Université Bordeaux I

Masters CSI et Théorie du Signal

Année 2008-2009

Analyse de Fourier

J. Esterle

Table des matières

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 $\sigma = (x_0, \ldots, x_n)$ telles que $a = x_0 < x_1 < \ldots < x_n = b$. 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 :

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

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[**?**] 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)

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

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 $(a_n)_{n\ge0}$ et $(b_n)_{n\ge0}$ sont deux suites de réels telles que les séries $\sum_{n\ge0}|a_n|^2$ et $\sum_{n\ge1}|b_n|^2$ soient convergentes.

Une réponse à ces questions à 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

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

Definition 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 $lim_{n\to+\infty} m(E_n) =$
$lim_{n\to+\infty} m(F_n)$, et dans ce cas on pose

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

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

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

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* $m(\cup_{n\geq 1}A_n) = lim_{n\to+\infty}m(A_n)$.

(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* $m(\cap_{n\geq 1}A_n) = lim_{n\to+\infty}m(A_n)$.

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'enonce 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* $\phi : \mathcal{P}(X) \to X$ *telle que* $\phi(A) \in A \ \forall A \in \mathcal{P}(X)$.

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 consistent 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

Definition 1.2.1. *On dit que* $f : \mathbb{R} \to \mathbb{R}$ *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 $f(x) = \lim_{n\to+\infty} f_n(x)$ 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 $x \neq E$. On dit qu'une fonction f est une *fonction en escalier* s'il existe une famille finie $E_1, \ldots, E_p$ d'ensembles mesurables de mesure finie et une famille $c_1, \ldots, c_p$ 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 $E_1, \ldots, E_p$ 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

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

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

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

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 $f(x) = lim_{n \to +\infty} f_n(x)$ pour tout $x \in \mathbb{R}$, et que la valeur (finie ou infinie) de $\lim_{n \to +\infty} \int_{\mathbb{R}} f_n(t)dt$ est indépendante du choix de la suite $(f_n)_{n \geq 1}$. Nous admettrons ces résultats.

Definition 1.2.3.

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

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

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 .

Definition 1.2.4. *Soit $E \subset \mathbb{R}$ un ensemble mesurable, soit $f : E \to \mathbb{C}$ une fonction et soit $\tilde{f} : \mathbb{R} \to \mathbb{C}$ 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

$$\int_E (\lambda f(t) + \mu g(t))dt = \lambda \int_E f(t)dt + \mu \int_E g(t)dt. \tag{1.6}$$

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

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

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) L'ensemble $\{x \in E \mid f(x) \neq g(x)\}$ 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) $lim_{n\to+\infty} f_n(t) = f(t)$ 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 $\int_E f(t)dt = lim_{n\to+\infty} \int_E f_n(t)dt$.

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 $\hat{f}(x) = \lim_{n\to+\infty} \hat{f}(x_n)$ 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 $x = \lim_{n\to+\infty} x_n$. 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)

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

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

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

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 $f(t) := lim_{n\to+\infty} f_n(t)$ soit finie pour presque tout $t \in E$. Alors on a*

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

Notons que dans le cas où $\lim_{n\to+\infty} \int_E f_n(t)dt = +\infty$, 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 $L \to +\infty$, et dans ce cas on pose $\int_a^{+\infty} f(t)dt = lim_{L\to+\infty} \int_a^L f(t)dt$. 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 $L \to +\infty$ 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 $f(t) = \lim_{n\to+\infty} f_n(t)$ 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 $\lim_{n\to+\infty} \int_a^n f(t)dt = +\infty$, que f est intégrable au sens de Lebesgue sur $[a, +\infty[$ si la suite
($\lim_{n\to+\infty} \int_a^n f(t)dt)_{n\geq 1}$ est convergente, et que dans ce cas on a, avec les notations du Corollaire

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

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

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 $m(E_2)$.

exercicez 3(Annales ESTIA, examens Transformées 2000 et 2001)
Soit $f \in L^1(\mathbb{R})$. On pose , pour $x \in \mathbb{R}$

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

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

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 $t \in \mathbb{R}$

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

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 $\lim_{t\to+\infty} F(t) = 0$.

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 $\lim_{x\to+\infty} G(x) = 0$.
3) Que peut-on dire du comportement de $G(x)$ quand $x \to -\infty$?

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 $\lim_{x\to1^+} F(x)$.

2-c) Déterminer $\lim_{x\to+\infty} F(x)$.
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 $\int_E \left[\sum_{n\geq 1} f_n(t)\right] dt = +\infty$, alors la série $\sum_{n\geq 1} \left[\int_E f_n(t)\right] dt$ est divergente, et que si
$\int_E \left[\sum_{n\geq 1} f_n(t)\right] dt < +\infty$, alors la série $\sum_{n\geq 1} \left[\int_E f_n(t)dt\right]$ 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 $\sum_{n\geq 1} \left[\int_E |f_n(t)|dt\right]$ 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

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

4) $\mathcal{C}_0(\mathbb{R})$ désigne l'ensemble des fonctions continues sur $\mathbb{R}$ telles que $\lim_{|t|\to+\infty} f(t) = 0$. 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 $f^{(0)} = f$,
$\lim_{|t|\to+\infty}|t|^p|f^{(q)}(t)| = 0 \ \ \forall p \geq 1, \forall q \geq 0.$

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

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

(2.2) $\|\lambda f\|_i = |\lambda|\|f\|_i$ pour toute fonction f et pour tout nombre complexe λ,

(2.3) $\|f\|_i \geq 0$ pour toute fonction f, et $\|f\|_i \neq 0$ 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 $\lim_{n\to+\infty} sup_{p\geq n, q\geq n}\|x_p - x_q\|_i = 0$, alors il existe un élément x de l'espace tel que $\lim_{n\to+\infty}\|x - x_n\|_i = 0$. 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 $t \longmapsto f(x - t)g(t)$ 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) $f * g = g * f \quad \forall f \in L^1(\mathbb{R}), \quad \forall g \in L^1(\mathbb{R}).$

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

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

Definition 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 appellée la transformée de Fourier de f, et l'application $\mathcal{F} : f \longmapsto \hat{f}$ 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 $\mathcal{F} : \mathcal{E}(\mathbb{R}) \longrightarrow \mathcal{E}(\mathbb{R})$ 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 $\mathcal{F} : L^1(\mathbb{R}) \longrightarrow \mathcal{C}_0(\mathbb{R})$ est **injective**. Par contre on peut montrer que $\mathcal{F} : L^1(\mathbb{R}) \longrightarrow \mathcal{C}_0(\mathbb{R})$ **n'est pas surjective** : il existe des fonctions $g \in \mathcal{C}_0(\mathbb{R})$ qui ne coincident 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 $\hat{f}.\hat{g} = \hat{h}$, 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

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

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

Posons $p(x) = a_n x^n + \ldots + a_1 x + a_0$ (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 $x \longmapsto \frac{\hat{h}(x)}{p(ix)}$ appartient à $\mathcal{E}(\mathbb{R})$, et l'unique solution f de l'equation 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 $(i\alpha_1, \ldots, i\alpha_k)$. Pour $1 \leq j \leq k$ soit m_j l'ordre de multiplicité de $i\alpha_k$, 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 on a, avec la convention $\hat{h}^{(0)} = \hat{h}$,

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

Réciproquement si la condition ci-dessus est satisfaite, on peut vérifier que la fonction $t \longmapsto \frac{\hat{h}(t)}{p(it)}$ 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 $t \longmapsto f(t)e^{-\alpha|t|}$ 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 $lim_{\alpha\to 0^+} \int_{-\infty}^{+\infty} f(t)e^{-itx-\alpha|t|}dt$ et $lim_{R\to+\infty} \int_{-R}^{R} f(t)e^{-itx}dt$ 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.

Definition 2.2.2. *Pour $f \in L^2(\mathbb{R})$, on définit $\hat{f}$ presque partout sur $\mathbb{R}$ par la formule*
$\hat{f}(x) = lim_{\alpha\to 0^+} \int_{-\infty}^{+\infty} f(t)e^{-itx-\alpha|t|}dt$ = $lim_{R\to+\infty} \int_{-R}^{R} f(t)e^{-itx}dt$

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

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

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

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 $\mathcal{F} : f \longmapsto \hat{f}$ 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

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

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

Nous terminons cette brève présentation par un exemple. On définit le **sinus cardinal** par la formule

$$sin_c(t) = \frac{sin(t)}{t},$$

avec la convention $sin_c(0) = 1$. On a donc le développement en série entière

$$sin_c(t) = \sum_{n=0}^{+\infty} \frac{t^{2n}}{(2n+1)!}.$$

On définit la **fonction porte** d'ordre a par la formule

$$p_a(t) = 0 \text{ si } |t| > a, p_a(t) = 1 \text{ si } t \in [-a, a].$$

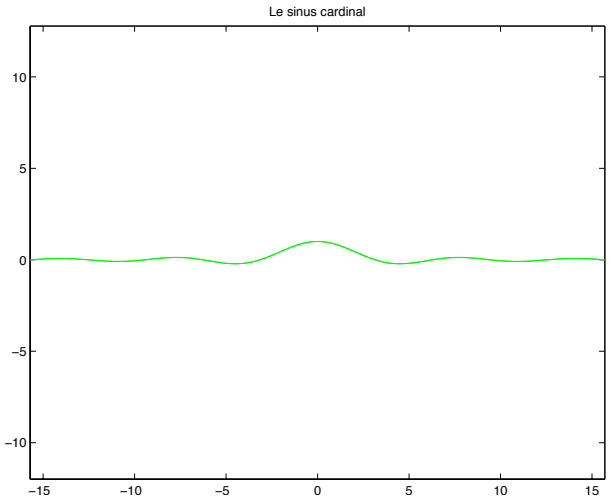
Un calcul simple donne

$$\widehat{p_a}(x) = \int_{-a}^{a} e^{-itx} dx = \left[\frac{e^{-itx}}{-ix}\right]_{-a}^{a} = \frac{e^{iax} - e^{-iax}}{ix} = 2asin_c(ax).$$

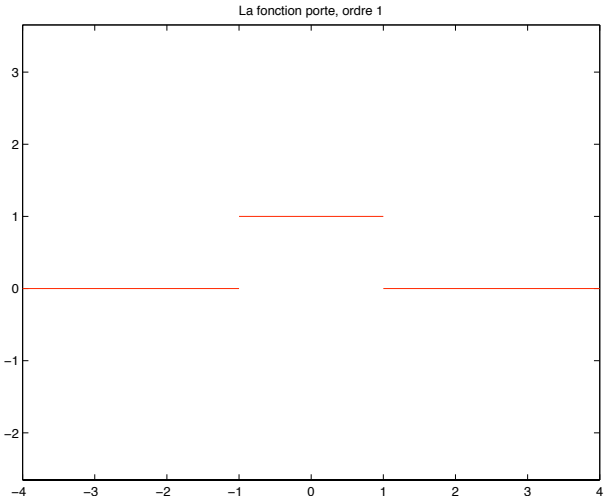
En pratique on est souvent amené à "tronquer" les fonctions, ce qui revient à les multiplier par une fonction porte d'ordre a, avec a assez grand. Au niveau de la transformée de Fourier, ceci revient à remplacer la transformée de Fourier de la fonction donnée par son produit de convolution avec $2asin_c(ax)$.

On illustre cet exemple par des graphiques. On trace sous Matlab le graphe du sinus cardinal et de la fonction porte d'ordre 1.

```
>> x=[-5*pi:0.01:5*pi];y=sin(x)./x;
 plot(x,y,'green');hold on;axis equal;
 title('La fonction sinus cardinal');
 print -depsc sincard
```

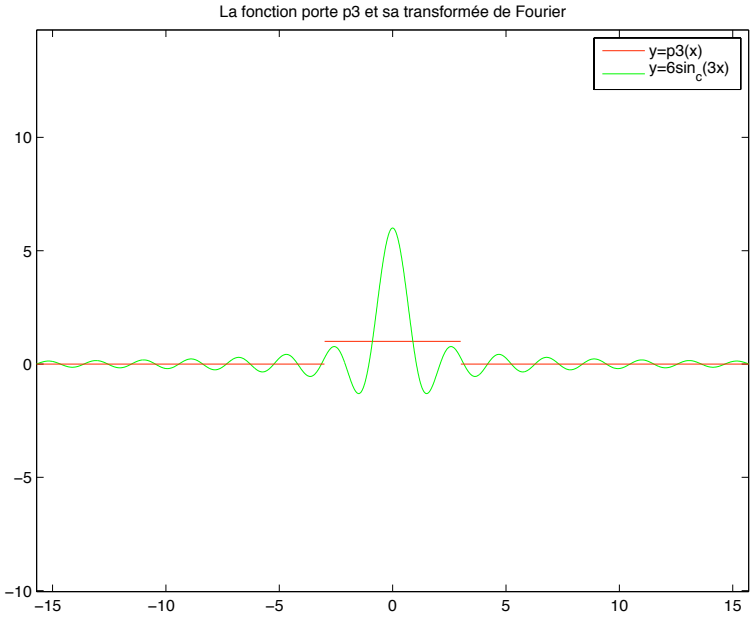



```
x0=[-1:0.01:1];y0=polyval(p,x0);
q=[0];x1=[-4:0.01:-1];x2=-x1;y1=polyval(q,x1);
y2=polyval(q,x2);plot(x0,y0,'red');hold on;
plot(x1,y1,'red');hold on; plot(x2,y2,'red');hold on;axis equal
title('La fonction porte, ordre 1');print -depsc fonctionporte
```



On trace aussi le graphe de la fonction porte p_3 d'ordre 3, ainsi que celui de sa transformée de Fourier $\widehat{p_3}$ (on a $\widehat{p_3}(x) = 6sin_c(3x)$)).

```
p=[1];x0=[-3:0.01:3];y0=polyval(p,x0);x1=[-5*pi:0.01:-3];
q=[0];y1=polyval(q,x1);x2=-x1;y2=polyval(q,x2);x3=[-5*pi:0.01:5*pi];
y3=2*sin(3*x3)./x3;plot(x0,y0,'red');hold on;plot(x3,y3,'green');hold on;
plot(x1,y1,'red');hold on; plot(x2,y2,'red');hold on;axis equal;
legend('y=p3(x)','y=6sin_c(3x)');
title('La fonction porte p3 et sa transformée de Fourier')
print -depsc p3
```



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 $u_m = \frac{(2m)!}{2^m (m!)} u_0$ 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 $\hat{f}(x) = \lim_{p \to +\infty} \int_{-\infty}^{+\infty} F_{p,x}(t) e^{-\frac{t^2}{2}} dt$.
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 $t \in R$

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

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

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

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 $g = f * \tilde{f}$. Vefifier 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

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

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 l'identité de Parseval).

Chapitre 3

Groupes, Anneaux, Corps

3.1 Groupes

Nous commencons par rappeler des définitions classiques

Definition 3.1.1. *Un groupe est une ensemble non vide G muni d'une loi de composition interne $(x, y) \longmapsto x \circ y$ possédant les propriétés suivantes*
(1.1) $x \circ (y \circ z) = (x \circ y) \circ z$ pour tout triplet (x, y, z) d'éléments de G.
(1.2)Il existe un élément e de G tel que $x \circ e = e \circ x = x$ pour tout $x \in G$.
(1.3)Pour tout $x \in G$, il existe $y \in G$ tel que $x \circ y = y \circ x = e$.

On dira qu'une loi de composition interne sur un ensemble E vérifiant la condition (1.1) est *associative*. Si $(G, \circ)$ est un groupe , l'élément e de G vérifiant la condition (1.2) ci-dessus est appelé *élément neutre* de G. On vérifie (exercice) que cet élément neutre est unique. L'élément y de G tel que $x \circ y = y \circ x = e$ est appelé *inverse* de x. Il est également unique. On vérifie plus généralement (exercice) que si $(E, \circ)$ est un ensemble muni d'une loi de composition associative pour laquelle il existe un élément neutre e, et si trois éléments x, y_1 et y_2 de E vérifient $x \circ y_1 = y_2 \circ x = e$ alors $y_1 = y_2$.

Definition 3.1.2. *On dit qu'un groupe $(G, \circ)$ est commutatif , ou abélien , si on a la condition suivante*
(1.4) $x \circ y = y \circ x$ pour tout couple (x, y) d'éléments de G.

La loi de composition d'un groupe abélien G sera souvent notée $+$. Dans ce cas l'élément neutre de G sera noté 0 , et l'inverse d'un élément x de G sera noté $-x$ et appelé l'*opposé de x.*

Exemple 3.1.3. *Notons $\mathbb{Z}$ l'ensemble des entiers relatifs , $\mathbb{Q}$ l'ensemble des rationnels , $\mathbb{R}$ l'ensemble des réels et $\mathbb{C}$ l'ensemble des nombres complexes. Alors $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens.*

Exemple 3.1.4. *Soit $p \geq 2$ un entier. Pour $0 \leq a \leq p-1$ on pose $\bar{a} = \{a + pn\}_{n \in \mathbb{Z}}$, et on pose $\bar{a} + \bar{b} = \bar{r}$ où r est le reste de la division de $a + b$ par p (d'après le cours de CM1 , on a bien $0 \leq r \leq p-1$). On vérifie que $(\mathbb{Z}/p\mathbb{Z}, +)$ est un groupe abélien.*

On peut illuster ceci par les tables d'addition de $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Ces deux exemples sont un cas particulier de la théorie des *groupes quotient* que nous présenterons un peu plus loin.On notera que la nature mathématique exacte des éléments $\bar{0}, \bar{1}, \ldots, p-\bar{1}$ de $\mathbb{Z}/p\mathbb{Z}$ ne joue guère de rôle en pratique.Ce qui compte est de pouvoir utiliser la table de l'addition(à laquelle on ajoutera plus loin une table de multiplication)

On peut également utiiser la notation multiplicative pour certains groupes abéliens ou non.On note alors $x.y$ au lieu de $x \circ y$. L'élément unité est noté 1 (ou I s'il s'agit de matrices) , et l'inverse de $x \in G$ est noté x^{-1} (la notation x^{-1} est utilisée dans tous les cas où la loi du groupe n'est pas notée additivement).

On notera $\mathbb{Q}^*$ l'ensemble des rationnels non nuls. On notera de même $\mathbb{R}^*$ l'ensemble des réels non nuls et $\mathbb{C}^*$ l'ensemble des nombres complexes non nuls.On pose d'autre part $\Gamma = \{z \in \mathbb{C} \mid |z| = 1$. Le produit de deux éléments x et y de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ sera noté $x.y$ (ou xy si aucune confusion n'est à craindre).

Exemple 3.1.5. $(\mathbb{Q}^*, .)$ *,* $(\mathbb{R}^*, .)$ *,* $(\mathbb{C}^*, .)$ *et* $(\Gamma, .)$ *sont des groupes abéliens pour le produit usuel.*

L'ensemble $Gl(2, \mathbb{R})$ *des matrices à deux lignes et deux colonnes à coefficients réels de déterminant non nul est un groupe non abélien pour le produit matriciel(dont la définition est rappellée plus loin).*

Notons que si $(G, \circ)$ est un groupe , on a les propriétés suivantes (exercice facile)

$$(1.5) \quad (x^{-1})^{-1} = x \qquad \forall x \in G.$$

$$(1.6) \quad (xy)^{-1} = y^{-1} \circ x^{-1} \qquad \forall x, y \in G.$$

Une notion importante en théorie des groupes est la notion de sous-groupe,
donnée par la définition suivante.

Definition 3.1.6. *Soit* $(G, \circ)$ *un groupe.On dit qu'une partie* H *de* G *est un sous-groupe de* G *si les deux conditions suivantes sont vérifiées*

(i) H *est non vide , et* $x \circ y \in H$ *pour tout couple* (x, y) *déléments de* H.

(ii) $(H, \circ)$ *est un groupe.*

La proposition suivante est utile pour éviter des vérifications fastidieuses.

Proposition 3.1.7. *Soit $(G, \circ)$ un groupe et soit $H \subset G$. Les deux conditions suivantes sont équivalentes*

(i) H est un sous-groupe de G.

(ii) H est non vide ,et $a \circ b^{-1} \in H$ pour tout couple (a, b) d'éléments de H.

Démonstration : Il est clair que tout sous-groupe de G vérifie (ii).Réciproquement soit $H \subset G$ vérifiant (ii) , et soit $a \in H$. On a $e = a \circ a^{-1} \in H$, donc H contient l'élément neutre e de G.On a $b^{-1} = e \circ b^{-1} \in H$ pour tout $b \in H$. Enfin d'après la propriété 1.6 on $a \circ b = a \circ (b^{-1})^{-1} \in H$ pour tout couple (a, b) d'éléments de H. ♣

3.2 Groupes cycliques, groupes quotient

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

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

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

On rappelle le théorème de Lagrange :

Théorème 3.2.1. *L'ordre d'un sous-groupe est un diviseur de l'ordre du groupe. En particulier, l'ordre d'un élément d'un groupe divise l'ordre de ce groupe.*

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

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

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

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

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

– Si $(m, n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$

Le nombre $\varphi(n)$ est aussi (presque par définition) le nombre d'éléments du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ formé des éléments de Z/nZ inversibles pour la multiplication.

Proposition 3.2.2. *Tout sous-groupe et tout quotient d'un groupe cyclique est aussi cyclique. Pour tout diviseur d de l'ordre d'un groupe cyclique, il existe dans ce groupe un unique sous-groupe d'ordre d, et ce groupe contient exactement $\varphi(d)$ éléments d'ordre d.*

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

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

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

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

Exemple : Tout groupe d'ordre premier est cyclique.

Soient $(G, \circ)$ et $(H, \circ)$ deux groupes.

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

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

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

La notion de quotient est plus subtile, nous la rappelons dans le cas des groupes commutatifs (dans le cas non commutatif il faut la notion de sous-groupe distingué). Si G est un groupe commutatif, et si H est un sous-groupe de G, on construit un troisième groupe noté G/H, appelé quotient de G par H, de la façon suivante (on note G additivement) :

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

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

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

Par exemple si $G = \mathbb{Z}$, $H = n\mathbb{Z}$, on obtient le groupe quotient $(\mathbb{Z}/n\mathbb{Z}, +)$ déjà vu plus haut.

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

Théorème 3.2.3 (Théorème de factorisation)**.** *Soit $f : G \to H$ un homomorphisme de G dans H. Soit $K = \ker(f)$ et soit $\pi : G \to G/K$ la surjection canonique. On définit*

une application $\overline{f} : G/K \to H$ *par :* $\overline{f}(\pi(x)) = f(x)$. *Alors* $\overline{f} = G/K \to H$ *est un homomorphisme injectif, qui définit un un isomorphisme de* G/K *sur* $Im(f)$.

Démonstration : Si $\pi(x) = \pi(y)$ on a$x + K = y + K$, donc $y \in x + K$, il existe $z \in K = Ker(f)$ tel que $y = x + z$ et $f(y) = f(x)$. Donc $\overline{f}$ est bien définie. On a $\overline{f}(\pi(x) + \pi(y)) = \overline{f}(\pi(x + y)) = f(x + y) = f(x) + f(y) = \overline{f}(\pi(xp) + \overline{f}(\pi(y)$, donc $\overline{f} : G/K \to G$ est un homomorphisme. Si $\overline{f}(\pi(x)) = 0$, on a $f(x) = 0, x \in Ker(f) = K$, donc $\pi(x) = 0$, $Ker(\overline{f}) = \{0\}$, et $\overline{f}$ est injectif. Il est clair que $Im(f) = Im(\overline{f})$ et $\overline{f}$ définit un isomorphisme de G/K sur $Im(f)$. □

3.3 Anneaux

On va maintenant s'intéresser aux ensembles munis de deux lois de composition interne.

Definition 3.3.1. *Soit* $(A, +, .)$ *un ensemble non vide possédant au moins deux éléments muni de deux lois de composition internes. On dit que* $(A, +, .)$ *est un anneau si les conditions suivantes sont vérifiées*

(i) $(A, +)$ *est un groupe abélien.*

(ii) $x.(y + z) = x.y + x.z$*et* $(y + z).x = y.x + z.x$ *pour tout triplet* (x, y, z) *d' éléments de* A.

(iii) $x.(y.z) = (x.y).z$ *pour tout triplet* (x, y, z) *d' éléments de* A.

(iv) Il existe un élément 1 *de* A *tel que* $x.1 = 1.x = x$ *pour tout* $x \in A$.

On dit qu'un anneau $(A, +, .)$ *est commutatif si on a de plus la propriété suivante*

(v) $x.y = y.x$ *pour tout couple* (x, y) *d'éléments de* A.

Pour éviter d'alourdir les notations on écrira "l'anneau A" au lieu de "l'anneau $(A, +, .)$" quand aucune confusion n'est à craindre.De même on écrira souvent xy au lieu de $x.y$.L'élément noté 1 dans la définition ci dessus est appellé *unité* de l'anneau A. On dit qu'un élément x de A est inversible s'il existe $y \in A$ tel que $xy = yx = 1$. Cet élément y , appelé *inverse de* x ,est alors noté x^{-1}. La formule 1.6 reste valable dans ce contexte , et on vérifie (exercice) que $(Inv(A), 1)$ est un groupe , $Inv(A)$ désignant l'ensemble des éléments inversibles d'un anneau A.

Il est clair que $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$, $(\mathbb{C}, +, .)$ sont des anneaux commutatifs. On peut également munir $\mathbb{Z}/p\mathbb{Z}$ d'une structure d'anneau commutatif naturelle

Exemple 3.3.2. *Soit* $p \geq 2$ *un entier. Pour* $0 \leq a \leq p - 1, 0 \leq b \leq p - 1$ *, on pose* $\bar{a}.\bar{b} = r$ *où* r *désigne le reste de la division de* $a.b$ *par* p. *Alors* $(\mathbb{Z}/p\mathbb{Z}, +, .)$ *est un anneau commutatif.*

Nous illustrons ceci en donnant les tables d'addition et de multiplication de $\mathbb{Z}/4\mathbb{Z}$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Soit maintenant $\mathcal{M}(2,\mathbb{R})$ l'ensemble des matrices carrées à deux lignes et deux colonnes à coefficients réels.On pose

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} . \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

Exemple 3.3.3. *$(\mathcal{M}(2,\mathbb{R}),+,.)$ est un anneau non commutatif qui a pour unité $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.*

Soit n un entier positif.On pose $C_n^0 = 1, C_n^1 = n$, et $C_n^p = \frac{n(n-1)...(n-p+1)}{p!}$ pour $2 \leq p \leq n$. Si A est un anneau , et si $ab = ba$, avec $a, b \in A$, on a , avec la convention $a^0 = b^0 = 1$, la *formule du binôme de Newton*

$$(1.7) \qquad (a+b)^n = \sum_{0 \leq p \leq n} C_n^p a^p b^{n-p}$$

On peut introduire la notion de sous-anneau, mais elle joue un rôle moins important que la notion de sous-groupe.Pour les anneaux commutatifs la notion importante est la notion d'*idéal* , que nous détaillerons pour les anneaux de polynômes.

3.4 Corps

Nous introduisons une dernière notion importante.

Definition 3.4.1. *Soit $(K,+,.)$ un ensemble muni de deux lois de composition internes.On dit que $(K,+,.)$ est un corps si $(K,+,.)$ est un anneau commutatif dans lequel tout élément non nul possède un inverse.*

Soit $(K,+,.)$ un corps, et soit K^* l'ensemble des éléments non nuls de K , 0 désignant l'élÕement neutre de l'addition.On vérifie que $(K^*,.)$ est un groupe abélien, et que $1 \neq 0$.

Exemple 3.4.2. *$(\mathbb{Q},+,.),(\mathbb{R},+,.),(\mathbb{C},+,.)$ sont des corps.On verra plus loin que $\mathbb{Z}/p\mathbb{Z}$ est un corps si p est un nombre premier.*

Il est clair que $\mathbb{Z}$ n'est pas un corps puisque 1 et -1 sont les seuls éléments inversibles de $\mathbb{Z}$. La table de mutiplication de $\mathbb{Z}/4\mathbb{Z}$ montre que $\bar{2}$ n'a pas d'inverse, donc $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps(on verra plus généralement que $\mathbb{Z}/p\mathbb{Z}$ n'est pas un corps si p n'est pas premier).Notons que le corps $\mathbb{Z}/2\mathbb{Z}$ ne possède que deux éléments.

On peut dans les corps se livrer à des calculs analogues aux calculs usuels dans $\mathbb{R}$.On peut noter $\frac{1}{a}$ l'inverse d'un élément non nul d'un corps K , et l'équation $ax = b$ a pour unique solution dans K $x = \frac{b}{a}$. De même la règle "*pour qu'un produit de facteurs soit nul il faut et il suffit que l'un des facteurs soit nul*" est valable dans un corps quelconque (mais pas dans un anneau quelconque puisque $\bar{2}.\bar{2} = 0$ dans $\mathbb{Z}/4\mathbb{Z}$).

3.5 Calculs dans $\mathbb{Z}/n\mathbb{Z}$ sous MUPAD

On peut utiliser MUPAD pour faire des calculs dans $\mathbb{Z}/n\mathbb{Z}$

Exemple 3.5.1. *Calculer* $\overline{3174667}+\overline{257985}$, $\overline{-}3174667+\overline{257985}$ *et* $\overline{3174667}.\overline{257985}$ *dans* $\mathbb{Z}/8786543\mathbb{Z}$.

On utilise la commande **modp**

```
modp(3174667 + 257985, 8786543);
```

```
modp(-3174667 + 257985, 8786543);
```

```
modp(3174667 * 257985, 8786543);
```

```
                                    3432652

                                    5869861

                                    5219879
```

On a donc $\overline{3174667}+\overline{257985} = \overline{3432652}$, $\overline{-}3174667+\overline{257985} = \overline{5869861}$, $\overline{3174667}.\overline{257985} = \overline{5219879}$.

On peut également calculer dans $\mathbb{Z}/n\mathbb{Z}$ des inverses, et des produits du type $\bar{a}.\bar{b}^{-1}$, mais il faut faire attention.

Exemple 3.5.2. *Calculer l'inverse de* $\bar{8}$ *dans* $\mathbb{Z}/48\mathbb{Z}$.

```
modp(1/6,48);
```

```
Error: impossible inverse modulo
```

MUPAD a raison : $\bar{6}.\bar{8} = \bar{0}$, donc $\bar{6}$ n'est pas inversible dans $\mathbb{Z}/48\mathbb{Z}$. Pour éviter cet écueil on va choisir n premier, car dans ce cas, comme on le verra au chapitre suivant , $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Exemple 3.5.3. *Calculer* $(\overline{317465})^{-1}$ *et* $\overline{317465}.(\overline{257985})^{-1}$ *dans* $\mathbb{Z}/nZ$, *où* n *est le* 34567^e *nombre premier.*

```
ithprime(34567);
```

```
409463
```

On voit donc que le nombre premier cherché est 409463, et on peut faire les calculs

```
modp(1/317465,409463);
```

```
modp(317465/257985,409463);
```

```
180813
```

```
335955
```

Donc $(\overline{317465})^{-1} = \overline{180813}$ et $\overline{317465}.(\overline{257985})^{-1} = \overline{335955}$ dans $\mathbb{Z}/409463\mathbb{Z}$.

3.6 Exercices pour le Chapitre 3

exercice 1 Si $n \geq 2$, vérifier que $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.

exercice 2 Donner les tables d'addition et de multiplication de $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/9\mathbb{Z}$.Quels sont les éléments inversibles de ces deux anneaux ?

exercice 3 Montrer que l'ensemble $\mathbb{T} = \{z \in \mathbb{C}^* | \ |z| = 1\}$ est un sous-groupe de $\mathbb{C}^*$. Montrer que $\mathbb{U}_n = \{z \in \mathbb{C}^* | \ z^n = 1\}$ est un sous-groupe de $\mathbb{T}$ pour $n \in \mathbb{Z}$.

exercice 4 Montrer que $GL_2(\mathbb{R})$, l'ensemble des matrices carrées d'ordre 2 inversibles, est un groupe (la loi du groupe étant la multiplication des matrices). Montrer que
$H := \{M \in GL_2(\mathbb{R}) \mid \det M = 1\}$ et $K := \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \ \theta \in \mathbb{R} \right\}$
sont des sous-groupes de $GL_2(\mathbb{R})$.

exercice 5 Soit G l'ensemble des quatre fonctions numériques

$$f_1(x) = x, \ f_2(x) = \frac{1}{x}, \ f_3(x) = -x, \ f_4(x) = -\frac{1}{x},$$

définies sur $\mathbb{R}^*$, muni de la composition des applications. Montrer que G est un groupe.

exercice 6 Soit $\mathcal{F}$, l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Montrer que $(\mathcal{F}, +, *)$ est un anneau commutatif, où $(f+g)(x) = f(x) + g(x)$ et $(f * g)(x) = f(x).g(x)$ pour $x \in \mathbb{R}$,$f, g \in \mathcal{F}$.

exercice 7 Prouver que tous les sous-groupes de $\mathbb{Z}$ sont de la forme $a\mathbb{Z}$, avec $a \in \mathbb{N}$.

exercice 8
Montrer que $A = \left\{a + b\sqrt{3}, a, b \in \mathbb{R}\right\}$ est un sous-anneau de $\mathbb{R}$. Est-ce que A est un sous-corps de $\mathbb{R}$?

exercice 9
Soit $(G, \circ)$ un groupe tel que $a \circ a = e$ pour $a \in G$. Montrer que G est commutatif et donner un exemple de groupe vérifiant cette propriété.

exercice 10 (sous MUPAD)
a) Déterminer le 456917^e nombre premier
b) Effectuer dans $\mathbb{Z}/n\mathbb{Z}$, n désignant le nombre trouvé à la question précédente, les opérations suivantes
$\overline{1723497} + \overline{5255675}$, $\overline{1723497} - \overline{5255675}$, $\overline{1723497}.\overline{5255675}$.
c) Résoudre dans $\mathbb{Z}/n\mathbb{Z}$ l'équation $\overline{5255675}x = \overline{1723497}$.

