CORRIGÉ DU TD N° 10

Polynômes irréductibles, polynômes d'interpolation de Lagrange et divers

17 mai 2021

Exercice 1 (Entraînement)**.**

1. Décomposer en produit d'irréductibles dans $\mathbb{R}[X]$ les polynômes suivants :

   (a) $X^4 + 3X^2 - 4$,

   (b) $X^8 - 1$,

   (c) $X^5 - 1$,

   (d) $X^9 + X^6 + X^3 + 1$

2. (a) Déterminer un polynôme de degré 2 tel que $P(-1) = 1$, $P(0) = -1$ et $P(1) = -1$. Ce polynôme est-il unique ?

   (b) Déterminer tous les polynômes $P \in \mathbb{R}[X]$ tels que $P(-1) = 1$, $P(0) = -1$ et $P(1) = -1$.

---

1. (a) On a $X^4 + 3X^2 - 4 = P(X^2)$ où $P = X^2 + 3X - 4$.
   Or $P = (X - 1)(X + 4)$.
   Donc $X^4 + 3X^2 - 4 = (X^2 - 1)(X^2 + 4) = (X - 1)(X + 1)(X^2 + 4)$.

   (b) $X^8 - 1 = (X^4 - 1)(X^4 + 1) = (X^2 - 1)(X^2 + 1)(X^4 + 1) = (X - 1)(X + 1)(X^2 + 1)(X^4 + 1)$. Il reste donc à factoriser $X^4 - 1$ en regardant les racines 4-ièmes de l'unité.

   $$\begin{aligned} X^4 + 1 &= (X - e^{i\pi/4})(X - e^{3i\pi/4})(X - e^{5i\pi/4})(X - e^{7i\pi/4}) \\ &= \big((X - e^{i\pi/4})(X - e^{7i\pi/4})\big)\big((X - e^{3i\pi/4})(X - e^{5i\pi/4})\big) \\ &= (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1). \end{aligned}$$

   Les deux polynômes de degré 2 que l'on obtient n'ont pas de racines réelles, ils sont donc irréductibles dans $\mathbb{R}[X]$.
   D'où
   $$X^8 - 1 = (X - 1)(X + 1)(X^2 + 1)(X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

   (c) On factorise sur $\mathbb{C}$ puis on regroupe les termes conjugués :

   $$\begin{aligned} X^5 - 1 &= (X - 1)(X - \mathrm{e}^{\frac{2i\pi}{5}})(X - \mathrm{e}^{\frac{4i\pi}{5}})(X - \mathrm{e}^{\frac{6i\pi}{5}})(X - \mathrm{e}^{\frac{8i\pi}{5}}) \\ &= (X - 1)(X - \mathrm{e}^{\frac{2i\pi}{5}})(X - \mathrm{e}^{\frac{-2i\pi}{5}})(X - \mathrm{e}^{\frac{4i\pi}{5}})(X - \mathrm{e}^{\frac{-4i\pi}{5}}) \\ &= (X - 1)(X^2 - 2\cos(\frac{2\pi}{5})X + 1)(X^2 - 2\cos(\frac{4\pi}{5})X + 1). \end{aligned}$$

