Simulation DS N°5

Fonctions Réelles Structures & Arithmétique

Problème 1 Formule de Taylor-Lagrange

Soit $a < b$ deux réels. Le but de cet exercice est de généraliser le théorème des accroissements finis en démontrant la formule de Taylor-Lagrange qui s'énonce comme suit.

Soit $n \in \mathbb{N}$, f de classe $\mathcal{C}^n$ sur $[a,b]$ et dérivable $n+1$ fois sur $]a,b[$. Il existe $c \in]a,b[$ tel que :

$$f(b) = \left(\sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a)\right) + \frac{(b-a)^{n+1}}{(n+1)!} f^{(n+1)}(c)$$

1. Justifier que si $n = 0$, on retrouve l'égalité des accroissements finis.
2. On pose, $\forall t \in [a,b]$, $\varphi(t) = f(b) - \left(\sum_{k=0}^{n} \frac{(b-t)^k}{k!} f^{(k)}(t)\right) - A\frac{(b-t)^{n+1}}{(n+1)!}$ où $A \in \mathbb{R}$ sera à déterminer.
   (a) Vérifier que $\varphi(b) = 0$.
   (b) Montrer que l'on peut choisir A de manière à avoir $\varphi(a) = \varphi(b)$, on ne cherchera pas à simplifier A.
   (c) Montrer que φ est continue sur $[a,b]$ et dérivable sur $]a,b[$ et que pour tout $t \in]a,b[$:
   $$\varphi'(t) = -\frac{(b-t)^n}{n!} f^{(n+1)}(t) + A\frac{(b-t)^n}{n!}$$
   (d) En appliquant le théorème de Rolle à la fonction φ, démontrer la formule de Taylor-Lagrange.

   Voyons à présent deux applications de ce résultat.
3. La série harmonique alternée est la suite définie par : $\forall n \in \mathbb{N}^*,\ T_n = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k}$.

   Le but de cette question est de déterminer $\lim_{n\to+\infty} T_n$.
   (a) On considère la fonction f définie sur $]-1,+\infty[$ par $f : x \mapsto \ln(1+x)$. Pour tout entier naturel non nul n, expliciter $f^{(n)}$.
   (b) Démontrer que : $\forall n \in \mathbb{N},\ \forall x \in [0,1],\ \exists c > 0,\ \ln(1+x) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} x^k + \frac{x^{n+1}}{(n+1)!} f^{(n+1)}(c)$.
   (c) Détailler la formule précédente à l'aide des expressions des dérivées successives de f trouvées dans la question (a).
   (d) En déduire que : $\forall n \in \mathbb{N}^*,\ \forall x \in [0,1],\ \left|\ln(1+x) - \sum_{k=1}^{n} \frac{(-1)^{k-1} x^k}{k}\right| \leq \frac{x^{n+1}}{n+1}$.
   (e) Déterminer $\lim_{n\to+\infty} T_n$.

   La question 4. est facultative.
4. On souhaite démontrer que e n'est pas algébrique de degré 2, c'est-à-dire qu'il est impossible de trouver trois entiers a, b et c non tous nuls tels que $ae^2 + be + c = 0$. On procède par l'absurde en supposant vraie une telle relation et on considère la fonction définie sur $\mathbb{R}$ par $f : x \mapsto ae^x + ce^{-x}$.
   (a) Démontrer que $f(1) \in \mathbb{Z}$.
   (b) Démontrer que :
   $$\forall n \in \mathbb{N},\ \exists c_{n+1} \in]0,1[,\ f(1) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} + \frac{f^{(n+1)}(c_{n+1})}{(n+1)!}$$
   (c) Démontrer que $\frac{f^{(n+1)}(c_{n+1})}{n+1}$ est un entier et que $\lim_{n\to+\infty} \frac{f^{(n+1)}(c_{n+1})}{n+1} = 0$.
   (d) En déduire l'absurdité recherchée et conclure.

Problème 2

Soient (u_n) et (v_n) deux suites de $\mathbb{R}^{\mathbb{N}}$, on appelle convolé de la suite (u_n) par la suite (v_n) la suite notée $(u \star v)$ définie par : $\forall n \in \mathbb{N}$, $(u \star v)_n = \sum\limits_{k=0}^{n} u_k v_{n-k}$. $\star$ est appelé produit de convolution sur les suites réelles et c'est une loi de composition interne par définition.