Chapitre 4

Un peu d'arithmétique

4.1 La division du CM

On se propose ici de donner sans démonstration quelques résultats classiques d'arithmétique. Une démarche analogue permet de developper *" l' arithmétique des polynômes"* qui joue un rôle important en algèbre linéaire, mais que nous n'aborderons pas dans ce cours.

Dans toute la suite $\mathbb{Z}$ désignera l'ensemble des entiers relatifs, $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 0\}$ l'ensemble des entiers naturels, et $\mathbb{N}^*$ l'ensemble des entiers positifs, munis des opérations usuelles.

Théorème 4.1.1. *Soit $a \in \mathbb{Z}$, et soit $b \in \mathbb{N}^*$. Il existe un couple unique (q, r) d'entiers possédant les deux proprifés suivantes*

(i) $a = bq + r$

(ii) $0 \leq r \leq b - 1$.

Ce résultat , souvent appelé "division euclidienne dans $\mathbb{Z}$", a été vu en CM1 pour $a > 0$ et l'extension aux entiers négatifs est évidente. L'unicité provient du fait que si $r - r' = b(q' - q)$, avec $q \neq q'$, alors $|r - r'| \geq b$, tandis que $|r - r'| \leq b - 1$ si r et r' vérifient (ii).

On dispose d'un moyen effectif pour calculer q et r

1	3	2	9
	4	2	14
		6	

qui donne $q = 14$ et $r = 6$ si $a = 132$, $b = 9$.

Definition 4.1.2. *Soient m et n deux entiers relatifs.On dit que m divise n s'il existe $p \in \mathbb{Z}$ tel que $n = mp$. On dit alors que n est un multiple de m.*

On a l'importante notion de plus grand commun diviseur (p.g.c.d.)

Théorème 4.1.3. *Soit $(a_1, \ldots, a_p)$ une famille finie d'entiers naturels non tous nuls. Il existe un unique entier positif d possédant les propriétés suivantes*

(i) d divise a_i pour $1 \leq i \leq p$.

(ii) Si un entier relatif δ divise a_i pour $1 \leq i \leq p$, alors δ divise d.
Cet entier positif d est appelé le p.g.c.d. de la famille $(a_1, \ldots, a_p)$.

Il est clair que le p.g.c.d. de $(a_1, \ldots, a_p)$ est égal à celui de $(|a_1|, \ldots, |a_p|)$, et que le p.g.c.d. d'une famille d'entiers ne change pas si on lui retire ses éléments nuls.

Pour calculer le p.g.c.d. d'une famille $(a_1, \ldots, a_p)$ on peut procéder par récurrence finie : si on note b_k le p.g.c.d de $(a_1, \ldots, a_k)$ alors b_{k+1} est le p.g.c.d de a_{k+1} et b_k. Il est clair que le p.g.c.d. de $(a_1, \ldots, a_p)$ est égal à celui de $(|a_1|, \ldots, |a_p|)$. Il suffit donc de savoir calculer le p.g.c.d. de deux entiers positifs a et b, ce qui se fait par *l'algorithme d'Euclide*. Celui-ci consiste à faire des *divisions successives*. Soient a et b deux entiers positifs , avec $a \geq b$, et soit d leur p.g.c.d. On procède de la manière suivante.On commence par écrire

$a = bq_1 + r_1$ avec $0 \leq r \leq b - 1$. Si $r = 0, d = b$.

Sinon on recommence
$b = r_1 q_2 + r_2$ avec $0 \leq r_2 \leq r_1 - 1$. Si $r_2 = 0, d = r_1$.

Sinon on recommence
$r_1 = r_2 q_3 + r_3$ avec $0 \leq r_3 \leq r_2 - 1$. Si $r_3 = 0, d = r_2$.

Sinon on recommence
....
$r_k = r_{k+1} q_{k+2} + r_{k+2}$ avec $0 \leq r_{k+2} \leq r_{k+1} - 1$. Si $r_{k+2} = 0, d = r_{k+1}$.

Sinon on recommence
...
On finit par avoir, à un certain rang p
$r_p = r_{p+1} q_{p+2} + r_{p+2}$ avec $0 \leq r_{p+2} \leq r_{p+1} - 1$, $r_{p+2} \neq 0$

$r_{p+1} = r_{p+2} q_{p+3} + r_{p+3}$ avec $r_{p+3} = 0$. On a alors $d = r_{p+2}$.

Autrement dit **"le p.g.c.d. est égal au dernier reste non nul dans l'algorithme d'Euclide."** Comme $r_k > r_{k+1}$ pour tout k , il est clair avec les notations ci-dessus que l'algorithme s'arrête avec $p + 2 \leq b - 1$. Le fait que le p.g.c.d. de a et b est bien égal au dernier reste non nul provient du fait que si u et v sont deux entiers positifs alors le p.g.c.d. de u et v est égal au p.g.c.d. de v et du reste de la division de u par v.

On a donc

$$p.g.c.d.(a, b) = p.g.c.d.(b, r_1) = p.g.c.d.(r_1, r_2) = \ldots = p.g.c.d.(r_{p+2}, 0) = r_{p+2}.$$

Exemple 4.1.4. *p.g.c.d. de 132 et 55*
$\mathbf{132 = 55 \times 2 + 22}$
$\mathbf{55 = 22 \times 2 + 11}$
$\mathbf{22 = 11 \times 2 + 0}$
Le p.g.c.d. de 132 et 55 est égal à 11.

On va maintenant énoncer le théorème de Bezout

Théorème 4.1.5. *Soit $(a_1, \ldots, a_p)$ une famille finie d'entiers naturels non tous nuls et soit d le p.g.c.d. de $(a_1, \ldots, a_p)$.Il existe une famille $(u_1, \ldots, u_p)$ d'éléments de $\mathbb{Z}$ vérifiant*

$$a_1u_1 + \ldots a_pu_p = d$$

Plus généralement l'équation $a_1v_1 + \ldots a_pv_p = n$ admet une solution $(v_1, \ldots, v_p)$ dans $\mathbb{Z}^p$ si et seulement si n est un multiple de d.

On dispose d'une *méthode effective* pour calculer deux entiers u et v tels que $au+bv = d$, d désignant le p.g.c.d. de deux entiers positifs a et b. Il suffit de **"remonter l'algorithme d'Euclide"**. On peut en effet utiliser l'avant dernière ligne de l'algorithme pour exprimer $d = r_{p+2}$ en fonction de r_{p+1} et r_p. En utilisant la ligne précedente on exprime r_{p+1} en fonction de r_p et r_{p-1} et en substituant on exprime d en fonction de r_p et r_{p-1}. En itérant ce procédé ligne par ligne vers le haut on obtient les coefficients u et v cherchés.

Exemple 4.1.6. *Trouver deux entiers u et v tels que $132u + 55v = 11$.*

$\mathbf{11 = 55 - 22 \times 2}$

$\mathbf{22 = 132 - 55 \times 2}$

$\mathbf{11 = 55 - (132 - 55 \times 2) \times 2}$

$\mathbf{55 \times 5 - 132 \times 2 = 11}$

Le couple (-2, 5) est donc solution

En fait on dispose d'une méthode rapide pour calculer u et v, en faisant des calculs intermédiaires pendant le déroulement de l'algorithme. L'idée est la suivante : si $r_{n+2} = au_{n+2} + bv_{n+2}$, en remontant l'algorithme on obtient $r_n = r_{n+1}q_{n+2} + r_{n+2}$, $r_{n+2} = -r_{n+1}q_{n+2} + r_n = a(q_{n+2}u_{n+1} - u_n) + b(q_{n+2}v_{n+1} - v_n)$. On obtient les relations de récurrence

$$\begin{cases} u_{n+2} = -q_{n+2}u_{n+1} + u_n \\ v_{n+2} = -q_{n+2}v_{n+1} + v_n \end{cases} \tag{4.1}$$

Avec les notations ci-dessus on peut alors écrire en colonne les valeurs successives de u_n et v_n. On a $u_1 = 1 = 1 - q_1 \times 0, v_1 = -q_1 = -q_1 + 0$, et on peut écrire "l'algorithme d'Euclide étendu"

	q_n	u_n	v_n
		1	0
		0	1
$\mathbf{132 = 55 \times 2 + 22}$	2	1	-2
$\mathbf{55 = 22 \times 2 + 11}$	2	-2	5
$\mathbf{22 = 11 \times 2 + 0}$			

On retrouve ainsi le fait que $(-2) \times 132 + 5 \times 55 = 11$.

4.2 Applications du théorème de Bezout

Definition 4.2.1. *Soient a et b deux entiers relatifs.On dit que a et b sont premiers entre eux si leur p.g.c.d. est égal à 1.*

On va maintenant donner deux conséquences importantes du théorème de Bezout.

Théorème 4.2.2. *(Gauss) Soient a, b, c trois entiers relatifs non nuls. Si a divise bc, et si a est premier avec b, alors a divise c.*

Démonstration : Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Donc $c = auc + bcv$. Comme a divise bc , il existe $w \in \mathbb{Z}$ tel que $bc = aw$. Donc $c = a(uc + vw)$, ce qui montre que a divise c. ♣

Corollaire 4.2.3. *Soient a et b deux entiers relatifs non nuls et soit d le p.g.c.d. de a et b. Soit $\mathcal{S} = \{(u, v) \in \mathbb{Z}^2 \mid au + bv = 0\}$. On a $\mathcal{S} = \{-nb', na'\}_{n\in\mathbb{Z}}$, où $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$*

Démonstration : Il résulte du théorème de Bezout que a' et b' sont premiers entre eux, et $\mathcal{S} = \{(u, v) \in \mathbb{Z}^2 \mid a'u + b'v = 0\}$. Il est clair que si $u = -nb'$ et si $v = na'$ alors $(u, v) \in \mathcal{S}$. Réciproquement si $a'u + b'v = 0$ alors a' divise $b'v$, donc a' divise v d'après le théorème de Gauss. Donc il existe $n \in \mathbb{Z}$ tel que $v = na'$. On a alors $ua' = -b'na'$, donc $u = -nb'$. ♣

On a alors le résultat suivant concernant l'équation de Bezout, dont la démonstration est laissée en exercice.

Corollaire 4.2.4. *Soient a et b deux entiers positifs premiers entre eux. Il existe alors un unique couple (u_0, v_0) d'entiers relatifs vérifiant les deux conditions suivantes*
(i) $au_0 + bv_0 = 1$
(ii) $0 \leq u_0 < b$.
De plus dans ce cas on a $v_0 \leq 0$ et $|v| < a$.
D'autre part les solutions entières de l'équation $au + bv = 1$ sont données par les couples de la forme $u = u_0 - nb, v = v_0 + na$ avec $n \in \mathbb{Z}$.

Ces résultats ont diverses applications pratiques. On peut par exemple les utiliser pour déterminer les points à coordonnées entières d'une droite dont les coefficients de l'équation sont entiers.

Exemple 4.2.5. *Déterminer les points a coordonnées entières de la droite Δ d'équation 55x + 132y = 13.*

Pour que de tels points existent, il faudrait que 13 soit un multiple du p.g.c.d. de 55 et 132, qui est égal à 11, ce qui est visiblement faux. Donc cette droite n'a pas de points à coordonnées entières.

Exemple 4.2.6. *Déterminer les points à coordonnées entières de la droite D d'équation 55x + 132y = 22.*

Ici 22 est un multiple de 11, donc l'équation $55x + 132y = 22$ a des solutions entières. Comme $55 \times 5 - 2 \times 132 = 1$ on obtient une solution particulière en posant $x_0 = 10, y_0 = -4$. Soient maintenant $(x, y) \in Z^2$. On a $55x + 132y - 22 = 55(x - x_0) + 132(y - y_0)$. On voit donc que $55x + 132y = 22$ si et seulement si $x = 10 + u$ et $y = -4 + v$, avec $55u + 132v = 0$. Comme $\frac{55}{11} = 5$ et $\frac{132}{11} = 12$ on voit que les points à coordonnées entières de D sont les points donc les coordonnées sont de la forme $(10-12n, -4+5n)$ avec $n \in \mathbb{Z}$.

On a la variante suivante du théorème de Gauss, dont la démonstration est laissée en exercice.

Théorème 4.2.7. *Soient $a, b_1, \ldots, b_p$ des entiers non nuls. Si a est premier avec b_k pour $1 \leq k \leq p$, alors a est premier avec le produit $b_1 \ldots b_k$.*

Corollaire 4.2.8. *Soient $a_1, ..., a_k$ des entiers premiers entre eux deux à deux. Si $x \in \mathbb{Z}$ est divisible par a_j pour $1 \leq j \leq k$, alors x est divisible par le produit $a_1...a_k$.*

Démonstration : Si $k = 1$, il n'y a rien à démontrer. Supposons maintenant que le résultat est vrai pour $k - 1$, avec $k \geq 2$. Soient $a_1, ..., a_k$ des entiers premiers entre eux deux à deux et supposons que $x \in \mathbb{Z}$ est divisible par a_j pour $1 \leq j \leq k$. Alors x est divisible par le produit $a_1...a_{k-1}$, donc x s'écrit sous la forme $x = a_1...a_{k-1}y$, avec $y \in \mathbb{Z}$. Il résulte du théorème ci-dessus que a_k est premier avec $a_1...a_{k-1}$, et on déduit alors du théorème de Gauss que a_k divise y. Donc x est divisible par $a_1...a_k$, et la propriété est vraie pour k. Le résultat est donc démontré par récurrence. ♣

4.3 Le théorème chinois

Soit p un entier positif. On dira que deux entiers relatifs a et b sont *congrus modulo p* , et on écrira $a \equiv b \ (p)$, quand $a - b$ est divisible par p.On v'erifie facilement que si $a \equiv a' \ (p)$ et si $b \equiv b' \ (p)$ alors $a + b \equiv a' + b' \ (p)$ et $ab \equiv a'b' \ (p)$.

On a le théorème suivant , dû à un mathématicien chinois anonyme.

Théorème 4.3.1. *Soient $p_1, \ldots, p_k$ des entiers positifs tels que p_i et p_j soient premiers entre eux pour $i \neq j$.Alors pour toute famille $(q_1, \ldots, q_k)$ dans $\mathbb{Z}^k$ le système d'équations de congruence*

$x \equiv q_1 \quad (p_1)$
$\dots$
$\dots$
$x \equiv q_k \quad (p_k)$

possède des solutions dans $\mathbb{Z}$. De plus si x_0 est une solution, alors la solution générale du système est donnée par la formule

$$x = x_0 + np_1...p_k,$$

avec $n \in \mathbb{Z}$.

Notons que si x_0 est une solution particulière alors $x \in \mathbb{Z}$ est solution du système si et seulement si $x - x_0 \equiv 0 \pmod{p_j}$ pour $1 \leq j \leq k$. Donc si $x = x_0 + np_1...p_k$, avec $n \in \mathbb{Z}$, alors x est solution du système. Réciproquement, si x est solution du système, alors $x - x_0$ est divisible par $p_1, p_2, ...$ et p_k, qui sont premiers entre eux deux à deux, donc il est divisible par le produit $p_1...p_k$ et on a $x = x_0 + np_1...p_k$ avec $n \in \mathbb{Z}$.

Pour démontrer l'existence d'une solution on procède par récurrence sur k et on est ramené à chaque étape à résoudre dans $\mathbb{Z}^2$ une équation du type $ax + by = c$, avec a , b , c entiers relatifs , a et b premiers entre eux. Ceci donne un moyen effectif de trouver des solutions pour ce type de systèmes d'équations de congruence, que nous décrivons dans l'exemple suivant

Exemple 4.3.2. *Trouver $x \in \mathbb{Z}$ vérifiant*

$x \equiv 1 \quad (2)$
$x \equiv -1 \quad (3)$
$x \equiv 2 \quad (5)$

Les solutions de la première équation sont de la forme $x = 1+2m, m \in \mathbb{Z}$. En reportant dans la seconde équation on obtient $1+2m = -1+3n$, avec $n \in \mathbb{Z}$, qui donne $3n-2m = 2$. L'équation $3u - 2v = 1$ admet pour solution triviale $u = 1, v = 1$. Donc on peut prendre $m = n = 2$, ce qui fait que $x = 1 + 4 = 5$ est solution du système formé par les deux premières équations.

La solution générale de ce système est de la forme $x = 5+6p$, avec $p \in \mathbb{Z}$. En reportant dans la dernière équation on trouve $5 + 6p = 2 + 5q$, soit $6p - 5q = -3$. L'équation $6u - 5v = 1$ a pour solution triviale $u = v = 1$. Donc on peut prendre $p = q = -3$, ce qui donne $x_0 = -13$ comme solution du système proposé.On voit facilement que la solution générale est de la forme $x = -13 + 2 \times 3 \times 5n = -13 + 30n$, avec $n \in \mathbb{Z}$.

La méthode utilisée ci-dessus est valable pour tous les systèmes d'équations de congruence vérifiant les hypothèses du théorème chinois, mais il faut en général utiliser l'algorithme d'Euclide étendu pour résoudre les équations du type Bezout rencontrées à chaque étape des calculs.

4.4 Décomposition en produit de nombres premiers

La notion de p.g.c.d. a pour pendant celle de plus grand commun multiple (p.p.c.m.). Nous nous limiterons au cas de deux entiers.

Théorème 4.4.1. *Soient a et b deux entiers relatifs. Il existe un unique entier $m \geq 0$, appelé p.p.c.m. de a et b, possédant les deux propriťés suivantes*

(i) m est un mutiple commun à a et b

(ii) Si n est un multiple commun à a et b, alors n est un multiple de m.

De plus si on note $a \wedge b$ le p.g.c.d. de a et b et $a \vee b$ le p.p.c.m. de a et b on a la relation$(a \wedge b)(a \vee b) = ab$ (avec la convention $0 \wedge 0 = 0$).

Exemple 4.4.2. *Comme le p.g.c.d. de 55 et 132 est égal à 11, le p.p.c.m. de 55 et 132 est égal à 660.*

Une autre notion importante est la notion de nombre premier.

Definition 4.4.3. *Soit $p \geq 2$ un entier. On dit que p est premier si 1 et p sont les seuls diviseurs positifs de p.*

Il est clair que si p est premier, et si q n'est pas un multiple de p, alors p et q sont premiers entre eux. En utilisant le théorème de Gauss, on obtient le résultat suivant

Théorème 4.4.4. *Soit $a \geq 2$ un entier. Il existe une unique suite finie croissante $(p_1, \ldots, p_k)$ de nombres premiers et une unique suite $(n_1, \ldots, n_k)$ d'entiers positifs telles que $a = p_1^{n_1} \ldots p_k^{n_k}$. Cette formule est appellée décomposition en facteurs premiers de n.*

En utilisant la décomposition en facteurs premiers de deux entiers on obtient le résultat suivant.

Proposition 4.4.5. *Soient $a \geq 2$ et $b \geq 2$ deux entiers. Le p.g.c.d. de a et b est égal au produit des diviseurs premiers communs à a et b, affectés du plus petit de leurs exposants dans les décompositions de a et b, et le p.p.c.m. de a et b est égal au produit des diviseurs premiers de a ou b, affectés du plus grand de leurs exposants dans les décompositions de a et b.*

Exemple 4.4.6. *Les décompositions en facteurs premiers de 110 et 132 sont $110 = 2 \times 5 \times 11$ et $132 = 2^2 \times 3 \times 11$. Les seuls diviseurs premiers communs à 55 et 132 sont 2 (avec l'exposant 1 pour 110 et l'exposant 2 pour 132) et 11 (avec l'exposant 1 dans les deux cas). Donc $110 \wedge 132 = 2 \times 11 = 22$, et $110 \vee 132 = 2^2 \times 3 \times 5 \times 11 = 660$.*

Cette deuxième méthode de calcul du p.g.c.d. est à première vue plus simple que l'algorithme d'Euclide mais pour les grands nombres le coût du calcul de la décomposition en facteurs premiers est élevé, et les logiciels de calcul utilisent des variantes de l'algorithme d'Euclide.

Pour dresser la liste des nombres premiers on utilise le "*crible d'Eratosthène*" que nous mettons en oeuvre pour déterminer les nombres premiers inférieurs ou égaux à 30.

On écrit la liste $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30$
On garde 2 et on raye les mutiples de 2.
$2, 3, ., 5, ., 7, ., 9, ., 11, ., 13, ., 15, ., 17, ., 19, ., 21, ., 23, ., 25, ., 27, ., 29, .$
Le premier nombre non rayé après 2 est 3. On le garde et on raye les multiples de 3.
$2, 3, ., 5, ., 7, ., ., ., 11, ., 13, ., ., ., 17, ., 19, ., ., ., 23, ., 25, ., ., ., 29, .$
Le premier nombre non rayé après 3 est 5. On le garde et on retire tous les multiples de 5.
$\mathbf{2}, \mathbf{3}, ., \mathbf{5}, ., \mathbf{7}, ., ., ., \mathbf{11}, ., \mathbf{13}, ., ., ., \mathbf{17}, ., \mathbf{19}, ., ., ., \mathbf{23}, ., ., ., ., ., \mathbf{29}, .$
Comme tout nombre non premier $n \geq 30$ admet un diviseur premier $p \leq \sqrt{30} < 6$, on vient d'écrire la liste des nombres premiers inférieurs ou égaux à 30.

Le plus grand nombre premier connu est $2^{6972593} - 1$ qui a $2.098.960$ chiffres.Ce résultat a rapporté en 1999 \$ 50.000 à ses auteurs. Une prime de \$ 100.000 sera attribuée à ceux qui construiront un nombre premier de plus de dix millions de chiffres (les grands nombres premiers jouent un rôle important en cryptographie).

Nous concluons ce chapitre par le résultat suivant.

Théorème 4.4.7. *Soit $p \geq 2$ un entier. Alors $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.*

Démonstration : Si p n'est pas premier il existe un diviseur d de p tel que $1 < d < p$. On a alors $p = dq$ avec $1 < q < p$. Donc $\bar{0} = \bar{d}\bar{q}$ avec $\bar{d} \neq 0$, $\bar{q} \neq 0$, et $\mathbb{Z}/p\mathbb{Z}$ n'est pas un corps.

Par contre si p est premier soit α un élément non nul de $\mathbb{Z}/p\mathbb{Z}$. On a $u = \bar{a}$ avec $1 \leq a < p$. Donc a et p sont premiers entre eux. D'après le théorème 2.1.5 il existe $u, v \in \mathbb{Z}$ tels que $au + pv = 1$ et $0 \leq u \leq p - 1$, et le reste de la division de au par p est égal à 1. Donc $\alpha\bar{u} = \bar{1}$ et tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible, ce qui prouve que $\mathbb{Z}/p\mathbb{Z}$ est un corps. ♣

4.5 Arithmétique sous MUPAD

On peut facilement calculer des p.g.c.d. sous MUPAD

Exemple 4.5.1. *Calculer le p.g.c.d. de* 298765435678976 *et* 34567891345298766.

On utilise la commande **igcd**.

```
igcd(298765435678976,34567891345298766);
```

```
14
```

Le p.g.c.d. cherché est donc 14, et MUPAD calcule aussi les coefficients de l'équation de Bezout.

Exemple 4.5.2. *Trouver deux entiers relatifs u et v tels que* $298765435678976.u+34567891345298766.v = 14$.

On utilise la commande **igcdex**

```
igcdex(298765435678976,34567891345298766);

                    14, -276327850495985, 2388262848289
```

On peut donc prendre $u = -276327850495985$ et $v = 2388262848289$.

On peut s'aider de MUPAD pour résoudre des équations de congruence à gros coefficients.

Exemple 4.5.3. *Trouver un entier relatif x vérifiant le système d'équations de congruence suivant*

$x \equiv 23467 \quad (5139204473593)$
$x \equiv 34567 \quad (3710417184184751041)$
$x \equiv 345921 \quad (19214672689)$

Conformément au cours, on va chercher x de la forme $x = 23467 + 5139204473593.n$, avec $n \in \mathbb{Z}$, et on va chercher à déterminer n de facon que x vérifie la seconde équation. On doit donc avoir $x - 34567 = 3710417184184751041.m$, avec $m \in \mathbb{Z}$. On obtient $-11100 + 5139204473593.n = 3710417184184751041.m$ soit $5139204473593.n - 3710417184184751041.m = 11100$.

On vérifie que 5139204473593 et 3710417184184751041 sont premiers entre eux et on cherche une solution de l'équation de Bezout $5139204473593.u+3710417184184751041.v = 1$.

```
igcdex(5139204473593,3710417184184751041);

                1, 211774982003123841, -293324141432
```

On peut donc prendre $u = 211774982003123841$. On multiplie par 11100

```
211774982003123841*11100;

                        2350702300234674635100
```

Donc $x = 23467 + 5139204473593 \times 2350702300234674635100$ est solution des deux premières équations.

```
23467 + 5139204473593 *
  2350702300234674635100;

                    120807397774513952984447248609377 67
```

Donc 120807397774513952984447248609377 67 est solution des deux premières équations.

Pour avoir une solution des trois équations on cherche x de la forme $x = 120807397774513952984447248609377$
$5139204473593 \times 3710417184184751041 \times p$, avec $p \in \mathbb{Z}$. On doit avoir $x - 345921 =$
$19214672689 \times q$, avec $q \in \mathbb{Z}$, soit $120807397774513952984447248609377 67 - 345921 +$
$5139204473593 \times 3710417184184751041 \times p = 19214672689 \times q$. Après calculs on obtient finalement

-92006627297481846863667070278609332417751150140596221093869947051494040 5217

Pour obtenir un nombre plus raisonnable on va remplacer le nombre trouvé par le reste de sa division par $5139204473593 \times 3710417184184751041 \times 19214672689$ avec la commande modp

```
     5139204473593* 3710417184184751041*
19214672689;

               3663967652924534495184966282210937431916 57


modp(-92006627297481846863667070278609332417751150140596221093869947051494040
3663967652924534495184966282210937431916 57);

               2155576584036174657225835705623981695491 97
```

On trouve donc que **215557658403617465722583570562398169549197 est solution de l'équation proposée.**

En fait la bibliothèque de MUPAD **permettait d'obtenir directement le résultat en une fraction de seconde avec la commande numlib : :ichrem**

```
numlib::ichrem([ 23467, 34567,345921],[5139204473593,3710417184184751041,1

                215557658403617465722583570562398169549197
```

On peut trouver aussi avec MUPAD la décomposition en facteurs premiers.Le premier nombre donné est le signe, et ensuite on trouve les facteurs premiers suivis de l'ordre de multiplicité.MUPAD peut bien sûr aussi calculer le p.p.c.m.

Exemple 4.5.4. *Décomposition en facteurs premiers et p.p.c.m. de 286439140625 et 9240262625.*

Pour la décomposition en facteurs premiers on utilise la commande **ifactor**.

```
ifactor( 286439140625);

                    [1, 5, 7, 11, 2, 157, 1, 193, 1]

ifactor( 9240262625);

                      [1, 5, 3, 11, 1, 6720191, 1]
```

Les décompositions en facteurs premiers sont donc $286439140625 = 5^7 \times 11^2 \times 157 \times 193$ et $9240262625 = 5^3 \times 11 \times 6720191$. Ceci montre que le p.g.c.d. est égal à $5^3 \times 11 = \mathbf{1375}$ et le p.p.c.m. à $5^7 \times 11^7 \times 157 \times 193 \times 6720191$ que l'on calcule sous MUPAD :

```
    5^7* 11^2*
157 * 193 * 6720191;

                            1924925734875859375
```

Le p.p.c.m. de 286439140625 et 9240262625 est donc égal à **1924925734875859375**.

On retrouve directement ces deux résultats en utilisant la commande **igcd** pour le p.g.c.d. et la commande **ilcm** pour le p.p.c.m.

```
igcd(286439140625 , 9240262625);

                                    1375

ilcm(286439140625 , 9240262625);

                              1924925734875859375
```

4.6 Exercices pour le Chapitre 4

exercice 1

a) En utilisant l'algorithme d'Euclide étendu, d'eterminer le p.g.c.d. de 90 et 72 et déterminer deux entiers relatifs u et v tels que $90u + 72v = 18$.

b) Décomposer 72 et 18 en facteurs premiers. Utiliser ces décompositions pour retrouver le p.g.c.d. de 90 et 72 et trouver leur p.p.c.m.

exercice 2

Trouver un entier n vérifiant les 3 propriétés suivantes

a) $n - 1$ est divisible par 4

b) $n + 3$ est divisible par 5

c) $n - 2$ est divisible par 7.

exercice 3

Vérifier que si $a, b \in \mathbb{Z}$, $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$. Montrer que $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

exercice 4

Prouver que $\sqrt{2}$ et $\sqrt{5}$ ne sont pas pas rationnels.

exercice 5

Soit $n \geq 1$; montrer que si $2^n - 1$ est premier alors n est premier.

exercice 6

a) Démontrer que pour tout $(x, n) \in \mathbb{N}^2$, $1 + x$ divise $1 + x^{2n+1}$.

b) En déduire si $2^m + 1$ est premier alors m est une puissance de 2.

exercice 7

Déterminer le reste de la division euclidienne de $(7077)^{377}$ par 11.

exercice 8

Soit $x = \overline{a_n a_{n-1} \cdots a_1 a_0}$ un entier écrit en système décimal.
a) Prouver que x est divisible par 11 si et seulement si $\sum_{k=0}^{n}(-1)^k a_k \equiv 0 \quad (11)$.
b) Prouver que x est divisible par 6 si et seulement si $4\sum_{k=1}^{n} a_k + a_0 \equiv 0 \quad (6)$.

exercice 9

Chercher l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ tels que :
a) $11x + 41y = 4$.
b) $8x + 30y = 7$.
c) $12x + 3y = 21$.

exercice 10

Résoudre dans $\mathbb{N}^2$, les deux équations suivantes :
(i) $a \vee b + 10\ a \wedge b = 142$.
(ii) $a \vee b + a \wedge b = b + 9$.

exercice 11

a) Déterminer les éléments inversibles de $\mathbb{Z}\backslash 20\mathbb{Z}$ et préciser leurs inverses.
b) Résoudre dans $\mathbb{Z}\backslash 20\mathbb{Z} \times \mathbb{Z}\backslash 20\mathbb{Z}$ le système ci-dessous :
$\overline{4}x + \overline{7}y = \overline{10}$
$\overline{5}x + \overline{14}y = \overline{18}$

exercice 12

Résoudre l'équation $\bar{x}^2 = \bar{1}$ dans $\mathbb{Z}\backslash 19\mathbb{Z}$ et $\mathbb{Z}\backslash 58\mathbb{Z}$.

exercice 13 [Petit théorème de Fermat]

Si p est un nombre premier et $n \geq 1$, montrer que $n^p \equiv n \ \ (p)$.

exercice 14 [cryptographie à clef publique]

Elaborer un algorithme qui calcule les diviseurs d'un entier naturel quelconque n. Est-ce que votre algorithme est utilisable en pratique (i.e. avec un ordinateur) si n est très grand ?

exercice 15 (sous MUPAD)

a) Déterminer le p.g.c.d. et le p.p.c.m. de 10987654654983 et 13987673897659876 et trouver deux entiers relatifs u et v tels que $10987654654983 \times u + 13987673897659876 \times v = 1$.

b)D'ecomposer 10987654654983 et 13987673897659876 en facteurs premiers et retrouver à partir de cette décomposition leur p.g.c.d. et leur p.p.c.m.

exercice 16 (sous MUPAD)
Trouver le plus petit entier positif x véifiant les trois équations suivantes

$$x \equiv 123 \qquad (10987654654983)$$

$$x \equiv -24567 \qquad (13987673897659876)$$

$$x \equiv 3456298 \qquad (6720227)$$

Chapitre 5

Transformée de Walsh

5.1 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

$$W_{k+1} = \begin{bmatrix} W_k & W_k \\ W_k & -W_k \end{bmatrix}. \tag{5.1}$$

On obtient

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

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 $\mathcal{W}_k : \mathbb{C}^{2^k} \to \mathbb{C}^{2^k}$.