   (d) On va commencer par décomposer $Q(X) = X^3 + X^2 + X + 1$, dont -1 est racine évidente. On en déduit
   $$Q(X) = (X + 1)(X^2 + 1) = (X + 1)(X - i)(X + i).$$
   On a $P(X) = Q(X^3) = (X^3 + 1)(X^3 - i)(X^3 + i)$ et il s'agit maintenant de trouver les racines 3-ièmes de -1, i et $-i$.
   Les racines cubiques de -1 sont -1, $e^{i\frac{\pi}{3}}$ et $e^{-i\frac{\pi}{3}}$.
   Les racines cubiques de $i = e^{i\frac{\pi}{2}}$ sont $e^{i\frac{\pi}{6}}$, $e^{i\frac{5\pi}{6}}$ et $e^{i\frac{9\pi}{6}} = e^{i\frac{3\pi}{2}} = -i$.
   Les racines cubiques de $-i$ sont les conjuguées de celles de i, à savoir $e^{-i\frac{\pi}{6}}$, $e^{-i\frac{5\pi}{6}}$ et i.
   On trouve donc la factorisation
   $$X^9 + X^6 + X^3 + 1 = (X+1)(X+i)(X-i)\left(X - \mathrm{e}^{i\pi/3}\right)\left(X - \mathrm{e}^{-i\pi/3}\right)\left(X - \mathrm{e}^{i\pi/6}\right)\left(X - \mathrm{e}^{-i\pi/6}\right)\left(X - \mathrm{e}^{i\pi/5}\right)\left(X - \mathrm{e}^{-i\pi/5}\right)$$
   Dans $\mathbb{R}[X]$, on peut factoriser sous la forme
   $$X^9 + X^6 + X^3 + 1 = (X + 1)(X^2 + 1)(X^2 - X + 1)(X^2 - \sqrt{3}X + 1)(X^2 + \sqrt{3}X + 1)$$

2. (a) Considérons les polynômes de Lagrange $L_0, Ł_1$ et L_2 associés à $x_0 = -1$, $x_1 = 0$ et $x_2 = 1$. Ils sont donnés par

$$L_0 = \frac{X(X-1)}{(-1)(-1-1)} = \frac{X^2 - X}{2},$$
$$L_1 = \frac{(X+1)(X-1)}{(0+1)(0-1)} = -(X^2-1),$$
$$L_2 = \frac{(X+1)X}{(1+1)1} = \frac{X^2+X}{2}.$$

Alors un polynôme qui convient est le polynôme

$$P_0 = 1L_0 - 1L_1 - 1L_2 = X^2 - X - 1.$$

C'est le seul qui convient, car si P est un polynôme de degré (inférieur ou égal à) 2 qui convient, alors $P - P_0$ est de degré au plus 2 et admet au moins 3 racines : c'est donc le polynôme nul.

(b) Soit P un tel polynôme. Alors, utilisant le polynôme P_0 introduit à la question précédente, et posant $Q = P - P_0$, on a $Q(-1) = Q(0) = Q(1) = 0$. Autrement dit, Q est divisible par $(X+1)X(X-1) = X^3 - X$, et P s'écrit

$$P(X) = X^2 - X - 1 + (X^3 - X)R$$

avec $R \in \mathbb{R}[X]$. Réciproquement, tous les polynômes de cette forme conviennent.

Exercice 2. Soit $a \in]0, \pi[$. Soit $n \in \mathbb{N}^*$. Factoriser dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$ le polynôme

$$X^{2n} - 2\cos(na)X^n + 1.$$

Les racines de $X^2 - 2\cos(na)X + 1$ sont e^{ina} et e^{-ina} puis que le produit des racines vaut $r_1 r_2 = 1$ et leur somme vaut $r_1 + r_2 = 2\cos(na)$.

Donc

$$X^{2n} - 2\cos(na)X^n + 1 = (X^n - \mathrm{e}^{ina})(X^n - \mathrm{e}^{-ina}).$$

Soit z une racine complexe de $X^n - \mathrm{e}^{ina}$.

Alors $z^n = \left(\mathrm{e}^{ia}\right)^n$ donc $\frac{z}{\mathrm{e}^{ia}}$ est une racine n-ième de l'unité.

Donc $\frac{z}{\mathrm{e}^{ia}} \in \left\{\mathrm{e}^{2ik\pi/n} \mid k \in \{0, \dots n-1\}\right\}$.

Donc les racines de $X^n - \mathrm{e}^{ina}$ sont les $\mathrm{e}^{ia+2ik\pi/n}$ où $k \in \{0, \dots, n-1\}$.

