Devoir à la maison n° 10

À rendre le 07 janvier

I. Convolution de suites

Soit $E = \mathbb{R}^{\mathbb{N}}$ l'ensemble des suites réelles. Pour $u \in E$, et $n \in \mathbb{N}$, on notera $u(n)$ au lieu de u_n le terme d'indice n de la suite u.
Pour $u, v \in E$, on appelle *somme des suites u et v* la suite $u + v \in E$ définie par :

$$\forall n \in \mathbb{N}, \quad (u+v)(n) = u(n) + v(n).$$

On sait que la loi de composition interne $+$ sur E ainsi définie munit E d'une structure de groupe commutatif d'élément nul égal à la suite constante nulle notée 0.
Pour $u, v \in E$, on appelle *convolée de la suite u par la suite v*, la suite $u \star v \in E$ définie par :

$$\forall n \in \mathbb{N}, \quad (u \star v)(n) = \sum_{k=0}^{n} u(k)v(n-k).$$

La loi $\star$, nommé loi de *convolution*, est une loi de composition sur E.

1) **a)** Montrer que $\star$ est commutative et associative.

b) On note ε la suite réelle définie par $\varepsilon(0) = 1$ et $\forall n \in \mathbb{N}^*$, $\varepsilon(n) = 0$.
Établir que ε est l'élément neutre pour $\star$.

c) Montrer que $\star$ est distributive sur $+$.

d) Que dire de la structure $(E, +, \star)$? Dans toute la suite, on considère E muni de cette structure.

2) **a)** Soit $\rho \in \mathbb{R}$ et u la suite réelle définie par $\forall n \in \mathbb{N}$, $u(n) = \rho^n$.
Montrer que l'élément u est inversible et déterminer son inverse.

b) On note $F = \mathbb{R}^{(\mathbb{N})}$ l'ensemble des suites réelles nulles à partir d'un certain rang.
Montrer que F est un sous-groupe de $(E, +)$, stable par $\star$ et qui contient ε (on dit que c'est un *sous-anneau* de $(E, +, \star)$).

c) Soit $f : E \to E$ définie par : si $u \in E$, la suite $f(u) \in E$ est donnée par $\forall n \in \mathbb{N}$, $[f(u)](n) = (-1)^n u(n)$.
Montrer que f est un automorphisme du groupe $(E, +)$, vérifiant les propriétés suivantes :
— $f(\varepsilon) = \varepsilon$;
— $\forall a, b \in E,\ f(a \star b) = f(a) \star f(b)$;
— $f \circ f = \mathrm{Id}_E$.
(On dit que f est un *automorphisme involutif* de l'anneau $(E, +, \star)$.)

3) On se propose maintenant de déterminer les éléments inversibles de l'anneau $(E, +, \star)$.

a) Soit u un élément inversible de l'anneau $(E, +, \star)$. Montrer que $u(0) \neq 0$.

b) Inversement soit $u \in E$, tel que $u(0) \neq 0$. Montrer que u est inversible.

4) On se propose maintenant de justifier l'intégrité de l'anneau $(E, +, \star)$.
Soit $u, v \in E$ tels que $u \neq 0$ et $v \neq 0$.
On pose $p = \min\{n \in \mathbb{N} \mid u(n) \neq 0\}$ et $q = \min\{n \in \mathbb{N} \mid v(n) \neq 0\}$.

a) Justifier l'existence de p et q.

b) Montrer que $(u \star v)(p + q) \neq 0$.

c) Conclure.

II. Anneaux $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}$, $n \geqslant 2$. Pour tout $k \in \mathbb{Z}$, on note $\overline{k}$ le reste de la division euclidienne de k par n.

1) Montrer que $\left\{\overline{k}, k \in \mathbb{Z}\right\} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. Cet ensemble est alors noté $\mathbb{Z}/n\mathbb{Z}$.