Definition 5.1.1. *Soit $f = \{f[0], f[1], ..., f[2^k - 1]\}$ 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

$$\begin{bmatrix} \mathcal{W}_k(f)[0] \\ . \\ . \\ . \\ \mathcal{W}_k(f)[2^k-1] \end{bmatrix} = W_k \begin{bmatrix} f[0] \\ . \\ . \\ . \\ f[2^k-1] \end{bmatrix} \tag{5.2}$$

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 $\mathcal{B} := \{\delta_0, ..., \delta_{2^k-1}\}$ n'est autre que la "base canonique" de $\mathbb{C}^{2^k}$ introduite dans le *Cours d'algèbre linéaire* [5]. 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 [5], on a

$$\mathcal{M}_{\mathcal{W}_k,\mathcal{B},\mathcal{B}} = W_k. \tag{5.3}$$

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

$$\mathcal{W}_k^{-1} = \frac{1}{2^k}\mathcal{W}_k. \tag{5.4}$$

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

$$[\,\mathcal{W}_k(f)[0], ..., \mathcal{W}_k(f)[2^k-1]\,] = [\,f[0], ..., f[2^k-1]\,]\,W_k \tag{5.5}$$

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.

5.2 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 5.2.1. *Soit $k \geq 1$ un entier. Pour $f \in \mathbb{C}^{2^k}$, $0 \leq j \leq 2^{k-1}-1$, posons*

$$\pi_0(f)[j] = f[j],\ \pi_1(f)[j] = f[2^{k-1}+j] \tag{5.6}$$

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

$$\pi_0\left(\mathcal{W}_k(f)\right) = \mathcal{W}_{k-1}(\pi_0(f)) + \mathcal{W}_{k-1}(\pi_1(f)),\ \ \pi_1\left(\mathcal{W}_k(f)\right) = \mathcal{W}_{k-1}(\pi_0(f)) - \mathcal{W}_{k-1}(\pi_1(f)) \tag{5.7}$$

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

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

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 apparaitre $\pi_0(f)$ 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 $10\text{x}2^{10} = 10240$ 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 $f = \{f[0], f[1], ..., f[2^k-1]\}$ 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 $0 \leq p \leq 2^{k-n}-1, 0 \leq q \leq 2^n-1$,
$f^{(n)}[2^np+q] = f^{(n-1)}[2^np+q] + f^{(n-1)}[2^np+q+2^{n-1}]$,
$f^{(n)}[2^np+q+2^{n-1}] = f^{(n-1)}[2^np+q] - f^{(n-1)}[2^np+q+2^{n-1}]$.
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 5.2.2. *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 $k = 3$.

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

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ -1 \\ -3 \\ 6 \\ -1 \\ 2 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 6 \\ 10 \\ 10 \\ 2 \\ -8 \\ -8 \\ 4 \\ -8 \end{bmatrix}$$

5.3 Application aux fonctions booléennes

Soit $p \geq 2$ un entier. On note $\mathbb{F}_p$ l'anneau $(\mathbb{Z}/p\mathbb{Z}, +, .)$ introduit dans le *cours d'algèbre* [4]. Formellement, les éléments de $\mathbb{Z}/p\mathbb{Z}$ sont les parties de $\mathbb{Z}$ de la forme $\overline{m} := m + p\mathbb{Z}$, de sorte que $\overline{m} = \overline{n}$ si et seulement si $m \equiv n$ mod(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.

$$\overline{m} + \overline{n} = \overline{m+n}, \ \ \overline{m}.\overline{n} = \overline{mn} \tag{5.8}$$

En pratique $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, ..., \overline{p-1}\}$, $\overline{m} + \overline{n} = \overline{r_{m+n}}$, où r_{m+n}, désigne le reste de la division de $m+n$ par p, et $\overline{m}.\overline{n} = \overline{r_{mn}}$, 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 [4]. 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 $(-1)^{\overline{m}} = -1^m$ pour $m \ \in \mathbb{Z}$, et on a $(-1)^{a+b} = (-1)^a(-1)^b$ pour $a, b \in \mathbb{F}_2$.

Definition 5.3.1. *Une* **fonction booléenne** *d'ordre k est une application $f : \mathbb{F}_2^k \to \mathbb{F}_2$. 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*

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

D'autre part on pose $X_i(x) = x_i$, pour $x = [x_0, ..., x_{k-1}] \in \mathbb{F}_2^n$, $0 \leq i \leq k-1$. Les fonctions de la forme $X_S := \Pi_{i \in S} X_i$, où $S \subset \{0, ..., k-1\}$ sont appelées des **monômes** *(on pose par convention $X_\emptyset(x) = \overline{1}$, 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 5.3.2. *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 $\delta_x(x) = \overline{1}$ et $\delta_x(y) = \overline{0}$ pour $x \neq y$). On considère bien entendu la fonction $X_\emptyset = \overline{1}$ comme un monôme, de sorte que la famille $\mathcal{M}_k = \{X_S\}_{S \subset \mathbb{F}_2^n}$ 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 $\lambda_{S_0} \neq 0$. Comme S_0 est fini il existe un sous-ensemble S_1 de S_0 tel que $\lambda_{S_1} \neq \overline{0}$ et tel que $\lambda_S = \overline{0}$ pour tout sous-ensemble S de ${\mathbb{F}_2}^k$ strictement inclus dans S_1. Posons $u(x) = \overline{1}$ si $x \in S_1$ et $u(x) = \overline{0}$ si $x \notin S_1$ (de sorte que $u = \overline{0}$ si $S_1 = \emptyset$ et $u = \overline{1}$ si $S_1 = \mathbb{F}_2^k$). Il est clair que $X_S(u) = \overline{0}$ si S n'est pas inclus dans S_1, et il résulte du choix de S_1 que $\lambda_S = \overline{0}$ si S est strictement inclus dans S_1. Comme $X_{S_1}(u) = \overline{1}$ on a $\left(\sum_{S \subset \mathbb{F}_2^k} \lambda_S X_S\right)(u) = \lambda_{S_1} \neq \overline{0}$, et

$\sum_{S\subset\mathbb{F}_2^k} \lambda_S X_S \neq \overline{0}$. 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 $\mathcal{B}_k$. ♣

Definition 5.3.3. *(i) On dit que $f \in \mathcal{B}_k$ est une* **fonction affine d'ordre** k *s'il existe $a = (a_0, ..., a_{k-1}) \in \mathbb{F}_2^k$ et $b \in \mathbb{F}_2$ tels que l'on ait*

$$f(x) = \sum_{j=0}^{k-1} a_j x_j + b \quad \forall x = (x_0, ..., x_{k-1}) \in \mathcal{B}_k, \tag{5.9}$$

et dans ce cas on pose $f = f_{a,b}$.
(ii) Pour $g, h \in \mathcal{B}_k$, on pose

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

(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 role 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 5.3.4. *On a, pour $f \in \mathbb{C}^{2^k}$*

$$\sum_{p=0}^{2^k-1} |\mathcal{W}_k(f)(p)|^2 = 2^k \sum_{p=0}^{2^k-1} |f(p)|^2 \tag{5.10}$$

Démonstration : On verra plus loin qu'il s'agit en fait d'un cas particulier de la formule de Plancherel-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 $g = \mathcal{W}_k(f)$, $f_0 = \pi_0(f)$, $f_1 = \pi_1(f)$, $g_0 = \pi_0(g)$, $g_1 = \pi_1(g)$,

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

$$= \sum_{p=0}^{2^{k-1}-1} |\mathcal{W}_{k-1}(f_0)(p) + \mathcal{W}_{k-1}(f_1)(p)|^2 + \sum_{p=0}^{2^{k-1}-1} |\mathcal{W}_{k-1}(f_0)(p) - \mathcal{W}_{k-1}(f_1)(p)|^2$$

$$2\sum_{k=0}^{2^{k-1}-1}|\mathcal{W}_{k-1}(f_0)(p)|^2+2\sum_{k=0}^{2^{k-1}-1}|\mathcal{W}_{k-1}(f_1)(p)|^2$$

$$=2^k\sum_{k=0}^{2^{k-1}-1}|f_0(p)^2|+2^k\sum_{k=0}^{2^{k-1}-1}|f_1(p)^2|=2^k\sum_{p=0}^{2^{k-1}}|f(p)|^2,$$

et le résultat est démontré par récurrence. ♣

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

$$x.y:=\sum_{j=0}^{k-1}x_jy_j \tag{5.11}$$

Lemme 5.3.5. *Pour* $0\leq p\leq 2^k-1$, *soit* $p=\sum_{j=0}^{k-1}p_j2^j$, *avec* $p_j\in\{0,1\}$, *la décomposition dyadique de* p, *et soit* $p^*:=(\overline{p}_0,...,\overline{p}_{k-1})$. *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* $0\leq p,q\leq k-1$,

$$w_{p,q}=(-1)^{p^*.q^*}=(-1)^{\sum_{0\leq j\leq k-1}p_jq_j} \tag{5.12}$$

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 $0\leq p\leq 2^{k-1}-1, 0\leq q\leq 2^{k-1}-1$,

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

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 $k\geq 0$. ♣

Definition 5.3.6. *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*

$$f^*\left(\sum_{j=0}^{2^k-1} p_j 2^j\right) = (-1)^{f(\overline{p}_0,\ldots,\overline{p}_{k-1})}. \tag{5.13}$$

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

Lemme 5.3.7. *Soit $f \in \mathcal{B}_k$, soit $a = (\overline{a}_0, ..., \overline{a}_{k-1}) \in \mathbb{F}_2^k$, avec $a_j \in \{0,1\}$, soit $\tilde{a} = \sum_{j=0}^{k-1} a_j 2^j \in \{0, ..., 2^k - 1\}$ l'entier associé à a et soit $f_a := f_{a,\overline{0}} : x \to a.x$ la fonction affine sans terme constant associée à a. Alors on a*

$$d(f, f_a) = 2^{k-1} - \frac{1}{2}\mathcal{W}_k(f^*)(\tilde{a}). \tag{5.14}$$

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

$$\mathcal{W}_k(f^*)(\tilde{a}) = \sum_{q=0}^{2^k-1} w_{\tilde{a},q} f^*(q) = \sum_{q=0}^{2^k-1} (-1)^{a.q^* + f(q^*)}$$

$$= \sum_{q=0}^{2^k-1} (-1)^{f_a(q^*)+f(q^*)} = \sum_{x \in \mathbb{F}_2^k} (-1)^{f_a(x)+f(x)} =$$

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

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

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

Théorème 5.3.8. *(i) Soit $f \in \mathcal{B}_k$ une fonction booléenne. On a*

$$d(f, \mathcal{A}_k) = 2^{k-1} - \frac{1}{2} max_{0 \leq p \leq 2^k-1} |\mathcal{W}_k(f^*)(p)| \leq 2^{k-1} - 2^{\frac{k}{2}-1}, \tag{5.15}$$

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

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

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

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

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* [5] 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,

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

$$= [\, 2h_{m-1}W_{2m-2}, 2h_{m-1}W_{2m-2}, 2h_{m-1}W_{2m-2}, 2h_{m-1}W_{2m-2} \,]$$
$$= [\, 2^m h_{m-1}, 2^m h_{m-1}, 2^m h_{m-1}, 2^m h_{m-1} \,] = 2^m h_m,$$

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 $p \in \{0, ..., 2^{2m} - 1\}$. On a

$$H_m(p) = (-1)^{\sum_{j=0}^{m-1} p_{2j} p_{2j+1}}. \tag{5.16}$$

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 $p^{(1)}_j = p^{(2)}_j = p^{(3)}_j = p^{(4)}_j = p_j$ pour $0 \leq j \leq 2m - 1$, $p^{(1)}_{2m} = p^{(1)}_{2m+1} = p^{(2)}_{2m+1} = p^{(3)}_{2m} = 0$,

$p_{2m}^{(2)} = p_{2m+1}^{(3)} = p_{2m}^{(4)} = p_{2m+1}^{(4)} = 1$. 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 $\left|\mathcal{W}_{2m}(f_{(2m)}(p))\right| = 2^m$ 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.

5.4 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

Definition 5.4.1. *Soit $k \geq 1$ un entier, soit $W_k = (w_{i,j})_{\substack{1 \leq j \leq 2^k-1 \\ 1 \leq j \leq 2^k-1}}$ la matrice de Walsh d'ordre k. On pose, pour $1 \leq j \leq 2^k - 1$,*

$$cs_k(i) = \frac{1}{2} \sum_{j=1}^{2^k-1} |w_{i,j-1} - w_{i,j}|. \tag{5.17}$$

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

.

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 $\mathcal{R}_k(i) = \{u_0, ..., u_{2^k-1}\} \subset \{0, ..., 2^k-1\}$, 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

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

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

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

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

Théorème 5.4.2. *Pour $k \geq 1$, l'application $j \to cs_k(j)$ est une bijection de l'ensemble $\{0, ..., 2^k - 1\}$ 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 $cs_k : \{0, ..., 2^k - 1\} \to \{0, ..., 2^k - 1\}$ est surjective, puisque toute application surjective d'un ensemble fini sur lui-même est bijective. C'est vrai si $k = 1$.

Notons $L_{i,k} = [w_{0,1}, ..., w_{0,2^k-1}]$ 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 $0 \leq i \leq 2^k - 1$

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

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 $p \in \{0, ..., 2^k - 1\}$ il existe $i \in \{0, ..., 2^k - 1\}$ tel que $cs_k(i) = p$, et soit $p \in \{0, ..., 2^{k+1} - 1\}$. 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 $i \in \{0, ..., 2^k - 1\}$ 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 $i \to cs_k(i)$ est bien une application surjective, donc bijective, de l'ensemble $\{0, ..., 2^k - 1\}$ sur lui même pour tout $k \geq 1$. ♣

Definition 5.4.3. *Soit $f = \{f[0], f[1], ..., f[2^k - 1]\} \in \mathbb{C}^{2^k}$, 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*

$$Comp_c(f) = (\mathcal{W}_k^{-1} \circ \mathcal{W}_{c,k})(f). \tag{5.18}$$

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

$$^t(\mathcal{W}_{c,k}(f)) = D_c^t(\mathcal{W}_k(f)) = D_c W_k^t f,\ Comp_c(f) = \frac{1}{2^k} W_k D_c W_k^t f.$$

Si on préfère faire les calculs avec les matrices lignes f et $f^{(c)}$, on obtient

$$f^{(c)} = \frac{1}{2^k} f W_k D_c W_k. \tag{5.19}$$

Pour $k = 2$, $c = 50\%$, on obtient

$$W_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, D_c = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\frac{1}{4} W_2 D_c W_2 = \frac{1}{4} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1/2 & 1/2 & 0 & 0 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 1/2 & 1/2 \end{bmatrix}.$$

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

$$c_3(1) = 0,\ c_3(1) = 7,\ c_3(2) = 3,\ c_3(3) = 4,\ c_3(4) = 1,\ c_3(5) = 6,\ c_3(6) = 2,\ c_3(7) = 5.$$

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.

```
M:=Dom::Matrix();
W:=proc(n) begin
if n=0 then M([[1]]) else
linalg::stackMatrix(linalg::concatMatrix(W(n-1),W(n-1)),
linalg::concatMatrix(W(n-1),-W(n-1)));
end_if
end_proc:

W(n) $n=0..3
```

Dom::Matrix()

$$(1),\ \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

```
W(4)
```

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

```
A:=M([[1, 2, -1, -3, 6, -1, 2, 0]]);W3(A):=A*W(3);
```

```
(1  2  −1  −3  6  −1  2  0)
(6  10  10  2  −8  −8  4  −8)
B :=M([[6,0,0,0,-8,0,4,0]]);C:=(1/8)*B *W(3);
(6  0  0  0  −8  0  4  0)
(1/4  1/4  −3/4  −3/4  5/4  5/4  9/4  9/4)
```

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 $j \geq c(2^k - 1)$. 0n 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 $f : [a, b] \to \mathbb{R}$. 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 . Nous donnons la version obtenue par G. Fenez et S. Ismais en 2006 à Bordeaux dans leur mémoire de master-crypto . On commence par écrire un programme pour le réarrangement par nombre de changements de signe.

On écrit

```
edit ncs
```

Matlab ouvre un fichier (une m-file), où on introduit un programme.

```
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 réarranger par nombre de changements de signes les nombres entiers compris entre 0 et $n-1$, n désignant une puissance de 2, il suffit alors 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
    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 fwt.

```
    function res = fwt(a)
[NN,N]=size(a);
if N==1
    res=a;
    return;
end
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 $a = [1\ 2\ -1\ -3\ 6\ -1\ 2\ 0]$. On retrouve bien le résultat obtenu 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 ce programme sur un signal à 1024 entrées. Le calcul est effectué instantanément, et on vérifie que la transformée de Walsh inverse de la transformée de Walsh du signal b coincide avec b aux erreurs d'arrondi près (l'ordre de grandeur de la différence est de 10^{-14} pour chaque terme). Nous n'affichons pas ces résultats.

```
>> a=[0:1:1023];b=sin(a);c=fwt(b);
d=b-(1/1024)*fwt(c);
```

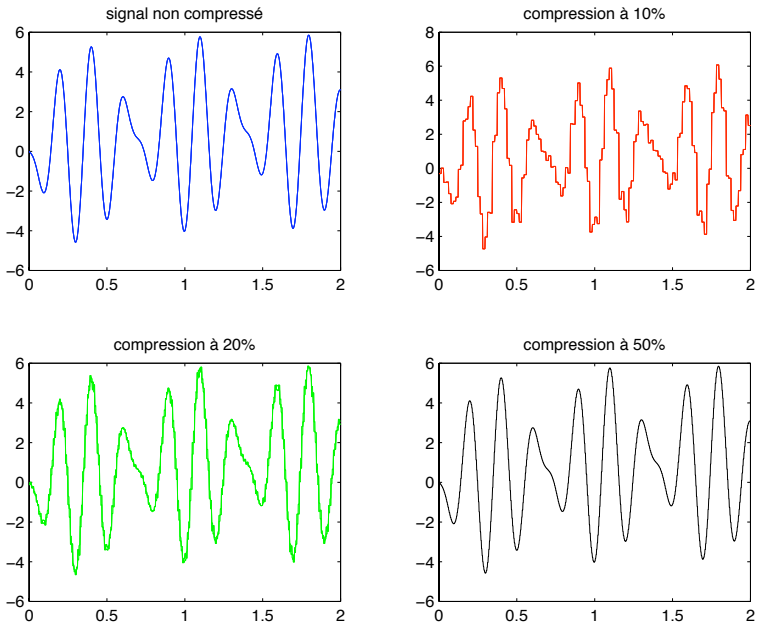
On va maintenant mettre en place la procédure de compression proprement dite, qui fait appel aux deux programmes précédents. On ouvre une m-file nommée compr1d, dont les entrées sont un signal 1D et un nombre qui va être en fait égal au produit du taux de compression cherché par la longueur du signal. On représente ensuite graphiquement le résultat obtenu.

```
function res=compr1d(entree,fact_red)
walsh=fwt(entree);
[u,v]=size(entree);
tab_chgt=ncs(v);
for k=1:v
    if tab_chgt(k)>(fact_red)*v -1
        walsh(k)=0;
```

```
    end
end
res=fwt(walsh)/v;
```

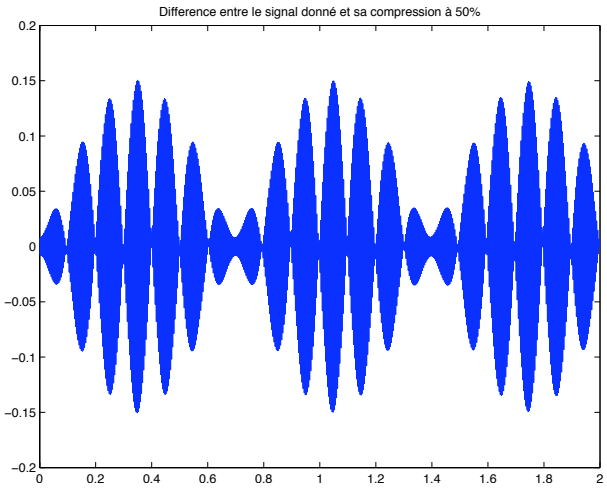
On applique ceci au signal obtenu à partir de la fonction $x \longrightarrow sin(x) - 3 * sin(27 * x) + 2sin(36 * x)$, discrétisée sur l'intervalle $[0, 2]$, avec des taux de compression de 10%, 20% et 50%.

```
 x=[0:2/1023:2];
y1=sin(x)-3*sin(27*x)+2*sin(36*x);
z11=compr1d(y1,0.10);
z12=compr1d(y1,0.20);
z13=compr1d(y1,0.50);subplot(221);plot(x,y1);
title('signal non compressé');hold on;subplot(222);plot(x,z11,'red');
title('compression à 10\%');
hold on;subplot(223);plot(x,z12,'green');title('compression à 20\%');
hold on;subplot(224);plot(x,z13,'black');
title('compression à 50\%');
print -depsc comp1d
```



On a l'impression que la compression à 50% coincide presque avec le signal initial. En fait l'erreur commise en remplaçant le signal initial par sa compression à 50% est très oscillante, comme le montre le graphique suivant.

```
>> plot(x,y1-z13);
title('Difference entre le signal donné et sa compression à 50\%');
 print -depsc erreur
```



5.5 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 come 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 $M = (m_{i,j})_{\substack{0\leq i\leq p-1\\ 0\leq j\leq q-1}}$.

Definition 5.5.1. *Soit $k \geq 1$. Une* **image numérisée** *à 2^{2k} pixels est une matrice $\Omega = (\Omega_{i,j})_{\substack{0\leq j\leq 2^k-1\\ 0\leq j\leq 2^k-1}}$ à coefficients réels.*

La transformée de Walsh horizontale $\mathcal{W}^{(k,hor)}(\Omega)$ d'une image numérisée Ω à 2^{2^k} 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 $C_j(\mathcal{W}^{(k,vert)}(\Omega) = W_kC_j(\Omega)$, et on obtient les formules

$$\mathcal{W}^{(k,hor)}(\Omega) = W_k\Omega,\ \mathcal{W}^{(k,vert)}(\Omega) = \Omega W_k,$$
$$\mathcal{W}^{(k)}(\Omega) = (\mathcal{W}^{(k,vert)} \circ \mathcal{W}^{(k,hor)})(\Omega) = W_k\Omega W_k = (\mathcal{W}^{(k,hor)} \circ \mathcal{W}^{(k,vert)})(\Omega). \tag{5.20}$$

On a alors

$$\left(\mathcal{W}^{(k)}\right)^{-1}(\Omega) = \frac{1}{2^{2k}}(\mathcal{W}^{(k)})(\Omega) = \frac{1}{2^{2k}}W_k\Omega W_k. \tag{5.21}$$

Par exemple considérons l'image numérisée à 4 pixels $\Omega = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. On a

$$\mathcal{W}_1(\Omega) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} a+b & a-b \\ c+d & c-d \end{bmatrix}$$
$$= \begin{bmatrix} a+b+c+d & a-b+c-d \\ a+b-c-d & a-b-c+d \end{bmatrix}.$$

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 $i \to cs_k(i)$ est une bijection de l'ensemble $\{0, ..., 2^k - 1\}$ sur lui-même, l'application $(i, j) \to cs_k(i) + cs_k(j)$ est une application surjective de l'ensemble $\{0, ..., 2^k - 1\} \times \{0, ..., 2^k - 1\}$ 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.

Definition 5.5.2. *Soient (i_1, j_1) et (i_2, j_2) deux éléments de l'ensemble $E_k := \{0, ..., 2^k - 1\} \times \{0, ..., 2^k - 1\}$. 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 $(i, j) \in E_k$,

$$\theta_k(i, j) = \text{Card}\left(\{(\alpha, \beta) \in E_k \mid (\alpha, \beta) \leq (i, j)\}\right). \tag{5.22}$$

Ceci permet de définir avec précision une procédure de compression d'images.

Definition 5.5.3. *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*

$$\mathcal{W}^{(k,c)}(\Omega)[i, j] = \mathcal{W}^{(k)}(\Omega)[i, j] \text{ si } \theta_k(i, j) \leq c2^{2k},\ \mathcal{W}^{(k,c)}(\Omega)[i, j] = 0 \text{ si } \theta_k(i, j) > c2^{2k},$$

et on définit la compression d'ordre c de Ω par la formule

$$\Omega^{(c)} = \left([\mathcal{W}^{(k)}]^{-1} \circ \mathcal{W}^{(k,c)}\right)(\Omega) = \frac{1}{2^{2k}} W^{(k)} (\mathcal{W}^{(k)}(\Omega) W^{(k)}.$$

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

$$\mathcal{W}^{(1,1/4)}(\Omega) = \begin{bmatrix} a+b+c+d & 0 \\ 0 & 0 \end{bmatrix}, \ \mathcal{W}^{(1,1/2)}(\Omega) = \begin{bmatrix} a+b+c+d & a-b+c-d \\ 0 & 0 \end{bmatrix},$$

$$\mathcal{W}^{(1,3/4)}(\Omega) = \begin{bmatrix} a+b+c+d & a-b+c-d \\ a+b-c-d & 0 \end{bmatrix},$$

$$\Omega^{(1/4)} = \frac{1}{4} \begin{bmatrix} a+b+c+d & a+b+c+d \\ a+b+c+d & a+b+c+d \end{bmatrix}, \Omega^{(1/2)} = \frac{1}{2} \begin{bmatrix} a+c & b+d \\ a+c & b+d \end{bmatrix},$$

$$\Omega^{(3/4)} = \frac{1}{4} \begin{bmatrix} 3a+b+c-d & 3b+a-c+d \\ 3c+a-b+d & 3d-a+b+c \end{bmatrix}.$$

5.6 Exercices sur le Chapitre 5

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 $\{0, ..., k-1\}$. Montrer que l'on a

$$(i) X_S.X_T = X_{S\cap T}.$$

$$(ii) X_{S\cup T} = X_S + X_T + X_S.X_T.$$

exercice 3

En utilisant le *Cours d'algèbre linéaire* [5], 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

$${}^tPW_kP = P^{-1}W_kP = 2^{\frac{k}{2}} \begin{bmatrix} I_{2^{k-1}} & 0 \\ 0 & -I_{2^{k-1}} \end{bmatrix},$$

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 $\delta_a(x) = \overline{0}$ si $x \neq a$, $\delta_a(x) = \overline{1}$ 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 $a = [a_1, ..., a_{k-1}] \in \mathbb{F}_2^k$

$$\delta_a = \Pi_{j=0}^{k-1}(X_j + a_j + \overline{1}).$$

3) On énumère les éléments de $\mathbb{F}_2^k$ en posant $a_{(p)} = [\overline{p}_0, ..., \overline{p}_{k-1}]$ pour $0 \leq p \leq 2^k - 1$, où $p = \sum_{j=0}^{k-1}$, avec $p_j \in \{-1, 1\}$, désigne la décomposition de p en base 2. De même on énumère les sous-ensembles S de $\{0, ..., k-1\}$ en posant $S_p := \{j \in \{0, ..., k-1\} \,|p_j = \overline{1}\}$.

Donner la matrice de passage de la base $\{a_(0), ..., a_{(2^k-1)}\}$ á la base $\{X_{S_0}, ..., X_{S_{2^k-1}}\}$ et la matrice de passage de la base $\{X_{S_0}, ..., X_{S_{2^k-1}}\}$ à la base $\{a_0, ..., a_{2^k-1}\}$. 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 moômes $f \in \mathcal{B}_k$ 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 $(i, j)_{\substack{0 \leq i \leq 3 \\ 0 \leq j \leq 3}}$ en suivant la procédure du cours.

3) Trouver la formule permettant de calculer la compression à 75% d'une image numérisée à 16 pixels.

Chapitre 6

Transformée de Fourier discrète

6.1 Définition de la transformée de Fourier discrète

On va définir la transformée de Fourier discrète sur $\mathbb{C}^N$.

Definition 6.1.1. *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 $f = (f[0], ..., f[N-1])$ par la formule*

$$\hat{f}[m] = \sum_{n=0}^{N-1} f[n]\omega_N^{-nm}, \;\; m \in \{0, ..., N-1\}. \tag{6.1}$$

L'application $= \mathcal{F}_N(f) : f \to \hat{f}$ 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 $\mathcal{F}_N(f) : \mathbb{C}^N \to \mathbb{C}^N$ dans la base canonique $\{\delta_0, ..., \delta_{N-1}\}$ de $\mathbb{C}^N$. On a alors les formules

$$\hat{f} = fA_N, \;\; {}^t\hat{f} = A_N \, {}^t f. \tag{6.2}$$

On définit la matrice conjuguée $\overline{B}$ d'une matrice $B = (b_{m,n})_{\substack{0 \leq i \leq p \\ 0 \leq j \leq q}}$ par la formule

$$\overline{B} := (\overline{b}_{m,n})_{\substack{0 \leq i \leq p \\ 0 \leq j \leq q}}.$$

On a

$$\sum_k = 0^{N-1} \omega_N^{mk} \omega_N - nk = \sum k = 0^{N-1} \left(\omega_N^{m-n}\right)^k.$$

Comme $\omega_N^N = 1$, on obtient, pour $0 \leq m \leq N-1$, $0 \leq m \leq N-1$,

$$\sum_{k=0}^{N-1} \omega_N^{mk}\omega_N^{-nk} = N \text{ si } m = n,$$

$$\sum_{k=0}^{N-1} \omega_N^{mk}\omega_N^{-nk} = \frac{1-\omega^{(m-n)N}}{1-\omega^{m-n}} = 0 \text{ si } m \neq n.$$

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

$$A_N^{-1} = \frac{1}{N} A_N. \tag{6.3}$$

On obtient alors la **"formule d'inversion de Fourier"** et les **formules de Plancherel-Parseval** dans le cas discret.

Proposition 6.1.2. *On a pour $f \in \mathbb{C}^N$ la formule d'inversion*

$$f[m] = \frac{1}{N} \sum_{n=0}^{N-1} \hat{f}[n]\omega_N^{mn}, \;\; 0 \leq m \leq N-1. \tag{6.4}$$

On a également pour $f, g \in \mathbb{C}^N$ la "formule de Plancherel"

$$\sum_{m=0}^{N-1} f[m]\hat{g}[m] = \frac{1}{N} \sum_{m=0}^{N-1} \hat{f}[m]\overline{\hat{g}[m]}. \tag{6.5}$$

En particulier on a pour $f \in \mathbb{C}^N$ la "formule de Parseval"

$$\sum_{m=0}^{N-1} |f[m]|^2 = \frac{1}{N} \sum_{m=0}^{N-1} |\hat{f}[m]|^2. \tag{6.6}$$

Démonstration : La formule d'inversion résulte du fait que $A_N^{-1} = \overline{A_N}$. D'autre part on a

$$\sum_{m=0}^{N-1} \hat{f}[m]\overline{\hat{g}}[m] = \hat{f}\overline{{}^t\hat{g}} = f A_N \overline{A_N {}^t g} = N f \overline{{}^t g} = N \sum_{m=0}^{N-1} f[m]\overline{\hat{g}[m]},$$

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

$$(\hat{f}[0], \hat{f}[1], \hat{f}[2]) = \hat{f} = fA_2 = (1, 0, 1) \begin{bmatrix} 1 & 1 & 1 \\ 1 & j^2 & j \\ 1 & j & j^2 \end{bmatrix} = (3, 0, 0),$$

$$(\hat{g}[0], \hat{g}[1], \hat{g}[2], \hat{g}[3]) = gA_3 = (1, 0, 0, i) \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}$$

$$= (1 + i, 0, 1 - i, 2).$$

Notons que dans le calcul de $\hat{f}$ on a utilisé le fait que $1 + j + j^2 = \frac{1-j^3}{1-j} = 0$.

