



HAL
open science

Signaux discrets périodiques

Rolland Robert

► **To cite this version:**

Rolland Robert. Signaux discrets périodiques. École thématique. Signaux discrets périodiques, En ligne, France. 2008, pp.15. <hal-04207162>

HAL Id: hal-04207162

<https://hal.science/hal-04207162v1>

Submitted on 14 Sep 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

SIGNAUX DISCRETS PÉRIODIQUES

par

Robert Rolland

1. Introduction - Notations

Nous allons étudier les signaux discrets périodiques, C'est-à-dire les fonctions du groupe fini $\mathbb{Z}/n\mathbb{Z}$ dans \mathbb{C} .

Plus précisément, nous fixons un entier $n > 1$. Notons G le groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Nous allons nous intéresser à l'algèbre sur le corps des complexes \mathbb{C} de toutes les fonctions de G dans \mathbb{C} . Nous noterons \mathcal{F} cet espace. Ce sera l'espace des signaux.

Voici la démarche que nous allons suivre et qui reproduit dans ce cas simple mais instructif ce qu'on fait habituellement dans le cas des signaux discrets (fonctions définies sur \mathbb{Z}), dans le cas des signaux continus (définis sur \mathbb{R}) ou des signaux continus périodiques (définis sur le tore \mathbb{R}/\mathbb{Z}).

- L'espace des signaux. On présente l'espace \mathcal{F} ainsi que la base des évaluations dans laquelle les composantes d'une fonction sont ses images.

- Les opérateurs de translation. On regarde l'action du groupe des translations sur les signaux. En particulier l'étude des vecteurs propres des opérateurs de translation met en lumière l'intérêt des caractères du groupe G .
- Les filtres stationnaires. Nous appelons filtre linéaire un opérateur linéaire de l'espace \mathcal{F} des signaux. Un signal arrive à l'entrée du filtre (signal d'entrée) et en ressort (signal de sortie) transformé par un opérateur linéaire. Un filtre est dit stationnaire lorsque la forme du signal de sortie ne dépend que du signal d'entrée et non de l'instant où celui-ci est appliqué. Autrement dit si on translate le signal d'entrée f d'un temps t , le signal de sortie obtenu est le signal de sortie de f translaté du même temps t .
- La convolution. On introduit la notion d'opérateur de convolution et on montre que cette notion coïncide avec la notion de filtre stationnaire : un filtre est stationnaire si et seulement si c'est un opérateur de convolution.
- La transformation de Fourier. Nous étudions les filtres stationnaires et donc nous nous plaçons dans une base de vecteurs propres de ces opérateurs, c'est-à-dire la base des caractères. Les coefficients d'un signal dans cette base sont à un facteur multiplicatif constant près les coefficients de Fourier.
- La transformation en Z . C'est l'analogue discret de la transformation de Laplace. Dans ce cas particulier, nous considérons les valeurs prises par un signal f comme les coefficients d'un polynôme. Nous indiquons les liens entre transformation de Fourier et transformation de Laplace.
- Les applications. Nous faisons fonctionner, sur des exemples, les notions que nous avons introduites précédemment.

2. L'espace \mathcal{F}

Il est immédiat de constater que l'espace \mathcal{F} des fonctions de $\mathbb{Z}/n\mathbb{Z}$ dans \mathbb{C} possède les propriétés suivantes

Théorème 2.1. — \mathcal{F} est une algèbre commutative pour l'addition des fonctions " + ", la multiplication des fonctions " \times ", la multiplication d'une fonction par un scalaire " \cdot ".

Donnons tout d'abord un exemple important de fonction dans \mathcal{F} .

À tout élément $\mathbf{a} \in \mathbf{G}$, associons la fonction $\mathbf{e}_{\mathbf{a}}$ définie par

$$\mathbf{e}_{\mathbf{a}}(\mathbf{x}) = \begin{cases} 1 & \text{si } \mathbf{x} = \mathbf{a}, \\ 0 & \text{si } \mathbf{x} \neq \mathbf{a}. \end{cases}$$