$z \in \mathbb{C}$ est racine de $X^n - \mathrm{e}^{ina}$ si et seulement si $\overline{z}$ est racine de $X^n - \mathrm{e}^{-ina}$ par passage au conjugué. Donc les racines de $X^n - \mathrm{e}^{-ina}$ sont les $\mathrm{e}^{-ia-2ik\pi/n}$ où $k \in \{0, \dots, n-1\}$.

Donc

$$X^{2n} - 2\cos(na)X^n + 1 = \prod_{k=0}^{n-1}(X - \mathrm{e}^{ia+2ik\pi/n}) \prod_{k=0}^{n-1}(X - \mathrm{e}^{-ia-2ik\pi/n}).$$

Il s'agit de la factorisation dans $\mathbb{C}[X]$.

On regroupe les termes conjugués pour obtenir la factorisation dans $\mathbb{R}[X]$:

$$X^{2n} - 2\cos(na)X^n + 1 = \prod_{k=0}^{n-1}(X - \mathrm{e}^{ia+2ik\pi/n})(X - \mathrm{e}^{-ia-2ik\pi/n}) = \prod_{k=0}^{n-1}(X^2 - 2\cos\left(a + \frac{2k\pi}{n}\right) X + 1).$$

Il s'agit de la factorisation dans $\mathbb{R}[X]$.

Exercice 3. Montrer que le polynôme $X^3 + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

Le polynôme $X^3 + X + 1$ étant de degré 3, nous avons vu en cours qu'il est irréductible si et seulement s'il n'admet pas de racines dans $\mathbb{Q}$.

Supposons qu'il existe $r \in \mathbb{Q}$ tel que r soit racine de $X^3 + X + 1$. r s'écrit $r = \frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ et on peut supposer p et q premiers entre eux.

On a donc $p^3 + pq^2 + q^3 = 0$, soit $p(p^2 + q^2) = -q^3$.

Donc $p \mid q^3$. Or p et q sont premiers entre eux donc d'après le lemme de Gauss, $p \mid q^2$, puis de même $p \mid q$ et enfin $p \mid 1$. Donc $p = \pm 1$.

On a $p^3 = -q(q^2 + pq)$ donc $q \mid p^3$. Donc $q = 1$.

Donc $r = \pm 1$.

Mais 1 et -1 ne sont pas racines de $X^3 + X + 1$.

Donc $X^3 + X + 1$ n'a pas de racines dans $\mathbb{Q}$ et est donc irréductible (car de degré ≤ 3).

Exercice 4. Montrer que pour tout $n \in \mathbb{N}$, il existe des réels λ_0, …, λ_n tels que pour tout $P \in \mathbb{R}_n[X]$,

$$\int_0^1 P(t)\mathrm{d}t = \sum_{k=0}^{n} \lambda_k P\left(\frac{k}{n}\right).$$

Posons, pour tout $k \in \{0, \dots, n\}$, $x_k = \dfrac{k}{n}$. Alors les x_k sont deux à deux distincts.

Notons L_0, …, L_n les polynômes de Lagrange associés aux x_k. Posons, pour tout $k \in \{0, \dots, n\}$, $\lambda_k = \int_0^1 L_k(t)\mathrm{d}t$,

Soit $P \in \mathbb{R}_n[X]$.

D'après le cours, on a $P = \sum_{k=0}^n P(x_k)L_k = \sum_{k=0}^n P\left(\dfrac{k}{n}\right) L_k$.

Donc en intégrant, on obtient

$$\int_0^1 P(t)\mathrm{d}t = \sum_{k=0}^{n} \int_0^1 P\left(\frac{k}{n}\right) L_k(t)\mathrm{d}t = \sum_{k=0}^{n} \int_0^1 L_k(t)\mathrm{d}t P\left(\frac{k}{n}\right).$$

D'où $\displaystyle\int_0^1 P(t)\mathrm{d}t = \sum_{k=0}^{n} \lambda_k P\left(\frac{k}{n}\right)$.