6.2 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

$$(f \overset{(N)}{*} g)[n] = \sum_{p=0}^{n} f[p]g[n-p] + \sum_{p=n+1}^{N-1} f(p)g(n+N-p), \quad 0 \leq n \leq N-1, \qquad (6.7)$$

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 6.2.1. *Soit $N \geq 1$. On a, pour $f = (f[n])_{0\leq n\leq N-1} \in \mathbb{C}^N, g = (g[n])_{0\leq n\leq N-1} \in \mathbb{C}^N$,*

$$\mathcal{F}_N\left(f \overset{(N)}{*} g\right) = \mathcal{F}_N(f)\mathcal{F}_N(g). \qquad (6.8)$$

Démonstration : Soit $n \in \{0, ..., N-1\}$, 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

$$(u * v)[m] = 0 \text{ pour } 0 \leq m \leq n-1, \ (u * v)[m] = (f \overset{(N)}{*} g)[m] \text{ pour } n \leq m \leq N-1,$$

$$(u*v)[m] = (f \overset{(N)}{*} g)(m-N) \text{ pour } N \leq m \leq n+N-1, \ (u*v)[m] = 0 \text{ pour } m \geq n+N.$$

Avec les notations du Chapitre 5, et compte tenu du fait que $\omega^{-nN} = 1$, on a

$$\mathcal{Z}(u*v)(\omega^n) = \sum_{m=0}^{+\infty}(u*v)[m]\omega^{-nm} = \sum_{m=n}^{N-1}(u*v)[m]\omega^{-nm} + \sum_{m=N}^{n+N-1}(u*v)[m]\omega^{-(m-N)n}$$

$$= \sum_{m=n}^{N-1}(f \overset{(N)}{*} g)[m]\omega^{-nm} + \sum_{n=0}^{n-1}(f \overset{(N)}{*} g)[m]\omega^{-mn} = \mathcal{F}_N\left(f \overset{(N)}{*} g\right)[n].$$

Il est clair que $\mathcal{Z}(u)(\omega^n) = \mathcal{F}(f)[n]$. D'autre part on a

$$\mathcal{Z}(v)(\omega^n) = \sum_{m=0}^{+\infty} v[m]\omega^{-mn} = \sum_{m=n}^{N-1} g[m]\omega^{-mn} + \sum_{m=n}^{n+N-1} g(m-N)\omega(m-N)n$$

$$\sum_{m=n}^{N-1} g[m]\omega^{-mn} + \sum_{m=0}^{n-1} g[m]\omega{-mn} = \mathcal{F}_N(g)[n].$$

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 6.2.2. *L'application $(f,g) \to f \overset{(N)}{*} g$ 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 $f \in \mathbb{C}^N$,

$$f \overset{(N)}{*} \delta_0 = \delta_0 \overset{(N)}{*} f = f, \tag{6.9}$$

de sorte que δ_0 est l'élément unité de $\mathbb{C}^N$ pour la loi de composition interne $\overset{(N)}{*}$.

On va voir si $N = 2^p$ est une puissance de 2, 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

$$f \overset{(N)}{*} g = \mathcal{F}_N^{-1}\left(\mathcal{F}_N(f)\mathcal{F}_N(g)\right). \tag{6.10}$$

6.3 FFT en décimation temporelle

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

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

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

$$\begin{cases} f_0 := (f[2n])_{0 \leq n \leq N/2-1} \\ f_1 := (f[2n+1])_{0 \leq n \leq N/2-1} \end{cases} \tag{6.11}$$

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

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

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

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

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

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

(6.12)

k	0	1	2	3	4	5	6	7
f	0	2	-1	0	1	0	1	1
$\tilde{f}$	0	1	-1	1	2	0	0	1

(6.13)

Remarquons que

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

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

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

(6.14)

6.4 FFT en décimation fréquentielle :

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

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

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

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

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

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

avec

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

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

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

(6.15)

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

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

6.5 Applications de la FFT au calcul de produits de polynômes ou d'entiers

On va utiliser la FFT pour calculer le produit des deux polynômes $p = 1 - x + x^2$ et $q = 1 + x^4 + x^5$. On peut effectuer les calculs dans $\mathbb{Z}/8\mathbb{Z}$, puisque le degré du produit est égal à 7. On calcule les transformées de Fourier de p et q par décimation fréquentielle,

ce qui donne lieu à un renversement de bits à la fin. On obtient la transformée de Fourier du produit pq (qui au niveau des coefficients des polynômes se traduit par un produit de convolution) en faisant le produit au sens usuel des transformées de Fourier de p et q, et on applique ensuite la transformation de Fourier inverse par décimation temporelle. Dans ce cas à chaque étape on effectue un calcul analogue à celui d'une FFT en remplaçant ω_n^{-1} par ω_n, et on divise le résultat obtenu par 8.

k	0	1	2	3	4	5	6	7
$p(k)$	1	-1	1	0	0	0	0	0
$\omega_8^{-1} = e^{-i\frac{\pi}{4}}$	1	-1	1	0	1	$e^{-i\frac{\pi}{4}}$	-i	0
$\omega_4^{-1} = -i$	2	-1	0	$(-i)(-1) = i$	$1-i$	$-e^{-i\frac{\pi}{4}}$	$1+i$	$e^{i\frac{\pi}{4}}$
$\omega_2^{-1} = -1$	1	3	i	$-i$	$(\sqrt{2}-1)e^{-i\frac{\pi}{4}}$	$(\sqrt{2}+1)e^{-i\frac{\pi}{4}}$	$(\sqrt{2}+1)e^{i\frac{\pi}{4}}$	$(\sqrt{2}-1)e^{i\frac{\pi}{4}}$
$F_8(p)(k)$ (Revbits)	1	$(\sqrt{2}-1)e^{-i\frac{\pi}{4}}$	i	$(\sqrt{2}+1)e^{i\frac{\pi}{4}}$	3	$(\sqrt{2}+1)e^{-i\frac{\pi}{4}}$	$-i$	$(\sqrt{2}-1)e^{i\frac{\pi}{4}}$
$q(k)$	1	0	0	0	1	1	0	0
$\omega_8^{-1} = e^{-i\frac{\pi}{4}}$	2	1	0	0	0	$-e^{-i\frac{\pi}{4}}$	0	0
$\omega_4^{-1} = -i$	2	1	2	$-i$	0	$-e^{-i\frac{\pi}{4}}$	0	$e^{-i\frac{\pi}{4}}$
$\omega_2^{-1} = -1$	3	1	$2-i$	$2+i$	$-e^{-i\frac{\pi}{4}}$	$e^{-i\frac{\pi}{4}}$	$e^{i\frac{\pi}{4}}$	$-e^{i\frac{\pi}{4}}$
$F_8(q)(k)$ (Revbits)	3	$-e^{-i\frac{\pi}{4}}$	$2-i$	$e^{i\frac{\pi}{4}}$	1	$e^{-i\frac{\pi}{4}}$	$2+i$	$-e^{i\frac{\pi}{4}}$
$F_8(p*q)(k)$	3	$(\sqrt{2}-1)i$	$1+2i$	$(\sqrt{2}+1)i$	3	$-(\sqrt{2}+1)i$	$1-2i$	$-(\sqrt{2}-1)i$
Rv$(F_8(p*q))(k)$	3	3	$1+2i$	$1-2i$	$(\sqrt{2}-1)i$	$-(\sqrt{2}+1)i$	$(\sqrt{2}+1)i$	$-(\sqrt{2}-1)i$
$\omega_2 = -1$	6	0	2	$4i$	$-2i$	$2\sqrt{2}i$	$2i$	$2\sqrt{2}i$
$\omega_4 = i$	8	-4	4	4	0	$-4e^{-i\frac{\pi}{4}}$	$-4i$	$4e^{i\frac{\pi}{4}}$
$\omega_8 = e^{i\frac{\pi}{4}}$	8	-8	8	0	8	0	0	8
$(p*q)(k)$ (diviser par 8)	1	-1	1	0	1	0	0	1

On obtient donc

$$pq = 1 - x + x^2 + x^4 + x^7.$$

Ceci est évidemment confiré par un calcul direct : on a $(1-x+x^2)(1+x^4+x^5) = 1-x+x^2+x^4-x^5+x^6+x^5-x^6+x^7 = 1-x+x^2+x^4+x^7$.

Notons que l'on peut appliquer ceci au calcul du produit

$$91\times 110001 = p(10)q(10) = pq(10) = 10^7+10^4+10^2+1-10 = 10010101-10 = 10010091.$$

L'utilisation de la FFT n'est bien sûr intéressante en pratique que pour des polynômes de degré très élevé et des nombres très grands.

Chapitre 7

Etude générale de la transformation de Fourier

7.1 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. Une **topologie** sur E est la donnée d'une famille $\mathcal{U}_\tau$ de parties de E possédant les propriétés suivantes

1. $E \in \mathcal{U}_\tau$ et $\emptyset \in \mathcal{U}_\tau$.
2. La réunion d'une famille quelconque déléments de $\mathcal{U}_\tau$ appartient à $\mathcal{U}_\tau$.
3. L'intersection de toute famille finie d'éléments de $\mathcal{U}_\tau$ appartient à $\mathcal{U}_\tau$.
4. Pour tout couple (x, y) d'éléments distincts de E il existe $U, V \in \mathcal{U}_\tau$ tels que $x \in U, y \in V$, and $U \cap V = \emptyset$.

On dit alors que (E, τ) est un espace topologique. Dans ce cas on dit que $U \subset E$ est **ouvert** si $U \in \mathcal{U}_\tau$, et on dit que $F \subset \mathcal{U}_\tau$ est **fermé** si son complémentaire $E \setminus F$ est ouvert.

Rappelons que si E_1 et E_2 sont deux ensembles, et si $f : E_1 \to E_2$ est une application, on pose, pour $A \subset E_2$,

$$f^{-1}(A) = \{x \in E_1 | f(x) \in A\}.$$

L'ensemble $f^{-1}(A)$ est appelé l'image réciproque de A par l'application f.

Definition 7.1.1. *Soient (E_1, τ_1) et (E_2, τ_2) deux espaces topologiques.*
On dit qu'une application $f : E_1 \to E_2$ est continue quand $f^{-1}(U) \in U_{\tau_1}$ pour tout $U \in U_{\tau_2}$.

Definition 7.1.2. *Soient Soient (E_1, τ_1), (E_2, τ_2), ...(E_p, τ_p) des espaces topologiques.*
On note $\mathcal{U}_{\tau_1 \times \tau_2 \times ... \times \tau_p}$ l'ensemble des parties du produit cartésien $E_1 \times E_2 \times ... \times E_p$ qui peuvent s'écrire comme réunion d'ensembles de la forme $U_1 \times U_2 \times ... \times E_p$, avec $U_1 \in \mathcal{U}_{\tau_1}$, $U_2 \in \mathcal{U}_{\tau_2}, ..., U_p \in \mathcal{U}_{\tau_p}$.

On vérifie facilement que la définition ci-dessus permet d'obtenir une topologie $\tau_1 \times \tau_2 \times ... \times \tau_p$ sur l'ensemble $E_1 \times E_2 \times ... \times E_p$, appelée **topologie produit** des topologies $\tau_1, \tau_2, ..., \tau_p$. 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 $f : E_1 \to E_2$ et $g : E_2 \to E_3$ sont continues, alors $g \circ f : E_1 \to E_3$ est continue. On retrouve les notions usuelles d'ouvert et de fermé sur $\mathbb{R}^p$ et la notion usuelle de continuité pour les applications de $\mathbb{R}^p$ dans $\mathbb{R}^q$. Remarquons également que si A est un sous-ensemble d'un espace tpoplogique (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 topologieinduite 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 $f : E_1 \to E_2$ est une application et si $f(E_1) \subset A \subset f(E_2)$, alors f est une application continue si et seulement si f, considérée comme 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 alors que $(U_{\lambda_j})_{1 \leq j \leq k}$ est un sous-recouvrement fini de $(U_\lambda)_{\lambda \in \Lambda}$ si $F \subset \cup_{1 \leq j \leq k} U_{\lambda_j}$, avec $\lambda_j \in \Lambda$ pour $1 \leq j \leq k$, k désignant un entier positif quelconque. Ceci permet d'introduire la notion suivante.

Definition 7.1.3. *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 E on peut extraire un sous-recouvremeni fini.*

L'ensemble vide est compact par convention, et on vérifie que toute partie compacte d'un ensemble topologique est fermée. On vérifie également que les parties compactes de $\mathbb{R}^p$ sont les parties fermées et bornées de $\mathbb{R}^p$.

On va maintenat introduire la notion de **groupe localement compact**.

Definition 7.1.4. *Soit $(G, \circ)$ un groupe et sot τ une topologie sur G. On dit que $(G, \circ, \tau)$ est un groupe topologique quand les deux conditions suivantes sont vérifiées*

1. *L' application $(x, y) \to x \circ y$ est une application continue de $(G \times G, \tau \times \tau)$ dans (G, τ).*
2. *L'application $x \to x^{-1}$ est une application continue de (G, τ) dans lui-même.*

On dit qu'un groupe topologique (G, τ) est **localement compact** *s'il existe un ouvert U et un compact K de G tels que $e \in U \subset K$, e désignant l'élément unité de G.*

Rappelons qu'un groupe $(G, \circ)$ est dit abélien quand $x \circ y = y \circ x$ pour tout couple (x, y) déléments de G. On va maintenant définir en toute généralité le **groupe dual** d'un groupe abélien localement compact.

Soient $(G_1, \circ)$ et $(G_2, \circ)$. Rappelons qu'on dit qu'une application $\theta : G_1 \to G_2$ est un **homomorphisme de groupes** si on a

$$\theta(x \circ y) = \theta(x) \circ \theta(y)$$

pour tout couple x, y déément de G. Dans ce cas le bf noyau $Ker(\theta)$ de θ sest défini par la formule

$$Ker(\theta) := \{x \in G_1 \mid \theta(x) = 1_{G_2}\},$$

où 1_{G_2} désigne l'élément unité de G_2.

Definition 7.1.5. *Soit $G = (G, \circ, \tau)$ un groupe abélien localement compact et soit $\mathbb{T} = \{z \in \mathbb{C} || z| = 1\}$ le cercle unité.*

On appelle **caractères** *de G les homomorphismes de groupes continus de $(G, \circ)$ dans $(\mathbb{T}, .)$.*

On notera $\widehat{G}$ l'ensemble des caractères de G, et pour $\phi, \psi \in \widehat{G}$, on définit $\phi.\psi : G \to \mathbb{T}$ par la formule

$$(\phi.\psi)(x) = \phi(x).\psi(x)\ \forall x \in G.$$

D'autre part pour $\phi \in \widehat{G}$, et pour $K \subset G$, K compact, on pose

$$U_{\phi,K,\epsilon} = \{\psi \in \widehat{G}\ | sup_{x\ \in K} |\phi(x) - \psi(x)| < \epsilon\},$$

et on note $\mathcal{U}_{\hat{\tau}}$ la familles de sous-ensembles de $\widehat{G}$ qui sont soit vides, soit réunion d'une famille d'ensembles $U_{\phi,K,\epsilon}$ du type ci-dessus.

Soient $(G_1, \circ, \tau_1)$ et $(G_2, \circ, \tau_2)$ deux groupes topologiques. On dira qu'une application $\theta : G_1 \to G_2$ est un **ismorphisme de groupes topologiques** si θ est un homomorphisme de groupes bijectif et si les applications $\theta : (G_1, \circ, \tau_1) \to (G_2, \circ, \tau_2)$ et $\theta^{-1} : (G_2, \circ, \tau_2) \to (G_1, \circ, \tau_1)$ sont continues.

Théorème 7.1.6. *Soit $(G, \circ, \tau)$ un groupe abélien localement compact. Alors $(\phi.\psi) \in \widehat{G}$ pour $\phi \in \widehat{G}, \psi \in \widehat{G}$, la famille $\mathcal{U}_{\hat{\tau}}$ est la famille des ensembles ouverts de $\widehat{G}$ pour une topologie $\hat{\tau}$ sur $\widehat{G}$ et $(\widehat{G}, .\hat{\tau})$ est un groupe topologique abélien localement compact.*

De plus si on pose, pour $x \in G$, $\phi \in \widehat{G}$,

$$\tilde{x}(\phi) = \phi(x),$$

alors $\tilde{x} \in \widehat{\widehat{G}}$ pour tout $x \in G$, et l'application $x \to \tilde{x}$ est un isomorphisme de groupes topologiques de $(G, ., \circ\tau)$ sur $\widehat{\widehat{G}}, ., \hat{\hat{\tau}})$.

Démonstration : Le fait que $(\widehat{G}, .\hat{\tau})$ est un groupe topologique abélien résulte de vérifications de routine. Le fait que ce groupe est localement compact est un peu plus délicat, et le fait que l'application $x \to \tilde{x}$ est un isomorphisme de groupes topologiques de $(G, ., \circ\tau)$ sur $(\widehat{\widehat{G}}, .\hat{\hat{\tau}})$ est un résultat profond et difficile.

Nous renvoyons à l'ouvrage classique de W. Rudin [10] pour des démonstrations détaillées. □

Notons que lélément 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 localement compact abélien noté additivement,

la condition $\phi(x \circ y) = \phi(x)\phi(y)$ dans la définition des caractères de G sécrit évidemment $\phi(x+y) = \phi(x)\phi(y)$.

L'exemple le plus simple de groupe localement compacts abélien est celui des groupes abéliens finis. Dans ce cas la seule topologie possible est la topologie discrète, qui est la topologie pour laquelle tout ensemble est ouvert.

On peut par exemple décrire les caractères du groupe additif $\mathbb{Z}/N\mathbb{Z}$.

Exemple 7.1.7. *Soit $N \geq 1$, et soit $\omega_N = e^{\frac{2i\pi}{N}}$. On pose, pour $0 \leq p \leq N-1$, $0 \leq q \leq N-1$,*

$$\phi_p(\overline{q}) = \omega_N^{pq}.$$

Alors l'application $\overline{p} \to \phi_p$ est un isomorphisme de groupes de $\mathbb{Z}/N\mathbb{Z}$ sur $\widehat{\mathbb{Z}/N\mathbb{Z}}$.

La formule ci-dessus permet en fait de définir ϕ_p pour $p \in \mathbb{Z}$, et une vérification de routine montre que ϕ_p est bien un homomorphisme de groupes de $(\mathbb{Z}/N\mathbb{Z}, +)$ dans $\mathbb{T}$. Un tel homomorphisme est automatiquement continu puisque la topologie de $\mathbb{Z}/N\mathbb{Z}$ est la topologie discrète, donc $\phi_p \in \widehat{\mathbb{Z}/N\mathbb{Z}}$. On a $\phi_{n+m} = \phi_m.\phi_n$ pour $n, m \in \mathbb{Z}$, de sorte que l'application $\theta : p \to \phi_p$ est un morphisme de groupes de $(Z, +)$ dans $(\widehat{\mathbb{Z}/N\mathbb{Z}}, .)$. D'autre part si ϕ est un caractère de $\mathbb{Z}/N\mathbb{Z}$, $\phi(\overline{1})$ est une racine N^e de l'unité, puisque $\phi(\overline{1})^N = \phi(N\overline{1}) = \phi(\overline{N}) = \phi(\overline{0}) = 1$. Donc il existe $p \in \{0, ..., N-1\}$ tel que $\phi(\overline{1}) = e^{\frac{2ip\pi}{N}}$, et $\phi(\overline{q}) = \phi(\overline{1})^q = \omega_N^{pq} = \phi_p(\overline{q})$ pour $0 \leq q \leq N-1$. Donc $\phi = \phi_p$, et θ est surjective. L'élément unité de $\widehat{\mathbb{Z}/N\mathbb{Z}}$ est le caractère e défini par la formule $e(\overline{q}) = 1$ pour $q \in \mathbb{Z}$. Donc si $\phi_p = e$ on a $1 = \phi_p(\overline{1}) = e^{\frac{2ip\pi}{N}}$, et $p \in N\mathbb{Z}$, et il est clair que réciproquement $\phi_p = e$ si $p \in N\mathbb{Z}$. Donc $Ker(\theta) = N\mathbb{Z}$ et il résulte du *théorème de factorisation* vu au Chapitre 3 que l'application $\overline{p} \to \phi_p$ est un isomorphisme de groupes de $\mathbb{Z}/N\mathbb{Z}$ sur $\widehat{\mathbb{Z}/N\mathbb{Z}}$.

On a le résultat suivant.

Proposition 7.1.8. *Soit $(G_1, \circ, \tau_1), ..., (G_p, \circ, \tau_p)$ une famille finie de groupes abéliens localement compacts et soit $(G_1 \times ... \times G_p, \circ, \tau_1 \times ... \times \tau_p)$ le groupe topologique obtenu en munissant le groupe produit $G_1 \times ... \times G_p)$ de la topologie produit $\tau_1 \times ... \times \tau_p$. Pour $(\phi_1, ..., \phi_p) \in \widehat{G_1} \times ... \times \widehat{G}_p$, $(x_1, ..., x_p) \in G_1 \times ... \times G_p$, posons*

$$(\phi_1 \times ... \times \phi_p)(x_1, ..., x_p) = \phi_1(x_1)...\phi_p(x_p).$$

Alors $(G_1 \times ... \times G_p, \circ, \tau_1 \times ... \times \tau_p)$ est un groupe localement compact abélien, et l'application $(\phi_1, ..., \phi_p) \to \phi_1 \times ... \times \phi_p$ est un isomorphisme de $(\widehat{G_1} \times ... \times \widehat{G_p}, \circ, \hat{\tau}_1 \times ... \times \hat{\tau}_p)$ sur le dual du groupe $(G_1 \times ... \times G_p, \circ, \tau_1 \times ... \times \tau_p)$.

Démonstration : La preuve se réduit à des vérifications de routine qui sont laissées au lecteur. □

En ce qui concerne le groupe additif ${\mathbb{F}_2}^k = (\mathbb{Z}/2\mathbb{Z})^k$, on a posé à la formule 5.11, pour $x = (x_1, ..., x_p) \in \mathbb{F}_2^k$, $y = (y_1, ..., y_p) \in \mathbb{F}_2^k$,

$$x.y = \sum_{j=0}^{k-1} x_j y_j.$$

Avec la convention $(-1)^{\overline{n}} = (-1)^n$ pour $nin\mathbb{Z}$, où $\overline{n} = n + 2\mathbb{Z}$ désigne la classe de n dans $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, posons, pour $x \in \mathbb{F}_2^k, y \in \mathbb{F}_2^k$,

$$\phi_y(x) = (-1)^{x.y}. \tag{7.1}$$

On peut alors décrire les caractères de $\mathbb{F}_2^k$.

Exemple 7.1.9. *L'application $\phi_y : x \to \phi_y(x)$ est un caractère de $\mathbb{F}_2^k$ pour tout $y \in \mathbb{F}_2^k$, et l'application $y \to \phi_y$ est un isomorphisme de groupes de $(\mathbb{F}_2^k, +)$ sur $(\widehat{\mathbb{F}_2^k}, .)$.*

En effet il est clair que ϕ_y est un caractère de $\mathbb{F}_2^k$ pour tout $y \in \mathbb{F}_2^k$, et que l'application $y \to \phi_y$ est un morphisme de groupes de $(\mathbb{F}_2^k, +)$ dans $(\widehat{\mathbb{F}_2^k}, .)$.

Les caractères de $\mathbb{F}_2$ sont de la forme $\overline{n} \to \epsilon^n$, où $\epsilon \in \{-1, 1\}$. Donc pour tout caractère de $\mathbb{F}_2^k$ il existe unique famille $(\epsilon_0, ..., \epsilon_{k-1})$ de $k-1$ éléments de $\{-1, 1\}$ tels que l'on ait

$$\phi(x_0, ..., x_{k-1}) = \epsilon_0^{x_0} ... \epsilon_{k-1}^{x_{k-1}}.$$

On voit alors qu'il existe un unique $y = (y_0, ..., y_{k-1}) \in \mathbb{F}_2^k$ tel que $\phi = \phi_y$. Cet élément y est donné par les formules $y_j = \overline{a}_j$, avec $a_j = 0$ si $\epsilon_j = 1$ et $a_j = 1$ si $\epsilon_j = -1$.

Signalons sans démonstration l'important théorème suivant.

Théorème 7.1.10. *Soit $(G, \circ)$ un groupe abélien fini non réduit à son élément unité. Alors il existe une famille finie $(N_1, ..., N_k)$ d'entiers ≥ 2 tels que G soit isomorphe au groupe produit $(Z/N_1\mathbb{Z}) \times ... \times \mathbb{Z}/N_k\mathbb{Z})$.*

On déduit immédiatement de l'exemple 7.1.7 et du théorème 7.1.10 que tout groupe abélien fini G est isomorphe à son groupe dual $\widehat{G}$. En particulier, G et $\widehat{G}$ ont le même nombre d'éléments. Ceci peut aussi se déduire du thèorème de dualité de Pontryagin. En effet on verra plus loin que si G est un groupe abélien fini les éléments de $\widehat{G}$ forment une famille libre de l'algèbre de groupe $\mathbb{C}[G]$, dont la dimension est égale au nombre d'éléments de G. La notation $|A|$ désignant le nombre d'éléments d'un ensemble fini A on obtient $|G| \geq \widehat{G}| \geq |\widehat{\widehat{G}}| = |G|$, et $|G| = |\widehat{G}|$.

On va maintenant identifier les caractères de $(\mathbb{R}, +)$. On a le lemme suivant.

Lemme 7.1.11. *Soit $\phi : \mathbb{R} \to \mathbb{C} \setminus \{0\}$ une application continue vérifiant, pour tout couple (s, t) de réels*

$$\phi(s + t) = \phi(s)\phi(t).$$

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 $h \neq 0$,

$$\psi(\alpha)\psi(h) = \int_0^\alpha \phi(t)\phi(h)dt = \int_0^\alpha \phi(t+h)dt = \int_\alpha^{\alpha+h} \phi(t)dt$$
$$= \psi(\alpha+h) - \psi(h).$$

On obtient

$$\psi(\alpha)\frac{\phi(h)-1}{h} = \frac{\psi(\alpha+h)-\psi(\alpha)}{h} - \frac{\psi(h)-\psi(0)}{h},$$

$$\lim \psi(\alpha)\frac{\phi(h)-1}{h} = \psi'(\alpha) - \psi'(0) = \phi(\alpha) - 1.$$

Comme $\phi(0) = 1$, et comme $\psi(\alpha) \neq 0$, on voit que ψ 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 $\phi'(s) = z\phi(s)$ for $s \in \mathbb{R}$, avec $z = \phi'(0)$. Donc $\phi(s) = \phi(0)e^{sz} = e^{sz}$ pour $s \in \mathbb{R}$. □

Proposition 7.1.12. *Posons $\phi_t(s) = e^{ist}$ pour $t \in \mathbb{R}, s \in \mathbb{R}$, de sorte que ϕ_t est un caractère de $(\mathbb{R}, +)$. Alors l'application $\theta_1 : t \to \phi_t$ est un isomorphisme de groupes topologiques de $(\mathbb{R}, +)$ sur $(\widehat{\mathbb{R}}, .)$.*

Démonstration : On a $\phi_t'(0) = it$, donc θ_1 est injective. Soit maintenant $\phi \in \widehat{\mathbb{R}}$. Il existe $z \in \mathbb{C}$ tel que $\phi(s) = e^{sz}$ pour tout $s \in \mathbb{R}$. On a $1 = |\phi(s)| = e^{sRe(z)}$ pour $s \in \mathbb{R}$, donc $Re(z) = 0$ et $\phi = \phi_t$ avec $t = Im(z) = i^{-1}z$. Il est clair que $\phi_{t_1+t_2} = \phi_{t_1}\phi_{t_2}$ pour $t_1, t_2 \in \mathbb{R}$, donc θ_1 est un homomorphisme de groupes de $(\mathbb{R}, +)$ sur $(\widehat{R}, .)$. Le fait que θ_1 et θ_1^{-1} sont continues résulte de considérations assez techniques que nous omettrons. □

Pour $x = (x_1, ..., x_p), y = (y_1, ..., y_p) \in \mathbb{R}^p$, on note $< x, y >= x_1y_1 + ... + x_py_p$ le produit scalaire de x et y.

On déduit alors de la proposition 7.1. 8 le résultat suivant.

Corollaire 7.1.13. *Posons $\phi_y(x) = e^{i<x,y>}$ pour $x \in \mathbb{R}^p, y \in \mathbb{R}^p$. Alors l'application $\theta_p : y \to \phi_y$ est un isomorphisme de groupes topologiques de $(\mathbb{R}^p, +)$ sur $(\widehat{\mathbb{R}^p}, .)$.*

La topologie discrète sur un ensemble E est la topologie pour laquelle tout sous-ensemble de E est ouvert, ce qui fait que toute application d'un ensemble muni de la topologie discrète dans un espace topologique quelconque est continue. En particulier un groupe quelconque devient un groupe topologique localement compact quand on le munit de la topologie discrète. On peut montrer qu'un groupe localement compact abélien 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 conterons ici de discuter la dualité entre le groupe discret $(\mathbb{Z}, +)$ et le groupe compact $(\mathbb{T}, .)$.

Théorème 7.1.14. *Posons $\phi_z(n) = \psi_n(z) = z^n$ pour $n \in \mathbb{Z}, z \in \mathbb{T}$. Alors l'application $z \to \phi_z$ est un isomorphisme de groupes topologiques de $(\mathbb{T}, .)$ sur $(\widehat{\mathbb{Z}}, .)$, et l'application $n \to \psi_n$ est un isomorphisme de groupes topologiques de $(\mathbb{Z}, +)$ sur $(\widehat{\mathbb{T}}, .)$.*

Démonstration : Il est clair que $\phi_z \in \widehat{\mathbb{Z}}$ pour tout $z \in \mathbb{T}$, et que $\phi_{z_1 z_2} = \phi_{z_1}\phi_{z_2}$ pour $z_1, z_2 \in \mathbb{T}$. Comme $z = \phi_z(1)$ on voit que l'application $z \to \phi_z$ est un homomorphisme injectif de $\mathbb{T}$ dans $\widehat{\mathbb{Z}}$. D'autre part si $\phi \in \widehat{T}$ posons $z = \phi(1)$. Alors $\phi(n) = z^n$ et $\phi(-n) = \phi(n)^{-1} = z^{-n}$ pour $n \geq 0$, donc $\phi = \phi_z$. Soit $(z_p)_{p\geq 1}$ une suite d'éléments de $\mathbb{T}$. Si la suite $(z_p)_{p\geq 1}$ converge vers $z \in \mathbb{T}$, alors $\phi_z(n) = z^n = \lim_{p\to+\infty} z_p^n = \lim_{p\to+\infty}\phi_{z_p}(n)$ pour tout $n \in \mathbb{Z}$. Comme les parties compactes de $\mathbb{Z}$ sont les parties finies de $\mathbb{Z}$, on en déduit que la suite $(\phi_{z_p})_{p\geq 1}$ converge vers ϕ_z dans $\widehat{\mathbb{Z}}$. Réciproquement si $(\phi_{z_p})_{p\geq 1}$ converge vers ϕ_z dans $\hat{\mathbb{Z}}$, alors $z = \phi_z(1) = \lim_{p\to+\infty}\phi_z(1) = z$, et on voit que l'isomorphisme de groupes $z \to \phi_z$ est en fait un isomorphisme de groupes topologiques de $(\mathbb{T}, .)$ sur $(\widehat{\mathbb{Z}}, .)$.

Il est clair que $\psi_n \in \hat{T}$ pour $n \in \mathbb{Z}$ et que l'application $n \to \psi_n$ est un homomorphisme de $(\mathbb{Z}, +)$ dans $\widehat{T}, .)$. Soit maintenant $\phi \in \widehat{T}$, et posons $\tilde{\psi}(x) = \psi(e^{ix})$ pour $x \in \mathbb{R}$. Alors $\tilde{\psi} \in \widehat{\mathbb{R}}$, et il existe $y \in \mathbb{R}$ tel que $\tilde{\psi}(x) = e^{ixy}$ pour $x \in \mathbb{R}$. En particulier $e^{2i\pi y} = \tilde{\psi}(2\pi) = \psi(e^{2i\pi}) = \psi(1) = 1$, donc $y \in \mathbb{Z}$ et $\psi(e^{ix}) = \tilde{\psi}(ix) = e^{inx} = (e^{ix})^y$ pour $x \in \mathbb{R}$, et $\psi = \psi_y$. Si $\psi_m = \psi_n$ avec $m, n \in \mathbb{Z}, m \geq n$, alors $z^{m-n} = \psi_{m-n}(z) = 1$ pour tout $z \in \mathbb{T}$, et par conséquent $m = n$ puisque l'équation $z^k = 1$ n'admet que k solutions dans $\mathbb{C}$ si k est un entier strictement positif. Soit maintenant $\psi_{n_0} \in \widehat{\mathbb{T}}$. Pour $n \neq n_0$ on a $\sup_{z\in\mathbb{T}}|\psi_n(z) - \psi_{n_0}(z| = \sup_{z\in\mathbb{T}}|1 - z^{n_0-n}| = 2$. Donc $\{\psi_{n_0}\} = \{\psi \in \widehat{T} \mid \sup_{z\in\mathbb{T}}|\psi(z) - \psi_{n_0}(z)| < 2\}$ est un ouvert de $\widehat{T}$, et la topologie de $\mathbb{T}$ est la topologie discrète. Donc l'isomorphisme $n \to \psi_n$ est trivialement un isomorphisme de groupes topologiques du groupe discret $(\mathbb{Z}, +)$ sur le groupe discret $(\widehat{\mathbb{T}}, .)$. □

7.2 Mesure de Haar et transformation de Fourier, théorie générale

On va maintenant décrire un résultat très général, la construction de Haar qui permet de munir tout groupe abélien localement compact $(G, \circ, \tau)$ d'une mesure positive m_G invariante par translations. On dira qu'un sous-ensemble de G est borné s'il est contenu dans un compact de G, et on pose $x \circ A := \{x \circ a\}_a \in A\}$ pour $x \in G, A \subset G$. On peut définir $m_G(U) \in]0, +\infty[$ pour tout ouvert borné U de G, avec la propriété que $m_G(x \circ U) = m_G(U)$ pour tout $x \in G$, puis $m_G(K) \in]0, +\infty[$ pour tout compact K de G. On développe alors pour G et m_G une théorie analogue à la théorie de la mesure et 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), et m_G est "invariante par translation", ce qui signifie que $m_G(x \circ A) = m_G(A) \in [0, +\infty]$ pour tout $x \in G$ et pour toute

partie mesurable A de G. On peut démontrer que m_G, que l'on appelle la mesure de Haar sur G, est invariante à une constante près : si une autre mesure non nulle m sur G vérifie la propriété ci-dessus alors il existe $\lambda > 0$ tel que $m = \lambda m_G$.