Théorème 2.2. — La famille $(\mathbf{e}_{\mathbf{a}})_{0 \leq \mathbf{a} \leq \mathbf{n}-1}$ est une base de \mathcal{F} . Ainsi \mathcal{F} est de dimension \mathbf{n} . Toute fonction $f \in \mathcal{F}$ se décompose sous la forme

$$f = \sum_{\mathbf{a}=0}^{\mathbf{n}-1} f(\mathbf{a})\mathbf{e}_{\mathbf{a}}.$$

Preuve. Supposons $\sum_{\mathbf{a}=0}^{\mathbf{n}-1} \lambda_{\mathbf{a}}\mathbf{e}_{\mathbf{a}} = 0$. Alors en appliquant cette fonction nulle à un élément quelconque $\mathbf{x} \in \mathbf{G}$ on trouve que

$$\sum_{\mathbf{a}=0}^{\mathbf{n}-1} \lambda_{\mathbf{a}}\mathbf{e}_{\mathbf{a}}(\mathbf{x}) = 0,$$

et donc $\lambda_{\mathbf{x}} = 0$. Ceci montre que le système est libre.

Pour montrer que le système est générateur il suffit de vérifier que toute fonction f s'écrit sous la forme indiquée dans l'énoncé du théorème. \square

Remarquons que quand on utilise la base précédente les composantes de f sont les images de f . Autrement dit, l'utilisation de la base $(\mathbf{e}_{\mathbf{a}})_{0 \leq \mathbf{a} \leq \mathbf{n}-1}$ revient à se donner f par la suite finie de ses images $(f(\mathbf{a}))_{0 \leq \mathbf{a} \leq \mathbf{n}-1}$.

3. Les opérateurs de translation sur \mathcal{F}

Pour tout $\mathbf{h} \in \mathbf{G}$ on définit l'opérateur linéaire $T_{\mathbf{h}}$ de \mathcal{F} dans lui même par

$$T_{\mathbf{h}}(f)(\mathbf{x}) = f(\mathbf{x} + \mathbf{h}).$$

Nous cherchons à étudier cet opérateur et en particulier ses valeurs propres et ses vecteurs propres.

Remarquons que

$$T_h = (T_1)^h,$$

ce qui prouve que si χ est un vecteur propre de T_1 , c'est aussi pour tout $h \in G$ un vecteur propre de T_h . On a donc pour tout $x \in G$ et tout $h \in G$

$$\chi(x+h) = \lambda_h \chi(x).$$

Remarquons tout d'abord qu'une fonction telle que $f(0) = 0$ ne peut pas être un vecteur propre de T_1 . En effet si f est vecteur propre alors

$$T_1(f)(x) = \lambda f(x),$$

c'est-à-dire

$$f(x+1) = \lambda f(x).$$

Si $f(0) = 0$ par récurrence on montre alors que $f(x) = 0$ pour tout x et donc que $f = 0$ ce qui est contraire à l'hypothèse. Donc tout vecteur propre est proportionnel à un vecteur propre χ vérifiant $\chi(0) = 1$.

On a donc en supposant que $\chi(0) = 1$ et en donnant à x la valeur 0

$$\chi(h) = \lambda_h,$$

et donc

$$\chi(x+h) = \chi(x)\chi(h).$$

Définition 3.1. — Les caractères de G sont les homomorphismes du groupe G dans le groupe multiplicatif \mathbb{C}^* , c'est-à-dire les fonctions χ de G dans \mathbb{C}^* vérifiant

$$\chi(x+y) = \chi(x)\chi(y).$$

Théorème 3.1. — Les caractères de G sont les n fonctions χ_u où $u \in G$ définies par

$$\chi_u(v) = e^{\frac{2i\pi uv}{n}}.$$

Preuve. Dans \mathbf{G} la somme $1 + \dots + 1$ formée de n termes égaux à 1 est nulle. On en déduit que $\chi(1)^n = \chi(0) = 1$. Donc $\chi(1)$ est une racine nième de l'unité. Connaissant $\chi(1)$ on peut calculer $\chi(x)$ en écrivant x comme somme de x termes égaux à 1. Par suite $\chi(x) = \chi(1)^x$. Ceci prouve qu'un caractère est nécessairement de la forme annoncée. On vérifie rapidement que toute fonction de cette forme est un caractère. \square

On pourra remarquer qu'en fait les caractères sont à valeurs dans le sous-groupe de \mathbb{C}^* constitué des nombres complexes de module 1. On peut donc dire aussi que les caractères sont les homomorphismes du groupe \mathbf{G} dans le groupe multiplicatif \mathbf{U} des nombres complexes de module 1.

