DEVOIR SURVEILLÉ n° 2 (4H)

Vendredi 23 septembre 2016

I — L'usage des calculatrices est interdit

Vous attacherez la plus grande importance à la clarté, la précision et la concision de votre rédaction, même si tout résultat qui n'est pas explicitement dans le cours de MPSI ou de MP doit être démontré. Si vous repérez ce qui lui semble être une erreur d'énoncé, signalez le sur votre copie et poursuivez votre composition en expliquant les raisons des initiatives que vous avez été amené à prendre.

Exercice 1

1. Résoudre dans $\mathbb{Z}/19\mathbb{Z}$ l'équation $\dot{x}^3 = 1$.

2. Résoudre dans $\mathbb{Z}/15\mathbb{Z}$ l'équation $\dot{x}^4 = 1$.

3. Déterminer une fonction Python `racineCubique(a,n)` dont les arguments sont deux entiers naturels `a` et `n`, qui renvoie tous les entiers $k \in [0, n-1]$ tels que $(k \bmod n)^3 =$ `a`.

4. Démontrer le théorème d'Euler :
Soit $n \geq 2$. Pour tout $x \in \mathbb{Z}$, si x et n sont premiers entre eux, alors $x^{\varphi(n)} \equiv (1 \bmod n)$.

5. Rappeler la définition d'un générateur d'un groupe multiplicatif $(G, \cdot)$.
Quel est le nombre de générateurs du groupe $(\mathbb{U}_{2016}, \times)$? (on détaillera les calculs)

Problème 1

Partie 1 : noyaux itérés et images itérées : résultats généraux

Soit E un espace vectoriel de dimension finie et $f \in \mathcal{L}(E)$.
On pose $N_k = \mathrm{Ker}(f^k)$ et $I_k = \mathrm{Im}(f^k)$.
On dit qu'une suite (A_n) d'ensembles est croissante (resp. décroissante) pour l'inclusion si et seulement si $\forall n \in \mathbb{N}, A_n \subset A_{n+1}$ (resp. $A_{n+1} \subset A_n$).

1. Rappeler l'énoncé du théorème du rang pour une application linéaire en dimension finie.

2. **a.** Démontrer que la suite $(N_k)_{k\in\mathbb{N}}$ est croissante pour l'inclusion puis que la suite $(I_k)_{k\in\mathbb{N}}$ est décroissante pour l'inclusion.

b. Justifier l'existence d'un plus petit entier naturel p_0 tel que $N_{p_0} = N_{p_0+1}$.

c. Ce résultat est-il encore vrai en dimension infinie ? (on pourra répondre après avoir regardé la partie 3...)

d. Soit un tel p_0. Montrer que $\forall k \geq 0, N_{p_0} = N_{p_0+k}$.

3. **a.** Démontrer que les suites $(N_k)_{k\in\mathbb{N}}$ et $(I_k)_{k\in\mathbb{N}}$ sont stationnaires à partir du même rang p_0.

b. Démontrer que $N_{p_0} \oplus I_{p_0} = E$.

4. Montrer que la restriction de f à I_{p_0} est un automorphisme de I_{p_0}.

5. Montrer que la restriction de f à N_{p_0} est un endomorphisme nilpotent de N_{p_0} et déterminer son ordre.

6. Démontrer que la suite $(\dim(N_{k+1}) - \dim(N_k))_{k\in\mathbb{N}}$ est décroissante.

7. Montrer que si g est un endomorphisme nilpotent de E, son ordre de nilpotence est inférieur ou égal à $\dim(E)$.

Partie 3 : un autre exemple

Soit $E = \mathbb{R}[X]$ et $P \in E$. On définit $\Delta(P) = P(X+1) - P(X)$.

1. Montrer que Δ est un endomorphisme de E.

2. Déterminer rigoureusement le noyau de Δ, puis pour tout $k \geq 2$, le noyau de Δ^k.
L'endomorphisme Δ est-il nilpotent ?

3. Soit $n \in \mathbb{N}^*$. Montrer que $\Delta(\mathbb{R}_n[X]) \subset \mathbb{R}_{n-1}[X]$.
On note δ l'endomorphisme de $\mathbb{R}_n[X]$ tel que $\delta(P) = P(X+1) - P(X)$ (δ est la restriction de Δ à $\mathbb{R}_n[X]$).

- **a.** Déterminer l'image de δ^k pour tout $k \in \mathbb{N}^*$. En déduire l'image de Δ.
- **b.** Justifier que δ est un endomorphisme nilpotent et déterminer son ordre de nilpotence.

4. **a.** Montrer que pour tout entier naturel p, $\delta^p(P) = \displaystyle\sum_{k=0}^{p} (-1)^{p-k} \binom{p}{k} P(X+k)$.

- **b.** En déduire l'existence de réels $(\lambda_1, \dots, \lambda_{n+1}) \in \mathbb{R}^{n+1}$ tels que pour tout $P \in \mathbb{R}_n[X]$,
$P(X) = \displaystyle\sum_{k=1}^{n+1} \lambda_k P(X+k)$.

