Arithmétique des polynômes

Aspects linéaires

Autocorrection A. ☑

Soit $f : \mathbb{C}_3[X] \to \mathbb{C}_3[X]$ l'application associant à un polynôme P le reste dans la division euclidienne de $(X^4 - 1)P$ par $X^4 + X^2$.

1. Montrer f est un endomorphisme bien défini et donner sa matrice dans la base canonique.
2. Déterminer $\mathrm{rg}(f)$, $\ker(f)$ et $\mathrm{im}(f)$.

Exercice 1.

Si $P \in K[X]$, on note $M_P = \{R \in K[X] \mid P \text{ divise } R\}$.

Montrer que M_P est un sous-espace vectoriel de K[X] et en donner un supplémentaire.

Exercice 2^{++}. *Mines (PSI)*

Soit $P \in \mathbb{R}[X]$ un polynôme de degré n et $a_0, a_1, \dots, a_n \in \mathbb{R}$ des scalaires distincts.

Montrer que $(P(X + a_i))_{i=0}^{n}$ est une base de $\mathbb{R}_n[X]$.

Exercice 3^{++}. *ÉNS Ulm*

Soit $P \in \mathbb{R}[X]$ un polynôme de degré $n > 0$ et $0 \leqslant k \leqslant n$.

Montrer que la famille$(1, X, \dots, X^{n-k-1}, P(X), P(X+1), \dots, P(X+k))$ est libre.

Multiplicité, polynômes scindés

Autocorrection B. ☑

Soit $n \geqslant 3$ et $P = X^{2n+1} - (2n+1)X^{n+1} + (2n+1)X^n - 1 \in \mathbb{R}[X]$. Calculer l'ordre de multiplicité $\mu_1(P)$.

Exercice 4. ☑

Montrer que $\displaystyle\sum_{k=0}^{n} \frac{X^k}{k!}$ n'a que des racines simples sur $\mathbb{C}$.

Exercice 5^{+}. *Mines* ☑

Soit $P(X) = nX^n - X^{n-1} - \cdots - X - 1$.

Montrer qu'à part 1, les racines de P sont de module < 1 puis que P est à racines simples.

Exercice 6.

Soit $n \in \mathbb{N}^*$ et $P \in \mathbb{R}[X]$ de degré n simplement scindé.

Montrer que les racines complexes du polynôme $P^2 + 1$ dans $\mathbb{C}$ sont toutes simples.

Exercice 7$^+$.

Soit $P \in \mathbb{R}[X]$ simplement scindé. Montrer que P n'a pas deux coefficients consécutifs nuls.

Exercice 8$^+$.

Soit $P \in \mathbb{R}[X]$ non constant, simplement scindé.

Montrer que pour tout $a \in \mathbb{C}$, les racines complexes de $P - a$ sont de multiplicité au plus 2.

Exercice 9$^+$. *Ulm*

Soit $P \in \mathbb{R}[X]$ scindé. Montrer que toute racine multiple de P' est racine de P.

Exercice 10$^+$.

Soit $P \in \mathbb{R}[X]$ simplement scindé, et $a \in \mathbb{R}$. Montrer que $P' + aP$ est simplement scindé.

Exercice 11$^+$.

Soit $d \in \mathbb{N}$.

1. Soit $P \in \mathbb{R}[X]$, unitaire de degré d.
   Montrer que P est scindé si et seulement si $\forall z \in \mathbb{C}, |P(z)| \geqslant |\mathrm{Im}(z)|^d$.
2. Soit $(P_n)_{n\in\mathbb{N}}$ une suite de polynômes unitaires de degré d scindés et $P \in \mathbb{R}[X]$.
   On suppose que $\forall k \in \mathbb{N}, \mathrm{coeff}_k(P_n) \xrightarrow[n\to+\infty]{} \mathrm{coeff}_k(P)$.
   Montrer que P est unitaire, de degré d, et scindé.

Exercice 12^{++}. *X*

Soit $U, V \in \mathbb{R}[X]$ non constants tels que les racines de $U + iV \in \mathbb{C}[X]$ soient de partie imaginaire > 0. Montrer que U et V sont scindés.

Relations coefficients-racines

Exercice 13.

Soit $n \in \mathbb{N}^*$.