Exercice 5. Considérons l'application

$$f : \mathbb{R}[X] \to \mathbb{R}[X],\ P(X) \mapsto XP'(X) - P(X)$$

définie sur l'ensemble $\mathbb{R}[X]$ des polynômes.

1. Montrer que f est linéaire.
2. Déterminer le noyau de f.
3. Soit $n \in \mathbb{N}^*$.
   (a) Montrer que $f(\mathbb{R}_n[X]) \subset \mathbb{R}_n[X]$.
   (b) Soit l'endomorphisme
   $$g : \mathbb{R}_n[X] \to \mathbb{R}_n[X],\ P(X) \mapsto XP'(X) - P(X).$$
   Écrire la matrice de g dans la base canonique de $\mathbb{R}_n[X]$.
   (c) Déterminer une base de $\mathrm{Im}(g)$.
4. L'application f est-elle surjective ?
5. Exprimer $(f \circ f)(P)$ pour tout $P \in \mathbb{R}[X]$.
6. Déterminer le noyau de $f \circ f$.

---

1. Soient $(P, Q) \in \mathbb{R}[X]^2$ et $(\lambda, \gamma) \in \mathbb{R}^2$:
   $$\begin{aligned} f(\lambda P + \gamma Q) &= X(\lambda P + \gamma Q)' - (\lambda P + \gamma Q) \\ &= \lambda(XP' - P) + \gamma(XQ' - Q) \\ &= \lambda f(P) + \gamma f(Q), \end{aligned}$$
   Donc f est donc linéaire.
2. Soit $P = \sum_{k=0}^n a_k X^k \in \mathbb{R}[X]$. Alors :
   $$\begin{aligned} P \in \mathrm{Ker}\,(f) \iff f(P) = 0 &\iff \sum_{k=0}^{n}(k-1)a_k X^k = 0 \\ &\iff \forall i \neq 1,\ a_i = 0 \iff P = a_1 X \iff P \in \mathrm{Vect}(X). \end{aligned}$$
   On a donc $\mathrm{Ker}\,(f) = \mathrm{Vect}(X)$.
3. (a) Soit $P \in \mathbb{R}_n[X]$. P est de la forme $\sum_{k=0}^n a_k X^k$. On a alors $f(P) = \sum_{k=0}^n (k-1)a_k X^k \in \mathbb{R}_n[X]$. Par conséquent, $f(\mathbb{R}_n[X]) \subset \mathbb{R}_n[X]$.

   Remarque 1 — *Ceci permet de montrer que l'application g de la question suivante est bien définie.*

(b) Pour tout $k \in \mathbb{N}, 0 \leq k \leq n$, $g(X^k) = (k-1)X^k$. On en déduit la matrice de g dans la base canonique $\mathcal{B}$:

$$\mathrm{M}_{\mathcal{B}}(g) = \mathrm{Diag}\,(-1, 0, 1, 2, \cdots, n-1) = \begin{pmatrix} -1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & n-1 \end{pmatrix}$$

(c) $\mathrm{Im(g)} = \mathrm{Vect}(g(1), g(X), g(X^2) \cdots, g(X^n)) = \mathrm{Vect}(-1, 0, X^2, \cdots, (n-1)X^n) = \mathrm{Vect}(1, X^2, \cdots, X^n)$. La famille $(1, X^2, \cdots X^n)$ est une famille génératrice de Im(g). C'est également une famille libre car c'est une sous-famille de la base canonique. C'est donc une base de Im(g).

4. L'application f n'est pas surjective car X n'a pas d'antécédent. En effet, pour tout $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$:

$$f(P) = \sum_{k=0}^{n} (k-1) a_k X^k \neq X$$

puisque le coefficient de X dans l'expression $f(P)$ vaut 0.
Remarquons que l'application g n'est pas surjective car $\dim \mathrm{Im}\,(g) = n < \dim \mathbb{R}_n[X] = n+1$. Donc $\mathrm{Im}(g) \neq \mathbb{R}_n[X]$.

