Devoir maison n° 18

Pour lundi 29 avril

Ce DM est constitué de trois exercices obligatoires (sur les thèmes : polynômes + un peu d'algèbre linéaire et de dénombrement), ainsi que de deux problèmes facultatifs (un premier d'analyse, un second d'arithmétique et d'algèbre).

Ces problèmes sont relativement longs, avec des questions parfois difficiles. On peut en traiter zéro, un ou deux, complètement ou partiellement.

Exercice 1 – Polynômes de Fibonacci

On rappelle que la suite de Fibonacci $(f_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ vérifie : $f_0 = 0$, $f_1 = 1$ et $f_{n+2} = f_{n+1} + f_n$ pour tout entier naturel n.

On définit une suite $(F_n)_{n\in\mathbb{N}} \in \mathbb{R}[X]^{\mathbb{N}}$ de polynômes (dits *polynômes de Fibonacci*) de la façon suivante :

$$\begin{cases} F_0 = 0 \text{ et } F_1 = 1, \\ \forall n \in \mathbb{N},\ F_{n+2} = XF_{n+1} + F_n \end{cases}$$

1. Calculer les polynômes F_2, F_3, F_4 et F_5.

2. Pour tout entier $n \in \mathbb{N}^*$, déterminer :

- ***a)*** le degré de F_n.
- ***b)*** le coefficient dominant de F_n.
- ***c)*** la parité de F_n.
- ***d)*** les valeurs de $F_n(0)$ et $F_n(1)$.

3. Montrer que $\forall n \in \mathbb{N}^*$, $\forall x \in \mathbb{R}_+^*$, $F_n(x) > 0$ et en déduire l'ensemble des racines réelles de F_n.

4. Soit $\alpha \in \mathbb{C}$ et $n \in \mathbb{N}^*$.
Montrer que si α est racine commune de F_n et F_{n+1}, alors α est aussi racine de F_{n-1}.
En déduire que F_{n+1} et F_n n'ont aucune racine commune.

5. Montrer l'égalité, valable pour tout $n \in \mathbb{N}^*$ et tout $z \in \mathbb{C}^*$: $\quad F_n(2i\,\mathrm{ch}(z)) = i^{n-1}\dfrac{\mathrm{sh}(nz)}{\mathrm{sh}(z)}$.

6. Pour quels nombres complexes z a-t-on $\mathrm{sh}(nz) = 0$?
En déduire que les $2i\cos\dfrac{k\pi}{n}$ sont racines de F_n, pour tout $k \in [\![1; n-1]\!]$.
Donner la multiplicité de ces racines.

7. ***a)*** Écrire la décomposition dans $\mathbb{C}[X]$ de F_n en facteurs irréductibles.
On pourra distinguer selon la parité de n.

b) En déduire la décomposition dans $\mathbb{R}[X]$ de F_n en facteurs irréductibles.
À nouveau, on pourra distinguer selon la parité de n.

8. Finalement, en déduire que les nombres de Fibonacci f_n vérifient l'identité suivante :

$$\forall n \in \mathbb{N}^*, \quad f_n = \prod_{\substack{1 \leqslant k \leqslant \frac{n-1}{2} \\ k \text{ entier}}} \left(1 + 4\cos^2 \frac{k\pi}{n}\right) = \prod_{\substack{1 \leqslant k \leqslant \frac{n-1}{2} \\ k \text{ entier}}} \left(3 + 2\cos \frac{2k\pi}{n}\right)$$

Exercice 2 – Formule d'inversion de Pascal

On s'intéresse dans cet exercice à la propriété encadrée ci-dessous, dite *formule d'inversion de Pascal*. Dans la première question, on démontre cette propriété en utilisant des méthodes d'algèbre linéaire. Dans les questions suivantes, on l'applique à un problème de dénombrement.