Utiliser les relations de Viète pour recalculer $\displaystyle\sum_{\omega\in\mathbb{U}_n} \omega$, puis pour calculer $\displaystyle\prod_{\omega\in\mathbb{U}_n} \omega$ et $\displaystyle\sum_{\omega\in\mathbb{U}_n} \omega^2$.

Exercice 14.

Soit $P \in \mathbb{C}[X]$ de degré $\geqslant 2$. Montrer que la moyenne des racines de P' (comptées avec multiplicité) est la même que celle des racines de P.

Exercice 15.

Soit $P \in K[X]$ de degré 3, possédant au moins deux racines dans K. Montrer que P est scindé.

Exercice 16$^+$ (Sommes de Newton).

1. Exprimer $x^2+y^2+z^2$ et $x^3+y^3+z^3$ en fonction de $\sigma_1 = x+y+z$, $\sigma_2 = xy+xz+yz$ et $\sigma_3 = xyz$.
2. Résoudre le systèmes suivants, d'inconnues $x, y, z \in \mathbb{C}$ (ou $\mathbb{C}^*$) :

$$\begin{cases} x+y+z = 1 \\ \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z} = 1 \\ xyz = -4. \end{cases} \qquad \begin{cases} x+y+z=2 \\ x^2+y^2+z^2 = 14 \\ x^3+y^3+z^3 = 20. \end{cases}$$

Exercice 17$^+$.

On note cot : $x \mapsto \dfrac{\cos x}{\sin x}$ la fonction cotangente.

1. Montrer l'existence d'un polynôme $P_n \in \mathbb{R}_n[X]$ tel que $\forall t \in \left]0, \dfrac{\pi}{2}\right[, P_n(\cot^2 x) = \dfrac{\sin\left((2n+1)x\right)}{\sin^{2n+1} t}$.
2. Déterminer les racines de P_n et calculer leur somme.
3. Montrer que $\forall t \in \left]0, \dfrac{\pi}{2}\right[, \cot^2 t \leqslant \dfrac{1}{t^2} \leqslant 1 + \cot^2 t$ et en déduire la valeur de $\zeta(2) = \lim\limits_{n \to +\infty} \sum\limits_{k=1}^{n} \dfrac{1}{k^2}$.

Arithmétique et racines

Autocorrection C.

Résoudre les quatre équations suivantes, d'inconnue $(A, B) \in \mathbb{R}[X]^2$:

(i) $(X^4 - X^3 - X^2 - X - 2)A + (X^3 - 7X - 6)B = 1$;

(ii) $(X^4 - X^3 - X^2 - X - 2)A + (X^3 - 7X - 6)B = X + 3$;

(iii) $(X^2 + 2X + 3)A + (X^2 - X - 3)B = 0$;

(iv) $X^2A + (2X + 1)B = X + 2$.

Autocorrection D.

Montrer par deux méthodes différentes que X^2 divise $(X + 1)^n - nX - 1$ pour tout $n \in \mathbb{N}$.

Exercice 18.

1. Soit $P \in K[X]$. Montrer que $P - X$ divise $P \circ P - X$.
2. Résoudre dans $\mathbb{C}$ l'équation $(z^2 + 3z + 1)^2 + 3z^2 + 8z + 4 = 0$.

Exercice 19.

Dans les trois questions suivantes, on donne deux polynômes $P, Q \in \mathbb{C}[X]$, et on demande de déterminer le reste de P dans la division euclidienne par Q.

(i) $P = X^{100}$ et $Q = (X - 1)^3(X + 1)$;

(ii) $P = X^{2n}$ et $Q = (X^2 + 1)^2$;

(iii) $P = (X + 1)^{2n+1} - X^{2n+1}$ et $Q = X^2 + X + 1$.

Exercice 20.

Trouver tous les couples $(\lambda, \mu) \in K^2$ tels que le polynôme $X^2 + 2$ divise $X^4 + X^3 + \lambda X^2 + \mu X + 2$.

Exercice 21.

Trouver les $a \in \mathbb{C}$ tels que le polynôme $X^4 - X + a$ soit divisible par $X^2 - aX + 1$.

Exercice 22.

Déterminer tous les polynômes $P \in \mathbb{R}[X]$ tels que $P = P' P''$.