Dans le cas de $\mathbb{R}$ ou $\mathbb{R}^n$, on retrouve la mesure de Lebesgue. Dans le cas du cercle unité on obtient la " mesure de Lebesgue normalisée" : les sous-ensembles mesurables A du cercle unité sont les ensembles de la forme $A = \{e^{ix}\}_{x\in\tilde{A}}$, où $\tilde{A}$ est une partie mesurable de $[0, 2\pi[$, 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" souvent la mesure de Haar sur G en imposant la condition $m_G(G) = 1$ (attention, cette condition n'est pas vérifiée par la mesure de comptage sur les groupes finis ayant au moins deux éléments). Un exemple évident de mesure de Haar est la "mesure de comptage" sur les groupes discrets, qui à $A \subset G$ associe le cardinal $|A|$ de A (avec la convention $|A| = +\infty$ si A est infini). Cette mesure est évidemment invariante par translation, et on a donc l'exemple banal suivant.

Exemple 7.2.1. *Soit $(G, \circ)$ un groupe discret. La mesure de comptage donnée par la formule $m_G(A) = |A|$ définit la mesure de Haar sur G.*

Dans la suite on munit un groupe localement compact abélien $(G, \circ, \tau)$ de la mesure de Haar m_G. On notera $\int_E f(x)dx$ l'intégrale sur un ensemble mesurable $E \subset G$ d'une fonction f intégrable sur E, les notions de mesurabilité et d'intégrabilité étant celles relatives à la mesure de Haar.

Definition 7.2.2. *On note $L^1(G)$ l'enemble des fonctions intégrables sur G et $L^2(G)$ l'ensemble des fonctions mesurables et de carré intégrable sur G. D'autre part on note $\mathcal{C}(G)$ l'ensemble des fonctions continues sur G, et on note $\mathcal{C}_0(G)$ l'enemble des fonctions continues sur G telles que pour tout $\epsilon > 0$ il existe un sous-ensemble compact K_ϵ de G pour lequel $sup_{x\in G\setminus K_\epsilon}|f(x)| < \epsilon$. L'ensemble des fonctions continues sur G nulles en dehors d'un compact de G, appelées fonctions continues à support compact sur G, sera 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 $\|f\|_2 = \sqrt{\int_G |f(x)|^2 dx}$. On pose également $\|f\| = max_{x\in G}|f(x)|$ pour $f \in \mathcal{C}_0(G)$.

Notons que, de même que sur $\mathbb{R}$, on identifie les fonctions mesurables sur g qui sont égales "presque partout", c'est à dire égales en dehors d'un ensemble de mesure de Haar nulle. On notera que si G est discret, le seul ensemble de mesure nulle est l'ensemble vide, et deux fonctions égales presque partout sur G sont en fait égales sur G.

On peut alors definir la transformée de Fourier sur $L^1(G)$.

Definition 7.2.3. *Soit $(G, \circ, \tau)$ un groupe abélien localement compact. Pour $f \in L^1(G)$ on définit la transformée de Fourier $\mathcal{F}_{\mathcal{G},\widehat{\mathcal{G}}}(f) = \widehat{f} : G \to \mathbb{C}$ par la formule*

$$\forall \chi \in \widehat{G}, \widehat{f}(\chi) = \int_G f(\chi)\overline{\chi}(x)dx. \tag{7.2}$$

Dans toute la suite on écrira $\mathcal{F}$ au lieu de $\mathcal{F}_{G,\widehat{G}}$ quand aucune confusion n'est à craindre. On obtient alors pour la transformée de Fourier sur $L^1(G)$ des résultats analogues aux résultats obtenus pour la transformée de Fourier sur $L^1(\mathbb{R})$.

Théorème 7.2.4. *(i) On a $\widehat{f} \in \mathcal{C}_0(\widehat{G})$ pour $f \in L^1(G)$.*

(ii) Soient $f, g \in L^1(G)$. Alors la fonction $s \to f(s)g(t-s)$ 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 $\chi \in \widehat{G}$,

$$\mathcal{F}(f * g)(\chi) = \mathcal{F}(f)(\chi)\mathcal{F}(g)(\chi). \tag{7.3}$$

Démonstration : La première propriété résulte d'une version convenable 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 sur G à support compact telles que $\lim_{n\to+\infty}\|f - f_n\|_1 = 0$. La deuxième propriété résulte d'une version convenable du théorème de Fubini.

Nous renvoyons à l'ouvrage de Rudin [10] pour plus de détails. □

7.3 Formule de Plancherel-Parseval et formule d'inversion de Fourier

On va maintenant donner une version générale de la formule de Plancherel-Parseval. Nous admettrons les lemmes suivants

Lemme 7.3.1. *Soit $(G, \circ, \tau)$ un groupe localement compact abélien. Il existe un réel $\lambda > 0$ tel que l'on ait, pour toute fonction $f \in \mathcal{C}_c(G)$*

$$\|f\|_2 = \lambda^2\|\widehat{f}\|_2.$$

Lemme 7.3.2. *Soit $(G, \circ, \tau)$ un groupe localement compact abélien. Il existe pour toute fonction $f \in L^2(G)$ une suite $(f_n)_{n\geq 1}$ de fonctions continues à support compact sur G telle que $\lim_{n\to+\infty}\|f - f_n\|_2 = 0$, et il existe $h \in L^2(\widehat{G})$ telle que $\lim_{n\to+\infty}\|h - \widehat{f_n}\|_2 = 0$.*

En fait la fonction h ci-dessus est indépendante du choix de la suite $(f_n)_{n\geq 1}$. En effet supposons que $\lim_{n\to+\infty}\|f - g_n\|_2 = 0$, avec $g_n \in \mathcal{C}_c(G)$ pour $n \geq 1$. On a alors

$$\|h - \widehat{g_n}\|_2 \leq \|h - \widehat{f_n}\|_2 + \|\widehat{f_n} - \widehat{g_n}\|_2 \leq \|h - \widehat{f_n}\|_2 + \frac{1}{\lambda^2}\|f_n - g_n\|_2$$
$$\leq \|h - \widehat{f_n}\|_2 + \frac{1}{\lambda^2}\|f_n - f\|_2 + \frac{1}{\lambda^2}\|f - g_n\|_2,$$

et par conséquent $\lim_{n\to+\infty}\|h - \widehat{g_n}\|_2 = 0$. Ceci permet d'introduire la définition suivante.

Definition 7.3.3. *Pour $f \in L^2(G)$, on définit $\mathcal{F}(f) = \widehat{f} \in L^2(\widehat{G})$ par la formule*

$$lim_{n\to+\infty}\|f - \widehat{f_n}\|_2 = 0,$$

où $(f_n)_{n\geq 1}$ est une suite quelconques de fonctions continues sur G à support compact vérifiant $lim_{n\to+\infty}\|f - f_n\|_2 = 0$.

On obtient alors une version très générale des formules de Plancherel-Parseval :

Théorème 7.3.4. *La transformée de Fourier $\mathcal{F} : f \to \widehat{f}$ est une application linéaire bijective de $L^2(G)$ sur $L^2(\widehat{G})$ et on a, pour $f, g \in L^2(G)$, la formule de Plancherel*

$$\int_G f(x)\overline{g(x)}dx = \lambda^2 \int_{\widehat{G}} \widehat{f}(\chi)\overline{\widehat{g}(x)}d\chi. \tag{7.4}$$

En particulier les fonctions $f \in L^2(G)$ vérifient la formule de Parseval :

$$\int_G |f(x)|^2 dx = \lambda^2 \int_{\widehat{G}} \widehat{f}(\chi)|^2 d\chi. \tag{7.5}$$

On va maintenant donner une version générale de la formule d'inversion de Fourier.

Théorème 7.3.5. *Soit $f \in L^1(G)$. Si $\widehat{f} \in L^1(\widehat{G})$, on a pour presque tout $x \in G$,*

$$f(x) = \lambda^2 \int_{\widehat{G}} \widehat{f}(\chi)\chi(x)d\chi \tag{7.6}$$

Notons que si $f \in L^2(G)$, et si $\widehat{f} \in \mathcal{C}_c(\widehat{G})$, on peut montrer que l'on a, pour presque tout $x \in G$,

$$f(x) = \lambda^2 \int_{\widehat{G}} \widehat{f}(\chi)\chi(x)dx.$$

On peut alors poser $\mathcal{F}^{-1}(g)(x) = \lambda^2 \int g(\chi)\chi(x)d\chi$ pour $g \in \mathcal{C}_c(\widehat{G})$, et définir $\mathcal{F}^{-1} : L^2(\widehat{G}) \to L^2(G)$ pour $g \in L^2(\widehat{g})$ par la formule

$$\lim_{n\to+\infty}\|\mathcal{F}^{-1}(g) - \mathcal{F}^{-1}(g_n)\|_2 = 0,$$

où $(g_n)_{n\geq 1}$ est une suite d'éléments de $\mathcal{C}_c(\widehat{G})$ telle que $\lim_{n\to+\infty}\|g-g_n\|_2 = 0$. De même que plus haut, on vérifie que cette définition ne dépend pas du choix de la suite $(g_n)_{n\geq 1}$, et on vérifie également que l'application ainsi définie est bien l'application réciproque de la transformation de Fourier $\mathcal{F} : L^2(G) \to L^2(\widehat{G})$.

Il serait tentant d'essayer de définir la transformée de Fourier $\widehat{f}$ de $f \in L^2(G)$ par une formule du type $\widehat{f}(\chi) = \lim_{n\to+\infty}\widehat{f}(\chi)$ pour presque tout $\chi \in \widehat{G}$, où (f_n) est une suite d'éléments de $\mathcal{C}_c(G)$ telle que $\lim_{n\to+\infty}\|f - f_n\|_2 = 0$. Malheureusement la réalité est plus compliquée et il faut en général remplacer la suite $(f_n)_{n\geq 1}$ par une sous-suite pour obtenir une telle limite ponctuelle presque partout. On peut également au lieu d'utiliser une suite $(f_n)_{n\geq 1}$ de fonctions continues à support compact utiliser une suite de fonctions de $L^1(G) \cap L^2(G)$. Dans le cas où $G = \mathbb{R}$ on peut par exemple utiliser la suite $(fu_n)_{n\geq 1}$, avec $u_n(x) = 0$ pour $|x| \leq 1/n$, $u_n(x) = 0$ pour $|x| > 1/n$, et dans ce cas le théorème de Carleson [2] (voir le Chapitre 2) montre que l'on a, pour presque tout $s \in \mathbb{R}$,

$$\widehat{f}(s) = \lim_{n\to+\infty}\widehat{fu_n}(s) = \lim_{n\to+\infty}\int_{-n}^{n} f(x)e^{-isx}dx,$$

où on a identifié la transformée de Fourier sur $\mathbb{R}$ décrite au Chapitre 2 et la transformée de Fourier sur $\mathbb{R}$ décrite ici en utilisant l'identification triviale décrite plus loin.

On peut faire des remarques analogues concernant la transformée de Fourier inverse, qui est en fait liée à la transformée de Fourier par la formule

$$[\mathcal{F}_{G,\widehat{G}}]^{-1}(g) = \lambda^2 \overline{\mathcal{F}_{\widehat{G},G}(\overline{g})}, \tag{7.7}$$

valable pour $g \in L^2(\widehat{G})$, formule où on a identifié G à $\widehat{\widehat{G}}$ en utilisant le théorème de dualité de Pontryagin. Ceci donne, pour $f \in L^2(G)$,

$$f = \lambda^2 \overline{\mathcal{F}_{\widehat{G},G}\left(\overline{\mathcal{F}_{G,\widehat{G}}(f)}\right)}. \tag{7.8}$$

On notera que la constante λ qui intervient dans la formule de Plancherel-Parseval dépend du choix des mesures de Haar sur G et $\widehat{G}$, et on peut toujours "normaliser" le choix des mesures de Haar sur G et $\widehat{G}$ de façon que cette constante λ soit égale à 1. C'est ainsi que certains auteurs définissent la transformée de Fourier sur $L^1(\mathbb{R})$ par la formule $\widehat{f}(s) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} f(x) e^{-isx} dx$, ce qui supprime le facteur $\frac{1}{2\pi}$ dans la formule de Parseval. Nous avons préféré nous en tenir à la définition utilisée au Chapitre 2, ce qui compte tenu de l'identification entre $\widehat{R}$ et $\mathbb{R}$ décrite ci-dessous correspond à une constante $\lambda = \frac{1}{\sqrt{2\pi}}$

On va maintenant expliciter cette théorie générale dans plusieurs cas particuliers importants.

7.4 Transformation de Fourier sur la droite

De même que plus haut, on pose $\phi_s(x) = e^{isx}$ pour $s, t \in \mathbb{R}$. Notons $\mathcal{F}_{\mathbb{R},\mathbb{R}} : L^1(\mathbb{R}) \to L^1(\mathbb{R})$ la transformation de Fourier introduite au Chapitre 2 et $\mathcal{F}_{\mathbb{R},\widehat{\mathbb{R}}}$ la transformation de Fourier introduite ci-dessus. On a vu que l'application $s \to \phi_s$ est un isomorphisme de groupes topologiques de $(\mathbb{R}, +)$ sur $(\widehat{\mathbb{R}}, .)$ et on a la formule

$$\mathcal{F}_{\mathbb{R},\mathbb{R}}(f)(s) = \mathcal{F}_{\mathbb{R},\widehat{\mathbb{R}}}(f(\phi_s)), \tag{7.9}$$

formule qui s'écrit plus simplement sous la forme $\mathcal{F}_{\mathbb{R},\mathbb{R}}(f) = \mathcal{F}_{\mathbb{R},\widehat{\mathbb{R}}}(f \circ \phi)$ si on note ϕ l'application $s \to \phi_s$, et qui reste valable pour $f \in L^2(\mathbb{R})$. Avec ces notations, la mesure de Haar sur $\mathbb{R}$ est la mesure de Lebesgue et la mesure de Haar sur $\widehat{\mathbb{R}}$ est la mesure $m_{\widehat{\mathbb{R}}}$ induite par la mesure de Lebesgue sur $\mathbb{R}$: un sous-ensemble A de $\widehat{\mathbb{R}}$ est mesurable si et seulement si $\phi^{-1}(A) = \{s \in \mathbb{R} \mid \phi_s \in A\}$ est mesurable au sens de Lebesgue, et dans ce cas on a

$$m_{\widehat{\mathbb{R}}}(A) = \int_{\phi^{-1}(A)} dx.$$

On a une interprétation analogue pour la transformation de Fourier sur $\mathbb{R}^p$.

7.5 Séries de Fourier et transformation de Fourier sur le cercle

Soit $T > 0$, et soit $f : \mathbb{R} \to \mathbb{C}$ une fonction de période T. Pour $z = e^{ix} \in \mathbb{T}$, posons $\tilde{f}(z) = f(\frac{xT}{2\pi})$. Notons que $f(\frac{(x+2k\pi)T}{2\pi}) = f(xT + kT) = f(\frac{xT}{2\pi})$ pour $k \in \mathbb{Z}$, de sorte que cette définition ne dépend pas du choix de l'argument x de z. Il est clair que $\tilde{f}$ est mesurable sur $\mathbb{T}$ si et seulement si f est mesurable sur $\mathbb{R}$, que $\tilde{f}$ est continue sur $\mathbb{T}$ si et seulement si f est continue sur $\mathbb{R}$, que $\tilde{f}$ est intégrable sur $\mathbb{T}$ si et seulement si f est intégrable sur $[0, T]$, et que $\tilde{f}$ est de carré intégrable sur $\mathbb{T}$ si seulement si f est de carré 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 $\mathbb{T}$, et intégrable sur $[0, T]$, on définit pour $n \in \mathbb{Z}$ le coefficient de Fourier d'ordre n de f par la formule

$$\widehat{f}(n) = \widehat{\tilde{f}}(\chi_n) = \frac{1}{2\pi} \int_0^{2\pi} \tilde{f}(e^{ix}) \overline{\chi}(x) dx = \frac{1}{2\pi} \int_0^{2\pi} f\left(\frac{xT}{2\pi}\right) e^{-inx} dx.$$

En posant $s = \frac{2\pi}{T}$, on obtient la formule classique

$$\widehat{f}(n) = \frac{1}{T} \int_0^T f(s) e^{-2i\pi ns} ds = \frac{1}{T} \int_0^T f(s) e^{-in\omega s} ds, \tag{7.10}$$

où $\omega := \frac{2\pi}{T}$ est la *fréquence* associée à la période T.

On notera $l^1(\mathbb{Z}) := \{u = ((u_n)_{n\in\mathbb{Z}} \in \mathbb{C}^{\mathbb{Z}} \mid \|u\|_1 := \sum_{n\in\mathbb{Z}} |u_n| < +\infty\}$ l'ensemble des suites sommables sur $\mathbb{Z}$, qui est l'espace L^1 associé à la mesure de comptage sur $\mathbb{Z}$, c'est à dire l'espace L^1 associé à la mesure de Haar sur $\mathbb{Z}$ muni de la topologie discrète, et on pose $c_0(\mathbb{Z}) := \{\{u = ((u_n)_{n\in\mathbb{Z}} \in \mathbb{C}^{\mathbb{Z}} \mid \lim_{n\to+\infty} u_n = 0\}$, 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 $\hat{g} \in C_0(\widehat{\mathbb{T}}) \simeq c_0(\mathbb{Z})$, et on obient le résultat standard suivant.

Proposition 7.5.1. *Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction périodique de période $\mathbb{T}$. Si f est intégrable sur $[0, T]$, on a*

$$lim_{|n|\to+\infty} \widehat{f}(n) = 0.$$

On sait qu'il existe une constante $\lambda > 0$ telle que l'on ait, pour $g \in L^2(\mathbb{T})$,

$$\frac{1}{2\pi} \int_0^{2\pi} |g(e^{is})|^2 ds = \lambda^2 \sum_{n\in\mathbb{Z}} |\widehat{g}(\chi_n)|^2.$$

En posant $g(e^{is}) = 1$ pour $s \in \mathbb{R}$, on obtient $\widehat{g}(\chi_0) = 1$, $\widehat{g}(\chi_n) = 0$ pour $n \neq 0$, donc $\lambda = 1$, ce qui donne

$$\frac{1}{2\pi} |g(e^{is})|^2 ds = \sum_{n\in\mathbb{Z}} |\widehat{g}(\chi_n)|^2. \tag{7.11}$$

Par changement de variables, on a, si f est mesurable sur $\mathbb{R}$, périodique de période T, et intégrable sur $[0, T]$,

$$\frac{1}{2\pi}|\tilde{f}(e^{is})|^2 ds = \frac{1}{2\pi}\int_0^{2\pi}\left|f\left(\frac{sT}{2\pi}\right)\right| ds = \frac{1}{T}\int_0^T |f(x)|^2 dx.$$

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 7.5.2. *Soient f et g deux fonctions mesurables sur $\mathbb{R}$, périodiques de période T, de carré intégrables sur $[0,T]$. On a alors*

$$\frac{1}{T}\int_0^T f(x)\overline{g(x)}dx = \sum_{n\in Z}\widehat{f}(n)\overline{\widehat{g}(n)}.$$

En particulier si f est mesurable sur $\mathbb{R}$, périodique de période T, et de carré intégrable sur $[0,T]$, on a

$$\frac{1}{T}\int_0^T |f(x)|^2 dx = \sum_{n\in Z}|\widehat{f}(n)|^2. \tag{7.12}$$

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 $x \in \mathbb{R}$,

$$g(e^{ix}) = \int_{\widehat{T}}\widehat{g}(\chi)\chi(e^{ix})d\chi = \sum_{n\ \in\mathbb{Z}}\widehat{g}(n)e^{inx}.$$

Par changement de variables, on voit que si $f : \mathbb{R} \to \mathbb{C}$ est périodique de période T, intégrable sur $[0,T]$, et si $\sum_{n\in\mathbb{Z}}\widehat{f}(n) < +\infty$, on a, pour presque tout $x \in \mathbb{R}$,

$$f(x) = \sum_{n\ \in\mathbb{Z}}\widehat{f}(n)e^{in\omega x}. \tag{7.13}$$

La série de Fourier d'une fonction $f : \mathbb{R} \to \mathbb{C}$, périodique de période T et intégrable sur $[0,T]$ est par définition la série

$$S(f)(x) = \sum_{n\in\mathbb{Z}}\widehat{f}(n)e^{in\omega x},$$

où $\omega = 2\pi/T$ est la fréquence associée à la période T.

Si f est de plus continûment dérivable sur $\mathbb{R}$, périodique de période T, on voit par intégration par parties que l'on a, pour $n \neq 0$,

$$\widehat{f'}(n) = \frac{1}{T}\int_0^T f'(x)e^{-in\omega x}dx = \frac{1}{T}\left[-in\omega f(x)e^{-in\omega x}\right]_0^{2\pi} + \frac{in\omega}{T}\int_0^{2\pi} f(x)e^{-in\omega x}dx$$

$$= \frac{in\omega}{T}\int_0^{2\pi} f(x)e^{-in\omega x}dx = in\omega\widehat{f}(n).$$

On déduit alors de l'inégalité de Cauchy-Schwartz et de l'identité de Parseval que l'on a

$$\sum_{n\in\mathbb{Z}\setminus\{0\}} |\widehat{f}(n)| \leq \left[\sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{1}{n^2}\right]^{1/2} \cdot \left[\sum_{n\in\mathbb{Z}\setminus\{0\}} n^2|\widehat{f}(n)|^2\right]^{1/2}$$

$$= \frac{\pi}{\omega\sqrt{6}} \sum_{n\in\mathbb{Z}} |\widehat{f'}(n)|^2 = \frac{1}{2\sqrt{6T}} \sqrt{\int_0^T |f'(x)|^2 dx} < +\infty.$$

On voit donc que dans ce cas la série de Fourier de f est absolument convergente, et que $f(x) = S(f)(x)$ pour tout $x \in \mathbb{R}$.

Plus généralement si f est dérivable en x la série de Fourier $S(f)(x)$ converge vers $f(x)$. Nous mentionnons pour mémoire les résultats classiques suivants.

Théorème 7.5.3. *Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction périodique sur T et intégrable sur $[0, T]$. Posons, pour $N \geq 0$,*

$$S_N(f)(x) = \sum_{n=-N}^{N} \widehat{f}(n)e^{in\omega x},\ \sigma_N(f)(x) = \frac{1}{N+1}\sum_{n=0}^{N} S_N(x).$$

(i) Si f est continue sur $\mathbb{R}$, alors $lim_{N\to+\infty}\sigma_N(f)(x) = f(x)$ pout tout $x \in \mathbb{R}$, et la convergence est uniforme sur $\mathbb{R}$.

(ii) Si f est de classe $\mathcal{C}^1$ par morceaux sur $\mathbb{R}$ alors $lim_{N\to+\infty}S_N(f)(x) = \frac{f^+(x)+f^-(x)}{2}$ pour tout $x \in \mathbb{R}$, où $f^+(x) = lim_{h\to 0^+} f(x+h)$ et $f^-(x) = lim_{h\to 0^-} f(x+h)$.

Le premier résultat est le théorème de Fejer, et le fait que la convergence est uniforme sur $\mathbb{R}$ signifie que $\lim_{N\to+\infty}\sup|f(x) - \sigma_N(f)(x)| = 0$. Le second résultat est le théorème de Dirichlet, et dire que la fonction périodique f est de classe $\mathcal{C}_1$ par morceaux sur $\mathbb{R}$ signifie qu'il existe une suite finie strictement croissante $\alpha_0, ..., \alpha_p$ telle que f coincide sur $]\alpha_j, \alpha_{j+1}[$ avec une fonction continûment dérivable sur $[\alpha_j, \alpha_{j+1}]$ pour $0 \leq j \leq p-1$.

Pour conclure ce bref rappel sur les séries de Fourier notons que puisque $e^{in\omega x} = cos(n\omega x) + isin(n\omega x)$ pour $n \in \mathbb{Z}$, on peut réecrire la série de Fourier de f sous la forme

$$S(f)(x) = a_0(f) + \sum_{n=1}^{+\infty} \left(a_n(f)cos(n\omega x) + b_n(f)sin(n\omega x)\right),$$

avec $a_0(f) = \widehat{f}(0) = \frac{1}{T}\int_0^T f(x)dx$ et, pour $n \geq 1$,

$$a_n(f) = \frac{2}{T}\int_0^T f(x)cos(n\omega x)dx,\ b_n(f) = \frac{2}{T}\int_0^T f(x)sin(n\omega x)dx.$$

On a alors

$$S_N(f)(x) = a_0(f) + \sum_{n=1}^{N} \left(a_n(f)cos(n\omega x) + b_n(f)sin(n\omega x)\right),$$

et on peut reformuler les résultats de convergence rappelés plus haut en utilisant cette version trigonométrique de la série et des sommes partielles de Fourier.

D'autre part on a $\widehat{f}(n) = \frac{a_n(f)+b_n(f)}{2}$, $\widehat{f}(-n) = \frac{a_n(f)-b_n(f)}{2}$; de sorte que $|\widehat{f}(n)|^2 + |\widehat{f}(-n)^2 = \frac{|a_n(f)|^2+|b_n(f)|^2}{2}$ pour $n \geq 1$. Donc si $f : \mathbb{R} \to \mathbb{C}$ est mesurable sur $\mathbb{R}$, périodique de période T, et de carré intégrable sur $[0, T]$, la formule de Parseval pour f peut s'écrire sous la forme

$$\frac{1}{T}\int_0^T |f(x)|^2 = |a_0(f)|^2 + \sum_{n=1}^{+\infty} \frac{|a_n(f)|^2 + |b_n(f)|^2}{2}. \tag{7.14}$$

7.6 Transformation de Fourier sur les groupes abéliens finis

Toute la théorie générale décrite plus haut s'applique en particulier aux groupes abéliens finis, qu'il suffit de munir de la topologie discrète. La mesure de Haar m_G est alors la mesure de comptage définie par la formule $m_G(A) = |A|$, où $|A|$ désigne le nombre d'éléments de A. Les espaces $L^1(G)$, $L^2(G)$, $\mathcal{C}(G) = (G) = \mathcal{C}_c(G)$ coincident alors avec l'espace $\mathbb{C}(G)$ de toutes les fonction $f : G \to \mathbb{C}$. Pour $f \in \mathbb{C}(G)$, $a \subset G$, on a alors

$$\int_A f(x)dx = \sum_{x\in G} f(x).$$

L'espace vectoriel $\mathbb{C}[G]$ est de dimension égale à $|G|$, car une base évidente de $\mathbb{C}[G]$ est fournie par la famille $(\delta_u)_{u\in G}$, où $\delta_u(u) = 1$ et $\delta_u(x) = 0$ pour $x \neq u$. 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 $u \in G$.

On obtient, pour $f, g \in \mathbb{C}[G], x \in G$,

$$(f * g)(x) = \sum_{y\in G} f(x \circ y^{-1})g(y)dy,$$

ce qui donne $(f * g)(x) = \sum_{x\in G} f(x - y)g(y)$ en notation additive.

On munit $\mathbb{C}[G]$ du "produit hermitien" défini pour $f, g \in \mathbb{C}[G]$ par la formule

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

L'élément unité de $\widehat{G}$ est le caractère 1_G défini par la formule $1_G(x) = 1$ pour tout $x \in G$. Soit maintenant $x \in \widehat{G}\setminus\{1_G\}$, et soit $u \in G$ tel que $\chi(u) \neq 1$. Comme l'application $x \to u \circ x$ est une bijection de G sur lui-même, on a

$$\sum_{x\in G} \chi(x) = \sum_{x\in G} \chi(u \circ x) = \chi(u)\sum_{x\in G} \chi(x),$$

ce qui donne $\sum_{x\in G}\chi(x)=0$. Soient maintenant $\phi,\psi\in\widehat{G}$. Alors $\phi\overline{\psi}\in\widehat{G}$, et $\phi\overline{\psi}=1_G$ si et seulement si $\phi=\psi$. On obtient, pour $\phi,\psi\in\widehat{G}$,

$$\begin{cases} <\phi,\psi>=0 \text{ si } \phi\neq\psi \\ <\phi,\psi>=1 \text{ si } \phi=\psi \end{cases} \tag{7.15}$$

Il est clair que $|\widehat{G}|$ est fini, car si $\phi\in\widehat{G}$, $x\in G$ on a $\phi(x)^{|G|}=1$ et ϕ est en fait un homomorphisme de G dans le groupe fini $U_n=\{z\in\mathbb{C}\mid z^n=1\}$ formé des racines n^e de l'unité, avec $n=|G|$. Supposons maintenant qu'une famille $(\lambda_\phi)_{\phi\in\widehat{G}}$ vérifie la condition $\sum_{\phi\in\widehat{G}}\lambda_\phi\phi=0$. On a alors $0=<\sum_{\phi\in\widehat{G}}\lambda_\phi\phi,\psi>=\lambda_\psi$ pour tout $\psi\in\widehat{G}$, donc $\widehat{G}$ est une famille libre déléments de $\mathbb{C}[G]$ et $|\widehat{G}|\leq|G|$. Comme $|\widehat{\widehat{G}}|=|G|$ d'après le théorème de dualité de Pontryagin, on obtient $|\widehat{G}|=|G|$, ce qui donne le résultat suivant.

Théorème 7.6.1. *Soit G un groupe abélien fini. Alors $\widehat{G}$ 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 $|\widehat{G}|=|G|$ qui ne font pas appel au théorème de dualité de Pontryagin. Nous en proposons une à l'exercice 5.

Nous explicitons maintenant les principaux résultats concernant la transformation de Fourier appliquée aux groupes abéliens finis. Comme la mesure de Haar sur un groupe abélien fini coincide avec la mesure de comptage, la transformation de Fourier $\mathcal{F}_G:\mathbb{C}[G]\to\mathbb{C}[\widehat{G}]$ associe à toute fonction $f\in\mathbb{C}[G]$ sa transformée de Fourier $\widehat{f}\in\mathbb{C}[\widehat{G}]$ définie pour $\chi\in\widehat{G}$ par la formule

$$\widehat{f}(\chi)=\sum_{x\in G}f(x)\overline{\chi(x)}. \tag{7.16}$$

On obtient les résultats suivants.

Théorème 7.6.2. *Soit G un groupe abélien fini. Pour $f,g\in\mathbb{C}[G]$, on a*

(i)

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

(ii) (formule de Plancherel)

$$\sum_{x\in G}f(x)\overline{g(x)}=\frac{1}{|G|}\sum_{\chi\in\widehat{G}}f(\chi)\overline{\widehat{g}(\chi)},$$

et en particulier on a pour $f\in\mathbb{C}[G]$,
(iii) (formule de Parseval)

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

D'autre part on a, pour $f\in\mathbb{C}[G]$,

(iv) (formule d'inversion de Fourier)

$$\forall x \in G, f(x) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(x).$$

Tous ces résultats sont des cas particuliers des résultats généraux valables pour les groupes localement compacts abéliens (le fait que la constante intervenant dans les formules de Plancherel-Parseval et dans la formule d'inversion de Fourier est égale à $\frac{1}{|G|}$ provient du fait que si 1_G est le caractère unité sur G, défini par la formule $1_G(x) = 1$ pour tout $x \in G$, on a $\widehat{1_G}(1_G) = 1$ et $\widehat{1_G}(\chi) = 0$ pour $\chi \in \widehat{G} \setminus \{1_G\}$). On peut aussi démontrer ces résultats directement, voir l'exercice 6.