Soient $(a_0, a_1, \ldots, a_n)$ et $(b_0, b_1, \ldots, b_n)$ deux $(n+1)$-uplets de réels.
On suppose que les b_p s'expriment en fonction des a_p par les relations suivantes :

$$\forall p \in [\![0; n]\!],\ b_p = \sum_{k=0}^{p} \binom{p}{k} a_k$$

Alors on peut exprimer les a_p en fonction des b_p par les relations :

$$\forall p \in [\![0; n]\!],\ a_p = \sum_{k=0}^{p} (-1)^{p-k} \binom{p}{k} b_k$$

1. On fixe un entier $n \in \mathbb{N}$ et on se place dans l'espace vectoriel $\mathbb{R}_n[X]$.
On note $\mathcal{B} = (1, X, X^2, \ldots, X^n) = (X^k)_{0 \leqslant k \leqslant n}$ la base canonique de $\mathbb{R}_n[X]$.
On définit aussi la famille $\mathcal{F} = (1, X+1, (X+1)^2, \ldots, (X+1)^n) = ((X+1)^k)_{0 \leqslant k \leqslant n}$.

a) Justifier que $\mathcal{F}$ est une base de $\mathbb{R}_n[X]$.

b) On appelle P la matrice de passage de la base $\mathcal{B}$ à la base $\mathcal{F}$.
Expliciter le format et les coefficients de la matrice P.

c) On appelle Q la matrice de passage de la base $\mathcal{F}$ à la base $\mathcal{B}$.
En remarquant que $X^k = (X + 1 - 1)^k$, expliciter de même la matrice Q.
Quelle relation vérifient les matrices P et Q ?

d) On se donne deux matrices-lignes dans $\mathcal{M}_{1,n+1}(\mathbb{R})$:

$$A = \begin{pmatrix} a_0 & a_1 & \ldots & a_n \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} b_0 & b_1 & \ldots & b_n \end{pmatrix}$$

On suppose que $B = AP$. Comment s'expriment alors les b_p en fonction des a_p ?

e) En déduire la formule d'inversion de Pascal.

2. Si E est un ensemble fini, on appelle *dérangement* de E une permutation $\sigma : E \to E$ sans point fixe (ou encore : une permutation σ de E dont le support $\{k \in E \mid \sigma(k) \neq k\}$ est égal à E tout entier). On appelle d_n le nombre de dérangements d'un ensemble à n éléments.

a) Déterminer à la main les valeurs de d_0, d_1, d_2, d_3 et d_4.

b) Soit $p \in \mathbb{N}$. Combien y a-t-il de permutations de $[\![1; p]\!]$?

En distinguant selon le cardinal de leur support, montrer qu'on a $p! = \displaystyle\sum_{k=0}^{p} \binom{n}{k} d_k$.

c) En déduire : $d_n = n! \displaystyle\sum_{k=0}^{n} \frac{(-1)^k}{k!}$ pour tout entier naturel n.

3. En écrivant une formule de Taylor bien choisie et en majorant le reste intégral, démontrer qu'on a pour tout réel x :

$$e^x = \lim_{n \to +\infty} \sum_{k=0}^{n} \frac{x^k}{k!}$$

4. En déduire que la proportion de dérangements parmi les permutations de $[\![1; n]\!]$ tend vers $\dfrac{1}{e}$ lorsque n tend vers $+\infty$.

Exercice 3 – Polynômes de Legendre

Pour tout $n \in \mathbb{N}$, on définit les polynômes à coefficients réels suivants :

$$P_n = (X+1)^n (X-1)^n \quad \text{et} \quad L_n = P_n^{(n)}$$

Les polynômes L_n sont appelés *polynômes de Legendre*.