1. Calculer la convolé de $(n)_n$ avec $(1)_n$.
2. Montrer que $\star$ est commutatif (on pensera à faire un changement d'indice dans la somme).
3. Soit $(u, v, w) \in (\mathbb{R}^{\mathbb{N}})^3$. Montrer que, pour tout $n \in \mathbb{N}$, $\sum\limits_{k=0}^{n} \sum\limits_{i=0}^{k} u_i v_{k-i} w_{n-k} = \sum\limits_{\substack{1 \leq i,j,\ell \leq n \\ i+j+\ell=n}} u_i v_j w_\ell$.

   En déduire que $(u \star v) \star w = u \star (v \star w)$. Qu'a-t-on démontrer ?
4. On note ε la suite définie par $\varepsilon_0 = 1$ et $\forall n \geq 1$, $\varepsilon_n = 0$. Montrer que, pour tout $u \in \mathbb{R}^{\mathbb{N}}$, $u \star \varepsilon = u$.
5. Montrer que $\star$ est distributif par rapport à $+$ (l'addition classique des suites).
6. Que peut-on en déduire sur $(\mathbb{R}^{\mathbb{N}}, +, \star)$.
7. Soit $q \in \mathbb{R}$, on considère u la suite géométrique de raison q. Montrer que u possède un symétrique pour la loi $\star$ que l'on déterminera. (On raisonnera par analyse synthèse).
8. Montrer qu'une suite u est symétrisable pour $\star$ si et seulement si $u_0 \neq 0$.
   En déduire que $(\mathbb{R}^{\mathbb{N}}, +, \star)$ n'est pas un corps.
9. On se propose maintenant de démontrer l'intégrité. Soit $(u, v) \in (\mathbb{R}^{\mathbb{N}})^2$ avec $u \neq 0$, $v \neq 0$.
   (a) Montrer que $p = \min\{n \in \mathbb{N} | u_n \neq 0\}$ et $q = \min\{n \in \mathbb{N} | v_n \neq 0\}$ sont bien définis.
   (b) Montrer que $(u \star v)_{p+q} \neq 0$.
   (c) Conclure sur l'intégrité.

Problème 3 Équation de Fermat, cas $n = 2$

On dit que $(x, y, z) \in (\mathbb{N}^*)^3$ est un triplet pythagoricien si et seulement si $x^2 + y^2 = z^2$. L'objectif de cet exercice est de déterminer tous les triplets pythagoriciens. On note dans tout cet exercice $x \wedge y = \text{pgcd}(x, y)$. Les diviseurs considérés dans ce problème sont des entiers naturels. Enfin, on dira que $a \in \mathbb{N}$ est un carré si et seulement si il existe $b \in \mathbb{N}$ tel que $a = b^2$.

1. Soit $d \in \mathbb{N}^*$ un diviseur commun à x, y et z, en factorisant par d montrer qu'il suffit de déterminer les triplets pythagoriciens qui n'ont pas d'autres diviseurs communs que 1.

   On dit alors que x, y et z sont premiers entre eux et on parle dans ce cas de triplet pythagoricien primitif. Dans toute la suite, on s'intéresse à un triplet pythagoricien primitif (x, y, z).

2. Montrer que $x \wedge y = x \wedge z = y \wedge z = 1$. En déduire que x et y ne sont pas tous les deux pairs.
3. A l'aide de congruences modulo 4, montrer que x et y ne sont pas tous les deux impairs.

   Les entiers naturels x et y sont de parités distinctes, sans perte de généralité on suppose dans toute la suite que x est pair et y impair.

4. Justifier qu'il existe $(u, v, w) \in (\mathbb{N}^*)^3$ tels que $x = 2u$, $z + y = 2v$ et $z - y = 2w$.
5. Montrer que $v \wedge w = 1$.
6. Montrer que vw est un carré, en déduire que v et w sont des carrés. On pose $v = n^2$ et $w = m^2$ où $(n, m) \in \mathbb{N}^2$.
7. Montrer que $n > m$ et que $n \wedge m = 1$. Exprimer u en fonction de n et m.
8. En déduire que (x, y, z) est un triplet pythagoricien primitif si et seulement si il existe deux entiers n et m premiers entre eux et de parités distinctes avec $n > m > 0$ tels que $x = 2nm$, $y = n^2 - m^2$ et $z = n^2 + m^2$ ou $x = n^2 - m^2$, $y = 2nm$ et $z = n^2 + m^2$.