Problème 2 : Résultant de deux polynômes

Définition et propriétés

Soient p et q deux naturels non nuls et soient

$$P = \sum_{k=0}^{p} a_k X^k \quad \text{et} \quad Q = \sum_{k=0}^{q} b_k X^k$$

deux polynômes de $\mathbb{C}[X]$ avec $a_0, ..., a_p \in \mathbb{C}$, $a_p \neq 0$, $b_0, ..., b_q \in \mathbb{C}$, $b_q \neq 0$.

On définit un nombre complexe appelé le résultant des polynômes P et Q et noté $Res(P,Q)$ comme étant égal à la valeur du déterminant à $p+q$ colonnes suivant :

$$Res(P,Q) = \begin{vmatrix}
a_0 & 0 & \dots & \dots & 0 & b_0 & 0 & \dots & 0 \\
a_1 & a_0 & \ddots & & \vdots & b_1 & b_0 & \ddots & \vdots \\
a_2 & a_1 & a_0 & \ddots & \vdots & b_2 & b_1 & \ddots & 0 \\
\vdots & & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & b_0 \\
a_p & & & \ddots & a_0 & \vdots & & \ddots & b_1 \\
0 & a_p & & & a_1 & b_q & & & b_2 \\
\vdots & \ddots & a_p & \vdots & a_2 & 0 & b_q & \vdots & \vdots \\
\vdots & & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\
0 & \dots & \dots & 0 & a_p & 0 & \dots & 0 & b_q
\end{vmatrix}$$

Les q premières colonnes contiennent les coefficients de P à chaque fois décalés d'un rang vers le bas, et les p suivantes ceux de Q, les autres positions étant remplies avec des zéros.

Par exemple si $P = 1 + 2X + 3X^2$ et $Q = 4 + 5X + 6X^2 + 7X^3$

$$Res(P, Q) = \begin{vmatrix} 1 & 0 & 0 & 4 & 0 \\ 2 & 1 & 0 & 5 & 4 \\ 3 & 2 & 1 & 6 & 5 \\ 0 & 3 & 2 & 7 & 6 \\ 0 & 0 & 3 & 0 & 7 \end{vmatrix}$$

La matrice servant à définir $Res(P, Q)$ pourra être notée $M_{P,Q}$:

$$Res(P, Q) = \det M_{P,Q}$$

On note $E = \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X]$ et $F = \mathbb{C}_{p+q-1}[X]$.
Pour $(A, B) \in E^2$ on pose

$$u(A, B) = PA + QB$$

1. **Cas où u est bijective**
   - **a.** Démontrer que pour $(A, B) \in E^2$ on a $u(A, B) \in F$.
     On définit ainsi une application
     $$u : \begin{cases} E & \rightarrow & F \\ (A, B) & \mapsto & PA + QB \end{cases}$$
   - **b.** Démontrer que u est une application linéaire.
   - **c.** Si on suppose que u est bijective, démontrer que P et Q sont premiers entre eux.
   - **d.** Si on suppose que P et Q sont premiers entre eux, déterminer $Ker(u)$ et en déduire que u est bijective

Matrice de u

On note
$$B = \big((1, 0), (X, 0), ..., (X^{q-1}, 0), (0, 1), (0, X), ..., (0, X^{p-1})\big)$$

2. Montrer que B est une base de E.

3. On note B' la base canonique de F. Rappeler l'expression de B' et la dimension de F.
4. - **a.** Donner l'expression de $u(X^i, 0)$ pour $i \in [0, q - 1]$ puis de $u(0, X^j)$ pour $j \in [0, p - 1]$.
   - **b.** En déduire la matrice de u exprimée dans les bases B et B' de E et F.
   - **c.** Démonter que $Res(P, Q) \neq 0$ si et seulement si P et Q sont premiers entre eux.
   - **d.** En déduire que $Res(P, Q) = 0$ si et seulement si P et Q ont au moins une racine commune complexe.

Application 1 : existence d'une racine multiple

5. - **a.** Démontrer qu'un polynôme P de $\mathbb{C}[X]$ admet une racine multiple dans $\mathbb{C}$ si et seulement si on a $Res(P, P') = 0$
   - **b.** *Application :* déterminer une condition nécessaire et suffisante sur des complexes a et b pour que le polynôme $X^3 + aX + b$ admette une racine multiple.

Application 2 : une courbe paramétrée

Soit $t \in \mathbb{R}$. On envisage l'ensemble Γ des points $M(t)$ de coordonnées $(x(t), y(t))$ avec $x(t) = t^2 + t$ et $y(t) = t^2 - t + 1$.
On pose pour $(x, y, t) \in \mathbb{R}^3$

$$A_x(t) = t^2 + t - x \text{ et } B_y(t) = t^2 - t + 1 - y.$$

6. Établir que si un point M de coordonnées (x, y) appartient à Γ, alors les fonctions polynomiales A_x et B_y ont une racine commune.
7. En déduire qu'un point M de coordonnées (x, y) appartenant à la courbe Γ vérifie

$$x^2 + y^2 - 2xy - 4y + 3 = 0.$$

Application 3 : nombre algébrique

8. En utilisant les polynômes $P = X^2 - 3$ et $Q_y = (y - X)^2 - 7$ pour $y = \sqrt{3} + \sqrt{7}$, déterminer un polynôme R de degré 4 à coefficients entiers tel que y soit une racine de R (on dit que y est un nombre algébrique).
9. Quelles sont les autres racines du polynôme R ?