Corrigé du TD n° 12

Polynômes irréductibles, polynômes d'interpolation de Lagrange et divers

4 juin 2021

Exercice 1. Déterminer le pgcd des polynômes suivants :

1. $X^5 - 2X^4 + X^2 - X - 2$ et $X^3 - X^2 - X - 2$,
2. $X^4 + X^3 - 2X + 1$ et $X^3 + X + 1$,
3. $X^n - 1$ par $(X-1)^n$ pour $n \in \mathbb{N}^*$.

---

1. L'algorithme d'Euclide permet de calculer le pgcd par une suite de divisions euclidiennes.
$$X^5 - 2X^4 + X^2 - X - 2 = \left(X^3 - X^2 - X - 2\right)\left(X^2 - X\right) + 2X^2 - 3X - 2,$$
puis
$$X^3 - X^2 - X - 2 = \left(2X^2 - 3X - 2\right)\left(\frac{1}{2}X + \frac{1}{4}\right) + \frac{3}{4}X - \frac{3}{2},$$
puis
$$2X^2 - 3X - 2 = \left(\frac{3}{4}X - \frac{3}{2}\right)\left(\frac{8}{3}X + \frac{4}{3}\right).$$
Le pgcd est le dernier reste non nul, divisé par son coefficient dominant :
$$\operatorname{pgcd}\left(X^3 - X^2 - X - 2, X^5 - 2X^4 + X^2 - X - 2\right) = X - 2$$
2. De la même manière,
$$X^4 + X^3 - 2X + 1 = \left(X^3 + X + 1\right)(X + 1) - X^2 - 4X,$$
puis
$$X^3 + X + 1 = \left(-X^2 - 4X\right)(-X + 4) + 17X + 1,$$
donc
$$\operatorname{pgcd}\left(X^4 + X^3 - 2X + 1, X^3 + X + 1\right) = \operatorname{pgcd}\left(-X^2 - 4X, 17X + 1\right) = 1$$
car $-X^2 - 4X$ et $17X + 1$ n'ont pas de racine (même complexe) commune. (*On pouvait aussi faire poursuivre l'algorithme d'Euclide, le dernier reste non nul est une constante, donc le pgcd vaut* 1.
3. Les diviseurs non constants de Q sont les polynômes du type $c(X-1)^p$, avec $1 \leq p \leq n$. Parmi ces diviseurs, seuls ceux de la forme $c(X-1)$ divisent aussi P (par exemple, car 1 est racine simple et non double de P, ou bien parce qu'on sait comment décomposer P en produits d'irréductibles...). Ainsi, $P \wedge Q = X - 1$.
4. Une idée possible est d'appliquer l'algorithme d'Euclide pour calculer le pgcd de ces deux polynômes. On suppose par exemple $n > m$, et on écrit $n = mp + r$, avec $0 \leq r < m$. Alors on a
$$X^n - 1 = X^{mp+r} - 1 = X^r\left(X^{mp} - 1\right) + X^r - 1$$
Le point crucial est que $X^{mp} - 1$ est divisible par $X^m - 1$. En effet,
$$X^{mp} - 1 = \left(X^m - 1\right)\left(X^{m(p-1)} + X^{m((p-1)-1)} + \cdots + X^m + 1\right)$$
Ainsi, $\operatorname{pgcd}\left(X^n - 1, X^m - 1\right) = \operatorname{pgcd}\left(X^m - 1, X^r - 1\right)$. Mais puisque $\operatorname{pgcd}(n, m) = \operatorname{pgcd}(m, r)$, on en déduit finalement que
$$\operatorname{pgcd}\left(X^n - 1, X^m - 1\right) = X^{\operatorname{pgcd}(n,m)} - 1$$

Exercice 2. Soit $A, B \in \mathbb{K}[X]$ non constants et premiers entre eux. Montrer qu'il existe un unique couple $(U, V) \in \mathbb{K}[X]^2$ tel que
$$AU + BV = 1 \text{ et } \begin{cases} \deg U < \deg B \\ \deg V < \deg A \end{cases}$$

• *Unicité :* Soit (U,V) et $(\hat{U},\hat{V})$ deux couples solutions. On a alors $A(U-\hat{U}) = B(\hat{V}-V)$.

Donc $A \mid B(\hat{V}-V)$ et $A \wedge B = 1$ donc, par le lemme de Gauss, $A \mid \hat{V}-V$. Or $\deg(\hat{V}-V) < \deg A$, donc $\hat{V}-V = 0$

Donc $\hat{V} = V$, puis $\hat{U} = U$

• *Existence :* Puisque $A \wedge B = 1$, d'après le théorème de Bezout, il existe $U, V \in \mathbb{K}[X]$ tels que

$$AU + BV = 1.$$

Réalisons la division euclidienne de U par B : $U = BQ + \hat{U}$ avec $\deg \hat{U} < \deg B$. Posons ensuite $\hat{V} = V + AQ$. On a

$$A\hat{U} + B\hat{V} = AU + BV = 1$$

avec $\deg \hat{U} < \deg B$. Comme $\deg A\hat{U} + B\hat{V} = 0$, on a $\deg A\hat{U} = \deg B\hat{V}$, d'où $\deg \hat{V} = \deg A + \deg \hat{U} - \deg B < \deg A$.