On va conclure cette discussion en donnant une version matricielle de la transformation de Fourier sur un groupe abélien fini. On notera que la formule obtenue dépend des énumérations choisies pour le groupe G et son groupe dual $\widehat{G}$.

Proposition 7.6.3. *Soit $G = \{x_0, ..., x_{n-1}\}$ un groupe abélien fini possédant n éléments et soit $\widehat{G} = \{\chi_0, ..., \chi_{n-1}\}$ 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*

$$a_{i,j} = \overline{\chi_i(x_j)}.$$

On a, pour $f = [f[x_0], ...f[x_{n-1}]] \in \mathbb{C}[G]$,

$$\begin{bmatrix} \widehat{f}[x_0] \\ . \\ . \\ . \\ \widehat{f}[x_{n-1}] \end{bmatrix} = A_G \begin{bmatrix} f[x_0] \\ . \\ . \\ . \\ f[x_{n-1}] \end{bmatrix}.$$

Démonstration : On munit $\mathbb{C}[G]$ de la base $\mathcal{B} := \{\delta_{x_0}, ..., \delta_{x_{n-1}}\}$ et on munit $\mathbb{C}[G]$ de la base $\widehat{\mathcal{B}} = \{\delta_{\phi_0}, ..., \delta_{\phi_{n-1}}\}$. Soit $\mathcal{M} := \mathcal{M}_{\mathcal{F}_G, \mathcal{B}, \widehat{\mathcal{B}}}$ la matrice représentant la transformée de Fourier $\mathcal{F}_G : C[G] \to \mathbb{C}[\widehat{G}]$ par rapport aux bases $\mathcal{B}$ et $\widehat{\mathcal{B}}$, c'est à dire la matrice dont la j^e colonne est formée des coordonnées de $\widehat{\delta_j}$ dans la base $\widehat{\mathcal{B}}$. Comme $\widehat{\delta_{x_j}}(\chi_i) = \sum_{l=0}^{n-1} \delta_{x_j}(x_i)\overline{\chi_i(x_l)} = \overline{\chi_i(x_j)}$, on voit que $\mathcal{M}$ coincide 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.

Considérons le groupe additif $\mathbb{F}_2^k = (\mathbb{Z}/2\mathbb{Z})^k$. On peut associer à tout élément $x = (\overline{x_0}, ..., \overline{x_{k-1}}) \in \mathbb{F}_2^k$, avec $x_j \in \{0, 1\}$ pour $0 \leq j \leq k-1$, l'entier $n(x) = \sum_{j=0}^{k-1} x_j 2^{j-1}$. On peut ainsi énumérer $\mathbb{F}_2^k$: à tout entier $j \in \{0, ..., 2^{k-1}\}$, écrit en base 2 sous la forme $j = j_{k-1}...j_0$, on associe $u_j = (\overline{j_0}, ..., \overline{j_{k-1}}) \in \mathbb{F}_2^k$.

Rappelons que pour $(\overline{x_0}, ..., \overline{x_{k-1}}), (\overline{y_0}, ..., \overline{y_{k-1}}) \in \mathbb{F}_2^k$, on pose

$$x.y = \sum_{j=0}^{n-1} \overline{x}_j \overline{y}_j, \phi_y(x) = (-1)^{x.y} := (-1)^{\sum_{j=0}^{k-1} x_j y_j}.$$

On a vu plus haut que l'application $y \to \phi_y$ est un isomorphisme de $(\mathbb{F}_2^k, +)$ sur son groupe dual $(\widehat{\mathbb{F}_2^k}, .)$ on déduit alors du lemme 5.3.5 que l'on a, pour $0 \leq i \leq k-1$, $0 \leq j \leq k-1$,

$$\phi_i(u_j) = w_{i,j},$$

où $(w_{i,j})_{\substack{1 \leq i \leq k \\ 1 \leq j \leq k}} = W_k$ 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 le groupe additif $\mathbb{F}_2^k$, réécrite en utilisant pour $f \in \mathbb{C}^{2^k}$, $0 \leq j \leq k-1$ la formule

$$\mathcal{W}_k(f)[j] = \mathcal{F}_{\mathbb{F}_2^k}(\tilde{f})[u_j],$$

où $\tilde{f}[u_j] = f[j]$ pour $0 \leq i \leq 2^k - 1$.

On voit donc que la formule d'inversion pour la transformée de Walsh n'est autre que la formule d'inversion de Fourier appliquée au groupe additif $\mathbb{F}_2^k$. La formule de Parseval donne, pour $f \in \mathbb{C}^{2^k}$,

$$\sum_{j=0}^{2^k-1} |f[j]|^2 = \sum_{j=0}^{2^k-1} |\tilde{f}[u_j]|^2 = \frac{1}{2^k} \sum_{j=0}^{2^k-1} |\mathcal{F}_2^k(\tilde{f})[u_j]^2 = \frac{1}{2^k} \sum_{j=0}^{2^k-1} |W_k(f)[j]|^2,$$

et on retrouve la formule 5.2, qui avait été établie directement au Chapitre 5.

Soit maintenant $N \geq 2$, et posons de nouveau $\omega_N = e^{\frac{2i\pi}{N}}$. On a vu plus haut que l'application $\chi_p : \overline{q} \to \omega_N^{pq}$ est un caractère de $\mathbb{Z}/N\mathbb{Z}$ pour $p \in \mathbb{Z}$, et que l'application $\overline{p} \to \chi_p$ est un isomorphisme de groupes de $(\mathbb{Z}/N\mathbb{Z}, +)$ sur son groupe dual $(\widehat{\mathbb{Z}/N\mathbb{Z}}, .)$. On munit $\mathbb{C}(\mathbb{Z}/N\mathbb{Z})$ de la base $\mathcal{B} = \{\delta_{\overline{0}}, ..., \delta_{\overline{N-1}}\}$ et on munit $\widehat{\mathbb{Z}/N\mathbb{Z}}$ de la base $\widehat{\mathcal{B}} = \{\delta_{\phi_0}, ..., \delta\phi_{N-1}\}$. La colonne d'indice $n \in \{0, ..., N-1\}$ de la matrice $\mathcal{M} = \mathcal{M}_{\mathbb{Z}/N\mathbb{Z}, \mathcal{B}, \widehat{\mathcal{B}}}$ représentant la transformation de Fourier $\mathcal{F}_{\mathbb{Z}/N\mathbb{Z}} : \mathbb{C}[\mathbb{Z}/N\mathbb{Z}] \to \mathbb{C}[\widehat{\mathbb{Z}/N\mathbb{Z}}]$ par rapport aux bases $\mathcal{B}$ et $\widehat{\mathcal{B}}$ est formée des coordonnées de $\widehat{\delta}_n$ dans la base $\widehat{B}$, et on a, pour $0 \leq m \leq N-1$,

$$\widehat{\delta_{\overline{n}}}(\chi_m) = \sum_{p=0}^{N-1} \delta_{\overline{n}}(\overline{p}) \overline{\chi}_m(\overline{p}) = e^{-2imn\pi} = \omega_N^{-nm}.$$

0n voit donc que la matrice de Fourier $\mathcal{M}$ associée à ces énumérations de $\mathbb{Z}/N\mathbb{Z}$ et $\widehat{\mathbb{Z}/N\mathbb{Z}}$ coincide avec la matrice de Fourier A_N introduite au Chapitre précédent, et la transformée de Fourier discrète n'est autre que la transformée de Fourier sur $\mathbb{Z}/N\mathbb{Z}$, réécrite en utilisant la formule

$$\hat{f}[m] = \mathcal{F}_{\mathbb{Z}/N\mathbb{Z}}(\tilde{f})(\chi_m),$$

où $\tilde{f}[\overline{n}] = f[n]$ pour $0 \leq n \leq N-1$. On voit ainsi que les résultats concernant la transformée de Fourier discrète obtenus au Chapitre 6 sont en fait un cas particulier de des propiétés de la transformée de Fourier sur un groupe abélien fini.

Pour conclure ce Chapitre, on va faire apparaitre le lien entre transformée de Fourier discrète et coefficients de Fourier d'une fonction périodique. Considérons en effet une fonction $f : \mathbb{R} \to \mathbb{C}$ continue et périodique de période 1. Pour $N \geq 2$, $0 \leq m \leq N-1$, posons

$$f_N[n] = f\left(\frac{n}{N}\right).$$

Notons $\widehat{f}$ la transformée de Fourier discrète de f_N. Les notations étant celles du Chapitre 6, on a, pour $0 \leq p \leq N-1$,

$$\widehat{f_N}[p] = \sum_{n=0}^{N-1} f_N[n] e^{-\frac{2inp\pi}{N}} = \sum_{n=0}^{N-1} f\left(\frac{n}{N}\right) e^{-\frac{2inp\pi}{N}}.$$

D'autre part les coefficients de Fourier $\hat{f}(p)$ peuvent s'obtenir comme limites de sommes de Riemann. On a en effet, pour $p \geq 0$,

$$\widehat{f}(p) = \int_0^1 f(x) e^{-2i\pi nx} dx = \lim_{N\to+\infty} \frac{1}{N} \sum_{n=0}^{N-1} f\left(\frac{n}{N}\right) e^{-\frac{2inp\pi}{N}}. \tag{7.17}$$

Un calcul analogue permet d'obtenir les coefficients de Fourier $\widehat{f}(p)$ pour $p \leq 0$, voir l'exercice 5.

Le lien entre transformée de Fourier discrète et transformée de Fourier sur $\mathbb{R}$, qui renvoie à une étude plus poussée de l'échantillonnage et au théorème de Shannon et se heurte aux principes d'incertitude, sera discuté dans la suite de ce cours.

7.7 Exercices sur le Chapitre 7

Exercice 1

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 2

Soit E un ensemble non vide. On dit qu'une application $d : (x, y) \to [0, +\infty[$ est une distance sur E si et seulement si les deux conditions suivantes sont vérifiées

(i) $d(x, z) \leq d(x, y) + d(y, z)\ \forall x, y, z \in E$,

(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 réunion d'ensembles de la forme $B_d(x, \epsilon) := \{y \in E \mid d(x, y) < \epsilon\}$. La topologie associée à la distance

d est la topologie τ_d associée à la famille $\mathcal{U}_{\tau_d}$ 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 $(G_1, \circ, \tau_1)$ et $(G_2, \circ, \tau_2)$ deux groupes topologiques métrisables, soit e_1 l'unité de G_1, soit e_2 l'unité de G_2, soit d_1 une distance sur G_1 telle que $\tau_1 = \tau_{d_1}$, soit d_2 une distance sur G_2 telle que $\tau_2 = \tau_{d_2}$ et soit $\theta : G_1 \to G_2$ un homomorphisme de groupes. Montrer que θ est continu si et seulement si $\lim_{n\to+\infty} d(e_2, \theta(x_n)) = 0$ pour toute suite $(x_n)_{n\geq 1}$ telle que $\lim_{n\to+\infty} d_1(e_1 - x_n) = 0$.

2) Soit $(G, \circ, \tau)$ un groupe 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 $\phi_1, \phi_2 \in G$,

$$d(\phi_1, \phi_2) = \sum_{n=1}^{+\infty} \frac{min(1, sup_{x\in\cup_{1\leq m\leq n} K_m} |\phi_1(x) - \phi_2(x)|}{2^n}.$$

Vérifier que d est une distance sur $\widehat{G}$ et que la topologie τ_d coincide sur $\widehat{G}$ avec la topologie $\hat{\tau}$ définie dans le cours (en termes savants, cette topologie $\hat{\tau}$ s'appelle la topologie de la convergence uniforme sur les compacts de G.

b) Montrer que l'application $\phi : s \to \phi_s$, où $\phi_s(x) = e^{isx}$ pour $x \in \mathbb{R}$, est une application continue de $\mathbb{R}$ dans $\widehat{R}$, et que l'application réciproque $\phi^{-1} : \widehat{\mathbb{R}} \to \mathbb{R}$ est également continue.

Exercice 3

Soit G un groupe abélien fini, soit $H \neq G$ un sous-groupe de G, et soit $x \in G \setminus H$.

1) Vérifier que l'ensemble $H(x) := \{x^n y\}_{n\in\mathbb{Z}, y\in H}$ est un sous-groupe de G contenant x et H.

2) Vérifier qu'il existe $m \geq 2$ tel que $x^m \in H$.

3) Soit d le plus petit entier tel que $x^d \in G$. Montrer que tout élément z de $H(x)$ s'écrit de manière unique sous la forme $z = x^n y$ avec $0 \leq n \leq d-1$, $y \in H$.

4) Soit $\chi \in \widehat{H}$, et soient $\alpha_1, ..., \alpha_d$ les d solutions dans $\mathbb{C}$ 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 coincide avec χ. En déduire que si $|\widehat{H}| = |H|$, alors $|\widehat{H(x)}| = |H(x)|$.

5) Déduire de ce qui précède que $|\widehat{G}| = |G|$ pour tout groupe abélien fini G.

Exercice 4

Soit G un groupe abélien fini possédant N éléments.

1) En utilisant les définitions de la transformée de Fourier et du produit de convolution sur $\mathbb{C}[G]$, montrer que l'on a, pour $f, g \in \mathbb{C}[G]$,

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

2) En utilisant le fait que $\widehat{G}$ forme une base orthonormale de $\mathbb{C}[G]$ pour le produit hermitien de $\mathbb{C}[G]$, démontrer les formules de Plancherel et de Parseval pour $\mathbb{C}[G]$.

3) En utilisant de nouveau le fait que $\widehat{G}$ forme une base orthonormale de $\mathbb{C}[G]$ pour le produit hermitien de $\mathbb{C}[G]$, démontrer que ${}^t\overline{A_G}A_G = nI_n$, où I_n désigne la matrice unité à n lignes et n colonnes.

En déduire la formule d'inversion de Fourier pour $\mathbb{C}[G]$.

Exercice 5

Soit f une fonction continue et périodique de période 1. On pose $\tilde{f}(x) = f(-x)$ pour $x \in \mathbb{R}$. Avec les notations de la formule 7.15, montrer que l'on a, pour $p \leq 0$,

$$\tilde{f}(p) = \lim_{N \to +\infty} \frac{(\tilde{f})_N(-p)}{N}.$$

Chapitre 8

Echantillonnage, principes d'incertitude et théorème de Shannon

8.1 Le principe d'incertitude pour la transformation de Fourier sur $\mathbb{R}$

Si $f : \mathbb{R} \to \mathbb{C}$ est mesurable, on note U_f l'ensemble des réels x pour lesquels il existe un intervalle ouvert I_x de $\mathbb{R}$ contenat x tel que $f(t) = 0$ presque partout sur I_x, et on appelle *support de f au sens des distributions* l'ensemble Supp$(f) = \mathbb{R} \setminus U_f$. On va voir que si une fonction intégrable $f : \mathbb{R} \to \mathbb{C}$ n'est pas nulle presque partout, alors f et sa transformée de Fourier ne peuvent pas être simultanément à support compact.

On a le résultat suivant

Proposition 8.1.1. *Soit $g \in L^1(\mathbb{R})$ une fonction à support compact. Posons $a_n = \frac{1}{n!}\int_0^n g(x)x^n dx$ pour $n \in \mathbb{N}$. Alors la série $\sum_{n=0}^{+\infty} a_n z^n$ converge pour tout $z \in \mathbb{C}$, et si on pose $F(z) = \sum_{n=0}^{+\infty} a_n z^n$, on a les propriétés suivantes*

(i) $\widehat{f}(x) = F(-ix)$ pour $x \in \mathbb{R}$.

(ii) La fonction $z \to F(z)$ est indéfiniment dérivable au sens complexe sur $\mathbb{C}$, et $F(z) = \sum_{n=0}^{+\infty} \frac{F^{(n)}(a)}{n!}(z-a)^n$ pour $a \in \mathbb{C}, z \in \mathbb{C}$.

Soit $A > 0$ tel que $f(x) = 0$ pour $|x| > A$, et soit $z \in \mathbb{C} \setminus \{0\}$. On a

$$|a_n z^n| \leq \frac{|z|^n}{n!}\int_{-A}^{A} |f(x)||x|^n dx \leq 2A^{n+1}|z|^n \|f\|_1.$$

Fixonx $p \geq \frac{1}{2A|z|}$. On a $\frac{1}{n!} \leq \frac{(2A|z|)^p}{p!}(2A|z|)^{-n}$ pour $n \geq p+1$. On obtient, pour $m \geq p+1$,

$$\sum_{n=0}^{m}|a_nz^n| \leq \sum_{n=0}^{p}|a_nz^n|+\frac{2^{p+1}|z|^pA^{p+1}\|f\|_1}{p!}\sum_{n=p+1}^{m}\frac{1}{2^m} \leq \sum_{n=0}^{p}|a_nz^n|+\frac{2^{p}|z|^pA^{p+1}\|f\|_1}{p!} < +\infty.$$

Donc la série $\sum_{n=0}^{m}|a_nz^n|$ est convergente, ce qui implique que la série $\sum_{n=0}^{+\infty}a_nz^n$ est convergente pour tout $z \in \mathbb{C}$. D'autre part on a, pour $m \geq p$,

$$\left|\sum_{n=0}^{m}\frac{z^nx^n}{n!}f(x)\right| \leq \left(\sum_{n=0}^{p}\frac{A^n|z^n|}{n!}+\frac{2^p|z|^pA^p\|f\|_1}{p!}\sum_{n=p+1}^{m}\frac{1}{2^m}\right)|f(x)|$$

En posant $K := \sum_{n=0}^{p}\frac{A^n|z^n|}{n!}+\frac{2^p|z|^pA^p\|f\|_1}{p!}$, on obtient, pour tout $m \geq 1$ et pour presque tout $x \in [-A, A]$,

$$\left|\sum_{n=0}^{m}\frac{z^nx^n}{n!}f(x)\right| \leq K|f(x)|.$$

Comme $\lim_{m\to+\infty}\sum_{n=0}^{m}\frac{z^nx^n}{n!}f(x) = e^{zx}f(x)$ pour presque tout $x \in [-A, A]$, on déduit du théorème de convergence dominée que l'on a

$$\int_{-\infty}^{+\infty}f(x)e^{zx}dx = \int_{-A}^{A}f(x)e^{zx}dx = \sum_{n=0}^{+\infty}\int_{-A}^{A}\frac{z^nx^n}{n!}f(x)dx = \sum_{n=0}^{+\infty}a_nz^n.$$

En posant $F(z) = \sum_{n=0}^{+\infty}a_nz^n$ pour $z \in \mathbb{C}$, on obtient $F(x) = \hat{f}(-ix)$ pour $x \in \mathbb{R}$. Le fait que F est indéfiniment dérivable au sens complexe sur $\mathbb{C}$, et le fait que $F(z) = \sum_{n=0}^{+\infty}\frac{F^{(n)}(a)}{n!}(z-a)^n$ pour $a \in \mathbb{C}, z \in \mathbb{C}$ provient des propriétés élémentaires des séries entières rappelées à l'annexe 1. □

On en déduit le principe d'incertitude suivant, qui montre en particulier q'une fonction non nulle et sa transformée de Fourier ne peuvent pas être simultanément à support compact.

Corollaire 8.1.2. *Soit $f \in L^1(\mathbb{R})$ une fonction à support compact. Si $\widehat{f}$ s'annulle sur un intervalle ouvert non vide de $\mathbb{R}$ alors f est nulle presque partout.*

Démonstration : Soit $f \in L^1(\mathbb{R})$ une fonction à support compact. Supposons que $\hat{f}$ s'annule sur un intervalle ouvert $]a, b[$ et soit $c = \frac{a+b}{2}$. Soit F la fonction donnée par la proposition précédente. On a $F(-ix) = \hat{f}(x) = 0$ pour $a \leq x \leq b$, donc $F^{(n)}(-ic) = 0$ pour tout $n \geq 0$, et on a

$$\widehat{f}(x) = F(-ix) : \sum_{n=0}^{+\infty} \frac{F^{(n}(ic)}{n!} i^n (c-x)^n = 0 \; \forall x \in \mathbb{R}.$$

On déduit alors de la formule d'inversion de Fourier que $f(x) = 0$ presque partout. □

8.2 Le principe d'incertitude discret

On considère maintenant un groupe abélien fini G. Pour $f \in \mathbb{C}[G]$, on pose $\text{Supp}(f) := \{x \in G \mid f(x) \neq 0\}$. On a le résultat suivant (principe d'incertitude discret).

Proposition 8.2.1. *Soit G un groupe abélien fini, et soit $f \in \mathbb{C}[G]$.*

Si $|Supp(f)||Supp(\widehat{f})| < |G|$, alors $f = 0$.

D'autre part si H est un sous-groupe de G, on a $|Supp(f_H)||Supp(\widehat{f_H})| = |G|$, où $f_H(x) = 1$ si $x \in H$, $f(x) = 0$ si $x \notin H$.

Démonstration : Soit $f \in \mathbb{C}(G)$, et soit $M = \sup_{x \in G} |f(x)|$. On a

$$\|f\|_2^2 = \sum_{x \in G} |f(x)|^2 = \sum_{x \in Supp(f)} |f(x)|^2 \leq M^2 \left|\text{Supp}(f)\right|.$$

Soit maintenant $x \in G$ tel que $|f(x)| = M$. D'après la formule d'inversion de Fourier, on a, comme $|\chi(x)| = 1$ pour tout $\chi \in \widehat{G}$,

$$M = |f(x)| = \frac{1}{|G|} \left| \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\chi(x) \right| \leq \frac{1}{|G|} \sum_{\chi \in \hat{G}} \left| \widehat{f}(\chi) \right|.$$

On déduit alors de l'inégalité de Cauchy-Schwartz que l'on a

$$M^2 \leq \frac{1}{|G|^2} \left[\sum_{\chi \in \text{Supp}(\widehat{f})} \left| \widehat{f}(\chi) \right|^2 \right] \left[\sum_{\chi \in \text{Supp}(\widehat{f})} 1 \right] = \frac{\left|\text{Supp}(\widehat{f})\right|}{|G|^2} \|\widehat{f}\|_2^2.$$

D'après l'identité de Parseval, on a

$$\sum_{x \in G} |f(x)|^2 = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \left| \widehat{f}(\chi) \right|^2,$$

et on voit que $\|f\|_2^2 = \frac{1}{|G|} \|\widehat{f}\|_2^2$. On obtient $M^2 \leq \frac{\|f\|_2^2}{|G|} \left|\text{Supp}(\widehat{f})\right|$. En appliquant la première des inégalités ci-dessus, on obtient

$$\|f\|_2^2 \leq \frac{\|f\|_2^2}{|G|} \left|\text{Supp}(f)\right| \times \left|\text{Supp}(\widehat{f})\right|.$$

Si $f \neq 0$, on a $\|f\|_2 > 0$, et on obtient le principe d'incertitude discret.

Soit maintenant H un sous-groupe de G. On a

$$\hat{f}_H(\chi) = \sum_{x\in G} f_H(x)\overline{\chi(x)} = \sum_{x\in H} \overline{\chi(x)}.$$

Donc $\hat{f}_H(\chi) = |H|$ si $\chi \in H^\perp$. Si $\chi \notin H^\perp$, il existe $x_0 \in H$ tel que $\chi(x_0) \neq 1$, et on a

$$\chi(x_0)\hat{f}_H(\chi) = \chi(x_0)\sum_{x\in H}\chi(x) = \sum_{x\in H}\chi(x_0x).$$

Comme l'application $x \longmapsto x_0x$ est une bijection de H sur lui-même, on a $\sum_{x\in H}\chi(x_0x) = \sum_{x\in H}\chi(x) = \hat{f}_h(\chi)$, et $(1-\chi(x_0))\hat{f}_h(\chi) = 0$, donc $\hat{f}_H(\chi) = 0$. On a donc bien $\hat{f}_H = |H|\, f_{H^\perp}$. D'autre part on peut montrer que le dual du groupe quotient G/H est isomorphe à $H^\perp$, donc $\left|H^\perp\right| = |G/H| = \frac{|G|}{|H|}$, ce qui montre que l'on a

$$|\text{Supp}(f_H)| \times \left|\text{Supp}(\hat{f}_H)\right| = |G|\,,$$

et on voit que l'inégalité fournie par le principe d'incertitude discret est optimale. □

8.3 La formule sommatoire de Poisson

Théorème 8.3.1. *(Formule sommatoire de Poisson) Soit f une fonction continue sur $\mathbb{R}$, et soit $c > 0$. On suppose qu'il existe $\alpha > 1$ tel que $\sup_{x\in\mathbb{R}}(1+|x|)^\alpha |f(x)| < +\infty$.*

Alors la série $\sum_{n\in\mathbb{Z}} f(cn)$ est absolument convergente, et on a

$$\sum_{n\in\mathbb{Z}} f(cn) = \frac{1}{c} lim_{p\to+\infty} \frac{1}{p+1}\sum_{q=0}^{p}\left[\sum_{m=-q}^{q}\hat{f}\left(\frac{2\pi m}{c}\right)\right]. \tag{8.1}$$

En particulier, si les séries $\sum_{m=1}^{+\infty}\hat{f}\left(-\frac{2\pi m}{c}\right)$ et $\sum_{m=0}^{+\infty}\hat{f}\left(\frac{2\pi m}{c}\right)$ sont convergentes, on a

$$\sum_{n\in\mathbb{Z}} f(cn) = \frac{1}{c}\sum_{n\in\mathbb{Z}}\hat{f}\left(\frac{2\pi n}{c}\right). \tag{8.2}$$

Démonstration : Soit $M > 0$ tel que $|f(x)| \leq M(1+|x|)^{-\alpha}$ pour $x \in \mathbb{R}$.
On a

$$\sum_{n\in\mathbb{Z}}|f(x+cn)| \leq 2M\sum_{n=0}^{+\infty}(1+cn)^{-\alpha} \leq 2M\sum_{n=0}^{+\infty}(1+cn)^{-\alpha} \leq 2M\left[1+\sum_{n=0}^{+\infty}\int_n^{n+1}\frac{dx}{(1+cx)^\alpha}\right]$$

$$= 2M\left[1+\int_0^{+\infty}\frac{dx}{(1+cx)^\alpha}\right] = 2M\left[1+\frac{1}{c(\alpha-1)}\right] < +\infty.$$

Donc les séries $\sum_{n=1}^{+\infty} f(x-cn)$ et $\sum_{n=0}^{+\infty} f(x+cn)$ sont absolument convergentes, donc convergentes. Posons

$$g(x) = \sum_{n\in\mathbb{Z}} f(x+cn).$$

On a

$$g(x+c) = \sum_{n\in\mathbb{Z}} f(x+cn+c) = g(x) = \sum_{n\in\mathbb{Z}} f(x+cn) = g(x),$$

donc g est périodique de période c sur $\mathbb{R}$.

Soit $a \in \mathbb{R}$, et soit $\epsilon > 0$. On a, pour $p \geq 1 + \frac{|a|}{c}$, $x \in [a-1, a+1]$, $|n| \geq p$,

$$|f(x+cn)| \leq M(1+|x+cn|)^{-\alpha} \leq M(c|n| - |a|)^{-\alpha}.$$

On obtient

$$\left|\sum_{|n|\geq p} f(x+cn)\right| \leq \sum_{|n|\geq p} |f(x+cn)| \leq 2M \sum_{n=p}^{+\infty} (cn-|a|)^{-\alpha} \leq 2M \int_{p-1}^{+\infty} \frac{dx}{(cx-|a|)^{\alpha}}$$

$$= \frac{2M}{(\alpha-1))c(c(p-1)-|a|)^{\alpha-1}}.$$

Fixons maintenant $p \geq 1 + \frac{|a|}{c}$ tel que $\frac{2M}{(\alpha-1))c(c(p-1)-|a|)^{\alpha-1}} < \frac{\epsilon}{4}$. On a, pour $x \in [a-1, a+1]$,

$$|g(x)-g(a)| \leq \sum_{-p}^{p} |f(x+nc)-f(a+nc)| + \left|\sum_{|n|\geq p} f(x+cn)\right| + \left|\sum_{|n|\geq p} f(a+cn)\right|$$

$$\leq \sum_{n=-p}^{p} |f(x+nc)-f(a+nc)| + \frac{\epsilon}{2}.$$

Comme f est continue sur $\mathbb{R}$, il existe $\delta > 0$ tel que $|f(x+cn)-f(a+cn)| < \frac{\epsilon}{2(p+1)}$ pour $|x-a| < \delta$, $-p \leq n \leq p$. Posons $\eta =$min$(\delta, 1)$. On a $|g(x)-g(a)| < \epsilon$ pour tout $x \in (a-\eta, a+\eta)$, ce qui prouve que g est continue sur $\mathbb{R}$.

On va maintenant calculer les coefficients de Fourier de g. En posant $\omega = \frac{2\pi}{c}$, on obtient, pour $n \in \mathbb{Z}$,

$$\hat{g}(m) = \frac{1}{c}\int_0^c g(t)e^{-im\omega t}dt = \frac{1}{c}\int_0^c \left(\sum_{n\in\mathbb{Z}} f(t+nc)\right) e^{-im\omega t}dt.$$

Posons $h_p(t) = \frac{1}{c} \sum_{|n|\leq p} f(t+nc)e^{-im\omega t}$ pour $p \geq 1, t \in [0,\delta]$. On a $\lim_{p\to+\infty} h_p(t) = g(t)e^{-im\omega t}$ pour tout $t \in [0,\delta]$. D'autre part

$$|h_p(t)| \leq \sum_{|n|\leq p} |f(t+cn)| \leq |f(t)| + \sum_{|n|\geq 1} |f(t+cn)| \leq 2M(1+\sum_{n=1}^{+\infty}(1+c(n-1))^{-\alpha} < +\infty.$$

Il résulte alors du théorème de convergence dominée que l'on a

$$\hat{g}(m) = \frac{1}{c} lim_{p\to+\infty} \int_0^c h_p(t)dt = \frac{1}{c} \sum_{n\in\mathbb{Z}} \int_0^c f(t+cn)e^{-im\omega(t+cn)}dt$$

$$= \frac{1}{c} \int_{-\infty}^{+\infty} f(t)e^{-im\omega t}dt = \frac{1}{c}\hat{f}\left(\frac{2\pi m}{c}\right).$$

Comme g est continue sur $\mathbb{R}$ et périodique de période c, on déduit du théorème de Féjer que la moyenne de Cesàro des sommes partielles de la série de Fourier de g converge uniformément vers g sur $\mathbb{R}$.

On obtient, pour $x \in \mathbb{R}$,

$$\sum_{n\in\mathbb{Z}} f(x+cn) = \frac{1}{c} lim_{p\to+\infty} \frac{1}{p+1} \sum_{q=0}^{p} \left[\sum_{m=-q}^{q} \hat{f}\left(\frac{2\pi m}{c}\right) e^{2im\pi x} \right].$$

En particulier on a

$$\sum_{n\in\mathbb{Z}} f(cn) = \frac{1}{c} lim_{p\to+\infty} \frac{1}{p+1} \sum_{q=0}^{p} \left[\sum_{m=-q}^{q} \hat{f}\left(\frac{2\pi m}{c}\right) \right],$$

et si les séries $\sum_{m=1}^{+\infty} \hat{f}\left(-\frac{2\pi m}{c}\right)$ et $\sum_{m=0}^{+\infty} \hat{f}\left(\frac{2\pi m}{c}\right)$ sont convergentes, ceci donne

$$\sum_{n\in\mathbb{Z}} f(cn) = \frac{1}{c} \sum_{n\in\mathbb{Z}} \hat{f}\left(\frac{2\pi n}{c}\right).$$

□

8.4 La formule de Poisson discrète

On peut se demander si la formule sommatoire de Poisson admet un analogue discret. En fait on peut identifier $\mathbb{R}$ au groupe dual $\widehat{\mathbb{R}}$ de $\mathbb{R}$ en utilisant l'application $x \to \chi_x$ où $\chi_x(t) = e^{2i\pi tx}$ pour $t \in \mathbb{R}$. Si on pose $H_c = c\mathbb{Z}$ on voit que H_c est un sous-groupe fermé de $\mathbb{Z}$ et que si on pose $H_c^{\perp} = \{x \in \mathbb{R} \mid \chi_x(t) = 1 \forall t \in H_c$ on a $H_c^{\perp} = \frac{2\pi x}{c}\mathbb{Z}$, et la formule sommatoire de Poisson peut s'écrire sous la forme

$$\sum_{x\in H_c} f(x) = \frac{1}{c}\sum_{u\in H_c^\perp} \widehat{f}(u).$$

L'analogue discret de la formule sommatoire de Poisson existe bien et est donné dans l'énoncé suivant.

