leq N$. On obtient

$$S_{2N}(u_p) = S_{2N}\left(\frac{p\pi}{A}\right) = \frac{Ae^{ip\pi}}{N} \hat{g}_{2N}^{(A)}[p] = (-1)^p \frac{A}{N} \hat{g}_{2N}^{(A)}[p].$$

On voit donc qu'une approximation de $\hat{g}\left(\frac{p\pi}{A}\right)$ est donnée pour $-N+1 \leq p \leq N$ par $(-1)^p \frac{A}{N} \hat{g}_{2N}^{(A)}[p]$. La qualité de cette approximation dépend du choix de A et de la possibilité de contrôler la différence $\left|S_{2N}(u_p) - \int_{-A}^A g(x)e^{-ixu_p}dx\right|$. Nous ne discuterons pas cette question ici.

On notera que A étant fixé, plus on augmente N , plus l'ensemble des points où on évalue \hat{f} est étalé. Ceci est lié au "principe d'incertitude en analyse harmonique", dont une forme élémentaire indique que si f n'est pas nulle alors f et \hat{f} ne peuvent être simultanément nulles en dehors d'un intervalle fermé borné. Signalons d'autre part que si $g = g^{(A)}$ pour un certain $A > 0$ on peut reconstituer \hat{g} à partir de la suite $\{\hat{g}\left(\frac{p\pi}{A}\right)\}_{p \in \mathbb{Z}}$, d'après la théorie de l'échantillonnage de Shannon, voir par exemple l'exercice 10 du Chapitre 2 de l'excellent ouvrage de G.Peyré [13]. Nous n'irons pas plus loin dans ce support de cours.

8.7 Exercices sur le Chapitre 8

Exercice 1

1) Démontrer que l'application $\phi_p : \bar{q} \rightarrow \omega_N^{pq}$ est un caractère de $\mathbb{Z}/N\mathbb{Z}$ pour $p \in \mathbb{Z}$, et que le dual de $\mathbb{Z}/N\mathbb{Z}$ est égal à l'ensemble $\{\phi_0, \dots, \phi_{N-1}\}$.

2) En utilisant les notations ci-dessus, écrire les tables de multiplication des groupes duaux de $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$.

Exercice 2

Montrer que l'application $x \rightarrow \phi_y(x)$ est un caractère de \mathbb{F}_2^k pour tout $y \in \mathbb{F}_2^k$, et l'application $y \rightarrow \phi_y$ est un isomorphisme de groupes de $(\mathbb{F}_2^k, +)$ sur $(\hat{\mathbb{F}}_2^k, \cdot)$.

Exercice 3

Soit E un espace topologique, et soient K_1 et K_2 deux sous-ensembles compacts de E . Montrer que $K_1 \cup K_2$ est compact.

Exercice 4

Soit E un ensemble non vide. On dit qu'une application $d : (x, y) \rightarrow [0, +\infty)$ est une distance sur E si et seulement si les deux conditions suivantes sont vérifiées

- (i) $d(x, z) \leq d(x, y) + d(y, z) \quad \forall x, y, z \in E$,
- (ii) $d(x, y) = 0$ si et seulement si $x = y$.

Dans ce cas on dit qu'un ensemble est d -ouvert s'il est vide ou s'il est une réunion d'ensembles de la forme $B_d(x, \epsilon) := \{y \in E \mid d(x, y) = 0\}$. La topologie τ_d associée à la distance d est la topologie associée à la famille \mathcal{U}_{τ_d} formée des ensembles d -ouverts. On dit qu'un espace topologique (E, τ) est métrisable s'il existe une distance d sur E telle que $\tau = \tau_d$.