Exercice 3. Soit P et Q des polynômes de $\mathbb{C}[X]$ de degré m et n. Montrer que les propriétés suivantes sont équivalentes :

1. la famille $\left(P, XP, \cdots, X^{n-1}P, Q, XQ, \cdots, X^{m-1}Q\right)$ est libre
2. il existe U et $V \in \mathbb{C}[X]$ tels que $UP + VQ = 1$.
3. P et Q n'ont pas de racines communes.

1) $\Rightarrow$ 2) : Si la famille est libre, c'est une base de $\mathbb{C}_{n+m-1}[X]$ car famille constituée de $n+m$ éléments qui est la dimension de $\mathbb{C}_{n+m-1}[X]$, donc il existe U et V tel que $UP + VQ = 1$.

2) $\Rightarrow$ 3) : Si $UP + VQ = 1$ et a une racine commune, alors $(UP+VQ)(a) = U(a)Q(a) + V(a)Q(a) = 0 = 1(a) = 1$. Ce qui est absurde. Donc P et Q n'ont pas de racine commune.

3) $\Rightarrow$ 1) : Comme on est dans $\mathbb{C}$, P et Q sont premiers entre eux. Supposons une relation de dépendance linéaire $UP+VQ = 0$ avec $\deg U < \deg Q$ et $\deg V < \deg P$. Alors, $P \mid V$ et donc $V = 0$ et $U = 0$. La famille est libre.

Exercice 4. Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante (pour l'inclusion) d'idéaux de $\mathbb{K}[X]$. Démontrer que la suite $(I_n)_{n\in\mathbb{N}}$ est stationnaire pour l'inclusion *(c'est-à-dire qu'il existe $n_0 \in \mathbb{N}$ telles que pour tout $n \geq n_0$, $I_n = I_{n_0}$)*.

• *Méthode 1* : Pour tout $n \in \mathbb{N}$, il existe un unique polynôme unitaire P_n tel que $I_n = (P_n)$. De plus, la condition $I_n \subset I_{n+1}$ entraîne que $P_{n+1} \mid P_n$. La suite $(\deg(P_n))_{n\in\mathbb{N}}$ est donc une suite d'entiers naturels décroissante : elle est stationnaire. Soit $p \in \mathbb{N}$ tel que, pour tout $n \geq p$, on a $\deg(P_n) = \deg(P_p)$ On a alors $P_n \mid P_p$, P_n et P_p sont unitaires et de même degré, donc ils sont égaux et $I_n = I_p$.La suite (I_n) est bien stationnaire.

• *Méthode 2 :* Posons $I = \bigcup_n I_n$. Puisque la suite (I_n) est croissante, il est facile de vérifier que I est un idéal. II existe $P \in \mathbb{K}[X]$ tel que $I = (P)$. Mais alors, il existe $N \in \mathbb{N}$ tel que $P \in I_N$. On prouve alors que pour tout $n \geq N$, on a $I_n = (P)$. En effet, on a $I_n \subset I = (P)$, et $P \in I_N \subset I_n \Longrightarrow (P) \subset I_n$

Exercice 5. On se place dans $\mathbb{C}_3[X]$, et on note $A = X^4 - 1$ et $B = X^4 - X$. On désigne par f l'application qui, à un polynôme P, associe le reste de la division de AP par B.

1. Montrer que f est un endomorphisme de $\mathbb{C}_3[X]$.
2. Déterminer le noyau de f.
3. Quelle est la dimension de $\mathrm{Im}(f)$? Montrer que $\mathrm{Im}(f) = (X-1)\mathbb{C}_2[X]$.
4. Déterminer les quatre racines z_1, z_2, z_3 et z_4 de B. 5. Montrer qu'en posant $P_k = \frac{B}{X-z_k}$, la famille (P_1, P_2, P_3, P_4) est une base de $\mathbb{C}_3[X]$.
5. Montrer que $f(P_k) = (z_k - 1)P_k$.