Problème 1 Corrigé

1. Si $n=0$, l'énoncé de la formule de Taylor-Lagrange devient : soit f continue sur $[a,b]$ et dérivable sur $]a,b[$, il existe $c\in]a,b[$ tel que :
$$f(b)=f(a)+(b-a)f'(c)$$
Ceci puisque la somme de la formule est réduite à un terme $\dfrac{(b-a)^0}{0!}f^{(0)}(a)$ qui est bien égal à $f(a)$. On retrouve exactement l'énoncé du théorème des accroissements finis.

2. (a) On a $\varphi(b)=f(b)-\left(\displaystyle\sum_{k=0}^{n}\frac{(b-b)^k}{k!}f^{(k)}(b)\right)-A\frac{(b-b)^{n+1}}{(n+1)!}=f(b)-f(b)=0.$
$$\boxed{\varphi(b)=0}$$
(b) On veut avoir $\varphi(a)=0$, c'est-à-dire : $f(b)-\left(\displaystyle\sum_{k=0}^{n}\frac{(b-a)^k}{k!}f^{(k)}(a)\right)-A\frac{(b-a)^{n+1}}{(n+1)!}=0$, pour cela il suffit de prendre :
$$A=\frac{(n+1)!}{(b-a)^{n+1}}\left(f(b)-\sum_{k=0}^{n}\frac{(b-a)^k}{k!}f^{(k)}(a)\right)$$
$$\boxed{\exists A\in\mathbb{R},\ \varphi(a)=\varphi(b)}$$
(c) La fonction φ est une somme de produits de fonctions polynomiales par les dérivées de la fonction f jusqu'à l'ordre n, toutes ces fonctions sont continues sur $[a,b]$ et dérivables sur $]a,b[$ puisque f est de classe $\mathcal{C}^n$ sur $[a,b]$ et dérivable $n+1$ fois sur $]a,b[$. La fonction φ est donc continue sur $[a,b]$ et dérivable sur $]a,b[$. Avec les règles usuelles de dérivation des sommes et des produits, on a pour tout $t\in]a,b[$:
$$\begin{aligned}\varphi'(t)&=\underbrace{-f'(t)}_{\text{correspondant à }k=0}-\left(\sum_{k=1}^{n}\left(\frac{-k(b-t)^{k-1}}{k!}f^k(t)+\frac{(b-t)^k}{k!}f^{(k+1)}(t)\right)\right)-A\frac{-(n+1)(b-t)^n}{(n+1)!}\\&=-f'(t)+\left(\sum_{k=1}^{n}\left(\frac{(b-t)^{k-1}}{(k-1)!}f^k(t)-\frac{(b-t)^k}{k!}f^{(k+1)}(t)\right)\right)+A\frac{(b-t)^n}{n!}\\&=-f'(t)+f'(t)-\frac{(b-t)^n}{n!}f^{(n+1)}(t)+A\frac{(b-t)^n}{n!}\\&=-\frac{(b-t)^n}{n!}f^{(n+1)}(t)+A\frac{(b-t)^n}{n!}\end{aligned}$$
On a pu simplifier ce calcul en reconnaissant une somme télescopique. On a trouvé l'expression de $\varphi'(t)$ annoncée :
$$\boxed{\forall t\in]a,b[,\ \varphi'(t)=-\frac{(b-t)^n}{n!}f^{(n+1)}(t)+A\frac{(b-t)^n}{n!}}$$
(d) La fonction φ vérifie les hypothèses du théorème de Rolle puisque :
► φ est continue sur $[a,b]$, nous l'avons justifié à la question précédente.
► φ est dérivable sur $]a,b[$.
► $\varphi(a)=\varphi(b)$.
Il existe alors $c\in]a,b[$ tel que $\varphi'(c)=0$. Or :
$$\varphi'(c)=0\Leftrightarrow-\frac{(b-c)^n}{n!}f^{(n+1)}(c)+A\frac{(b-c)^n}{n!}=0\Leftrightarrow A=f^{(n+1)}(c)$$