Théorème 8.4.1. *(Formule de Poisson discrète) Soit G un groupe abélien fini, soit $f \in \mathbb{C}[G]$, et $H \subset G$ un sous-groupe de G. On a :*

$$\sum_{x\in H} f(x) = \frac{1}{|H^\perp|}\sum_{\chi\in H^\perp} \widehat{f}(\chi). \tag{8.3}$$

Démonstration : On applique la formule de Plancherel en prenant pour g la fonction indicatrice de H, définie par la formule

$$g(x) = 1 \text{ si } x \in H,\ g(x) = 0 \text{ si } x \notin H. \tag{8.4}$$

On a vu dans l'étude du principe d'incertitude discret que l'on a $\hat{g}(\chi) = 0$ si $\chi \notin H^\perp$, $\hat{g}(\chi) = 1$ si $\chi \in H^\perp$. La formule de Plancherel devient donc :

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

□

8.5 Le théorème d'échantillonnage de Shannon

On s'intéresse ici aux fonctions de $L^2(\mathbb{R})$ dont la transformée de Fourier est à support compact, autrement dit aux signaux continus qui sont "bornés en fréquence". On a déjà vu que ces fonctions sont la restriction à la droite réelle de fonctions développables en série entière sur $\mathbb{C}$. On va voir maintenant que de telles fonctions peuvent être entièrement reconstruites à partir de leurs valeurs sur l'ensemble $\delta\mathbb{Z} := \{\delta n\}_{n\in\mathbb{Z}}$ si δ est assez petit. On note $\|f\|_2 = \int_{-\infty}^{+\infty} |f(t)|^2 dt$ la norme associée au produit hermitien usuel sur $L^2(\mathbb{R})$.

Pour $T > 0$, on pose

$$\mathcal{E}_T = \{f \in L^2(\mathbb{R}) \mid \widehat{f(x)} = 0 \ p.p. \ pour |t| > \frac{T}{2}\},$$

et on munit $L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$ du produit hermitien (et de la norme associée) de $L^2(\mathbb{R})$.

Posons $e_m(t) = e^{in\omega t}$ pour $t \in \left[-\frac{T}{2}, \frac{T}{2}\right]$, $e_m(t) = 0$ pour $|t| > \frac{T}{2}$, avec $\omega = \frac{2\pi}{T}$. Des calculs effectués dans l'annexe 2 montrent que l'on a, pour $g \in L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$,

$$g = \sum_{m\in\mathbb{Z}} c_m(g) e_m, \tag{8.5}$$

la série ci -dessus étant convergente au sens de la norme de $L^2(\mathbb{R})$, où le coefficient de Fourier $c_m(g)$ (calculé ici au sens du coefficient de Fourier de la fonction périodique de période T obtenue en prolongeant g par périodicité à $\mathbb{R}$) est donné par la formule

$$c_m(g) = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} g(x)e^{-im\omega x}dx.$$

On a $L^2\left[-\frac{T}{2},\frac{T}{2}\right] \subset L^1(\mathbb{R})$, puisque, d'après l'inégalité de Cauchy-Schwartz, on a, pour $g \in L^2\left[-\frac{T}{2},\frac{T}{2}\right]$,

$$\int_{-\infty}^{+\infty}|g(x)|dx = \int_{-\frac{T}{2}}^{\frac{T}{2}}|g(x)|dx \leq \sqrt{\int_{-\frac{T}{2}}^{\frac{T}{2}}|g(x)|^2dx}\sqrt{\int_{-\frac{T}{2}}^{\frac{T}{2}}dx} = \sqrt{T}\|g\|_2 < +\infty.$$

Comme la transformation de Fourier $\mathcal{F} : L^2(\mathbb{R}) \to L^2(\mathbb{R})$ est bijective, sa restriction $\tilde{\mathcal{F}}$ à $\mathcal{E}_T$ est une bijection de $\mathcal{E}_T$ sur $L^2\left[-\frac{T}{2},\frac{T}{2}\right]$, et on a, pour $t \in \mathbb{R}$, $g \in L^2\left[-\frac{T}{2},\frac{T}{2}\right]$,

$$\tilde{\mathcal{F}}^{-1}(g)(t) = \mathcal{F}^{-1}(g)(t) = \frac{1}{2\pi}\int_{-\frac{T}{2}}^{\frac{T}{2}} g(x)e^{ixt}dx.$$

En particulier si $f \in \mathcal{E}_T$, et si $g = \mathcal{F}(f)$, on a

$$c_m(g) = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} g(x)e^{-im\omega x}dx = \frac{2\pi}{T}\mathcal{F}^{-1}(g)(-\omega m) = \frac{2\pi}{T}f\left(-\frac{2\pi m}{T}\right).$$

Posons $u_m = \frac{2\pi}{T}\mathcal{F}^{-1}(e_m)$. On a, d'après la formule 8.5, au sens de la norme de $L^2(\mathbb{R})$, pour $f \in \mathcal{E}_T$, avec $g = \mathcal{F}(f)$,

$$f = \sum_{m\in\mathbb{Z}} c_m(g)\mathcal{F}^{-1}(e_m) = \sum f\left(\frac{2\pi m}{T}\right)u_{-m}. \tag{8.6}$$

D'autre part

$$\mathcal{F}^{-1}(e_m) = \frac{1}{2\pi}\int_{-\frac{T}{2}}^{\frac{T}{2}} e^{im\omega x}e^{ixt}dx = \frac{1}{2\pi}\left[\frac{e^{i(m\omega+t)x}}{i(m\omega+t)}\right]_{-\frac{T}{2}}^{\frac{T}{2}}$$

$$= \frac{1}{\pi(m\omega+t)}sin\left(\pi m + \frac{tT}{2}\right) = \frac{T}{2\pi}\frac{sin\left(\pi m + \frac{tT}{2}\right)}{\pi m + \frac{tT}{2}} = \frac{T}{2\pi}sin_c\left(\pi m + \frac{tT}{2}\right),$$

où sin_c désigne le sinus cardinal défini par la formule $sin_c(s) = \frac{sin(s)}{s}$, avec $sin_c(0) = 1$.

On obtient

$$u_{-m}(t) = sin_c\left(\frac{tT}{2} - \pi m\right). \tag{8.7}$$

Notons que si $t \in \frac{2\pi}{T}\mathbb{Z}$ la série $\sum f\left(\frac{2\pi m}{T}\right) sin_c\left(\frac{tT}{2} - \pi m\right)$ n'a qu'un seul terme non nul. Sinon il existe $k > 0$ tel que $|sin_c\left(\frac{tT}{2} - \pi m\right)| \leq \frac{k}{1+|m|}$, donc $\sum\limits_{m\in\mathbb{Z}} |sin_c\left(\frac{tT}{2} - \pi m\right)|^2 < +\infty$. D'autre part il résulte de la formule de Parseval que $\sum\limits_{m\in\mathbb{Z}} |c_m(\hat{f})|^2 < +\infty$, donc $\sum\limits_{m\in\mathbb{Z}} |f\left(\frac{2\pi m}{T}\right)|^2 < +\infty$ pour $f \in \mathcal{E}_T$. On obtient, pour $f \in \mathcal{E}_T$,

$$\sum_{m\in\mathbb{Z}} \left|f\left(\frac{2\pi m}{T}\right)\right| \left|sin_c\left(\frac{tT}{2} - \pi m\right)\right| \leq \sqrt{\sum_{m\in\mathbb{Z}} |f\left(\frac{2\pi m}{T}\right)|^2} \sqrt{\sum_{m\in\mathbb{Z}} \left|sin_c\left(\frac{tT}{2} - \pi m\right)\right|^2} < +\infty.$$

Donc la série $\sum\limits_{m\in\mathbb{Z}} f\left(\frac{2\pi m}{T}\right) sin_c\left(\frac{tT}{2} - \pi m\right)$ converge pour tout $t \in \mathbb{R}$ si $f \in \mathcal{E}_T$ et on déduit des formules 8.6 et 8.7 que l'on a, en posant de même que plus haut $\omega = \frac{2\pi}{T}$.

$$f(t) = \sum_{m\in\mathbb{Z}} f\left(\frac{2\pi m}{T}\right) sin_c\left(\frac{tT}{2} - \pi m\right) = \sum_{m\in\mathbb{Z}} f\left(m\omega\right) sin_c\left(\frac{\pi}{\omega}(t - m\omega)\right). \tag{8.8}$$

Il est clair que cette formule fonctionne si $f \in \mathcal{E}_{T'}$ avec $0 \leq T' \leq T$ car dans ce cas $\mathcal{E}_{T'} \subset \mathcal{E}_T$. Si $f \in L^2(\mathbb{R})$, et si $\hat{f}$ est à support compact, on obtient donc le résultat suivant

Théorème 8.5.1. *(Théorème de Shannon-Nyquist) Soit $f \in L^2(\mathbb{R})$ telle que $\widehat{f}$ est à support compact, et soit a le plus petit réel positif tel que $\hat{f}(x)$ soit nulle presque partout pour $|x| > a$. Posons $freq_{max}(f) = \frac{a}{2\pi}$. Alors on peut reconstituer f à partir des valeurs $\{f(m\delta)\}_{m\in\mathbb{Z}}$ si $\frac{1}{\delta} \geq 2freq_{max}(f)$, et on a alors, pour $t \in \mathbb{R}$,*

$$f(t) = \sum_{m\in\mathbb{Z}} \delta f\left(m\delta\right) \frac{sin\left(\frac{\pi}{\delta}(t - m\delta)\right)}{\pi(t - m\delta)}.$$

On vérifie que la valeur $2freq_{max}(f)$ est optimale. Pour des échantillonnages plus grossiers, on se heurte à des phénomènes de "recouvrement de spectre" (aliasing en anglais).

Chapitre 9

Annexe 1 : Un peu d'analyse complexe

9.1 Propriétés élémentaires des séries entières

Rappelons qu'on dit qu'une série $\sum_{n=0}^{+\infty} u_n$ de nombres complexes est **convergente** si la suite $(\sum_{n=0}^{N} u_n)_{N\geq 0}$ admet une limite quand $N \to +\infty$. La limite de cette suite, appelée somme de la série considérée, est également notée $\sum_{n=0}^{+\infty} u_n$.

Supposons maintenant que $u_n \geq 0$ pour tout $n \geq 0$. Si la série $\sum_{n=0}^{+\infty} u_n$ est convergente alors la suite $(\sum_{n=0}^{N} u_n)_{N\geq 0}$ est croissante. Comme toute suite de réels croissante et majorée est convergente on voit que la série $\sum_{n=0}^{+\infty} u_n$ est convergente si et seulement si il existe $M > 0$ tel que $\sum_{n=0}^{N} u_n \leq M$ pour tout $N \geq 0$.

Soit maintenant $\sum_{n=0}^{+\infty} v_n$ une série à termes réels. Posons $v_n^+ = \max(v_n, 0)$ et $v_n^- = \max(-v_n, 0)$ pour $n \geq 0$, de sorte que $v_n = v_n^+ - v_n^-$. Si la série $\sum_{n=0}^{+\infty} |v_n|$ est convergente, alors $\sum_{n+0}^{N} v_n^+ \leq \sum_{n=0}^{+\infty} |v_n| < +\infty$ et $\sum_{n+0}^{N} v_n^- \leq \sum_{n=0}^{+\infty} |v_n| < +\infty$ pour tout $N \geq 0$, ce qui montre que les séries $\sum_{n=0}^{+\infty} v_n^+$ et $\sum_{n=0}^{+\infty} v_n^-$ sont convergentes. Donc dans ce cas la série $\sum_{n=0}^{+\infty} v_n$ est convergente, et $\sum_{n=0}^{+\infty} v_n = \sum_{n=0}^{+\infty} v_n^+ - \sum_{n=0}^{+\infty} v_n^-$. Plus généralement on dit qu'une série $\sum_{n=0}^{+\infty} u_n$ de nombres complexes est **absolument convergente** quand la série $\sum_{n=0}^{+\infty} |u_n|$ est

convergente. Dans ce cas les séries $\sum_{n=0}^{+\infty} |Re(u_n)|$ et $\sum_{n=0}^{+\infty} |Im(u_n)|$ sont convergentes, donc les séries $\sum_{n=0}^{+\infty} Re(u_n)$ et $\sum_{n=0}^{+\infty} Im(u_n)$ sont convergentes. Il en résulte que toute série absolument convergente est convergente et vérifie l'inégalité

$$\left|\sum_{n=0}^{+\infty} u_n\right| = \lim_{N\to\infty} \left|\sum_{n=0}^{N} u_n\right| \leq \lim_{N\to+\infty} \sum_{n=0}^{N} |u_n| = \sum_{n=0}^{+\infty} |u_n|.$$

Soit U un ouvert de $\mathbb{C}$. Rappelons également qu'on dit qu'une fonction $f : U \to \mathbb{C}$ est **dérivable au sens complexe** en $a \in U$ s'il existe $b \in \mathbb{C}$ tel que $b = \lim_{\substack{h\to 0 \\ h\in\mathbb{C}\setminus\{0\}}} \frac{f(a+h)-f(a)}{h}$. Dans ce cas on pose $f'(z) = b$, et on définit de même le cas échéant les dérivées successives de f. De même que plus haut on pose $C(a,r) := \{z \in \mathbb{C} \mid |z-a| = r\}$, $D(a,r) := \{z \in \mathbb{C} \mid |z-a| < r\}$ pour $a \in \mathbb{C}, R > 0$. Les cercles sont orientés dans le sens inverse des aiguilles d'une montre, ce qui fait que si $f : C(a,r) \to \mathbb{C}$ est continue, on a

$$\int_{C(a,r)} f(\zeta)d\zeta = \int_0^{2\pi} ire^{it} f(a + re^{it})dt,$$

ce qui revient à poser $\zeta = a + re^{it}$, de sorte que $d\zeta = ire^{it}dt$.

Rappelons également qu'on dit qu'une série $\sum_{n=0}^{+\infty} u_n$ de nombres complexes est **convergente** si la suite $(\sum_{n=0}^{N} u_n)_{N\geq 0}$ admet une limite quand $N \to +\infty$. La limite de cette suite, appelée somme de la série considérée, est également notée $\sum_{n=0}^{+\infty} u_n$. Si $u_n \geq 0$ pour tout $n \geq 0$, on déduit du fait que toute suite de réels croissante et majorée est convergente que la série $\sum_{n=0}^{+\infty} u_n$ est convergente si et seulement si il existe $M > 0$ tel que $\sum_{n=0}^{N} u_n \leq M$ pour tout $N \geq 0$. Rappelons enfin qu'on dit qu'une série $\sum_{n=0}^{+\infty} u_n$ est **absolument convergente** quand la série $\sum_{n=0}^{+\infty} |u_n|$ est convergente. Dans ce cas la série $\sum_{n=0}^{+\infty} u_n$ est convergente, et on a

$$\left|\sum_{n=0}^{+\infty} u_n\right| \leq \sum_{n=0}^{+\infty} |u_n|.$$

Nous démontrons en détail le résultat suivant, qui intervient dans la démonstration du principe d'incertitude.

Théorème 9.1.1. *Soit $\sum_{n=0}^{+\infty} \alpha_n z^n$ une série entière. On suppose que la série $\sum_{n=0}^{+\infty} \alpha_n u^n$ converge, avec $u \in \mathbb{C} \setminus \{0\}$. Alors la série $\sum_{n=0}^{+\infty} \alpha_n z^n$ converge pour tout $z \in D(0, |u|)$. De plus si on*

pose $f(z) = \sum_{n=0}^{+\infty} \alpha_n z^n$ *pour* $|z| < |u|$, *alors* f *est indéfiniment dérivable au sens complexe sur* $D(0,|u|)$, *et si* $|a| < |u|$, *la série* $\sum_{n=0}^{+\infty} \frac{f^{(n)}(a)}{n!}(z-a)^n$ *converge pour* $|z-a| < |u| - |a|$, *et on a, pour* $|z-a| < |u| - |a|$,

$$\sum_{n=0}^{+\infty} \frac{f^{(n)}(a)}{n!}(z-a)^n = f(z) \tag{9.1}$$

Démonstration : Posons $R = |u|$. Dire que la série $\sum_{n=0}^{+\infty} \alpha_n u^n$ converge signifie que la suite $(\sum_{n=0}^{p} \alpha_p u^p)_{n\geq 0}$ est convergente. En particulier

$$\lim_{n\to+\infty} \alpha_n u^n = \lim_{n\to+\infty} \left(\sum_{p=0}^{n} \alpha_p u^p - \sum_{p=0}^{n-1} \alpha_p u^p \right) = 0,$$

et il existe $M > 0$ tel que $|\alpha_n| R^n \leq M$ pour tout $n \geq 0$. On a, pour $|z| \leq R$,

$$\sum_{p=0}^{+\infty} |\alpha_n z^n| \leq \sum_{p=0}^{+\infty} M \frac{|z|^n}{R^n} = \frac{MR}{R-|z|} < +\infty.$$

Ceci montre que la série $\sum_{n=0}^{+\infty} \alpha_n z^n$ est absolument convergente, donc convergente sur $D(0,|z|)$. De plus on a, pour $|z| \leq R$,

$$|f(z)| = \left| \sum_{n=0}^{+\infty} \alpha_n (z-a)^n \right| \leq \sum_{p=0}^{+\infty} |\alpha_n z^n| \leq \frac{MR}{R-|z|} < +\infty.$$

On pourrait utiliser les inégalités ci-dessus pour démontrer que f est continue sur $D(0,R)$, mais ceci découle de toutes façons de la dérivabilité de f sur $D(0,R)$ au sens complexe.

Fixons maintenant $a \in D(0,R)$ et $r \in]0, R-|a|[$, de sorte que $C(a,r) \subset D(0,R)$. Il est clair que la fonction $t \to f(a + re^{it}$ est intégrable au sens de Lebesgue sur $[0, 2\pi]$. Posons, pour $n \geq 0$, $z \in D(a,r)$,

$$f_n(z) = \frac{n!}{2i\pi} \int_{C(a,r)} \frac{f(\zeta)}{(\zeta - z)^{n+1}} d\zeta.$$

On a, pour $z \in D(a,r)$, $|h| < r - |a|$,

$$\frac{f_n(z+h) - f_n(z)}{h} - f_{n+1}(z)$$

$$= \frac{n!}{2i\pi} \int_{C(a,r)} \frac{(\zeta - z)^{n+1} - (\zeta - z - h)^{n+1}}{h} \frac{f(\zeta)}{(\zeta - z - h)^{n+1}(\zeta - z)^{n+1}} d\zeta - \frac{(n+1)!}{2i\pi} \int_{C(a,r)} \frac{f(\zeta)}{(\zeta - z)^{n+2}} d\zeta$$

$$= \frac{n!}{2i\pi}\int_{C(a,r)} f(\zeta)\left(\frac{\sum_{j=0}^{n}(\zeta-z)^j(\zeta-z-h)^{n-j}}{(\zeta-z)^{n+1}(\zeta-z-h)^{n+1}} - \frac{(n+1)}{(\zeta-z)^{n+2}}\right)d\zeta$$

$$= \frac{n!}{2i\pi}\int_{C(a,r)} f(\zeta)\sum_{j=0}^{n}\frac{1}{(\zeta-z)^{n+1-j}}\left(\frac{1}{(\zeta-z-h)^{1+j}} - \frac{1}{(\zeta-z)^{1+j}}\right)d\zeta$$

$$\frac{n!}{2\pi r^n}\int_0^{2\pi} f(re^{it})e^{-int}\sum_{j=0}^{n} r^j e^{jt}\left(\frac{1}{(re^{it}+a-z-h)^{1+j}} - \frac{1}{(re^{it}-z)^{1+j}}\right)dt.$$

Soit $(h_p)_{p\geq 1}$ une suite d'éléments de $D(0, r-|z-a|)$ qui converge vers 0, et soit $\delta = \min_{p\geq 1} r - |h_n + z - a|$. On a $\delta > 0$, et on a, pour tout $p \geq 1$ et pour tout $t \in [0, 2\pi]$,

$$\left| f(re^{it})e^{-int}\sum_{j=0}^{n} r^j e^{jt}\left(\frac{1}{(re^{it}-h_p)^{1+j}} - \frac{1}{(re^{it})^{1+j}}\right)\right| \leq \frac{MR}{R-|a|-r}\sum_{j=0}^{n} r^j(r^{-1-j}+\delta^{-1-j}).$$

Comme $\lim_{p\to+\infty} f(re^{it})e^{-int}\sum_{j=0}^{n} r^j e^{jt}\left(\frac{1}{(re^{it}+a-z-h_p)^{1+j}} - \frac{1}{(re^{it}-z)^{1+j}}\right) = 0$ pour tout $t \in [0, 2\pi]$, on déduit alors du théorème de convergence dominée que $\lim_{\substack{h\to 0 \\ h\in\mathbb{C}\setminus\{0\}}} \frac{f_n(z+h_p)-f_n(z)}{h_p} = f_{n+1}(z)$. Donc f_0 est indéfiniment dérivable au sens complexe sur $D(a, r)$, et $f_0^{(n)}(z) = f_n(z)$ pour $n \geq 1$.

On a

$$f_0(z) = \frac{r}{2\pi}\int_0^{2\pi}\frac{e^{it}f(a+re^{it})}{a+re^{it}-z}dt = \frac{r}{2\pi}\int_0^{2\pi}\lim_{p\to+\infty} G_p(t)dt,$$

où $G_p(t) = \frac{e^{it}}{a+re^{it}-z}\sum_{m=0}^{p}\alpha_m(a+re^{it})^m$.

On a, pour $p \geq 1$, $t \in \mathbb{R}$,

$$|G_p(t)| \leq \frac{1}{r-|z-a|}\sum_{m=0}^{p}|\alpha_n|(a+r)^m \leq \frac{M}{r-|z-a|}\sum_{m=0}^{p}\left(\frac{r+|a|}{R}\right)^m \leq \frac{MR}{(r-|z-a|)(R-|a|-r)}.$$

On déduit de nouveau du thérème de convergence dominée que l'on a

$$f_0(z) = lim_{p\to\infty}\frac{r}{2\pi}\int_0^{2\pi} G_p(t)dt = lim_{p\to\infty}\sum_{m=0}^{p}\frac{\alpha_m}{2\pi}\int_0^{2\pi} re^{it}\frac{(a+re^{it})^m}{a+r^{e^{it}}-z}dt.$$

On a

$$\frac{re^{it}}{a+re^{it}-z} = \frac{1}{1-\frac{z-a}{re^{it}}} = \sum_{j=0}^{+\infty}(z-a)^j r^{-j}e^{-ijt},$$

et

$$\left|(a+re^{it})^m\sum_{j=0}^{q}(z-a)^j r^{-j}e^{-ijx}\right| \leq (|a|+r)^m\sum_{j=0}^{q}\left(\frac{|z-a|}{r}\right)^j \leq \frac{r(|a|+r)^m}{r-|z-a|},$$

et on déduit comme plus haut du théorème de convergence dominée que l'on a

$$\frac{1}{2\pi}\int_0^{2\pi}\frac{re^{it}(a+re^{it})^m}{re^{it}+a-z}dt = \sum_{j=0}^{+\infty}\frac{1}{2\pi}\int_0^{2\pi}(a+re^{it})^m(z-a)^j r^{-j}e^{-ijt}dt.$$

Comme $\int_0^{2\pi} e^{ikt}dt = 0$ pour $k \in \mathbb{Z}\setminus 0$, on obtient

$$\frac{1}{2\pi}\int_0^{2\pi}\frac{re^{it}(a+re^{it})^m}{re^{it}+a-z}dt = \sum_{j=0}^{m}C_m^j a^j(z-a)^{m-j} = (a+z-a)^m = z^m,$$

$$f_0(z) = \sum_{m=0}^{+\infty}\alpha_m z^m = f(z).$$

On voit donc que f est indéfiniment dérivable au sens complexe sur $D(0,R)$ et que pour $a \in D(0,R)$, $|z-a| < R-|a|$, $|z-a| < r < R-|a|$, on a

$$f^{(n)}(z) = \frac{n!}{2i\pi}\int_{C(a,r)}\frac{f(\zeta)}{(\zeta-z)^n}d\zeta, \tag{9.2}$$

formule qui est un cas particulier de la célèbre *formule de Cauchy*
On a en particulier

$$f(z) = \frac{1}{2i\pi}\int_{C(a,r)}\frac{f(\zeta)}{\zeta-z}d\zeta = \frac{1}{2\pi}\int_0^{2\pi}\frac{re^{it}f(a+re^{it})}{re^{it}+a-z}dt = \frac{1}{2\pi}\int_0^{2\pi}f(a+re^{it})\left(\sum_{j=0}^{+\infty}(z-a)^j r^{-j}e^{-ijt}\right)dt.$$

De même que plus haut, on déduit du théorème de convergence dominée que l'on a

$$\frac{1}{2\pi}\int_0^{2\pi}f(a+re^{it})\left(\sum_{j=0}^{+\infty}(z-a)^j r^{-j}e^{-ijt}\right)dt = \sum_{j=0}^{+\infty}\frac{(z-a)^j}{2\pi}\int_0^{2\pi}f(a+re^{it})r^{-j}e^{-ijt}dt$$

$$= \sum_{j=0}^{+\infty}\frac{(z-a)^j}{2i\pi}\int_{C(0,r)}\frac{f(\zeta)}{(\zeta-a)^{n+1}}d\zeta.$$

Il résulte de la formule 9.2 que $\frac{1}{2i\pi}\int_{C(0,r)}\frac{f(\zeta)}{(\zeta-a)^{n+1}}d\zeta = \frac{f^{(n)}(a)}{n!}$. Donc la série $\sum_{j=0}^{+\infty}\frac{f^{(n)}(a)}{n!}(z-a)^n$ converge pour $|a|<R$, $|z-a|+|a|<R$, et on a dans ce cas on a

$$f(z) = \sum_{j=0}^{+\infty}\frac{f^{(n)}(a)}{n!}(z-a)^n.$$

9.2 Exercices pour l'annexe 1

Exercice 1

On suppose qu'il existe $u \in D(0,R)$ tel que la série $\sum_{n=0}^{+\infty} \alpha_n u^n$ converge. En utilisant l'inégalité $|\alpha_n z^n| \leq M(\frac{|z|}{R})^n$ pour $|z| < R$, montrer directement que la somme de cette série est continue sur $D(0,R)$.

Exercice 2

Les notations étant celles du théorème 9.1, montrer que $\alpha_n = \frac{f^{(n)}(0)}{n!}$ pour $n \geq 0$, et que $f^{(p)}(z) = \sum_{n=p}^{+\infty} n(n-1)...(n-p+1)\alpha_n z^{n-p}$ pour $p \geq 1$. Montrer plus généralement que l'on a

$$f^{(p)}(z) = \sum_{n=p}^{+\infty} n(n-1)...(n-p+1)\frac{f^{(n)}(a)}{n!}(z-a)^{n-p}$$

pour $|a| + |z-a| < R$ (on pourra utiliser la formule 9.2).

Exercice 3

1) Montrer que la série $\sum_{n=0}^{+\infty} \frac{z^n}{n!}$ converge pour tout $z \in \mathbb{C}$.

2) On pose $F(z) = \sum_{n=0}^{+\infty} \frac{z^n}{n!}$ pour $z \in \mathbb{C}$. En utilisant l'exercice précédent, montrer que $F'(z) = F(z)$ pour tout $z \in \mathbb{C}$. En déduire que $F(z) \neq 0$ pour tout $z \in \mathbb{C}$.

3) Soit G une fonction dérivable au sens complexe sur $\mathbb{C}$ telle que $G'(z) = G(z)$ pour tout $z \in \mathbb{C}$. On pose $H(z) = \frac{G(z)}{F(z)}$. Montrer que H est constante, et en déduire que $G(z) = G(0)F(z)$ pour tout $z \in \mathbb{C}$.

4) Déduire de la question précédente que $F(u+v) = F(u)F(v)$ pour $u, v \in \mathbb{C}$.

5) Montrer que $F(x) = e^x$ pour tout $x \in \mathbb{R}$.

6) On pose $f(x) = e^{ix}$ pour $x \in \mathbb{R}$. Montrer que $f + f" = 0$. En déduire que $f(x) = cos(x) + isin(x)$.

7) Déduire de ce qui précède que $F(z) = e^{Re(z)}\left(cos(Im(z)) + isin(Im(z))\right)$.

La fonction $z \to F(z)$ est appelée fonction exponentielle complexe, et est notée e^z.

Chapitre 10

Annexe 2 : Espaces de Hilbert

10.1 Orthogonalité, produit scalaire, produit hermitien

Au lycée, on apprend la formule $\overrightarrow{AB}\cdot\overrightarrow{CD} = \overrightarrow{HK}\cdot\overrightarrow{CD}$ où H et K désignent les projetés orthogonaux de A et B sur la droite (CD) (avec $\overrightarrow{AB}\cdot\overrightarrow{CD} = 0$ si $C = D$).

Les mesures algébriques sont calculées en munissant (CD) d'un vecteur unitaire $\overrightarrow{u}$.

Si f et g sont continues sur $[a, b]$ à valeurs réelles, on peut poser

$$< fg >:= \int_a^b f(t)g(t)dt. \tag{10.1}$$

Ces deux lois qui associent à un couple d'éléments un nombre réel ont des propriétés analogues. Nous aurons besoin d'une version complexe de cette notion très générale de produit scalaire.

Definition 10.1.1. *Soit E un espace vectoriel complexe. Un **produit hermitien** sur E est une application $\varphi : E \times E \to \mathbb{C}$ possédant les propriétés suivantes :*

1. $< u, v >= \overline{< v, u >}\ \forall u, v \in E$
2. $< \lambda_1 u_1 + \lambda_2 u_2, v >= \lambda_1 < u_1, v > +\lambda_2 < u_2, v >\ \ \forall u_1, u_2, v \in E,\ \lambda_1, \lambda_2 \in \mathbb{C}$
3. $< u, u > > 0\ \forall u \in E \setminus \{0\}$.

*Au produit hermitien est associée une **norme** sur E :*

$$\|u\| := \sqrt{< u, u >} \tag{10.2}$$

Par exemple, pour f, g continues sur $[a, b]$ à valeurs dans $\mathbb{C}$, on peut poser

$$< fg >:= \int_a^b f(t)\overline{g(t)}dt. \tag{10.3}$$

Proposition 10.1.2. *On a pour $u, v \in E$, $\lambda \in \mathbb{C}$*

- $\|u\| \geq 0$,
- $\|u\| = 0$ *si et seulement si* $u = 0$,

– $\|u+v\| \leq \|u+\|v\|$,
– $\|\lambda u\| = |\lambda|\|u\|$.

Dans toute la suite on appellera **espace préhilbertien** un espace vectoriel complexe muni d'un produit hermitien. Le résultat suivant est connu sous le nom d'inégalité de Cauchy-Schwartz.

Théorème 10.1.3. *Soit $(E, , <.,.>)$ un espace préhilbertien. On a*

$$|<u,v>| \leq \|u\|.\|v\| \ \forall u, v \in E. \tag{10.4}$$

En particulier pour f et g continues sur $[a,b]$, on a

$$<f,g> = \left| \int_a^b f(t)\overline{g(t)}dt \right| \leq \sqrt{\int_a^b |f(t)|^2 dt}.\sqrt{\int_a^b |g(t)|^2 dt} \tag{10.5}$$

Definition 10.1.4. *On dit que u et v sont **orthogonaux** quand $<u,v>=0$. Si $\emptyset \neq A \subseteq E$, on pose*

$$A^{\perp} := \{v \in E \mid \ <u,v>=0 \ \forall u \in A\}. \tag{10.6}$$

On dispose dans le plan ou dans l'espace de la notion de **projection orthogonale** sur une droite ou sur un plan vectoriel. L'algorithme suivant va permettre d'étendre ces notions aux espaces vectoriels complexes.

10.2 Algorithme de Gram-Schmidt

Definition 10.2.1. *On dit qu'une famille $(e_\lambda)_{\lambda \in \Lambda}$ de E est **orthonormale** (ou **orthonormée**) si les deux conditions suivantes sont vérifiées :*

1. $e_\lambda \perp e_\mu \ \forall \lambda \neq \mu$,
2. $\|e_\lambda\| = 1 \ \forall \lambda$.

On peut munir $\mathbb{C}^n$ du produit hermitien usuel, défini pour $x = [x_1, ..., x_n] \in \mathbb{C}^n, y = [y_1, ..., y_n] \in \mathbb{C}^n$ par la formule

$$<x,y> = \sum_{j=1}^{n} x_j \overline{y_j}. \tag{10.7}$$

Pour $p, q \in \mathbb{Z}$, on notera $\delta_{p,q}$ le symbole de Kronecker, défini par la formule $\delta_{p,q} = 0$ si $p \neq q$, $\delta_{p,q} = 1$ si $p = q$. . Il est clair que si on pose $e_m = (\delta_{m,j})_{1 \leq j \leq n}$ pour $m \in \{1, ..., n\}$, alors $\mathcal{B}_0 := [e_1, ..., e_n]$ est une base orthonormale de $\mathbb{C}^n$, appelée base canonique de $\mathbb{C}^n$.