Exercice 23.

Soit $P, Q \in \mathbb{C}[X]$ et $m \in \mathbb{N}^*$. Montrer que $P \mid Q \Leftrightarrow P(X^m) \mid Q(X^m)$.

Exercice 24.

Pour tout $n \in \mathbb{N}^*$, on considère le polynôme complexe $P_n = X^n - 1$. Soit $a, b \geqslant 2$.

1. Montrer que $a \mid b$ si et seulement si $P_a \mid P_b$.
2. Montrer que $a \perp b$ si et seulement si $P_a P_b \mid (X - 1)P_{ab}$.

Exercice 25.

Déterminer $P \in \mathbb{R}[X]$ de degré 5 tel que

$$(X-1)^3 \mid P+1 \qquad \text{et} \qquad (X+1)^3 \mid P-1.$$

Exercice 26$^+$.

Soit $P \in \mathbb{C}[X]$ de degré $d \geqslant 1$, que l'on identifie à sa fonction polynomiale $\mathbb{C} \to \mathbb{C}$.

1. Soit $y \in \mathbb{C}$. Montrer que y possède $d - \deg\big((P-y) \wedge P'\big)$ antécédents par f.
2. En déduire que, pour toute partie finie V de $\mathbb{C}$,

$$d\big(|V|-1\big) < \left|P^{-1}[V]\right| \leqslant d\ |V|$$

et donner des exemples démontrant que cet encadrement est optimal.

Exercice 27$^+$.

Soit K un corps de caractéristique nulle. Déterminer $\{P \in K[X] \mid P' \text{ divise } P\}$.

Questions d'irréductibilité

Exercice 28$^+$. *Ulm*

1. Soit $P \in \mathbb{Q}[X]$ irréductible. Montrer que P n'a pas de racine double dans $\mathbb{C}$.
2. Soit $P \in \mathbb{Q}[X]$ de degré 5, possédant une racine double dans $\mathbb{C}$. Montrer que P a une racine rationnelle.

Exercice 29^{++} (Premier contact avec les polynômes cyclotomiques).

1. Soit p un nombre premier. Montrer qu'il existe $\Phi_p \in \mathbb{Z}[X]$ tel que $X^p - 1 = (X-1)\Phi_p(X)$.
2. Calculer $\Phi_p(X+1)$ et en déduire que Φ_p est un polynôme irréductible de $\mathbb{Q}[X]$.
3. Écrire le polynôme $X^{2p} - 1$ comme produit de polynômes irréductibles de $\mathbb{Q}[X]$.
4. Montrer qu'il existe $\Phi_{p^2} \in \mathbb{Z}[X]$ tel que $X^{p^2} - 1 = (X-1)\Phi_p(X)\Phi_{p^2}(X)$.
   (a) Factoriser $\Phi_{p^2}(X)$ dans $\mathbb{C}[X]$.
   (b) Montrer que $\Phi_{p^2}(X)$ est irréductible dans $\mathbb{Q}[X]$.
5. Soit $k \in \mathbb{N}^*$. Factoriser $X^{p^k} - 1$ dans $\mathbb{Q}[X]$.
6. Trouver le plus petit entier $n \in \mathbb{N}^*$ tel que $X^n - 1$ n'ait pas été factorisé dans $\mathbb{Q}[X]$ lors des questions précédentes, et factoriser ce polynôme.

Exercice 30.

Déterminer tous les polynômes irréductibles de $\mathbb{F}_2[X]$ de degré $\leqslant 4$.

Exercice 31.

Soit $b, c \in \mathbb{Z}$ et p un nombre premier impair. Montrer que $X^2 + bX + c$ est irréductible dans $\mathbb{F}_p[X]$ si et seulement si $[b^2 - 4c]_p$ n'est pas un carré dans $\mathbb{F}_p$.

Exercice 32^{++}.

1. Soit p un nombre premier.
   (a) Montrer que $\left\{x^2 \,\middle|\, x \in \mathbb{F}_p^\times\right\}$ est un sous-groupe du groupe multiplicatif $\mathbb{F}_p^\times$, et déterminer son cardinal.
   (b) En déduire qu'au moins l'une des classes $[-1]_p$, $[2]_p$ et $[-2]_p$ est un carré dans $\mathbb{F}_p$.
2. Montrer que X^4+1 est un polynôme irréductible dans $\mathbb{Q}[X]$, mais que, quel que soit p premier, X^4+1 est réductible dans $\mathbb{F}_p[X]$.