La formule de Taylor-Lagrange découle alors de l'égalité $\varphi(a) = 0$ puisque :

$$\varphi(a) = 0 \Leftrightarrow f(b) = \Big(\sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a)\Big) + f^{(n+1)}(c)\frac{(b-a)^{n+1}}{(n+1)!}$$

On a bien démontré que :

$$\boxed{\exists c \in]a, b[,\ f(b) = \Big(\sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a)\Big) + f^{(n+1)}(c)\frac{(b-a)^{n+1}}{(n+1)!}}$$

3. (a) Notons $I =]-1, +\infty[$. La fonction f est de classe $\mathcal{C}^\infty$ sur I par composition car :

$$\forall x \in I,\ 1 + x \in \mathbb{R}_+^* \text{ et } \ln \text{ est de classe } \mathcal{C}^\infty \text{ sur } \mathbb{R}_+^*$$

En calculant les premières dérivées de f, on peut conjecturer la formule suivante valable pour $n \in \mathbb{N}^*$:

$$\mathcal{H}_n\ :\ \forall x \in I,\ f^{(n)}(x) = \frac{(-1)^{n-1}(n-1)!}{(1+x)^n}$$

▶ **Initialisation.** Pour tout $x \in I$: $f'(x) = \dfrac{1}{1+x}$, ce qui correspond bien à la formule annoncée pour $n = 1$.

▶ **Hérédité.** On fixe $n \in \mathbb{N}^*$ et l'on suppose que :

$$\forall x \in I,\ f^{(n)}(x) = \frac{(-1)^{n-1}(n-1)!}{(1+x)^n}$$

On dérive la relation précédente :

$$\forall x \in I,\ f^{(n+1)}(x) = -n\frac{(-1)^{n-1}(n-1)!}{(1+x)^{n+1}} = \frac{(-1)^n n!}{(1+x)^{n+1}}$$

Ce qui démontre que $\mathcal{H}_{n+1}$ est vraie et achève la récurrence.

$$\boxed{\forall n \in \mathbb{N}^*,\ \forall x \in I,\ f^{(n)}(x) = \frac{(-1)^{n-1}(n-1)!}{(1+x)^n}}$$

(b) Dans toute la suite n désigne un entier naturel. Soit $x \in]0, 1]$, on va appliquer la formule de Taylor-Lagrange sur l'intervalle $[0, x]$ à la fonction f. Les hypothèses sont vérifiées puisque f est de classe $\mathcal{C}^\infty$ sur I donc en particulier de classe $\mathcal{C}^\infty$ sur $[0, x]$. Ainsi :

$$\exists c \in]0, x[,\ \ln(1+x) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!}x^k + \frac{x^{n+1}}{(n+1)!}f^{(n+1)}(c)$$

On remarque que cette relation est également vraie pour $x = 0$, finalement :

$$\boxed{\forall x \in [0, 1],\ \exists c > 0,\ \ln(1+x) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!}x^k + \frac{x^{n+1}}{(n+1)!}f^{(n+1)}(c)}$$

(c) On reprend la formule précédente en isolant le terme $k=0$ dans la somme, il vient :

$$\forall x \in [0,1],\ \exists c>0,\ \ln(1+x)=\ln(1)+\sum_{k=1}^{n}\frac{(-1)^{k-1}(k-1)!x^k}{k!}+\frac{x^{n+1}(-1)^n n!}{(1+c)^{n+1}(n+1)!}$$

En simplifiant cela donne :

$$\boxed{\forall x \in [0,1],\ \exists c>0,\ \ln(1+x)=\sum_{k=1}^{n}\frac{(-1)^{k-1}x^k}{k}+\frac{x^{n+1}(-1)^n}{(1+c)^{n+1}(n+1)}}$$

(d) Comme $c>0$, on a $(1+c)>1$ donc $(1+c)^{n+1}>1$, ainsi en reprenant l'expression précédente, on a pour tout $x\in[0,1]$:

$$\left|\ln(1+x)-\sum_{k=1}^{n}\frac{(-1)^{k-1}x^k}{k}\right|=\left|\frac{x^{n+1}(-1)^n}{(1+c)^{n+1}(n+1)}\right|\leq\frac{x^{n+1}}{(n+1)}$$