1) Soient (G_1, o, τ_1) et (G_2, o, τ_2) deux groupes topologiques métrisables et soit $\theta : G_1 \rightarrow G_2$ un homomorphisme de groupes (c'est à dire une application $\theta : G_1 \rightarrow G_2$ telle que $\theta(xoy) = \theta(x)o\theta(y)$ pour tout couple (x, y) d'éléments de E . Montrer que θ est continu si et seulement si $1_{G_2} = \lim_{n \rightarrow \infty} \theta(x_n)$ pour toute suite $(x_n)_{n \geq 1}$ d'éléments de E telle que $1_{G_1} = \lim_{n \rightarrow \infty} x_n$.

2) Soit (G, o, τ) un groupe topologique abélien localement compact.

a) On suppose qu'il existe une suite $(K_n)_{n \geq 1}$ de sous-ensembles compacts de G tels que $G = \cup_{n \geq 1} K_n$. On pose, pour $\phi_1, \phi_2 \in \hat{G}$,

$$d(\phi_1, \phi_2) = \sum_{n=1}^{+\infty} \frac{\min(1, \sup_{x \in \cup_{1 \leq m \leq n} K_m} |\phi_1(x) - \phi_2(x)|)}{2^n}.$$

Vérifier que d est une distance sur \hat{G} , et que la topologie τ_d coïncide avec la topologie de \hat{G} définie dans le cours (en termes savants, cette topologie est la topologie de la convergence uniforme sur tous les compacts de G).

b) Montrer que l'application $\theta_1 : t \rightarrow \phi_t$, où $\phi_t(s) = e^{ist}$ pour $s \in \mathbb{R}$, est une application continue de \mathbb{R} dans $\hat{\mathbb{R}}$ et que l'application réciproque $\theta_1^{-1} : \hat{\mathbb{R}} \rightarrow \mathbb{R}$ est également continue.

Exercice 5

Soit G un groupe abélien fini, et soit H un sous-groupe de G . On suppose que H est strictement contenu dans G . On considère $x \in G \setminus H$.

1) Vérifier que l'ensemble $H(x) := \{x^n y\}_{n \in \mathbb{Z}, y \in H}$ est un sous-groupe de G contenant H et x .

2) Montrer qu'il existe un entier $m \geq 2$ tel que $x^m \in H$.

3) Soit d le plus petit entier ≥ 2 tel que $x^d \in G$. Montrer que tout élément u de $H(x)$ s'écrit de manière unique sous la forme $u = x^n y$, avec $0 \leq n \leq d-1$, $y \in H$.

4) Soit χ un caractère de H , et soient $\alpha_1, \dots, \alpha_d$ les d solutions complexes de l'équation $z^d = \chi(x^d)$. Pour $1 \leq j \leq d$, $u = x^n y \in H(x)$, avec $0 \leq n \leq d-1$, on pose

$$\chi_j(u) = \alpha_j^n \chi(y).$$

Montrer que χ_j est un caractère de $H(x)$ dont la restriction à H coïncide avec χ . En déduire que si $|\hat{H}| = |H|$, alors $|H(x)| = |H(x)|$.

5) Déduire de ce qui précède que $|\hat{G}| = |G|$ pour tout groupe abélien fini G .

Exercice 6

Soit G un groupe abélien fini possédant n éléments.

1) En utilisant la définition de la convolution sur $\mathbb{C}(G)$ et la définition de la transformée de Fourier sur $\mathbb{C}(G)$, montrer que la transformée de Fourier de $f * g$ est égale au produit des transformées de Fourier de f et de g pour $f, g \in \mathbb{C}(G)$.

2) En utilisant le fait que \hat{G} forme une base orthonormale de $C(G)$ pour le "produit hermitien" de $\mathbb{C}(G)$, démontrer les formules de Plancherel et Parseval sur $\mathbb{C}(G)$.

3) En utilisant de nouveau le fait que \hat{G} forme une base orthonormale de $C(G)$ pour le "produit hermitien" de $\mathbb{C}(G)$, démontrer que ${}^t\bar{A}_G A_G = nI_n$, où I_n est la matrice unité à n lignes et n colonnes.

En déduire la formule d'inversion de Fourier pour $\mathbb{C}(G)$.