Théorème 3.2. — Les caractères forment une base de \mathcal{F} constituée de vecteurs propres de T_h . La valeur propre de T_h associée au vecteur propre χ_u est la racine nième de l'unité

$$e^{\frac{2i\pi hu}{n}}.$$

4. Les filtres stationnaires

Soit H un opérateur de \mathcal{F} . On suppose que cet opérateur est stationnaire c'est-à-dire que si on translate le signal d'entrée d'un temps t la sortie est tradlatée du même temps (autrement dit la forme du signal de sortie ne dépend pas de l'instant où on a envoyé le signal d'entrée). Ceci s'exprime en écrivant que

$$H(T_t(f)) = T_t(H(f)),$$

ou encore que

$$H \circ T_t = T_t \circ H.$$

Donc un opérateur H est stationnaire si et seulement s'il commute avec les opérateurs de translation.

Soit χ un caractère et λ la valeur propre de T_1 associée à χ . Alors

$$T_1(H(\chi)) = H(T_1(\chi)) = H(\lambda\chi) = \lambda H(\chi).$$

Ceci prouve que ou bien $H(\chi) = 0$, ou bien $H(\chi)$ est un vecteur propre de T_1 associé à la valeur propre λ . Dans tous les cas on peut écrire $H(\chi) =$

$\mu\chi$. Les caractères forment donc aussi une base de vecteurs propres de H .

Remarque : $\mu = H(\chi)(0)$.

Remarquons encore que H , qui commute avec T_1 , peut s'écrire de manière unique sous la forme

$$H = \sum_{i=0}^{n-1} \alpha_i T_1^i.$$

Ceci est conséquence du théorème suivant

Théorème 4.1. — Soit T un opérateur à spectre simple d'un espace vectoriel de dimension finie n (T a n valeurs propres distinctes). Un opérateur H commute avec T si et seulement si H peut s'écrire sous la forme

$$H = \sum_{i=0}^{n-1} \alpha_i T^i.$$

De plus dans ce cas cette écriture est unique.

Preuve. Il suffit d'une part de constater qu'un opérateur qui s'écrit sous cette forme commute avec T , d'autre part que si un opérateur commute avec T il s'écrit sous cette forme de manière unique. Il suffit de choisir une base de vecteurs propres de T , les matrices de T^i sont alors diagonales. En écrivant que H commute avec T on trouve aussi que dans cette base H est diagonale. En écrivant la relation cherchée, on trouve les coefficients α_i de manière unique en résolvant un système de Vandermonde. \square

Ce théorème sur l'écriture d'un filtre stationnaire H nous permet d'énoncer le théorème suivant

Théorème 4.2. — L'espace des filtres stationnaires est de dimension n .

Preuve. Il suffit de constater que les T_1^i sont linéairement indépendants.

5. Convolution et filtres stationnaires

Définition 5.1. — Soient f et g deux fonctions de \mathcal{F} . Le produit de convolution de f par g est la fonction $f \star g \in \mathcal{F}$ définie par

$$f \star g(\mathbf{u}) = \sum_{\mathbf{v}+\mathbf{w}=\mathbf{u}} f(\mathbf{v})g(\mathbf{w}).$$

Remarquons qu'on peut aussi écrire

$$f \star g(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbf{G}} f(\mathbf{v})g(\mathbf{u} - \mathbf{v}) = \sum_{\mathbf{v} \in \mathbf{G}} f(\mathbf{v})T_{-\mathbf{v}}(g)(\mathbf{u}).$$

On vérifie immédiatement le résultat suivant

Théorème 5.1. — \mathcal{F} muni de l'addition " + ", du produit de convolution " \star " et du produit par un scalaire " . " est une algèbre commutative.

Fixons maintenant une fonction $\mathbf{h} \in \mathcal{F}$ et définissons l'opérateur $H_{\mathbf{h}}$ de \mathcal{F} par

$$H_{\mathbf{h}}(f) = \mathbf{h} \star f.$$

Définition 5.1. — Un opérateur du type $H_{\mathbf{h}}$ est appelé un opérateur de convolution.