Ce qui démontre bien le résultat voulu :

$$\boxed{\forall n\in\mathbb{N}^*,\ \forall x\in[0,1],\ \left|\ln(1+x)-\sum_{k=1}^{n}\frac{(-1)^{k-1}x^k}{k}\right|\leq\frac{x^{n+1}}{n+1}}$$

(e) Prenons $x=1$ dans l'inégalité précédente :

$$\forall n\in\mathbb{N}^*,\ \left|\ln(2)-\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k}\right|\leq\frac{1}{n+1}$$

Ce qui démontre que :

$$\boxed{\lim_{n\to+\infty}T_n=\ln(2)}$$

4. (a) On part de la relation que l'on a supposée vérifiée :

$$ae^2+be+c=0\Leftrightarrow ae+b+ce^{-1}=0\Leftrightarrow ae+ce^{-1}=-b\Leftrightarrow f(1)=-b$$

Par hypothèse b est un entier, ainsi :

$$\boxed{f(1)\in\mathbb{Z}}$$

(b) Il s'agit d'appliquer la formule de Taylor-Lagrange à la fonction f sur l'intervalle $[0,1]$. Les hypothèses sont vérifiées puisque la fonction f est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$. Comme le réel c fourni par la formule dépend de n, nous le notons ici c_{n+1} :

$$\boxed{\forall n\in\mathbb{N},\ \exists c_{n+1}\in]0,1[,\ f(1)=\sum_{k=0}^{n}\frac{f^{(k)}(0)}{k!}+\frac{f^{(n+1)}(c_{n+1})}{(n+1)!}}$$

(c) D'après la relation précédente, on a :

$$f(1)-\sum_{k=0}^{n}\frac{f^{(k)}(0)}{k!}=\frac{f^{(n+1)}(c_{n+1})}{(n+1)!}$$

On multiplie par $n!$, il vient :

$$f(1)n! - \sum_{k=0}^{n} \frac{f^{(k)}(0)n!}{k!} = \frac{f^{(n+1)}(c_{n+1})}{n+1}$$

Montrons que les différents termes du membre de gauche sont des entiers relatifs :

▶ La fonction f est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$ et pour tout réel x et tout entier naturel k, on $f^{(k)}(x) = ae^x + (-1)^k ce^{-x}$, en particulier $f^{(k)}(0) = a + (-1)^k c \in \mathbb{Z}$ car a et c sont des entiers.

▶ Pour tout $k \in [\![0, n]\!]$, $\dfrac{n!}{k!} \in \mathbb{N}$.

$$\boxed{\frac{f^{(n+1)}(c_{n+1})}{n+1} \text{ est un entier relatif}}$$

D'autre part, on a :

$$\left|\frac{f^{(n+1)}(c_{n+1})}{n+1}\right| = \left|\frac{ae^{c_{n+1}} + (-1)^{n+1}ce^{-c_{n+1}}}{n+1}\right| \leq \frac{|a|e + |c|}{n+1} \underset{n\to+\infty}{\longrightarrow} 0$$

Ceci en utilisant l'inégalité triangulaire et le fait que $e^{c_{n+1}} \leq e$ et $e^{-c_{n+1}} \leq 1$ car $c_{n+1} \in]0, 1[$.

$$\boxed{\lim_{n\to+\infty} \frac{f^{(n+1)}(c_{n+1})}{n+1} = 0}$$

(d) La question précédente nous apprend que $\left(\dfrac{f^{(n+1)}(c_n)}{n+1}\right)$ est une suite d'entiers relatifs qui converge vers 0, d'après un exercice classique que nous avons fait dans le chapitre sur les suites cela implique que la suite est stationnaire, c'est-à-dire que :

$$\exists N \in \mathbb{N},\ \forall n \geq N,\ f^{(n+1)}(c_{n+1}) = ae^{c_{n+1}} + (-1)^{n+1}ce^{-c_{n+1}} = 0$$

Comme une exponentielle est strictement positive ceci implique que : $\forall n \geq N$, a et $(-1)^{n+1}c$ sont de signes opposés. Ceci n'est possible que si $a = c = 0$ et puisque $ae^2 + be + c = 0$, on en déduit que $b = 0$. C'est absurde car on a supposé que a, b et c ne sont pas tous les trois nuls.

$$\boxed{\text{Il est impossible que } ae^2 + be + c = 0 \text{ avec } (a, b, c) \in \mathbb{N}^3 \setminus \{(0, 0, 0)\}}$$

Le nombre e est transcendant, c'est-à-dire qu'il n'est racine d'aucun polynôme non nul à coefficients entiers, mais c'est plus difficile à démontrer.