5. Soit $P \in \mathbb{R}[X]$:

$$(f \circ f)(P) = f(f(P)) = X(XP' - P)' - (XP' - P) = X^2 P'' - XP' + P$$

6. Soit $P \in \mathbb{R}[X]$. On utilise la formule de la question précédente. Si $P = \sum_{k=0}^{n} a_k X^k$, alors :

$$(f \circ f)(P) = \sum_{k=0}^{n} \left[k(k-1) - k + 1\right] a_k X^k = \sum_{k=0}^{n} (k-1)^2 a_k X^k$$

En raisonnant de la même façon que dans la question 1., on trouve $\mathrm{Ker}(f \circ f) = \mathrm{Vect}(X)$.

Exercice 6 (Bonus)**.** Soit P un élément de $\mathbb{R}[X]$ tel que pour tout $x \in \mathbb{R}$, $P(x) \geq 0$. Montrer qu'il existe deux polynômes A et B de $\mathbb{R}[X]$ tels que

$$P = A^2 + B^2.$$

- Soit $x_0 \in \mathbb{R}$. Montrons que si x_0 est racine de P de multiplicité α (non nulle) alors α est pair.
  P s'écrit $P = (X - x_0)^\alpha Q$ où $Q \in \mathbb{R}[X]$.
  P admet un nombre fini de racines donc il existe un voisinage de x_0 de la forme $]x_0 - h, x_0 + h[$ sur lequel Q n'admet pas de racines. La continuité de Q vu comme fonction polynomiale assure que Q garde un signe constant. Si α était impair, pour tout $x \in]x_0, x_0 + h[$, P serait du signe de Q et sur $]x_0 - h, x_0[$, P serait de signe opposé, contredisant sa positivité. Donc α est pair.
- Le coefficient dominant c de P est strictement positif. En effet, on exclut le cas où P est constant et où son coefficient dominant est donc positif par hypothèse. Notons $d = \deg(P)$. Alors $P(x) \sim cx^d$ au voisinage de $+\infty$. Donc si c était strictement négatif, la limite en $+\infty$ de P serait $-\infty$, contredisant sa positivité. Donc $c > 0$.
- Soit $Q \in \mathbb{C}[X]$. Notons $Q = Q_1 + iQ_2$ où $(Q_1, Q_2) \in \mathbb{R}[X]^2$.
  Alors $Q\overline{Q} = Q_1^2 + Q_2^2$.
- Le décomposition de P dans $\mathbb{C}[X]$ s'écrit donc

$$P = \omega^2 \prod_{i=1}^{p} (X - x_i)^{2\gamma_i} \prod_{j=1}^{q} (X - z_j)^{\beta_j} (X - \overline{z}_j)^{\beta_j},$$

  où $\omega^2 = x$, $x_1, \ldots, x_n$ sont les racines réelles deux à deux distinctes de P et z_1, $\overline{z}_1$, …, z_q, $\overline{z}_q$ sont les racines complexes non réelles deux à deux distinctes de P, $2\gamma_i$ la multiplicité de x_i et β_j celle de z_j et $\overline{z}_j$. (Rappelons que z est racine de multiplicité m P à coefficients réels si et seulement $\overline{z}$ est racine de P de même multiplicité m.)
  Posons $Q = \prod_{j=1}^{q} (X - z_j)^{\beta_j}$. Alors $\overline{Q} = \prod_{j=1}^{q} (X - \overline{z}_j)^{\beta_j}$ et donc

$$\prod_{j=1}^{q} (X - z_j)^{\beta_j} (X - \overline{z}_j)^{\beta_j} = Q_1^2 + Q_2^2,$$

  où $Q_1 = \mathrm{Re}(Q)$ et $Q_2 = \mathrm{Im}(Q)$.
  Donc $P = P_1^2 + P_2^2$ où $P_1 = \omega \prod_{i=1}^{n} (X - x_i)^{\gamma_i} Q_1$ et $P_2 = \omega \prod_{i=1}^{n} (X - x_i)^{\gamma_i} Q_2$.