Théorème 5.2. — Les opérateurs de convolution sont les filtres stationnaires. En particulier

$$T_{\mathbf{u}}(f \star g) = f \star T_{\mathbf{u}}(g).$$

De plus

$$\mathbf{h} = H_{\mathbf{h}}(\mathbf{e}_0).$$

Preuve. Montrons tout d'abord qu'un opérateur de convolution est stationnaire.

$$\begin{aligned} T_{\mathbf{u}}(H_{\mathbf{h}}(f))(x) &= H_{\mathbf{h}}(f)(\mathbf{u} + x) = \mathbf{h} \star f(\mathbf{u} + x), \\ &= \sum_{\mathbf{v} \in \mathbf{G}} \mathbf{h}(\mathbf{v})f(\mathbf{u} + x - \mathbf{v}) = \sum_{\mathbf{v} \in \mathbf{G}} \mathbf{h}(\mathbf{v})T_{\mathbf{u}}(f)(x - \mathbf{v}), \\ &= \mathbf{h} \star T_{\mathbf{u}}(f)(x) = H_{\mathbf{h}}(T_{\mathbf{u}}(f))(x). \end{aligned}$$

Montrons maintenant que l'espace des opérateurs de convolution est aussi de dimension n . Ceci finira de prouver le théorème. Pour cela étudions le noyau de l'application linéaire de \mathcal{F} dans l'espace des opérateurs de convolution qui à tout h associe H_h . Supposons $H_h = 0$, c'est-à-dire $h * f = 0$ pour toute fonction $f \in \mathcal{F}$. Soit x fixé. Considérons la fonction $f = e_0$. Alors

$$h * e_0(x) = \sum_{u+v=x} h(u)e_0(v) = h(x).$$

On en déduit $h(x) = 0$ et ceci pour tout x . \square

Remarque : Soit H un filtre stationnaire. Alors on sait que H se décompose de manière unique sous la forme

$$H = \sum_{i=0}^{n-1} a_i T_1^i.$$

Remarquons alors que

$$T_1(f) = e_{n-1} * f, T_1^2(f) = e_{n-2} * f, \dots, T_1^{n-1}(f) = e_1 * f.$$

En conséquence

$$H(f) = \sum_{i=0}^{n-1} a_i e_{n-i} * f = \left(\sum_{i=0}^{n-1} a_i e_{n-i} \right) * f.$$

Donc

$$h = \sum_{i=0}^{n-1} a_i e_{n-i},$$

et encore

$$h(u) = a_{-u}.$$

Enfin en utilisant l'égalité

$$e_u * e_v = e_{u+v},$$

on déduit que

$$H(\mathbf{e}_{-\mathbf{u}})(0) = \mathbf{a}_{-\mathbf{u}} = \mathbf{h}(\mathbf{u}).$$

Regardons maintenant la matrice d'un opérateur de convolution H_h dans la base $(\mathbf{e}_a)_{a \in G}$. Le coefficient $h_{i,j}$ qui se trouve à la ligne $0 \leq i \leq n-1$ et dans la colonne $0 \leq j \leq n-1$ est la composante sur \mathbf{e}_i de l'image de \mathbf{e}_j autrement dit,

$$h_{i,j} = H_h(\mathbf{e}_j)(i).$$

Donc,

$$h_{i,j} = \mathbf{h} * \mathbf{e}_j(i) = \sum_{\mathbf{u}+\mathbf{v}=\mathbf{i}} \mathbf{h}(\mathbf{u})\mathbf{e}_j(\mathbf{v}) = \mathbf{h}(\mathbf{i}-\mathbf{j}).$$

Cette matrice s'écrit

$$\mathcal{H} = \begin{pmatrix} \mathbf{h}(0) & \mathbf{h}(n-1) & \cdots & \mathbf{h}(1) \\ \mathbf{h}(1) & \mathbf{h}(0) & \cdots & \mathbf{h}(2) \\ \vdots & \vdots & & \vdots \\ \mathbf{h}(n-1) & \mathbf{h}(n-2) & \cdots & \mathbf{h}(0) \end{pmatrix}.$$

C'est une matrice circulante. Les matrices circulantes sont les matrices des opérateurs de convolution (ou des filtres stationnaires).

6. La structure hermitienne

Munissons maintenant \mathcal{F} du produit scalaire hermitien

$$\langle f, g \rangle = \sum_{i=0}^{n-1} f(i)\overline{g(i)}.$$

Nous allons montrer que les caractères forment une base orthogonale de \mathcal{F} .