Problème 2

1. Soit $n\in\mathbb{N}$, $((n)_n\star(1)_n)_n=\sum\limits_{k=0}^{n}k\times 1=\frac{n(n+1)}{2}$ donc $((n)_n\star(1)_n)=(\frac{n(n+1)}{2})_n$.

2. Soit $(u,v)\in(\mathbb{R}^{\mathbb{N}})^2$, $\forall n\in\mathbb{N}$, $(u\star v)_n=\sum\limits_{k=0}^{n}u_kv_{n-k}=\sum\limits_{i=0}^{n}u_{n-i}v_i$ en posant $i=n-k$.
Donc $(u\star v)_n=(v\star u)_n$ et $\star$ est commutatif.

3. Soit $(u,v,w)\in(\mathbb{R}^{\mathbb{N}})^3$. Soit $n\in\mathbb{N}$, $\sum\limits_{k=0}^{n}\sum\limits_{i=0}^{k}u_iv_{k-i}w_{n-k}=\sum\limits_{i=0}^{n}\sum\limits_{k=i}^{n}u_iv_{k-i}w_{n-k}$. De l'autre côté,
$\sum\limits_{\substack{1\leq i,j,\ell\leq n\\ i+j+\ell=n}}u_iv_jw_\ell=\sum\limits_{i=0}^{n}\sum\limits_{j=0}^{n-i}u_iv_jw_{n-i-j}=\sum\limits_{i=0}^{n}\sum\limits_{k=i}^{n}u_iv_{k-i}w_{n-k}$ en posant $k=i+j$ (donc $j=k-i$) d'où le résultat. On a alors $((u\star v)\star w)_n=\sum\limits_{k=0}^{n}(u\star v)_kw_{n-k}=\sum\limits_{k=0}^{n}\sum\limits_{i=0}^{k}u_iv_{k-i}w_{n-k}=\sum\limits_{\substack{1\leq i,j,\ell\leq n\\ i+j+\ell=n}}u_iv_jw_\ell$ et
$(u\star(v\star w))_n=\sum\limits_{i=0}^{n}u_i(v\star w)_{n-i}=\sum\limits_{i=0}^{n}\sum\limits_{j=0}^{n-i}u_iv_jw_{n-i-j}=\sum\limits_{\substack{1\leq i,j,\ell\leq n\\ i+j+\ell=n}}u_iv_jw_\ell$. Donc $(u\star v)\star w=u\star(v\star w)$ et on a montré que $\star$ est associatif.

4. Soit $u\in\mathbb{R}^{\mathbb{N}}$. Pour tout $n\in\mathbb{N}$, $(u\star\varepsilon)_n=\sum\limits_{k=0}^{n}u_k\varepsilon_{n-k}$ mais le seul terme non nul de ε est pour $\varepsilon_0=1$ donc finalement $\sum\limits_{k=0}^{n}u_k\varepsilon_{n-k}=u_n$ et $u\star\varepsilon=u$. (Donc par associativité et commutativité, ε est le neutre pour $\star$.)

5. Par commutativité, il suffit de faire la distributivité à droite. Soit $(u,v,w)\in(\mathbb{R}^{\mathbb{N}})^3$. Soit $n\in\mathbb{N}$, $(u\star(v+w))_n=\sum\limits_{k=0}^{n}u_k(v+w)_{n-k}=\sum\limits_{k=0}^{n}u_kv_{n-k}+\sum\limits_{k=0}^{n}u_kw_{n-k}=(u\star v)_n+(u\star w)_n$ d'où le résultat.

6. On sait déja que $(\mathbb{R}^{\mathbb{N}},+)$ est un groupe abélien et comme $\star$ est une loi de composition interne, associative, commutative, muni d'un neutre et distributive par rapport à $+$, $(\mathbb{R}^{\mathbb{N}},+,\star)$ est un anneau commutatif.

