BASE DES POLYNOMES DE HILBERT

1 Séries polynomiales

Voici un exemple d'utilité des bases en dimension finie, qui peut constituer une alternative à l'exemple classique des bases utilisées pour calculer la suite de Fibonacci. Il s'agit de la base des polynômes de Hilbert.

PROBLEME : Soit P un polynôme de $\mathbb{R}[X]$. Calculer pour tout n, $S_P(n) := P(0) + P(1) + \ldots + P(n)$.

Pour cela, supposons que l'on ait trouvé un polynôme Q tel que

$$\boxed{Q(X+1) - Q(X) = P(X),\ Q(0) = 0.}$$

Alors, le problème sera résolu, puisque

$$S_P(n) = P(0)+P(1)+\ldots+P(n) = Q(1)-Q(0)+Q(2)-Q(1)+\ldots+Q(n+1)-Q(n) = Q(n+1),$$

par simplifications en cascades.

Remarque : Le problème s'apparente à l'intégration de P. On dit que P est la dérivée *discrète* de Q et donc que Q est une primitive discrète de P. On notera dans la suite D la dérivée discrète : $DQ(X) = Q(X+1) - Q(X)$.

On note maintenant H_n le n-ième polynôme de Hilbert :

$$\boxed{H_k := \tfrac{1}{k!}X(X-1)\ldots(X-k+1).}$$

Alors, il est clair que H_k est un polynôme de degré k et

$$\boxed{DH_{k+1} = H_k.}$$

Effectivement :

$$DH_{k+1}(X) = H_{k+1}(X+1)-H_{k+1}(X) = \frac{1}{(k+1)!}(X+1)(X)\ldots(X-k+1)-\frac{1}{(k+1)!}(X)(X-1)\ldots(X-k)$$

$$= \frac{1}{(k+1)!}X(X-1)\ldots(X-k+1)[X+1-X+k)] = H_k(X).$$

Donc (H_k) est une base de l'espace vectoriel des polynômes $\mathbb{R}[X]$ et de plus, si on décompose P dans la base des H_k,

$$P = \alpha_0 H_0 + \alpha_1 H_1 + \ldots + \alpha_m H_m,$$

et si on pose

$$Q = \alpha_0 H_1 + \alpha_1 H_2 + \ldots + \alpha_m H_{m+1},$$

Il vient par linéarité de D :

$$DQ = \alpha_0 DH_1 + \alpha_1 DH_2 + \ldots + \alpha_m DH_{m+1} = \alpha_0 H_0 + \alpha_1 H_1 + \ldots + \alpha_m H_m = P.$$

Ce qui fournit la solution à notre problème : $S_P(n) = Q(n+1)$.

2 Dual des polynômes de Hilbert

Il reste à comprendre comment trouver les coordonnées de P dans la base des polynômes de Hilbert, et ceci revient à en connaître la base duale.

Soit $E_n = \mathbb{R}[X]_n$ l'espace des polynômes réels de dimension inférieure ou égale à n. On considère pour tout k l'application Δ_k de E_n dans $\mathbb{R}$ définie par

$$\boxed{\Delta_k(P) = D^k(P)(0).}$$

L'application Δ_k est clairement une forme linéaire sur E_n.

On trouve $\Delta_k(H_k) = D^k(H_k)(0) = H_0(0) = 1$. Maintenant, si $k > m$, il est clair que $D^k(H_m) = 0$, et donc $\Delta_k(H_m) = 0$. Enfin, si $k < m$, alors $\Delta_k(H_m) = D^k(H_m)(0) = H_{m-k}(0) = 0$.

Conclusion, $(H_0, H_1, \cdots, H_n)$ et $(\Delta_0, \Delta_1, \cdots, \Delta_n)$ sont des bases duales. Ceci permet d'écrire par la formule bien connue $x = e_1^*(x)e_1 + \cdots + e_n^*(x)e_n$ des coordonnées d'un vecteur dans une base $(e_1, \cdots, e_n)$ à l'aide de la base duale, que pour tout P de E_n :

$$P = \Delta_0(P)H_0 + \Delta_1(P)H_1 + \cdots + \Delta_n(P)H_n.$$

3 Application à l'arithmétique

Nous allons donner un critère pour qu'un polynôme réel P (ou complexe, ça marche aussi !) définisse une fonction polynomiale de $\mathbb{Z}$ dans $\mathbb{Z}$, c'est-à-dire que $P(a) \in \mathbb{Z}$ pour tout $a \in \mathbb{Z}$.

Théorème. Un polynôme P de E_n vérifie $P(a) \in \mathbb{Z}$ pour tout a dans $\mathbb{Z}$ si et seulement si ses coordonnées dans la base des polynômes de Hilbert sont entières, ou dit autrement, si et seulement si $\Delta_k(P)$ est entier pour tout k de 0 à n.

Preuve. Supposons que $P(a) \in \mathbb{Z}$ pour tout a dans $\mathbb{Z}$. Alors, $D(P)(a) = P(a+1) - P(a)$ est également entier pour tout a dans $\mathbb{Z}$, et par récurrence, $D^k(P)(a)$ est entier pour tout a dans $\mathbb{Z}$ et pour tout k. En particulier $\Delta_k(P) \in \mathbb{Z}$, d'où l'implication.

Réciproquement, si l'on montre que pour tout k et tout entier a, $H_k(a)$ est entier, alors la propriété sera également vraie pour tout polynôme combinaison entière des H_k.

Ceci est vrai pour $H_0 = 1$, puis, par récurrence, pour $k \geq 0$ en utilisant la formule

$$H_{k+1}(a) = H_{k+1}(a) - H_{k+1}(0) = H_k(0) + H_k(1) + \cdots + H_k(a-1).$$

Remarque. On a une méthode alternative pour montrer que $H_n(\mathbb{Z}) \subset \mathbb{Z}$. En fait, si $a \in \mathbb{Z}$, alors, soit 1) $a \geq n$, $H_n(a) = \binom{a}{n}$, soit 2) $0 \leq a \leq n-1$, $H_n(a) = 0$, soit 3) $a \leq -1$, $H_n = (-1)^n \binom{n-1-a}{n}$.