Nous avons tout d'abord besoin d'un lemme

Lemme 6.1. — Soit $\chi_{\mathbf{u}}$ un caractère non trivial ($\mathbf{u} \neq 0$). Alors

$$\sum_{\mathbf{v} \in G} \chi_{\mathbf{u}}(\mathbf{v}) = 0.$$

Preuve. Remarquons que

$$\chi_u(\mathbf{v}) = \left(e^{\frac{2i\pi\mathbf{u}}{n}} \right)^{\mathbf{v}},$$

et que de plus du fait que $0 < \mathbf{u} < n$ on a $e^{\frac{2i\pi\mathbf{u}}{n}} \neq 1$. En conséquence

$$\sum_{\mathbf{v} \in \mathbf{G}} \chi_u(\mathbf{v}) = \frac{1 - \left(e^{\frac{2i\pi\mathbf{u}}{n}} \right)^n}{1 - e^{\frac{2i\pi\mathbf{u}}{n}}} = 0. \quad \square$$

Théorème 6.1. — Les caractères forment une base orthogonale de \mathcal{F} . La norme de chaque caractère est \sqrt{n} .

Preuve. Nous devons montrer que

$$\langle \chi_u, \chi_v \rangle = \begin{cases} n & \text{si } \mathbf{u} = \mathbf{v}, \\ 0 & \text{si } \mathbf{u} \neq \mathbf{v}. \end{cases}$$

Pour cela écrivons successivement

$$\begin{aligned} \langle \chi_u, \chi_v \rangle &= \sum_{\mathbf{w} \in \mathbf{G}} \chi_u(\mathbf{w}) \chi_v(-\mathbf{w}) = \sum_{\mathbf{w} \in \mathbf{G}} \chi_w(\mathbf{u}) \chi_w(-\mathbf{v}), \\ \langle \chi_u, \chi_v \rangle &= \sum_{\mathbf{w} \in \mathbf{G}} \chi_w(\mathbf{u} - \mathbf{v}) = \sum_{\mathbf{w} \in \mathbf{G}} \chi_{\mathbf{u} - \mathbf{v}}(\mathbf{w}). \end{aligned}$$

Le résultat attendu découle du lemme. \square

Définition 6.1. — Soit $f \in \mathcal{F}$. Les coefficients de Fourier de f sont les produits scalaires $\hat{f}(\mathbf{v}) = \langle f, \chi_v \rangle$. Ainsi

$$\hat{f}(\mathbf{v}) = \sum_{\mathbf{u} \in \mathbf{G}} f(\mathbf{u}) \overline{\chi_v(\mathbf{u})} = \sum_{\mathbf{u} \in \mathbf{G}} f(\mathbf{u}) e^{-\frac{2i\pi\mathbf{u}\mathbf{v}}{n}}.$$

La fonction \hat{f} qui est elle aussi dans \mathcal{F} est la transformée de Fourier de la fonction f .

Remarque : Bien que f et sa transformée de Fourier \hat{f} soient toutes deux des fonctions de \mathcal{F} , il n'est pas bon de considérer qu'elles sont dans le même espace.

Comme la base des caractères est orthogonale, les coefficients de Fourier sont à un facteur près les composantes de f sur la base des caractères. Plus précisément

Théorème 6.2. — La décomposition de f sur la base des caractères s'écrit

$$f(\mathbf{u}) = \frac{1}{n} \sum_{\mathbf{v}=0}^{n-1} \hat{f}(\mathbf{v}) e^{\frac{2i\pi\mathbf{u}\mathbf{v}}{n}}.$$

7. Étude plus complète de la transformation de Fourier

Nous avons pour la transformation de Fourier les résultats suivants

Théorème 7.1. — La transformation de Fourier discrète est un isomorphisme de l'algèbre $(\mathcal{F}, +, \star, \cdot)$ sur l'algèbre $(\mathcal{F}, +, \times, \cdot)$. Autrement dit

$$\begin{aligned} \widehat{f + g} &= \hat{f} + \hat{g}, \\ \widehat{\lambda \cdot f} &= \lambda \cdot \hat{f}, \\ \widehat{f \star g} &= \hat{f} \times \hat{g}, \\ \widehat{e_0} &= \chi_0. \end{aligned}$$

Théorème 7.2. — L'inverse de la transformée de Fourier est donnée par la formule d'inversion

$$f(\mathbf{u}) = \frac{1}{n} \hat{f}(-\mathbf{u}).$$

Théorème 7.3. — On a aussi

$$\begin{aligned} \widehat{f \times g} &= \frac{1}{n} \hat{f} \star \hat{g}, \\ \|\hat{f}\| &= \sqrt{n} \|f\|. \end{aligned}$$

Voici quelques exemples simples de transformées de Fourier

- $\hat{e}_{\mathbf{u}} = \chi_{-\mathbf{u}}$.
- $\hat{\chi}_{\mathbf{u}} = n e_{\mathbf{u}}$.