7. <u>Analyse</u> : Si la suite est symétrisable, il existe (v_n) telle que, pour tout $n\in\mathbb{N}$, $\varepsilon_n=\sum\limits_{k=0}^{n}q^kv_{n-k}$.
Pour $n=0$, on obtient $v_0=1$. Pour $n=1$, on obtient $qv_0+v_1=0$ donc $v_1=-q$. Pour $n=2$, on obtient $q^2v_0+qv_1+v_2=0$ donc $v_2=0$ et alors $\forall n\geq 2$, $v_n=0$. Donc $(v_n)=(1,-q,0,\dots)$.
<u>Synthèse</u> : Ça marche.

8. <u>$\Rightarrow$</u> : Soit u symétrisable et v son symétrique, pour $n=0$, on a $u_0v_0=1$ donc $u_0\neq 0$.
<u>$\Leftarrow$</u> Soit u telle que $u_0\neq 0$, on cherche v telle que $u\star v=\varepsilon$. Pour $n=0$, on obtient $v_0=\frac{1}{u_0}$ puis pour les n suivants $\sum\limits_{k=0}^{n}u_kv_{n-k}=0$ donc $u_0v_n=-\sum\limits_{k=1}^{n}u_kv_{n-k}$ donc $v_n=-\frac{1}{u_0}\sum\limits_{k=1}^{n}u_kv_{n-k}$ et on construit alors bien le symétrique par récurrence.
D'après le résultat que l'on vient de montrer, la suite $(0,1,0,\dots)$ est non nulle et non symétrisable donc $(\mathbb{R}^{\mathbb{N}},+,\star)$ n'est pas un corps.

9. (a) L'ensemble $\{n\in\mathbb{N}|u_n\neq 0\}$ est non vide, minoré par 0 et inclus dans $\mathbb{N}$ donc il possède un minimum. On fait de même pour le deuxième.
   (b) $(u\star v)_{p+q}=\sum\limits_{k=0}^{p+q}u_kv_{p+q-k}$. Remarquons alors que pour tout $k<p$, $u_k=0$ par définition de p et pour tout $k>p$, $p+q-k<q$ donc $v_{p+q-k}=0$ par définition de q donc le seul terme restant de la somme est pour $k=p$ donc $(u\star v)_{p+q}=u_pv_q\neq 0$.
   (c) On a montrer que $u\neq 0$, $v\neq 0\Rightarrow(u\star v)\neq 0$ donc par contraposée, $\star$ est intègre.