1. Calculer L_0, L_1, L_2 et L_3.

2. Montrer que L_n est de degré n pour tout entier n et préciser son coefficient dominant.

3. Comparer les polynômes $L_n(X)$ et $L_n(-X)$. Que dire de la parité de L_n ?

4. ***a)*** Soient $n \in \mathbb{N}$ et $k \in [\![0; n-1]\!]$. Déterminer les valeurs $P_n^{(k)}(-1)$ et $P_n^{(k)}(1)$.

b) Montrer que pour tout entier n, le polynôme L_n est scindé à racines simples et que toutes ses racines appartiennent à l'intervalle $]-1; 1[$.

5. Pour $n \in \mathbb{N}$, appliquer la formule de Leibniz à l'expression $\Big((X+1)^n (X-1)^n\Big)^{(n)}$ et en déduire les valeurs $L_n(1)$ et $L_n(-1)$.

6. ***a)*** Vérifier les deux égalités :

$$(A) \quad \forall n \in \mathbb{N}, \quad P'_{n+1} = 2(n+1) X P_n$$

$$(B) \quad \forall n \in \mathbb{N}^*, \quad P''_{n+1} = 2(n+1)(2n+1) P_n + 4n(n+1) P_{n-1}$$

b) Soit un entier $n \geqslant 1$. En dérivant n fois la relation (A) et $n-1$ fois la relation (B), trouver une relation simple liant L_{n+1}, L_n et L_{n-1}.

Problème A – Fonctions à variation bornée

On se donne un segment $[a;b]$ de $\mathbb{R}$, avec $a<b$. On rappelle qu'une subdivision de $[a;b]$ est un $(n+1)$-uplet $\sigma=(x_0,x_1,\ldots,x_n)$ (où $n\geqslant 1$) qui vérifie :

$$a=x_0<x_1<\cdots<x_n=b$$

On note $\mathcal{S}([a;b])$ l'ensemble de toutes les subdivisions du segment $[a;b]$.

Soit $f:[a;b]\to\mathbb{R}$ une fonction définie sur $[a;b]$.

Pour toute subdivision $\sigma=(x_0,x_1,\ldots,x_n)$ de $[a;b]$, on définit : $V(f,\sigma)=\sum_{k=0}^{n-1}\left|f(x_{k+1})-f(x_k)\right|$

Le réel positif $V(f,\sigma)$ est appelé la *variation de f le long de σ*.

Si $V(f,\sigma)$ est majoré lorsque σ parcourt $\mathcal{S}([a;b])$, on dit que f est *à variation bornée* et pose :

$$V_a^b(f)=\sup_{\sigma\in\mathcal{S}([a;b])}V(f,\sigma)$$

Le réel $V_a^b(f)$ est appelé *variation de f sur* $[a;b]$.

Enfin, on note $\mathcal{VB}([a;b])$ l'ensemble des fonctions à variation bornée sur $[a;b]$.

Une partie de la difficulté de l'exercice (en particulier dans les dernières questions) réside dans la rédaction rigoureuse des propriétés liées aux bornes sup.

1. *Des exemples.*

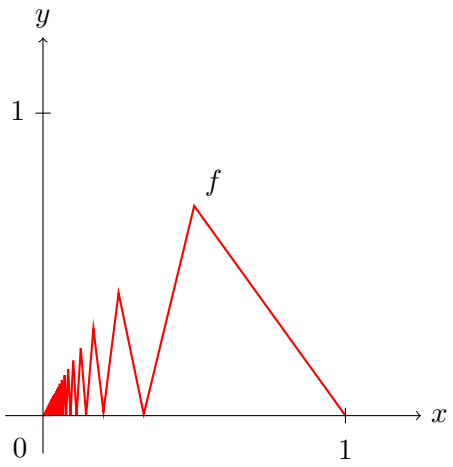
a) Soit f une fonction croissante sur $[a;b]$.
Exprimer $V(f,\sigma)$ pour tout $\sigma\in\mathcal{S}([a;b])$.
En déduire que f est à variation bornée sur $[a;b]$ et expliciter $V_a^b(f)$.

b) Énoncer un résultat analogue pour f décroissante.