2) a) Soient $k, \ell \in \mathbb{Z}$. Montrer que $\overline{k} = \overline{\ell}$ si et seulement si $k \equiv \ell[n]$.

b) Soient $k, k', \ell, \ell' \in \mathbb{Z}$ tels que $\overline{k} = \overline{k'}$ et $\overline{\ell} = \overline{\ell'}$. Montrer que $\overline{k + \ell} = \overline{k' + \ell'}$.
Ceci permet de définir une addition $\oplus$ sur $\mathbb{Z}/n\mathbb{Z}$: soient $a, b \in \mathbb{Z}/n\mathbb{Z}$. Alors il existe $k, \ell \in \mathbb{Z}$ tels que $a = \overline{k}$ et $b = \overline{\ell}$. On pose alors $a \oplus b = \overline{k + \ell}$, c'est-à-dire $\overline{k} \oplus \overline{\ell} = \overline{k + \ell}$, ce qui est défini sans ambiguité grâce à la question 2b). Pour plus de commodités, $\oplus$ sera aussi notée $+$.

c) Soient $k, k', \ell, \ell' \in \mathbb{Z}$ tels que $\overline{k} = \overline{k'}$ et $\overline{\ell} = \overline{\ell'}$. Montrer que $\overline{k \times \ell} = \overline{k' \times \ell'}$.
Ceci permet de définir une multiplication $\otimes$ sur $\mathbb{Z}/n\mathbb{Z}$: soient $a, b \in \mathbb{Z}/n\mathbb{Z}$. Alors il existe $k, \ell \in \mathbb{Z}$ tels que $a = \overline{k}$ et $b = \overline{\ell}$. On pose alors $a \otimes b = \overline{k \times \ell}$, c'est-à-dire $\overline{k} \otimes \overline{\ell} = \overline{k \times \ell}$, ce qui est défini sans ambiguité grâce à la question 2c). Pour plus de commodités, $\otimes$ sera aussi notée $\times$.

3) Pour vérifier que vous avez bien compris :

a) Donner les éléments de $\mathbb{Z}/6\mathbb{Z}$.

b) Dans $(\mathbb{Z}/6\mathbb{Z}, +, \times)$, calculer $\overline{2} + \overline{3}$, $\overline{3} + \overline{5}$, $\overline{1} + \overline{5}$, $\overline{3} \times \overline{5}$ et $\overline{2} \times \overline{3}$.

4) a) Montrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien (on vérifiera que la loi $+$ est associative et commutative, qu'il existe un neutre que l'on précisera, et on précisera également l'inverse de tout élément).

b) Montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau (on vérifiera que la loi $\times$ est associative, qu'elle est distributive par rapport à $+$, et qu'il existe un neutre que l'on précisera).

5) a) Soit $k \in [\![2, n-1]\!]$ tel que $k|n$. Montrer alors qu'il existe $a \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \neq 0$ et $\overline{k} \times a = \overline{0}$.

b) Soit $k \in [\![2, n-1]\!]$ tel que k et n ne soient pas premiers entre eux. Montrer alors qu'il existe $a \in \mathbb{Z}/n\mathbb{Z}$ tel que $a \neq 0$ et $\overline{k} \times a = \overline{0}$.

c) Soit $k \in [\![1, n-1]\!]$ tel que $k \wedge n = 1$. En utilisant le théorème de Bézout, montrer qu'il existe $m \in \mathbb{Z}$ tel que $\overline{k \times m} = \overline{1}$. En déduire que $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ pour la loi $\times$.

6) Montrer que $(\mathbb{Z}/n\mathbb{Z}, +\times)$ est un corps si et seulement si n est premier.

7) Pour vérifier que vous avez bien compris : dans $\mathbb{Z}/150\mathbb{Z}$, dire si 81 et 143 sont inversibles. Pour chacun d'eux, donner son inverse s'il existe, sinon donner un élément non nul a de $\mathbb{Z}/150\mathbb{Z}$ tel que $a \times b = \overline{0}$ (avec $b = \overline{81}$ ou $\overline{143}$).

— FIN —