Problème 3

Équation de Fermat, cas $n = 2$

1. Soit $d \in \mathbb{N}^*$ un diviseur commun de x, y et z, il existe $(X, Y, Z) \in (\mathbb{N}^*)^3$ tels que $x = dX$, $y = dY$ et $z = dZ$. On a :
$$x^2 + y^2 = z^2 \Leftrightarrow (dX)^2 + (dY)^2 = (dZ)^2 \Leftrightarrow X^2 + Y^2 = Z^2$$
Il suffit de chercher les solutions sans diviseur commun, on obtiendra toutes les solutions en multipliant par un entier quelconque les trois coordonnées du triplet.
2. Soit $d \in \mathbb{N}^*$ un **nombre premier** tel que $d|x$ et $d|y$ alors $d|x^2 + y^2 = z^2$. Comme d divise z^2 alors d apparait dans la décomposition en facteurs premiers de z^2 donc il apparait dans la décomposition en facteurs premiers de z. En effet, les facteurs premiers de z et z^2 sont les mêmes, seules les valuations changent, ceci étant dû à l'unicité de la décomposition en facteurs premiers. Finalement d divise z. D'après l'hypothèse, un diviseur positif de x, y et z est égal à 1. On vient de démontrer que x et y n'ont pas de facteur premier en commun, d'après le cours cela implique qu'ils sont premiers entre eux.
On démontre de la même façon que $x \wedge z = y \wedge z = 1$.
$$\boxed{x \wedge y = x \wedge z = y \wedge z = 1}$$
Il est alors clair que x et y ne sont pas tous les deux pairs sinon ils auraient 2 comme facteur commun, ce qui est contradictoire avec le résultat précédent.
3. Par l'absurde, si x et y sont impairs alors il existe $(k, l) \in \mathbb{N}^2$ tels que $x = 2k + 1$ et $y = 2l + 1$. On a $x^2 = 4k^2 + 4k + 1$ et $y^2 = 4l^2 + 4l + 1$, ainsi $x^2 \equiv 1[4]$ et $y^2 \equiv 1[4]$ donc $z^2 \equiv 2[4]$. C'est absurde car on vérifie immédiatement avec une table de congruence qu'un carré est congru à 0 ou 1 modulo 4.
$$\boxed{x \text{ et } y \text{ sont de parités distinctes}}$$
4. L'entier naturel x est pair et y est impair donc x^2 est pair et y^2 est impair, ce qui implique que z^2 est impair et par suite z est impair. On en déduit que $z + y$ et $z - y$ sont impairs. D'autre part, étant donné que x, y et z sont non nuls, on a : $x \geq 1$, $z + y \geq 1$ et $z - y \geq 1$ car $z^2 = y^2 + x^2 \geq y^2 + 1$. Finalement :
$$\boxed{\exists (u, v, w) \in (\mathbb{N}^*)^3,\ x = 2u,\ z + y = 2v \text{ et } z - y = 2w}$$
5. Soit $d \in \mathbb{N}^*$ tel que $d|v$ et $d|w$ alors $d|v + w = z$ et $d|v - w = y$. Or $y \wedge z = 1$ donc $d = 1$.
$$\boxed{v \wedge w = 1}$$
6. On a $4vw = (z + y)(z - y) = z^2 - y^2 = x^2 = 4u^2$.
$$\boxed{vw = u^2}$$
On reprend l'égalité précédente en utilisant la décomposition en facteurs premiers :
$$vw = \Big(\prod_{p \in \mathcal{P}} p^{\nu_p(u)}\Big)^2$$
Soit $p \in \mathcal{P}$ un nombre premier qui apparait dans la décomposition précédente alors $p|vw$. Comme v et w sont premiers entre eux alors p divise v et p ne divise pas w ou p ne divise pas v et p divise w. Dans la décomposition précédente en regroupant les facteurs premiers selon qu'ils divisent v ou w, on obtient :
$$v = \Big(\prod_{p \in \mathcal{P},\ p|v} p^{\nu_p(u)}\Big)^2 \text{ et } w = \Big(\prod_{p \in \mathcal{P},\ p|w} p^{\nu_p(u)}\Big)^2$$
$$\boxed{\exists (n, m) \in \mathbb{N}^2,\ v = n^2 \text{ et } w = m^2}$$

7. On a $2v - 2w = 2y > 0$ donc $v > w$ d'où $n^2 > m^2$ et par suite :

$$\boxed{n > m}$$

Si $d \in \mathbb{N}^*$ avec $d|n$ et $d|m$ alors $d|n^2 = v$ et $d|m^2 = w$, or $v \wedge w = 1$ d'où $d = 1$.

$$\boxed{n \wedge m = 1}$$

On a vu que $vw = u^2$ donc $n^2m^2 = u^2$ donc $u = nm$ puisque l'on travaille avec des entiers naturels.

$$\boxed{u = nm}$$

8. On vient de démontrer que les conditions données dans cette question sont des conditions nécessaires, l'autre triplet étant obtenu en supposant x impair et y pair. En effet, $x = 2u = 2nm$, $y = v - w = n^2 - m^2$ et $z = w + v = n^2 + m^2$ et m et n sont bien de parités distinctes car y est impair.
Réciproquement, on a bien :

$$x^2 + y^2 = (2nm)^2 + (n^2 - m^2)^2 = 4n^2m^2 + n^4 - 2n^2m^2 + m^4 = (n^2 + m^2)^2 = z^2$$

et (x, y, z) est un triplet Pythagoricien car si d est un nombre premier tel que $d|x$, $d|y$ et $d|z$ alors $d|2n^2 = y + z$ et $d|2m^2 = z - y$. Or d n'est pas pair car y (ou x) est impair puisque n et m sont de parités distinctes. Ainsi $d|m^2$ et $d|n^2$ donc $d|m$ et $d|n$, comme m et n sont premiers entre eux cela implique que $d = 1$. On a bien un triplet Pythagoricien primitif.