c) Soit f une fonction k-lipschitzienne sur $[a;b]$. Pour $\sigma\in\mathcal{S}([a;b])$ quelconque, majorer $V(f,\sigma)$.
En déduire que f est à variation bornée et majorer $V_a^b(f)$ en fonction de a, b et k.

d) Soit $f:[0;1]\to\mathbb{R}$ telle que :

$$\begin{cases} f(0)=0 \\ \text{Pour tout } p\in\mathbb{N}^*,\ f\left(\dfrac{1}{p}\right)=\begin{cases}0 & \text{si } p \text{ est impair}\\ \ln\left(1+\dfrac{2}{p}\right) & \text{si } p \text{ est pair}\end{cases} \\ f \text{ est affine sur chaque intervalle } \left[\dfrac{1}{p+1};\dfrac{1}{p}\right]\ (p\in\mathbb{N}^*)\end{cases}$$



Justifier que f est correctement définie et montrer qu'elle est continue sur $[0;1]$, mais qu'elle n'est pas à variation bornée.

On pourra s'intéresser à une subdivision $\sigma_n = \left(0, \frac{1}{2n}, \frac{1}{2n-1}, \ldots, \frac{1}{3}, \frac{1}{2}, 1\right)$.

On voit en particulier qu'il n'y a pas de rapport simple entre la continuité et le fait d'être à variation bornée.

2. *Des propriétés élémentaires.*

a) Montrer qu'une fonction à variation bornée est bornée.

b) Montrer qu'une fonction f est constante sur $[a;b]$ si et seulement si elle est à variation bornée et sa variation est nulle.

c) Soient σ, $\tau \in \mathcal{S}([a;b])$ deux subdivisions. Montrer que si τ est plus fine que σ, alors on a l'inégalité $V(f,\sigma) \leqslant V(f,\tau)$.

3. *Fonctions $\mathcal{C}^1$.*

On suppose dans cette question seulement que f est $\mathcal{C}^1$ sur $[a;b]$.

a) Montrer que f est à variation bornée avec $V_a^b(f) \leqslant \displaystyle\int_a^b |f'(t)|\,\mathrm{d}t$.

b) Montrer qu'on a en fait égalité : $V_a^b(f) = \displaystyle\int_a^b |f'(t)|\,\mathrm{d}t$.

4. *Structure vectorielle.*

On suppose dans cette question que f et g sont à variation bornée sur $[a;b]$.

a) Soit $\lambda \in \mathbb{R}$. Montrer que λf est à variation bornée et $V_a^b(\lambda f) = |\lambda| V_a^b(f)$.

b) Montrer que $f+g$ est à variation bornée avec $V_a^b(f+g) \leqslant V_a^b(f) + V_a^b(g)$.

c) En déduire que $\mathcal{V}B([a;b])$ est un sous-espace vectoriel de $\mathbb{R}^{[a;b]}$.

5. *Relation de Chasles.*

Soit $f \in \mathcal{V}B([a;b])$ une fonction à variation bornée sur $[a;b]$. Soit c un réel tel que $a < c < b$. Montrer que f (ou plus rigoureusement : ses restrictions) est à variation bornée sur $[a;c]$ et $[c;b]$ et qu'on a : $V_a^b(f) = V_a^c(f) + V_c^b(f)$.

6. *Caractérisation de $\mathcal{V}B([a;b])$.*

Soit f à variation bornée sur $[a;b]$. On définit $g : [a;b] \to \mathbb{R}$ par $g(x) = V_a^x(f)$.

a) Montrer que g est une fonction croissante sur $[a;b]$.

b) Montrer que la fonction $h = f - g$ est décroissante sur $[a;b]$.

c) Montrer qu'une fonction de $[a;b]$ dans $\mathbb{R}$ est à variation bornée si et seulement si elle est somme d'une fonction croissante et d'une fonction décroissante.

d) En déduire finalement que $\mathcal{V}B([a;b])$ est le sous-espace vectoriel de $\mathbb{R}^{[a;b]}$ engendré par l'ensemble des fonctions croissantes.