Revenons sur la matrice \mathcal{H} circulante de la section précédente. Cette matrice est la matrice dans la base $(\mathbf{e}_\alpha)_{\alpha \in G}$ de la convolution avec \mathbf{h} . Nous savons que les $(\chi_\mathbf{u})_{\mathbf{u} \in G}$ forment une base de vecteurs propres. Les valeurs propres sont les

$$H(\chi_\mathbf{u})(0) = \mathbf{h} \star \chi_\mathbf{u}(0) = \sum_{\mathbf{v} \in G} \mathbf{h}(\mathbf{v})\chi_\mathbf{u}(-\mathbf{v}) = \hat{\mathbf{h}}(\mathbf{u}).$$

En conséquence

$$\det(\mathcal{H}) = \prod_{\mathbf{u}=0}^{n-1} \hat{\mathbf{h}}(\mathbf{u}).$$

On a donc le théorème suivant

Théorème 7.4. — Pour que l'opérateur stationnaire H soit inversible il faut et il suffit que la transformée de Fourier $\hat{\mathbf{h}}$ ne s'annule pas.

Remarquons qu'on peut écrire

$$H(\chi_\mathbf{u}) = \hat{\mathbf{h}}(\mathbf{u})\chi_\mathbf{u}.$$

La fonction $\hat{\mathbf{h}}$ est appelée la fonction de transfert de H . Cette fonction est importante pour la description de la transformation H . En particulier si nous travaillons sur les transformations de Fourier alors

$$\widehat{H(f)} = \widehat{\mathbf{h}} \star \widehat{f} = \hat{\mathbf{h}}\hat{f}.$$

8. La transformation en Z

La transformation en Z est l'analogie discret de la transformation de Laplace.

Soit \mathcal{L} l'application de \mathcal{F} dans $\mathbb{C}[Z]/(1 - Z^n)$ qui à toute fonction $f = \sum_{\mathbf{u} \in G} \mathbf{a}_\mathbf{u} \mathbf{e}_\mathbf{u} \in \mathcal{F}$ fait correspondre

$$\mathcal{L}(f)(Z) = \sum_{\mathbf{u} \in G} \mathbf{a}_\mathbf{u} Z^{-\mathbf{u}}.$$

En ce qui concerne les notations, nous noterons

$$P(Z) \equiv Q(Z) \pmod{Z^n - 1}$$

lorsque les polynômes $P(Z)$ et $Q(Z)$ définissent le même élément de l'algèbre $\mathbb{C}[Z]/(1 - Z^n)$.

Théorème 8.1. — La transformée en Z d'un produit de convolution est le produit des transformées en Z

$$\mathcal{L}(f \star g)(Z) \equiv \mathcal{L}(f)(Z)\mathcal{L}(g)(Z) \pmod{Z^n - 1}.$$

La transformation \mathcal{L} est un isomorphisme de l'algèbre $(\mathcal{F}, +, \star, \cdot)$ sur l'algèbre $(\mathbb{C}[Z]/(1 - Z^n), +, \times, \cdot)$ des polynômes modulo $1 - Z^n$.

La transformée en Z est liée à la transformation de Fourier grâce au théorème suivant

Théorème 8.2. — Soit $f \in \mathcal{F}$. Alors pour tout $\mathbf{u} \in \mathbb{G}$

$$\hat{f}(\mathbf{u}) = \mathcal{L}(f)(e^{\frac{2i\pi\mathbf{u}}{n}}).$$

En conséquence le produit de deux polynômes modulo $1 - Z^n$ peut se faire par transformation de Fourier discrète. Ceci est intéressant par le fait qu'il existe un algorithme rapide de calcul de transformation de Fourier discrète : la transformée de Fourier rapide.