Exercice 7

Soit G un groupe abélien fini. On se propose de démontrer le *principe d'incertitude discret*, qui dit que l'on a, pour toute fonction $f \in \mathbb{C}(G)$ non nulle

$$|\text{Supp}(f)| \times |\text{Supp}(\hat{f})| \geq |G|. \quad (8.16)$$

1) Vérifier ce résultat directement dans le cas où $G = \mathbb{Z}/2\mathbb{Z}$.

2) On revient au cas d'un groupe abélien fini G quelconque. Soit $f \in \mathbb{C}(G)$, et soit $M = \sup_{x \in G} |f(x)|$. On pose $\|f\| = \sqrt{\langle f, f \rangle}$, de sorte que $\|f\|^2 = \frac{1}{|G|} \sum_{x \in G} |f(x)|^2$. Montrer que l'on a

$$\|f\|^2 \leq \frac{M^2}{|G|} |\text{Supp}(f)| \quad \text{et} \quad M \leq \frac{1}{|G|} \sum_{\chi \in \hat{G}} |\hat{f}(\chi)|.$$

En utilisant l'inégalité de Cauchy-Schwartz, en déduire que

$$M^2 \leq \frac{|Supp(f)|}{|G|} \|\hat{f}\|^2, \quad \text{puis} \quad M^2 \leq \|\hat{f}\|^2 |Supp(\hat{f})|.$$

En déduire le principe d'incertitude discret.

3) Soit H un sous-groupe de G , et soit f_H sa fonction caractéristique, définie par la formule $f_H(x) = 1$ si $x \in H$, $f_H(x) = 0$ sinon. On pose

$$H^\perp = \{\chi \in \hat{G} \mid \chi(x) = 1 \quad \forall x \in H\}.$$

Montrer que l'on a $\hat{f} = |H| f_{H^\perp}$, et en déduire que $|Supp(f_H)| \times |Supp(\hat{f}_H)| = |G|$.

Exercice 8

Soit f une fonction continue, périodique de période 1, et intégrable sur $[0, 1]$. On pose $\tilde{f}(x) = f(-x)$ pour $x \in \mathbb{R}$. Avec les notations de la formule 8.15, montrer que l'on a, pour $p \leq 0$,

$$\hat{f}(p) = \lim_{N \rightarrow \infty} \frac{(\tilde{f})_N(-p)}{N}.$$

Bibliographie

- [1] Archimède : *Eureka*, Communication orale, Syracuse (vers l'an -215).
- [2] C. Bachoc. Mathématiques discrètes de la transformée de Fourier, Cours de Master CSI, Université Bordeaux 1, 2005.
- [3] E.O.Brigham, Fast Fourier Transform and its applications, Prentice Hall, Englewood Cliffs, 1988.
- [4] L. Carleson, *On convergence and growth of partial sums of Fourier series*, Acta Mathematica **116** (1966), 135-157.
- [5] X.Dussau, J.Esterle, F.Zarouf et R.Zarouf, Cours d'algèbre, ESTIA, 2006.
- [6] X.Dussau, J.Esterle, F.Zarouf et R.Zarouf, Cours d'algèbre linéaire, ESTIA, 2003.
- [7] X.Dussau, J.Esterle, O.Réjasse et F.Zarouf, Analyse élémentaire, ESTIA, 2003.
- [8] J.Esterle, J.Giol et O.Réjasse, Courbes, surfaces et calcul différentiel, ESTIA, 2004.
- [9] G.Fenez et R. Ismais, Applications de la transformée de Fourier au traitement des images numériques, TER, Master Crypto 1, Bordeaux, 2006.
- [10] E.L.Jury, Theory and application of the z -transform method, Robert E. Krieger Publishing Company, Malabar, Florida, 1964.
- [11] Le Moal et Ponsonnet, Transformée de Walsh et FFT appliquées au traitement du signal et de l'image, TER, Master Crypto 1, Bordeaux, 2006.
- [12] F.Luthon, Initiation au traitement de signal, IUT Informatique, Chateau Neuf, Place Paul Bert, 64100, Bayonne, 2004.
- [13] G.Peyré, L'algèbre discrète de la transformée de Fourier, Collection Mathématiques à l'Université, Ellipses, 2004.
- [14] W.H.Press et Al, Numerical Recipes in C : the Art of Scientific Computing, Cambridge University Press, Cambridge, 1988.
- [15] D. N. Rockmore, *The FFT : an algorithm the whole family can use* , Computing in Science and Engineering 2 (2000), 60-64.
- [16] W. Rudin, Fourier analysis on groups, Interscience Publishers, 1962.

