Devoir facultatif n° 5

On appelle $\mathscr{A} = \mathbb{C}^{\mathbb{N}^*}$ l'ensemble des fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$ (ensemble des fonctions *arithmétiques*).

Pour tout entier n non nul, on note $\mathscr{D}^+(n)$ l'ensemble des diviseurs positifs de n :

$$\mathscr{D}^+(n) = \{d \in \mathbb{N}^* \ , \ d \mid n\} .$$

Si $f, g \in \mathscr{A}$, on définit la fonction $f * g : \mathbb{N}^* \to \mathbb{C}$ par :

$$\forall n \in \mathbb{N}^*, \ (f * g)(n) = \sum_{d \in \mathscr{D}^+(n)} f(d) g\left(\frac{n}{d}\right).$$

On pourra remarquer que

$$\forall n \in \mathbb{N}^*, \ (f * g)(n) = \sum_{a,b \in \mathbb{N}^*, \ ab=n} f(a) g(b).$$

Cette opération $*$ est appelée *convolution de Dirichlet* et définit naturellement une loi de composition interne sur $\mathscr{A}$.

On définit deux éléments δ et $\mathbf{1}$ de $\mathscr{A}$ par :

$$\forall n \in \mathbb{N}^*, \ \delta(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$$

et

$$\forall n \in \mathbb{N}^*, \ \mathbf{1}(n) = 1.$$

I - Structure de $(\mathscr{A}, +, *)$.

1) Justifier que $*$ est associative sur $\mathscr{A}$.

2) La loi $*$ est-elle commutative sur $\mathscr{A}$?

3) Montrer que δ est un élément neutre pour $*$ dans $\mathscr{A}$.

4) Soit $f \in \mathscr{A}$ vérifiant $f(1) = 0$. Cet élément f est-il inversible ? Est-ce que $(\mathscr{A}, *)$ possède une structure de groupe ?

5) La réciproque du résultat précédent est-elle vraie ?

6) Montrer que $(\mathscr{A}, +, *)$ a une structure d'anneau.

7) Cet anneau est-il intègre ?

II - Fonction et formule d'inversion de Möbius.

On définit l'élément μ de $\mathscr{A}$ (fonction de Möbius) de la manière suivante : pour tout $n \in \mathbb{N}^*$:

- si n est divisible par le carré d'un nombre premier, $\mu(n) = 0$;
- si n s'écrit comme le produit de k nombres premiers distincts, $\mu(n) = (-1)^k$.

8) Soit I un ensemble fini non vide. Justifier que I possède autant de parties de cardinal pair que de parties de cardinal impair.

Remarque : on se rappellera que si $0 \leqslant k \leqslant n$, tout ensemble fini contenant n éléments possède exactement $\binom{n}{k}$ parties ayant k éléments.

9) En déduire que pour tout $n \in \mathbb{N}^*$ différent de 1 :

$$\sum_{d \in \mathscr{D}^+(n)} \mu(d) = 0.$$

10) Comment peut-on réécrire le résultat précédent, en fonction de $\mathbf{1}$ et au regard des objets introduits dans la première partie ?

11) En déduire la formule d'inversion de Möbius : pour tout $f, g \in \mathscr{A}$,

$$\left(\forall n \in \mathbb{N}^*,\ g(n) = \sum_{d \in \mathscr{D}^+(n)} f(d)\right) \Leftrightarrow \left(\forall n \in \mathbb{N}^*,\ f(n) = \sum_{d \in \mathscr{D}^+(n)} g(d)\mu\left(\frac{n}{d}\right)\right).$$

III - Une application.

Soit $n \in \mathbb{N}^*$. On note $\omega = \mathrm{e}^{\frac{2i\pi}{n}}$ et on rappelle que

$$\mathbb{U}_n = \left\{\omega^k,\ 0 \leqslant k \leqslant n-1\right\}.$$

Si $z \in \mathbb{U}_n$, on appelle *ordre* de z le plus petit entier $d \geqslant 1$ tel que $z^d = 1$.

Si $d \geqslant 1$, on note $\varphi(d)$ le nombre d'entiers de $[\![1, d]\!]$ premiers avec d :

$$\varphi(d) = \operatorname{Card}\left\{k \in [\![1, d]\!],\ k \wedge d = 1\right\}.$$

12) Soit $z \in \mathbb{U}_n$, montrer que l'ordre de z est bien défini, et qu'il divise n.

13) Soit $d \in [\![1, n-1]\!]$ tel que $d|n$. Montrer qu'il y a exactement $\varphi(d)$ éléments d'ordre d dans $\mathbb{U}_n$.
Indication : avec $e \in [\![1, n-1]\!]$ tel que $d.e = n$, considérer ω^e.

14) En déduire que pour tout $n \geqslant 1$, $\varphi(n) = \sum_{\substack{a,b \in \mathbb{N}^* \\ ab=n}} a\mu(b)$.

— FIN —