9. Applications

On dispose de trois algèbres isomorphes entre elles et on passe de l'une à l'autre en fonction du problème posé. Ces trois algèbres sont $(\mathcal{F}, +, \star, \cdot)$, $(\mathcal{F}, +, \times, \cdot)$ et $(\mathbb{C}[Z]/(1 - Z^n), +, \times, \cdot)$.

Voici un premier exemple. L'opérateur T_1 de translation est bien sûr un opérateur de convolution

$$T_1(f) = e_{n-1} \star f.$$

En conséquence la transformée en Z associée est la multiplication par Z . Autrement dit

$$\mathcal{L}(\mathbb{T}_1(f))(Z) \equiv Z\mathcal{L}(f)(Z) \pmod{Z^n - 1}.$$

L'opérateur Δ défini par

$$\Delta(f)(\mathbf{u}) = f(\mathbf{u} + 1) - f(\mathbf{u}),$$

qui peut aussi s'exprimer par

$$\Delta = \mathbb{T}_1 - \mathbb{I},$$

correspond à la multiplication par $(Z - 1)$.

Essayons de résoudre l'équation

$$\mathbb{H}(f) = g,$$

ou encore

$$\mathbf{h} * f = g,$$

où \mathbf{h} et g sont connues et f à trouver. Posons

$$P_h(Z) = \mathcal{L}(\mathbf{h})(Z), \quad P_g(Z) = \mathcal{L}(g)(Z), \quad P_f(Z) = \mathcal{L}(f)(Z).$$

On doit donc avoir

$$P_h(Z)P_f(Z) \equiv P_g(Z) \pmod{Z^n - 1}.$$

Notons $G(Z) = \text{pgcd}(P_h(Z), Z^n - 1)$. Si $P_g(Z)$ n'est pas divisible par $G(Z)$ il n'y a pas de solution. Sinon on est amené à chercher tous les polynômes P_f de degré $\leq n - 1$ tels que

$$P_f(Z)P_1(Z) \equiv P_2(Z) \pmod{Q(Z)},$$

où

$$P_1(Z) = \frac{P_h(Z)}{G(Z)}, \quad P_2(Z) = \frac{P_g(Z)}{G(Z)}, \quad Q(Z) = \frac{Z^n - 1}{G(Z)}.$$

Maintenant, $P_1(Z)$ et $Q(Z)$ sont premiers entre eux. On peut donc inverser $P_1(Z)$ modulo $Q(Z)$ on obtient $P_1'(Z)$ tel que

$$P_1(Z)P_1'(Z) \equiv 1 \pmod{Q(Z)}.$$

Les solutions sont donc les polynômes P_f de degré $\leq n - 1$ de la forme

$$P_f(Z) = P_1'(Z) \cdot P_2(Z) + K(Z)Q(Z).$$

Prenons comme exemple pour H l'opérateur Δ qui correspond à la multiplication par $Z-1$. Alors $\text{pgcd}(Z-1, Z^n-1) = (Z-1)$. Donc $\Delta(f) = g$ n'a de solution que si $P_g(Z)$ est divisible par $Z-1$, c'est-à-dire si $P_g(1) = 0$ ou encore $\sum_{u=0}^{n-1} g(u) = 0$ (cette dernière somme est aussi $\hat{g}(0)$). Dans ce cas on a

$$P_1(Z) = 1, \quad Q(Z) = 1 + Z + \dots + Z^{n-1},$$

donc

$$P_f(Z) = \frac{P_g(Z)}{Z-1} + C(1 + Z + \dots + Z^{n-1}),$$

où C est une constante.

Remarque : La fonction h étant donnée, essayons de trouver f telle que

$$h \star f = e_0.$$

D'après ce qu'on vient de voir il n'a de solution que si

$$\text{pgcd}(P_h(Z), Z^n - 1) = 1.$$

On retrouve ainsi la condition déjà énoncée au paragraphe 7 : pour que h soit inversible il faut et il suffit que la transformée de Fourier de h ne s'annule pas, ce qui s'exprime ici en disant qu'aucune racine de l'unité n 'annule $P_h(Z)$. Ce ci se voit aussi directement sur la transformation de Fourier car h a un inverse pour la convolution si et seulement si :

$$\hat{h}\hat{f} = \hat{e}_0 = 1.$$