Factorisations

Autocorrection E.
Donner la factorisation dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$, des polynômes suivants :

(i) X^2+X+1 ;
(ii) X^4-4 ;
(iii) X^4+1 ;
(iv) X^6+27 ;
(v) $(X^2-X+1)^2+1$;
(vi) $X^5-10X^4+25X^3-25X^2+10X-1$;
(vii) $X^3-8X^2+23X-28$, en sachant que la somme de deux des racines est égale à la troisième ;
(viii) $X^4+12X-5$, en sachant qu'il y a deux racines dont la somme vaut 2.

Exercice 33.
On considère le polynôme $P=(1-X^2)^3+8X^3$.

1. Déterminer les solutions complexes de l'équation $\left(\dfrac{1-z^2}{2z}\right)^3=-1$.
2. En déduire la factorisation du polynôme P dans $\mathbb{C}$, puis dans $\mathbb{R}$.

Exercice 34.
Soit $a \in]0,\pi[$ et $n \in \mathbb{N}$. Factoriser $X^{2n}-2\cos(na)X^n+1$ dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

Exercice 35.
Déterminer tous les polynômes $P \in \mathbb{C}[X]$ tels que $P(X^2)=P(X)\,P(X-1)$.

Exercice 36^{+}.
Si K est un corps, on note $\mathcal{M}_K$ l'ensemble des polynômes unitaires irréductibles de K.

On appelle *valuation (discrète, normalisée)* sur un anneau A une application surjective $\nu : A \to \mathbb{N}\cup\{+\infty\}$ vérifiant les axiomes

(i) $\forall x \in A, \nu(x)=+\infty \Leftrightarrow x=0$;
(ii) $\forall x,y \in A, \nu(xy)=\nu(x)+\nu(y)$;
(iii) $\forall x,y \in A, \nu(x+y) \geqslant \min(\nu(x),\nu(y))$.

1. Soit $P \in \mathcal{M}_K$. Définir une « valuation P-adique » $\nu_P : K[X] \to \mathbb{N}\cup\{+\infty\}$, c'est-à-dire une valuation sur $K[X]$ telle que $\nu_P(P)=1$.
2. Réciproquement, montrer que tout valuation sur $K[X]$ est une des valuations construites à la question précédente.
3. Soit $P \in \mathcal{M}_{\mathbb{C}}$. Montrer que la restriction $(\nu_P)_{|\mathbb{R}[X]}$ est une valuation sur $\mathbb{R}[X]$, et expliciter dans ce cas la conclusion de la question précédente.

Mélange

Exercice 37.

Trouver les polynômes $P \in \mathbb{C}[X]$ tels que P et $P \circ P$ aient exactement les mêmes racines.

Exercice 38$^+$.

Déterminer les $(P, Q) \in \mathbb{C}[X]^2$ tels que $\forall z \in \mathbb{C}, |P(z)| \leqslant |Q(z)|$.

Exercice 39$^+$.

1. Soit $\mathcal{S} = \left\{A^2 + B^2 \,\middle|\, A, B \in \mathbb{R}[X]\right\}$. Montrer que $\mathcal{S}$ est stable par produit.
2. Soit $P \in \mathbb{R}[X]$. Montrer l'équivalence $P \in \mathcal{S} \Leftrightarrow \forall x \in \mathbb{R}, P(x) \geqslant 0$.

Exercice 40^{++}.

Soit $P \in \mathbb{R}[X]$. Montrer $\big(\forall x \in \mathbb{R}_+, P(x) \geqslant 0\big) \Leftrightarrow \big(\exists A, B \in \mathbb{R}[X] : P = A^2 + X B^2\big)$.

Exercice 41^{++}.

Soit $P, Q \in \mathbb{Z}[X]$ sans racine complexe commune. Montrer que $\big(P(n) \wedge Q(n)\big)_{n \in \mathbb{N}}$ est périodique.

Exercice 42$^+$ (Théorèmes de Mason-Stothers et de Liouville).