Problème B – Entiers de Gauss

On définit l'ensemble $\mathbb{Z}[i] = \{x + iy \mid (x,y) \in \mathbb{Z}^2\}$ des nombres complexes dont les parties réelles et imaginaires sont des entiers. Les éléments de $\mathbb{Z}[i]$ sont appelés les *entiers de Gauss*.

1. Montrer que $\mathbb{Z}[i]$ est stable pour l'addition, la multiplication et la conjugaison et que $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif.

2. *Unités.*

On dit que $m \in \mathbb{Z}[i]$ est une *unité* de $\mathbb{Z}[i]$ si m est inversible dans $\mathbb{Z}[i]$, c'est à dire s'il existe un élément $m' \in \mathbb{Z}[i]$ tel que $mm' = 1$. On note U l'ensemble des unités de $\mathbb{Z}[i]$.

a) Montrer que $m \in \mathbb{Z}[i]$ est une unité si et seulement si $|m| = 1$.

b) En déduire que $U = \{1, i, -1, -i\}$.

c) Pour a et $b \in \mathbb{Z}[i]$, on dit que a divise b (et on note $a \mid b$) s'il existe $m \in \mathbb{Z}[i]$ tel que $b = ma$.
On dit que a et b sont *associés* si $a \mid b$ et $b \mid a$.
Montrer que a et b sont associés si et seulement si $\exists u \in U$, $b = ua$.

3. *Nombres premiers de Gauss.*

On dit que $m \in \mathbb{Z}[i]$ est un élément *irréductible* de $\mathbb{Z}[i]$, ou encore un *nombre premier de Gauss*, si m n'est pas une unité et n'est pas le produit de deux entiers de Gauss qui ne sont pas des unités. En d'autres termes, si :

$$m \notin U \quad \text{et} \quad \forall a, b \in \mathbb{Z}[i],\ m = ab \Rightarrow (a \in U \text{ ou } b \in U)$$

a) Montrer que $1 + i$, 3 et $1 - 2i$ sont des nombres premiers de Gauss.

b) Montrer que 2, $4i$ et 17 ne sont pas des nombres premiers de Gauss.

4. *Division euclidienne.*

a) Soit $z \in \mathbb{C}$ un nombre complexe quelconque. Montrer qu'il existe $q \in \mathbb{Z}[i]$ tel que $|z - q| < 1$.

b) Soient a, $b \in \mathbb{Z}[i]$ deux entiers de Gauss, avec b non nul. Déduire de la question précédente la propriété de division euclidienne dans $\mathbb{Z}[i]$:

$$\text{Il existe } (q,r) \in \mathbb{Z}[i] \text{ tel que } \begin{cases} a = bq + r \\ |r| < |b| \end{cases}$$

On attire cependant l'attention sur le fait qu'il n'y a pas toujours unicité du couple (q,r).

c) Effectuer la division euclidienne de $2018 + 2019i$ par $3 + 14i$.

5. *Structure des idéaux.*

On appelle *idéal* de $\mathbb{Z}[i]$ toute partie non vide $I \subset \mathbb{Z}[i]$ stable pour l'addition et absorbante pour la multiplication.

Montrer que tout idéal I de $\mathbb{Z}[i]$ peut s'écrire $I = m\mathbb{Z}[i]$, où m est un entier de Gauss.