On va voir maintenant un exemple de famille orthonormale infinie.

Exemple 10.2.2. *Soit $\mathcal{C}[0, 2\pi]$ l'espace vectoriel des fonctions continues sur $[0, 2\pi]$, à valeurs complexes, muni du produit hermitien*

$$< f, g >= \frac{1}{2\pi} \int_0^{2\pi} f(t)\overline{g}(t)dt. \tag{10.8}$$

Posons $e_n(t) = e^{int}$ *pour* $n \in \mathbb{Z}, t \in [0, 2\pi]$. *Alors* $(e_n)_{n\in\mathbb{Z}}$ *est une famille orthonormale de* $\mathcal{C}[0, 2\pi]$.

En effet, pour $n \neq m$

$$< e_n, e_m >= \frac{1}{2\pi} \int_0^{2\pi} e^{int}\overline{e^{imt}}dt = \frac{1}{2\pi} \int_0^{2\pi} e^{i(n-m)t}dt = \frac{1}{2\pi} \frac{1}{i(n-m)} \left[e^{i(n-m)t}\right]_{t=0}^{2\pi} = 0,$$

et, pour $m = n$,

$$\frac{1}{2\pi} \int_0^{2\pi} e^{int}\overline{e^{int}}dt = \sqrt{\frac{1}{2\pi} \int_0^{2\pi} dt} = 1.$$

L'algorithme de Gram-Schmidt, présenté ci-dessous, permet d'associer à toute famille finie et libre d'éléments d'un espace préhilbertien une famille orthonormale engendrant le même sous-espace vectoriel. Ceci donne procédé concret permettant de fabriquer des bases orthonormales en dimension finie.

Théorème 10.2.3. *(Algorithme de Gram-Schmidt)*
Soit E *un espace préhilbertien, soit* $e_1, \ldots, e_p$ *une famille libre d'éléments de* E, *et soit* F *le sous-espace vectoriel de* E *engendré par* $(e_1, \ldots, e_p)$. *On pose* $f_1 = e_1$ *et* $f_k = f_k - \sum_{1\leq j\leq k-1} \frac{<e_k, f_j>}{\|f_j\|^2} f_j$ *pour* $2 \leq k \leq p$. *Alors* $(f_1, \ldots, f_p)$ *est une base orthogonale de* F, *de sorte que* $(\frac{f_1}{\|f_1\|}, \ldots, \frac{f_p}{\|f_p\|})$ *est une base orthonormale de* F.

Démonstration : On va démontrer par récurrence finie que la famille $(f_1, \ldots, f_k)$ est orthogonale, que $f_k \neq 0$, et que f_k appartient au sous-espace vectoriel de E engendré par $(e_1, \ldots, e_k)$ pour $1 \leq k \leq p$. C'est évident si $k = 1$. Supposons maintenant que ces propriétés sont vérifiées pour un entier k tel que $1 \leq k \leq p - 1$. Il est clair que $f_{k+1} \neq 0$ et que f_{k+1} appartient alors au sous-espace vectoriel de E engendré par $(f_1, \ldots, f_{k+1})$. D'autre part on a, pour $i \leq k$,

$$< f_{k+1}, f_i >=< f_{k+1}, f_i > - < \sum_{1\leq j\leq k} \frac{< e_{k+1}, f_j >}{\|f_j\|^2} f_j, f_i >=< e_{k+1}, f_i >$$

$$- \sum_{1\leq j\leq k} < e_{k+1}, f_j > \frac{< f_j, f_i >}{\|f_j\|^2} =< e_{k+1}, f_i > - < e_{k+1}, f_i >= 0.$$

Donc $(f_1, \ldots, f_{k+1})$ est orthogonale, ce qui prouve les deux propriétés par récurrence finie. On voit donc que $(f_1, \ldots, f_p)$ est une famille orthogonale d'éléments de F.

On a $f_k = e_k - \sum_{1\leq j\leq k-1} \alpha_j e_j$, avec $\alpha_1, \ldots, \alpha_{j-1} \in \mathbb{R}$. On voit donc que la matrice P représentant $(f_1, \ldots, f_p)$ dans la base $(e_1, \ldots, e_p)$ de F est une matrice triangulaire supérieure dont tous les termes diagonaux sont égaux à 1. Donc $det(P) = 1$, P est inversible, ce qui montre que $(f_1, \ldots, f_p)$ est une base de F. Donc $(\frac{f_1}{\|f_1\|}, \ldots, \frac{f_p}{\|f_p\|})$ est une base orthonormale de F. □

Proposition 10.2.4. *Soit E un espace préhilbertien de dimension finie muni d'une base $(e_i)_{i=1,\ldots,n}$ orthonormale pour un produit hermitien. On a alors, pour tout $u \in E$,*

$$u = \sum_{j=1}^{n} < u, e_j > e_j, \tag{10.9}$$

d'où $< u, v >= \sum_{j=1}^{n} < u, e_j > \overline{< v, e_j >}$ $\forall u, v \in E$ et en particulier on a, pour tout $u \in E$,

$$\|u\| = \sqrt{\sum_{j=1}^{n} |< u, e_j >|^2}. \tag{10.10}$$

Théorème 10.2.5. *Soit E un espace préhilbertien et soit F un sous-espace de dimension finie de E. Alors il existe pour tout $u \in E$ un unique élément v de F tel que $\|u - v\| \leq \|u - v'\|$ pour tout $w \in F$.*

De plus, on a

$$v = \sum_{j=1}^{n} < u, e_j > e_j, \tag{10.11}$$

$(e_1, \ldots, e_n)$ désignant une base orthonormale quelconque de F, et $u - v \perp v'$ pour tout $v' \in F$.

Démonstration : Soit $(e_1, \ldots, e_n)$ une base orthonormale de F, et posons $v = \sum_{j=1}^{n} < u, e_j > e_j$. On a $v \in E$. On a, pour $1 \leq i \leq n$,

$$< u-v, e_i >=< u, e_i > - < \sum_{j=1}^{n} < u, e_j > e_j, e_i >=< u, e_i > - \sum_{j=1}^{n} < u, e_j >< e_j, e_i >$$
$$=< u, e_i > - < u, e_i >= 0.$$

Comme $(e_1, \ldots, e_n)$ est une base de F, on a $u - v \perp w$ pour tout $w \in F$.

Soit $h \in F \setminus \{0\}$. On a $< u - v, h >= 0$, donc $< h, u - v >= \overline{< u - v, h >} = 0$, et on obtient

$$\|u-v-h\|^2 =< u-v-h, u-v-h >=< u-v, u-v > + < h, u-v > + < u-v, h > + < h, h >$$
$$=< u - v, u - v > + < h, h >= \|u - v\|^2 + \|h\|^2.$$

Ceci montre que $\|u-w\| > \|u-v\|$ pour $w \in F, w \neq v$, ce qui achève la démonstration. □

Definition 10.2.6. *Avec les notations précédentes, on pose alors*

$$P_F(u) := v \tag{10.12}$$

*et on appelle P_F la **projection orthogonale** de E sur F.*

On va maintenant introduire deux notions classiques associées à la norme d'un espace préhilbertien.

Definition 10.2.7. *Soit $(u_n)_{n\in\mathbb{Z}}$ une suite d'éléments d'un espace préhilbertien.*
- *On dit que u_n converge vers u quand $lim_{n\to\infty}\|u_n - u\| = 0$.*
- *On dit que la suite (u_n) est **une suite de Cauchy** si on a la propriété suivante :*

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N}\ :\ p \geq N, q \geq N \Rightarrow \|u_p - u_q\| < \epsilon \tag{10.13}$$

Ceci permet d'introduire l'importante notion suivante.

Definition 10.2.8. *Un **espace de Hilbert** H est un espace vectoriel préhilbertien dans lequel toute suite de Cauchy est convergente.*

Exemple 10.2.9. *Posons*

$$\begin{cases} f_n(t) = 0 \text{ pour } t \in \left[0, \frac{1}{2} - \frac{1}{n+2}\right], \\ f_n(t) = \frac{2}{n}\left(t - \frac{1}{n+1}\right) \text{ pour } t \in \left[\frac{1}{2} - \frac{1}{n+2}, \frac{1}{2}\right], \\ f_n(t) = 1 \text{ pour } t \in \left[\frac{1}{2}, 1\right] \end{cases}$$

On vérifie que $(f_n)_{n\geq 1}$ est de Cauchy dans l'espace préhilbertien $\mathcal{C}([0, 2\pi])$ mais elle n'a pas de limite continue. *Donc $\mathcal{C}([0, 2\pi])$ n'est pas un espace de Hilbert pour le produit hermitien introduit plus haut.*

Definition 10.2.10. *Une **base hilbertienne** d'un espace de Hilbert H est une suite orthonormale $(e_n)_{n\geq 1}$ qui engendre un sous-espace dense de H.*

Les bases hilbertiennes d'un espace vectoriel de Hilbert H de dimension finie sont les bases orthonormales de H. En dimension infinie la situation est plus compliquée, comme le montre le résultat suivant.

Théorème 10.2.11. *Soit H un espace de Hilbert. On suppose que H possède une base hilbertienne $(e_n)_{n\geq 1}$. Alors la série $\sum_{n=1}^{\infty} |< u, e_n >|^2$ converge pour tout $u \in H$ et*

$$lim_{p\to\infty}\|u - \sum_{n=1}^{p} < u, e_n > e_n\| = 0. \tag{10.14}$$

Autrement dit, pour tout $u \in H$ on a

$$u = \sum_{n=1}^{\infty} < u, e_n > e_n. \tag{10.15}$$

On en déduit

$$< u, v >= \sum_{n=1}^{\infty} < u, e_n > \overline{< v, e_n >} \quad \forall u, v \in H \tag{10.16}$$

et en particulier

$$\|u\|^2 = \sum_{n=1}^{\infty} |< u, e_n >|^2 \quad \forall u \in H. \tag{10.17}$$

On peut montrer qu'un espace de Hilbert H possède une base hilbertienne si et seulement si H est séparable, ce qui signifie qu'il existe une suite $(u_n)_{n\geq 1}$ d'éléments de H qui est dense dans H, c'est à dire vérifie $\inf_{n\geq 1}\|x - u_n\| = 0$ pour tout $x \in H$.

Definition 10.2.12. *On dit qu'un sous-ensemble A d'un espace de Hilbert H est **fermé** si la limite de toute suite convergente d'éléments de A appartient à A.*

On peut montrer que tout sous-espace vectoriel fermé F d'un espace de Hilbert séparable H est séparable. On en déduit que si H possède une base hilbertienne, alors tout sous-espace vectoriel de H en possède également une. Dans ce cas on peut étendre la notion de la projection orthogonale à tout sous-espace vectoriel fermé de H.

Théorème 10.2.13. *Soit H un espace de Hilbert séparable, et soit F un sous-espace vectoriel fermé de H. Alors pour tout $u \in H$ il existe un unique élément u_F de F tel que $\|u - u_F\| \geq \|u - v\|$ pour tout $u \in F$, et $u - u_F \in F^{\perp}$. D'autre part, l'application $P_F : u \mapsto u_F$ est linéaire et on a*

$$P_F(u) = \sum_{n=0}^{\infty} < u, f_n > f_n, \tag{10.18}$$

$(f_n)_{n\geq 0}$ désignant une base hilbertienne quelconque de F.

Démonstration :Il suffit de reprendre l'argument utilisé quand F est de dimension finie, en remplaçant les sommes finies par des séries. □

Le théorème concernant la projection orthogonale signifie qu'un sous-espace vectoriel fermé F de H est en **somme directe** avec son orthogonal, c'est à dire que tout élément de H s'écrit de manière unique comme somme d'un élément de F et d'un élément de $F^{\perp}$, ce qui s'écrit sous la forme

$$H = F \oplus F^{\perp}. \tag{10.19}$$

On dit qu'un sous-espace vectoriel G de H est **dense** dans H si tout élément de H est égal à la limite d'une suite d'éléments de G (ce qui implique que $G = H$ si G est fermé). On déduit de ce qui précède que G est dense dans H si et seulement si $G^{\perp} = \{0\}$. Dans ce cas, il existe une base hilbertienne $(g_n)_{n\geq 1}$ de H formée d'éléments de G, et la formule

$$u = \sum_{n=1}^{\infty} < u, g_n > g_n = \lim_{p\to\infty} \sum_{n=0}^{p} < u, g_n > g_n \tag{10.20}$$

permet d'obtenir tout élément de H comme limite d'une suite d'éléments de G.

10.3 Exemples d'espaces de Hilbert

L'espace $\mathbb{C}^n$ muni de son produit hermitien usuel est un espace de Hilbert de dimension n. En fait tout espace de Hilbert de dimension finie est isomorphe en tant qu'espace de Hilbert à un espace $\mathbb{C}^n$, comme le montre le résultat suivant, qui résulte immédiatement des propriétés des bases orthonormales.

Proposition 10.3.1. *Soit H un espace de Hilbert de dimension finie, et soit $(e_1, ..., e_p)$ une base orthonormale de H. Posons, pour $x = (x_1, ..., x_p) \in \mathbb{C}^p$,*

$$\phi(x) = \sum_{j=1}^{p} x_j e_j.$$

Alors ϕ est une bijection linéaire de $\mathbb{C}^p$ sur H, et on a, pour $x, y \in \mathbb{C}^p$,

$$< \phi(x), \phi(y) >=< x, y > . \tag{10.21}$$

En particulier $\|\phi(x)\| = \|x\|$ pour tout $x \in \mathbb{C}^p$.

En dimension infinie, on a l'exemple fondamental suivant

Exemple 10.3.2. *Soit $l^2 := l^2(\mathbb{N}) := \{x = (x_n)_{n\geq 0} \in \mathbb{C}^{\mathbb{N}} \mid \sum_{n=0}^{+\infty} |x_n|^2 < +\infty\}$.*

On pose, pour $x = (x_n)_{n\geq 1}, y = (y_n)_{n\geq 1} \in l^2$,

$$< x, y >= \sum_{n=0}^{+\infty} x_n . \overline{y_n}. \tag{10.22}$$

Alors l^2 est un espace de Hilbert, et si on pose $e_m = (\delta_{m,n})_{n\geq 0}$ pour $m \geq 0$, la famille $(e_m)_{m\geq 0}$ est une base hilbertienne de l^2.

En effet il résulte de l'inégalité de Cauchy-Schwartz que pour $x = (x_n)_{n\geq 1}, y = (y_n)_{n\geq 1} \in l^2$, $p \geq 0$ on a

$$\sum_{n=0}^{p} |x_n||y_n| \leq \sqrt{\sum_{n=0}^{p} |x_n|^2} \sqrt{\sum_{n=0}^{p} |y_n|^2} \leq \sqrt{\sum_{n=0}^{+\infty} |x_n|^2} \sqrt{\sum_{n=0}^{+\infty} |y_n|^2} < +\infty.$$

Par conséquent la série $\sum x_n . \overline{y_n}$ est absolument convergente, donc convergente. Il est clair que l'application $(x, y) \rightarrow < x, y >$ est bien un produit hermitien sur l^2, et que la famille $(e_m)_{m\geq 0}$ est une famille orthonormale qui engendre un sous-espace vectoriel dense de l^2. Soit maintenant $(x^{(m)})_{m\geq 1} = ((x_n^{(m)})_{n\geq 0})_{m\geq 1}$ une suite de Cauchy d'éléments de l^2.

On a $|x_n^{(p)} - x_n^{(q)}| \leq \|x^{(p)} - x^{(q)}\|$ pour $n \geq 0$, $p \geq 1$, $q \geq 1$, donc la suite $(x_n^{(m)})_{m\geq 1}$ est une suite de Cauchy dans $\mathbb{C}$ pour tout $n \geq 0$.

Posons $x_n = \lim_{m\to+\infty} x_n^{(m)}$ pour $n \geq 0$, et posons $x = (x_n)_{n\geq 0}$.

Comme la suite $(x^{(m)})_{m\geq 1}$ est une suite de Cauchy, il existe $M > 0$ tel que $\|x^{(m)}\| \leq M$ pour tout $m \geq 1$, et on a, pour $k \geq 0$,

$$\sum_{n=0}^{k} |x_n|^2 = \lim_{m\to+\infty} \sum_{n=0}^{k} |x_n^{(m)}|^2 \leq M^2.$$

Donc $\sum_{n=0}^{+\infty} |x_n|^2 \leq M^2 < +\infty$, et $x \in l^2$.

Soit maintenant $\epsilon > 0$, et soit $N \geq 1$ tel que $\|x^{(p)} - x^{(q)}\| < \frac{\epsilon}{2}$ pour $p \geq N, q \geq N$. On a, pour $p \geq N$, $k \geq 0$,

$$\sum_{n=0}^{k} |x_n - x_n^{(p)}|^2 = \lim_{q\to+\infty} \sum_{n=0}^{k} |x_n^{(q)} - x_n^{(p)}|^2 < \frac{\epsilon^2}{4}.$$

Par conséquent on a, pour $p \geq N$,

$$\|x - x^{(p)}\| = \lim_{k\to+\infty} \sqrt{\sum_{n=0}^{k} |x_n - x_n^{(p)}|^2} \leq \frac{\epsilon}{2} < \epsilon,$$

et $\lim_{p\to+\infty} \|x - x^{(p)}\| = 0$, ce qui montre que l^2 est bien un espace de Hilbert.

On montre de même que $l^2(\mathbb{Z}) := \{x = (x_n)_{n\in\mathbb{Z}} \in \mathbb{C}^{\mathbb{Z}} \mid \sum_{n=-\infty}^{+\infty} |x_n|^2 < +\infty\}$ est un espace de Hilbert, et que si on pose $e_m = (\delta_{m,n})_{n\in\mathbb{Z}}$ pour $m \in \mathbb{Z}$, la famille $(e_m)_{m\in\mathbb{Z}}$ est une base hilbertienne de $l^2(\mathbb{Z})$. En fait ces espaces fournissent un modèle pour tous les espaces de Hilbert séparables de dimension infinie.

Proposition 10.3.3. *Soit H un espace de Hilbert séparable de dimension infinie, et soit $(e_n)_{n\geq 0}$ une base hilbertienne de H. Posons, pour $x = (x_n)_{n\geq 0} \in l^2$,*

$$\phi(x) = \sum_{j=1}^{+\infty} x_j e_j.$$

Alors ϕ est une bijection linéaire de l^2 sur H, et on a, pour $x, y \in l^2$,

$$< \phi(x), \phi(y) > = < x, y > . \tag{10.23}$$

En particulier $\|\phi(x)\| = \|x\|$ pour tout $x \in l^2$.

Démonstration : Soit $x = (x_n)_{n\geq 0} \in l^2$, et posons $\phi^p(x) = \sum_{j=1}^{p} x_j e_j$ pour $p \geq 0$. Soit $\epsilon > 0$, et soit $N \geq 1$ tel que $\sum_{N+1}^{+\infty} |x_n|^2 < \epsilon^2$.

On a, pour $q > p \geq N$,

$$\|\phi_q(x) - \phi_p(x)\|^2 = \sum_{p+1}^{q} |x_n|^2 \leq \sum_{N+1}^{+\infty} |x_n|^2 < \epsilon^2,$$

de sorte que $\|\phi_q(x)-\phi_p(x)\| < \epsilon$ pour tout couple (p,q)d'entiers tels que $p \geq N, q \geq N$. Donc $(\phi_p(x))_{p\geq 0}$ est une suite de Cauchy dans H, et la série $\sum_{j=1}^{+\infty} x_j e_j$ est convergente dans H. Donc $\phi : l^2 \to H$ est bien définie, et ses propriétés résultent immédiatement du fait que $(e_n)_{n\geq 0}$ est une base hilbertienne de H. $\square$

Si G est un groupe abélien localement compact, l'espace $L^2(G)$, muni du produit hermitien associé á la mesure de Haar sur G, est un espace de Hilbert. Dans le cas où $G = \mathbb{Z}$ muni de la topologie discrète, on retrouve l'espace $l^2(\mathbb{Z})$ évoqué plus haut, et $l^2 = l^2(\mathbb{N})$ s'identifie de manière évidente au sous-espace fermé $l^2(\mathbb{Z})^+$ de $l^2(\mathbb{Z})$ défini par la formule

$$l^2(\mathbb{Z})^+ := \{x = (x_n)_{n\in\mathbb{Z}} \in l^2(\mathbb{Z}) \mid x_n = 0 \ \forall n < 0\}.$$

Dans le cas où $G = \mathbb{R}$, on obtient l'espace de Hilbert $L^2(\mathbb{R})$ formé des fonctions mesurables de carré sommable sur $\mathbb{R}$, où on identifie les fonctions égales presque partout sur $\mathbb{R}$ pour la mesure de Lebesgue. Il s'agit d'un espace de Hilbert séparable, de même que les espaces de Hilbert $L^2(\mathbb{R}^p)$ pour $p \geq 2$.

Soit maintenant $T > 0$. L'espace $L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$ est l'espace des fonctions mesurables et de carré sommable sur $[-\frac{T}{2}, \frac{T}{2}]$, que l'on munit du produit hermitien défini pour $f, g \in L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$ par la formule

$$< f, g >= \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} f(t)\overline{g(t)}dt. \tag{10.24}$$

On notera $\|f\|_2 = \sqrt{< f, f >}$ la norme sur $L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$ associée à ce produit hermitien.

On peut considérer les fonctions appartenant à $L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$ comme des fonctions périodiques de période T définies sur $\mathbb{R}$ tout entier en les prolongeant par périodicité, ce qui permet de faire le cas échéant les calculs de coefficients de Fourier sur des intervalles de longueur T autres que $[-\frac{T}{2}, \frac{T}{2}]$. Ces coefficients de Fourier sont définis pour $f \in L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$, $n \in \mathbb{Z}$ par la formule

$$\widehat{f}(n) = \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} f(t)e^{-in\omega t}dt, \tag{10.25}$$

où $\omega = \frac{2\pi}{T}$. Autrement dit si on pose $e_n(t) = e^{in\omega t}$ pour $n \in \mathbb{Z}$, on a

$$\widehat{f}(n) =< f, e_n > . \tag{10.26}$$

On pose alors, pour $p \geq 0$,

$$S_p(f)(t) = \sum_{n=-p}^{p} \widehat{f}(n)e^{in\omega t}, \sigma_p(f)(t) = \frac{1}{p+1}\sum_{k=0}^{p} S_p(f)(t). \tag{10.27}$$

On peut montrer que les fonctions f continues sur $\left[-\frac{T}{2}, \frac{T}{2}\right]$ et telle que $f\left(-\frac{T}{2}\right) = f\left(\frac{T}{2}\right)$ sont denses dans l'espace de Hilbert $L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$. D'autre part si f est continue sur $\left[-\frac{T}{2}, \frac{T}{2}\right]$ et telle que $f\left(-\frac{T}{2}\right) = f\left(\frac{T}{2}\right)$, on a, d'après le théorème de Féjer

$$\lim_{p\to+\infty}\left[\sup_{|t|\leq\frac{T}{2}}|f(t) - \sigma_p(f)(t)|\right] = 0, \tag{10.28}$$

d'où

$$\lim_{p\to+\infty}\|f - \sigma_p(f)\|_2 = 0.$$

On en déduit que le sous-espace vectoriel de $L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$ engendré par la famille $(e_m)_{m\in\mathbb{Z}}$ est dense dans $L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$. Comme $< e_n, e_m >= \delta_n, m$ pour $n, m \in \mathbb{Z}$, on obtient le théorème suivant, qui contient les formules de Plancherel et Parseval.

Théorème 10.3.4. *On pose $\omega = \frac{2\pi}{T}$ et $e_n(t) := e^{in\omega t}$ pour $n \in \mathbb{Z}$ et $t \in \left[-\frac{T}{2}, \frac{T}{2}\right]$. Alors la famille $(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de $L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$, ce qui donne, pour $f \in L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$,*

$$f = \sum_{n\in\mathbb{Z}} \widehat{f}(n)e_n, \tag{10.29}$$

la série ci-dessus étant convergente au sens de la norme $\|.\|_2$.
En particulier toute fonction $f \in L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$ vérifie la formule de Parseval

$$\frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} |f(t)|^2\, dt = \sum_{n\in\mathbb{Z}} \left|\widehat{f}(n)\right|^2, \tag{10.30}$$

et pour $f \in L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$, $g \in L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$, on a la formule de Plancherel

$$\frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} f(t)\overline{g(t)}dt = \sum_{n\in\mathbb{Z}} \widehat{f}(n)\overline{\widehat{g}(n)}. \tag{10.31}$$

Notons que le fait que la série $\sum_{n\in\mathbb{Z}} \widehat{f}(n)e_n$ converge vers f au sens de la norme $\|.\|_2$ pour $f \in L^2\left[-\frac{T}{2}, \frac{T}{2}\right]$ n'implique pas à priori que la série $\sum_{n\in\mathbb{Z}} \widehat{f}(n)e^{in\omega t}$ converge presque partout vers $f(t)$, mais ceci résulte du difficile théorème de Carleson mentionné plus haut [2].

10.4 Exercices pour l'annexe 2

Exercice 1

Soit $ABCD$ un parallélogramme du plan usuel. Montrer que $AB^2 + BC^2 + CD^2 + DA^2 = AC^2 + BD^2$.

Exercice 2

Dans le plan affine euclidien rapporté à un repère orthonormé $(O, \vec{i}, \vec{j})$ on considère la droite D d'équation

$$ax + by + c = 0,$$

avec $(a, b) \neq (0, 0)$.

1) Ecrire l'équation de la droite perpendiculaire à D et passant par le point M_0 de coordonnées (x_0, y_0).

2) En déduire que la distance de M_0 à la droite D est donnée par la formule

$$d(M_0, D) = \frac{|ax_0 + by_0 + c|}{\sqrt{a^2 + b^2}}.$$

Exercice 3

Dans l'espace affine euclidien usuel rapporté à un repère orthonormé $(O, \vec{i}, \vec{j}, \vec{k})$, on considère le plan P d'équation

$$ax + by + cz + d = 0,$$

avec $(a, b, c) \neq (0, 0, 0)$.

1) Ecrire l'équation de la droite perpendiculaire à P et passant par le point M_0 de coordonnées (x_0, y_0, z_0).

2) En déduire que la distance de M_0 au plan D est donnée par la formule

$$d(M_0, P) = \frac{|ax_0 + by_0 + cz_0 + d|}{\sqrt{a^2 + b^2 + c^2}}.$$

Exercice 4

Dans l'espace affine euclidien usuel rapporté à un repère orthonormé $(O, \vec{i}, \vec{j}, \vec{k})$, on considère les droites D_1 et D_2 d'équations paramétrées

$$\begin{cases} x = x_0 + \lambda u_0 \\ y = y_0 + \lambda v_0 \\ z = z_0 + \lambda w_0 \end{cases}$$

$$\begin{cases} x = x_1 + \lambda u_1 \\ y = y_1 + \lambda v_1 \\ z = z_1 + \lambda w_1 \end{cases}$$

On suppose D_1 et D_2 non parallèles. Donner l'équation de la perpendiculaire commune à D_1 et D_2.

Exercice 5

Soit $\mathcal{E}$ l'espace vectoriel des fonctions continues et périodiques de période 2π sur $\mathbb{R}$, que l'on munit du produit hermitien défini pour $f, g \in \mathcal{E}$ par la formule

$$< f, g >= \frac{1}{2\pi} \int_0^{2\pi} f(t)\overline{g(t)}dt.$$

On définit e_1, e_2, $e_3 \in \mathcal{E}$ par les formules

$$e_1(t) = 1, \;\; e_2(t) = cos(t), \;\; e_3(t) = cos^2(t).$$

Déterminer la famille orthonormale obtenue en appliquant à $\{e_1, e_2, e_3\}$ le procédé d'orthonormalisation de Gram-Schmidt.

Exercice 6

On considère l'espace vectoriel $\mathcal{E}$ des fonctions continues et périodiques de période 2π sur $\mathbb{R}$, muni du produit sacalaire introduit à la question précédente. On pose $u_0(t) = 1$, et, pour $n \geq 1$,

$$u_n(t) = cos(nt), \quad v_n(t) = sin(nt).$$

1) Montrer que la famille $\mathcal{B} := (\cup_{n\geq 0} u_n) \cup (\cup_{n\geq 1} v_n)$ est une famille orthonormale d'éléments de $\mathcal{E}$.

2) Pour $p \geq 1$, on note F_p le sous-espace vectoriel de $\mathcal{E}$ engendré par $\{u_0, ..., u_p\} \cup \{v_1, ..., v_p\}$. Soit P la projection orthogonale de $\mathcal{E}$ sur F_p. En utilisant une formule du cours, expliciter $P(f)(x)$ pour $f \in \mathcal{E}$, $x \in \mathbb{R}$. Quel est le lien entre le polynôme trigonométrique $P(f)$ et la série de Fourier de f?

Exercice 7

Soit F l'image de $\mathbb{C}^3$ par l'application $u : X \longmapsto \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & 2 \\ 1 & 0 & 1 \end{bmatrix} X$.

Trouver une base orthogonale de F, et calculer la matrice représentant la projection orthogonale de $\mathbb{R}^3$ sur F par rapport à la base canonique de $\mathbb{R}^3$.

Exercice 8

En s'aidant d'un logiciel de calcul formel, répondre aux mêmes questions que dans l'exercice précédent pour $G := \{AX\}_{X \in \mathbb{R}^8}$, avec

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 \\ 15 & 13 & 11 & 9 & 7 & 5 & 3 & 1 \\ 1 & 4 & 7 & 10 & 13 & 16 & 19 & 22 \\ 22 & 19 & 16 & 13 & 10 & 7 & 4 & 1 \\ 1 & 5 & 9 & 13 & 17 & 21 & 25 & 29 \end{bmatrix}.$$

Exercice 9

On pose $\psi(t) = 1$ si $t \in [0, 1/2]$, $\psi(t) = -1$ si $t \in]1/2, 1]$, $\psi(t) = 0$ si $t \in]-\infty, 0[\cup]1, +\infty[$. D'autre part pour $j, n \in \mathbb{Z}$, $t \in \mathbb{R}$, on pose

$$\psi_{j,n}(t) = \frac{1}{\sqrt{2^j}} \psi(\frac{t - 2^j n}{2^j}).$$

Montrer que la famille $(\psi_{j,n})_{j \in \mathbb{Z}, n \in \mathbb{Z}}$ est une base hilbertienne e $L^2(\mathbb{R})$ (on admettra que les fonctions continues à support compact sont denses dans $L^2(\mathbb{R})$).

Exercice 10

Soit H un espace de Hilbert. Une partie C de H est dite convexe si $tx + (1-t)y \in C$ pour tout couple (x, y) déléments de C et tout réel $t \in [0, 1]$.

Soit maintenant C une partie convexe fermée de H. On pose $d = \inf_{y \in H} \|x - y\|$.

1) Montrer que $x \in C$ si $d = 0$.

2) On suppose $d > 0$. Pour $n \geq 1$, soit $y_n \in C$ tel que $\|x - y_n\| < \frac{1}{n}$. Montrer que la suite $(y_n)_{n \geq 1}$ est de Cauchy.

3) En déduire qu'il existe un unique élément $u_C(x)$ de C tel que $\|x - u(x)\| \leq \|x - y\|$ pour tout $y \in C$.

4) Montrer que l'application $x \to u_C(x)$ est linéaire si C est un sous-espace vectoriel de H. En déduire dans ce cas une construction de la projection orthogonale sur C indépendante de la construction d'une base hilbertienne de C.

Bibliographie

[1] Archimède : *Eureka*, Communication orale, Syracuse (vers l'an -215).

[2] L. Carleson,*On convergence and growth of partial sums of Fourier series*, Acta Mathematica **116** (1966), 135-157.

[3] C. Bachoc. Mathématiques discrètes de la transformée de Fourier, Cours de Master CSI, Université Bordeaux 1, 2005.

[4] X. Dussau, J. Esterle et F. Zarouf, Cours d'algèbre, ESTIA, 2001.

[5] X.Dussau, J. Esterle et F. Zarouf, Cours d'algèbre linéaire, ESTIA, 2001.

[6] X. Dussau, J. Esterle,O. Réjasse et F. Zarouf, Analyse élémentaire, ESTIA, 2003.

[7] E.L. Jury, Theory and application of the z-transform method, Robert E. Krieger Publishing Company, Malabar, Florida, 1964.

[8] F. Luthon, Initiation au traitement de signal, IUT Informatique, Chateau Neuf, Place Paul Bert, 64100, Bayonne, 2004.

[9] G. Peyré, L'algèbre discrète de la transformée de Fourier, Collection Mathématiques à l'Université, Ellipses, 2004.

[10] W. Rudin, Fourier analysis on groups, Intersience Publishers, 1962.

Index