TD 8. Transformée de Fourier discrète

Exercice 1
Soient n un entier naturel et K un corps (commutatif) de caractéristique nulle ou de caractéristique première à n. On considère le polynôme $P_n(X) = X^n - 1 \in K[X]$. On suppose que P_n a toutes ses racines dans K.

1. a) Montrer que le polynôme dérivé P_n' ne s'annule qu'en 0, en déduire que P_n n'a que des racines simples.
   b) Montrer que l'ensemble $\{x_i, 1 \leq i \leq n\}$ des racines de P_n forme un sous-groupe multiplicatif de $K^\times$, que l'on note μ_n.
   c) Soit d un diviseur de n, montrer que $X^n - 1 = (X^d - 1)\Big(1 + X^d + \cdots + (X^d)^{\frac{n}{d}-1}\Big)$.
2. On suppose $n = p^k$ avec p premier et $k \geq 1$.
   a) Vérifier que $X^p - 1 \mid P_{p^k}$. En déduire que μ_{p^k} contient au moins $p-1$ éléments d'ordre p.
   b) Montrer que $(X-1)(1 + X^p + \cdots + (X^p)^{p^{k-1}-1}) \not\equiv 0$ modulo $(X^p - 1)$. En déduire que $1 + X^p + \cdots + (X^p)^{p^{k-1}-1}$ n'a pas de racine d'ordre p, puis que μ_{p^k} contient exactement $p-1$ éléments d'ordre p.
   c) Montrer que μ_{p^k} est cyclique.
3. On suppose que $n = p_1^{k_1} p_2^{k_2} m$ avec p_1 et p_2 premiers distincts et m entier premier à p_1 et p_2.
   a) Montrer que, pour $i = 1, 2$, $P_{p_i^{k_i}}$ divise P_n et que μ_n contient un élément x_i d'ordre $p_i^{k_i}$.
   b) En déduire que μ_n contient un élément d'ordre $p_1^{k_1} p_2^{k_2}$, puis que μ_n est cyclique.
   c) Soit U_d le sous-ensemble des éléments d'ordre d de μ_n, pour d entier divisant n. Vérifier que $\#U_n = \varphi(n)$ et, pour tout diviseur d de n, $\#U_d = \varphi(d)$. Retrouver la formule
   $$n = \sum_{d|n} \varphi(d) \ .$$
4. On pose, pour tout entier n,
   $$\Phi_n(X) = \prod_{x \in U_n} (X - x)$$
   a) Montrer que $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
   b) Calculer Φ_n pour $1 \leq n \leq 8$.
   c) Soit A le sous-anneau de K engendré par 1 (c'est-à-dire $A = \mathbb{Z}$ si $\mathrm{car}(K) = 0$, $A = \mathbb{F}_q$ si $\mathrm{car}(K) = q$). Montrer à l'aide de 4.a) et 4.b) que $\Phi_n(X) \in A[X]$ pour tout entier n.
5. Soit B un anneau contenant A.
   a) On suppose que ω est une racine primitive d'ordre n dans B, montrer que $\Phi_n(\omega) = 0$.
   On peut en déduire que n est inversible dans B (les déterminants des matrices de Hadamard H_ω et $H_{\omega^{-1}}$ sont inversibles et $H_\omega H_{\omega^{-1}} = nI_n$, où I_n est la matrice identité d'ordre n).
   b) On suppose maintenant que n est inversible dans B et que ω est une racine de Φ_n dans B.

(i) Montrer que $\omega^n = 1$.

(ii) On écrit $X^n - 1 = \Phi_n(X)Q(X)$. En dérivant et en évaluant en ω, montrer que $\Phi_d(\omega)$ est inversible pour tout d diviseur strict de n, puis de même pour $1 - \omega^d$.

(iii) Soit i un entier avec $1 \leq i < n$. Montrer que $\omega^i - 1 \mid \omega^d - 1$, où d est le pgcd de i et n. En déduire que ω est une racine primitive d'ordre n.

Exercice 2

On utilise la méthode de Cooley-Tuckey pour $n = 12 = 3 \times 4$ dans l'anneau $\mathbb{C}$.

a) Vérifier que ij est une racine primitive d'ordre 12 dans $\mathbb{C}$ (i et j sont les nombres complexes habituels).

b) Écrire les matrices de Hadamard H_3 et H_4 pour la DFT en dimensions respectives 3 et 4, associées respectivement aux racines primitives $(ij)^4$, d'ordre 3, et $(ij)^3$, d'ordre 3.

c) Soit $a = (a_0, \ldots, a_{11}) \in A^{12}$. Écrire les matrices $A = (a_{4m+n})_{m,n}$, $B = H_3A$, $B^* = (b^*_{m,n})_{m,n}$, où $b^*_{m,n} = b_{n,m}\omega^{nm}$, et $C = H_4B^*$.

d) En déduire les transformées de Fourier des polynômes $X^4 - 1$ et $X^8 + X^4 + 1$, puis leur produit.

Exercice 3

Écrire la méthode de Cooley-Tuckey pour calculer la DFT en dimension $n = 3^3$.