▷ *À partir de là, il est possible d'utiliser des notions et des propriétés adaptées de l'arithmétique de $\mathbb{Z}$ et de $\mathbb{K}[X]$: existence d'un PGCD et d'un PPCM de deux éléments, théorème de Bézout, lemme de Gauss, existence et unicité de la factorisation en nombres premiers de Gauss, etc... Les constructions et les preuves sont analogues à celles de $\mathbb{Z}$ et $\mathbb{K}[X]$.*

6. *Détermination des nombres premiers de Gauss*

a) Soit $m \in \mathbb{Z}[i]$ un nombre premier de Gauss. Montrer qu'il existe un nombre premier (usuel) $p \in \mathbb{Z}$ tel que m divise p (au sens de $\mathbb{Z}[i]$).

b) Soit $p \in \mathbb{Z}$ un nombre premier qui est une somme de deux carrés ($p = a^2 + b^2$ avec a, $b \in \mathbb{N}$.) Montrer que p n'est pas un nombre premier de Gauss, et que les nombres premiers de Gauss qui divisent p sont associés à $a \pm ib$.

c) Soit $p \in \mathbb{Z}$ un nombre premier qui n'est pas une somme de deux carrés. Montrer que p est un nombre premier de Gauss.

On a ainsi déterminé tous les nombres premiers de Gauss : à une unité près, ce sont :
— les nombres premiers usuels qui ne sont pas somme de deux carrés,
— les $a \pm ib$ pour tous les a et b tels que $a^2 + b^2$ est un nombre premier usuel.

d) Donner la liste de tous les nombres premiers de Gauss de module inférieur à 10.

7. *Détermination des nombres premiers sommes de deux carrés.*

On va montrer qu'un nombre premier (usuel) $p \in \mathbb{N}$ est somme de deux carrés si et seulement si on a $p = 2$ ou $p \equiv 1$ [4].

a) Montrer que 2 est une somme de deux carrés.
Montrer que si $p \equiv 3$ [4] alors p n'est pas somme de deux carrés.

b) Soit E un ensemble fini et $\sigma : E \to E$ une involution de E (c'est-à-dire une permutation telle que $\sigma \circ \sigma = \mathrm{Id}_E$).
Que peut-on dire du cardinal des orbites de σ ? Montrer que E est de cardinal impair si et seulement si σ a un nombre impair de points fixes.

c) On se donne un nombre premier $p \in \mathbb{N}$ tel que $p \equiv 1$ [4] (on notera $p = 4k + 1$ avec $k \in \mathbb{N}$).
On définit l'ensemble $E = \{\ (x,y,z) \in \mathbb{N}^3 \ \mid \ x^2 + 4yz = p\ \}$.
On définit aussi l'application $\sigma : E \to E$ telle que, pour tout $(x,y,z) \in E$:

$$\sigma(x,y,z) = \begin{cases} (\ x + 2z,\ z,\ y - x - z\ ) & \text{si } x < y - z \\ (\ 2y - x,\ y,\ x - y + z\ ) & \text{si } y - z < x < 2y \\ (\ x - 2y,\ x - y + z,\ y\ ) & \text{si } 2y < x \end{cases}$$

Montrer que E est un ensemble fini, que σ est bien définie et réalise une involution de E.

d) Montrer que σ a un unique point fixe dans E.

e) On définit maintenant $\tau : E \to E$ par $\tau(x,y,z) = (x,z,y)$. Montrer que τ est correctement définie et qu'elle est aussi une involution de E.

f) En déduire que τ a au moins un point fixe dans E et que p est somme de deux carrés.

8. *Application à la résolution de quelques équations diophantiennes.*

a) On veut résoudre l'équation en nombres entiers $x^2 - 2xy + 5y^2 = 22$, d'inconnue $(x,y) \in \mathbb{Z}^2$. Pour ce faire, on va travailler dans $\mathbb{Z}[i]$.
▷ Montrer que 11 est un nombre premier de Gauss.
▷ Écrire $x^2 - 2xy + 5y^2$ comme somme de deux carrés, factoriser cette expression dans $\mathbb{Z}[i]$.
▷ Montrer que l'équation initiale n'a pas de solution.

b) Résoudre de même $x^2 - 2xy + 5y^2 = 65$.