Index

- $L^2(\mathbb{R})$, 17
- $L^2(\mathbb{R}^k)$, 28
- $L^1(G)$, 114
- $L^1(g)$, 115
- $L^2(G)$, 114, 116
- $L^2(\hat{G})$, 116
- $L^1(R)$, 11
- $L^1(\mathbb{R})$, 13–15, 31, 38, 39
- $L^1(\mathbb{R}^k)$, 25, 26
- $L^1_{loc}(\mathbb{R}^+)$, 38
- $L^2(\mathbb{R})$, 13, 16, 17
- $L^2(\mathbb{R}^k)$, 27
- $L^\infty(\mathbb{R})$, 13
- $L^\infty(\mathbb{R}^k)$, 25
- $\mathbb{Z}/p\mathbb{Z}$, 64
- $\mathcal{C}_0(G)$, 114
- $\mathcal{C}_c(G)$, 116
- $\mathcal{C}_0(\mathbb{R})$, 13, 15
- $\mathcal{C}_0(\mathbb{R}^k)$, 25
- $\mathcal{E}(\mathbb{R})$, 14–16
- $\mathcal{E}(\mathbb{R}^k)$, 25
- $\mathcal{L}(f)$, 37, 38
- \mathbb{F}_p , 64
- échantillonnage, 123
- échantillonnage, 58
- équation différentielle, 16, 42

- théorème de convergence dominée, 12
- $L^1(\mathbb{R})$, 17, 37
- $L^1_{loc}(\mathbb{R}^+)$, 38
- $\text{Dom}(\mathcal{L}(f))$, 37
- méthode de Simpson, 2
- série entière, 52
- théorème de convergence monotone, 12
- transformée de Fourier, 38

- associativité de la convolution cyclique, 91
- axiome du choix, 4

- Borel, 4
- borné, 3, 21, 22, 27

- Carleson, 17
- Cauchy-Schwartz, 24
- coefficient de Fourier, 54
- commutativité de la convolution cyclique, 91
- compression d'images, 81
- convolution, 14, 15, 26, 27, 38
- convolution acyclique, 91
- convolution cyclique, 91
- convolution sur \mathbb{N} , 55
- Cooley et Tukey, 91
- cours d'algèbre linéaire, 43
- cours d'algèbre, 42
- Cours d'algèbre linéaire, 69
- cours d'algèbre linéaire, 43
- Cours d'Analyse, 42
- critère de Cauchy, 36

- décimation fréquentielle, 91, 94–97
- décimation temporelle, 91, 93, 97, 99
- décomposition d'une fonction booléenne en somme de moômes, 84
- dérivée partielle, 25, 27
- diagonalisable, 43
- distance aux fonctions affines, 66
- distance d'une fonction booléenne à une fonction affine, 68
- distance de deux fonctions booléennes, 66
- diviser pour régner, 63

- Dom($\mathcal{L}(f)$), 36, 39
- Dom($\mathcal{L}(f)$), 36
- domaine de convergence absolue de la transformée en Z , 52
- domaine de convergence absolue de la transformée en Z bilatérale, 51
- domaine de convergence absolue de la transformée en Z unilatérale, 56
- domaine de convergence de la transformée en Z , 52
- domaine de convergence de la transformée en Z bilatérale, 51
- domaine de convergence de la transformée en Z unilatérale, 56