Dans cet exercice, on note n_P le nombre de racines complexes de tout polynôme $P \in \mathbb{C}[X]$.

Soit A, B et C trois polynômes premiers entre eux dans leur ensembles et tels que le produit ABC ne soit pas constant.

Nous allons montrer que si $A + B + C = 0$, alors $n_{ABC} \geqslant 1 + \max(\deg A, \deg B, \deg C)$ (*théorème de Mason-Stothers, 1981*). On suppose donc dans la suite $A + B + C = 0$.

1. Montrer que A, B et C sont deux à deux premiers entre eux.
2. On définit $P = AB' - A'B$.
   (a) Montrer que pour toute racine z de A, $\mu_z(P) \geqslant \mu_z(A) - 1$.
   (b) Montrer $\deg P \geqslant \deg(ABC) - (n_A + n_B + n_C)$.
3. Conclure la démonstration du théorème de Mason-Stothers.
4. **Application.** Soit $n \geqslant 3$. Résoudre l'équation $x^n + y^n = z^n$, d'inconnues $x, y, z \in \mathbb{C}[X]$.
   (Ce résultat a été obtenu par Liouville en 1879).

Exercice 43$^+$.

Soit $P \in \mathbb{R}[X]$ un polynôme de degré $n \geqslant 1$.

1. Montrer que si P est simplement scindé, alors $\forall j \in [\![1, n-1]\!], \forall x \in \mathbb{R}, P^{(j)}(x)^2 > P^{(j-1)}(x)\, P^{(j+1)}(x)$.
2. Soit $Q \in \mathbb{R}[X]$ tel que $\forall x \in \mathbb{R}, Q'(x)^2 > Q(x)\, Q''(x)$. Montrer
   - que les racines réelles de Q sont simples, et qu'il en possède au moins une ;
   - que Q' possède exactement une racine de moins que Q, et les localiser.
3. Montrer la réciproque de la première question.

Exercice 44$^+$ (Théorème de De Bruijn).

Soit $a \leqslant b \leqslant c$ et $A \leqslant B \leqslant C$ des entiers $\geqslant 1$. On s'intéresse dans cet exercice à la possibilité de paver un pavé de taille $A \times B \times C$ par des briques de taille $a \times b \times c$. Donnons des définitions précises.

- Une *brique* est une partie de $\mathbb{N}^3$ de la forme $\mathcal{B} = [\![x, x']\!] \times [\![y, y']\!] \times [\![z, z']\!]$.
- La *taille* d'une telle brique sera le triplet de ses trois « dimensions » $x'-x+1$, $y'-y+1$, $z'-z+1$, rangées par ordre croissant. Par exemple, $[\![3, 5]\!] \times [\![1, 6]\!] \times [\![2, 4]\!]$ est une brique de taille $(3, 3, 6)$.
- On se demande si le pavé $P = [\![1, A]\!] \times [\![1, B]\!] \times [\![1, C]\!]$ de taille (A, B, C) peut s'écrire comme union disjointe de briques de taille (a, b, c) : on dira alors pour simplifier que P est (a, b, c)-pavable.

1. Montrer que le pavé de taille $(5, 6, 6)$ n'est pas $(1, 2, 4)$-pavable.

Étant donné une partie finie $E \subseteq \mathbb{N}^3$, on définit son *poids* $w(E) = (X-1)^3 \sum_{(i,j,k)\in E} X^{i+j+k} \in \mathbb{R}[X]$.

2. Calculer le poids $w(P)$ du pavé $P = [\![1, A]\!] \times [\![1, B]\!] \times [\![1, C]\!]$.
3. Montrer que si P est (a, b, c)-pavable, alors $(X^a - 1)(X^b - 1)(X^c - 1) \mid w(P)$.
4. Montrer que le pavé de taille $(10, 10, 10)$ n'est pas $(1, 2, 4)$-pavable
5. Montrer que le pavé de taille $(7, 8, 9)$ n'est pas $(1, 2, 4)$-pavable.
6. Montrer le *théorème de De Bruijn* (1969) : si a divise b et b divise c, alors P est (a, b, c)-pavable si et seulement si, quitte à échanger A, B et C, on a $a \mid A$, $b \mid B$ et $c \mid C$.