- effet papillon, 63
- ensemble compact, 108
- ensemble fermé, 107
- ensemble ouvert, 107
- espace de Banach, 14, 26
- espace de Fréchet, 14, 26
- espace normé, 14
- espace topologique, 107

- Fast Fourier Transform, 91
- Fatou, 17
- Fefferman, 17
- fermé, 3, 21
- FFT, 91
- filtrage de signaux, 54
- Fischer, 2
- fonction de transfert d'un filtre récursif causal, 57
- fonction holomorphe, 54
- fonctions affines, 70
- fonctions affines d'ordre k , 66
- fonctions booléennes, 64, 84
- fonctions courbes, 70, 84
- formule d'inversion de Fourier, 15, 17, 19, 28, 37, 62, 88, 115
- formule d'inversion de la transformée en Z unilatérale, 56
- formule de Leibnitz, 16
- formule de Parseval, 17, 19, 20, 28, 66, 69, 88, 115, 117, 119
- formule de Plancherel, 17, 28, 88, 115, 117
- Fraenkel, 4
- groupe compact, 112
- image numérisée, 81
- inégalité de Cauchy-Schwartz, 6, 17
- input, 55
- intégrable, 5–8, 11, 13, 14, 17, 23, 25, 27, 30
- intégrable sur \mathbb{R} , 6
- intégrale curviligne, 54
- intégrale de Riemann, 1, 2, 6, 9
- intégrale de Riemann généralisée, 8, 9
- intégrale de Riemann généralisée, 8, 11, 39
- inversion de Fourier, 27, 28

- Lacey et Thiele, 17
- le nombre j des mathématiciens, 89
- le nombre j des physiciens, 89
- Lebesgue, 2–4, 7, 9, 11

- méthode des rectangles, 2
- méthode des trapèzes, 2
- matrice conjuguée, 87
- matrice de changement de base, 84
- matrice de Fourier, 87
- matrice de Walsh, 61, 83, 84
- mesurable, 3–7, 13, 22, 23, 27–30, 35
- mesure, 3, 7, 9
- mesure de Haar, 113
- monôme, 84
- monôme, 65
- Mupad, 43, 49, 73, 83

- nombre de changements de signe, 70
- ordre de multiplicité, 16
- output, 55
- ouvert, 3, 21
- partition, 1, 2

- pixel, 81
- polynôme caractéristique, 42, 43, 84
- presque partout, 6, 7, 13, 15, 25, 27, 38
- réarrangement par changements de signe, 70
- rayon de convergence d'une série entière, 51, 52
- série absolument convergente, 51, 56
- série convergente, 56
- série de Fourier, 9
- série entière, 51
- série produit, 56
- séries de Fourier, 54
- Solovay, 4, 5
- somme de Riemann, 2
- sommes de Riemann, 123
- symbole de Kronecker, 56
- système différentiel linéaire, 42
- système différentiel linéaire, 41
- table des transformées en Z unilatérales, 56
- théorème de Fubini, 30
- théorème de convergence dominée, 8, 11, 24, 37
- théorème de convergence monotone, 9, 25
- théorème de dualité de Pontryagin, 109
- théorème de Fubini, 21, 28–30
- théorème de Fubini, 33
- théorème de Schwarz, 32
- théorème des accroissements finis, 37
- topologie discrète, 110, 112
- topologie induite, 108
- topologie sur un ensemble, 107
- transformée de Fourier, 13–17, 26, 27, 62
- transformée de Fourier discrète, 87, 123
- transformée de Fourier inverse, 97
- transformée de Laplace, 35–37, 41, 42, 45
- transformée de Walsh, 61, 66, 81, 123
- transformée de Walsh inverse, 62
- transformée de Walsh rapide, 63, 72, 73
- transformée en Z unilatérale, 55
- Zermelo, 4