1. Commençons par prouver que $f(\mathbb{C}_3[X]) \subset \mathbb{C}_3[X]$. Par division euclidienne de AP par B, le degré du reste est strictement inférieur à celui de B. Ici, B étant de degré 4 , $f(P)$ sera de degré inférieur ou égal à 3 quel que soit le polynôme P (peu importe d'ailleurs que P appartienne à $\mathbb{C}_3[X]$).
   Montrons que l'application f est linéaire.
   Soient donc deux polynômes P_1 et P_2, alors si on effectue la division euclidienne de AP_1 et de AP_2 par B, on obtient les égalités
   $$AP_1 = BQ_1 + R_1 \text{ et } AP_2 = BQ_2 + R_2.$$
   On peut effectuer la combinaison de ces deux équations :
   $$A(\lambda P_1 + \mu P_2) = B(\lambda Q_1 + \mu Q_2) + (\lambda R_1 + \mu R_2).$$
   Comme $d(\lambda R_1 + \mu R_2) \leqslant \max(d(R_1), d(R_2)) < 4$, il s'agit nécessairement la division euclidienne de $A(\lambda P_1 + \mu P_2)$ par B, donc $f(\lambda P_1 + \mu P_2) = \lambda R_1 + \mu R_2 = \lambda f(P_1) + \mu f(P_2)$. L'application f est donc linéaire.
   C'est bien un endomorphisme de $\mathbb{C}_3[X]$.

2. On peut caractériser les polynômes du noyau par la condition AP est divisible par B, mais ce n'est pas pratique à expliciter. Mieux vaut expliciter en calculant les images des polynômes de la base canonique comme $A = B + X - 1, f(1) = X - 1$; de même $AX = BX + X^2 - X$, donc $f(X) = X^2 - X$ puis $f\left(X^2\right) = X^3 - X^2$. Un tout petit peu plus de réflexion pour la dernière : $AX^3 = BX^3 + X^4 - X^3 = BX^3 + \left(X^4 - X\right) + X - X^3 + B\left(X^3 + 1\right) + X - X^3$ donc $f\left(X^3\right) = X - X^3$. Cherchons maintenant le noyau : si $P = a + bX + cX^2 + dX^3$, alors $f(P) = -a + (a - b + d)X + (b - c)X^2 + (c - d)X^3$, donc P appartient au noyau si $b = c = d$ (à cause des deux derniers coefficients) et $a = 0$ (premier coefficient). La deuxième équation est alors toujours vérifiée, donc $\ker(f) = \left\{bX + bX^2 + bX^3, x \in \mathbb{C}\right\} = \text{Vect}\left(X + X^2 + X^3\right)$.
3. Puisque $\dim(\ker(f)) = 1$ et $\dim\left(\mathbb{C}_3[X]\right) = 4$, le théorème du rang assure que $\dim(\text{Im}(f)) = 3$. Comme l'image de f contient $X - 1, X^2 - X = X(X - 1)$ et $X^3 - X^2 = X^2(X - 1)$ (qui sont images de trois des polynômes de la base canonique), elle contient tous les polynômes de la forme $(X - 1)\left(a + bX + cX^2\right)$, donc $(X - 1)\mathbb{C}_2[X]$. Comme ce dernier espace est de dimension 3 comme $\text{Im}(f)$, il y a nécessairement égalité entre les deux.
4. Il faut donc résoudre l'équation $X^4 - X = 0$, soit $X\left(X^3 - 1\right) = 0$. les quatre racines sont $z_1 = 0, z_2 = 1, z_3 = j = e^{i\frac{2\pi}{3}}$ et $z_4 = \bar{j} = e^{i\frac{-2\pi}{3}}$ (les trois dernières étant les racines cubiques de l'unité).
5. Écrivons les quatre polynômes : $P_1 = X^3 - 1; P_2 = X\left(X^2 + X + 1\right) = X^3 + X^2 + X; P_3 = X(X - 1)(X - \bar{j}) = X^3 + jX^2 + \bar{j}X$ et $P_4 = X(X - 1)(X - j) = X^3 + \bar{j}X^2 + jX$. Pour prouver que c'est une base, supposons $aP_1 + bP_2 + cP_3 + dP_4 = 0$, et profitons du fait que ces polynômes ont des racines en commun. Pour $x = 0$, l'équation devient $-a = 0$, ce qui implique $a = 0$; pour $x = 1$, on trouve $3b = 0$, donc $b = 0$; pour $x = j, cj(j - 1)(j - \bar{j}) = 0$ donc $c = 0$; de même pour $d = 0$, la famille est donc libre. Comme elle contient quatre polynômes, c'est une base de $\mathbb{C}_3[X]$.
6. On $A = B + X - 1$, et $(X - z_k)\, P_k = B$, donc

$$AP_k = BP_k + (X - 1)P_k = BP_k + (X - z_k)\, P_k + (z_k - 1)\, P_k = B\,(P_k + 1) + (z_k - 1)\, P_k.$$

Il s'agit de la division euclidienne de AP_k par B, donc $f\,(P_k) = (z_k - 1)\, P_k$.
Pour détailler un peu plus, $f\,(P_1) = -P_1$ $f\,(P_2) = 0; f\,(P_3) = (j - 1)P_3$ et $f\,(P_4) = (\bar{j} - 1)P_4$.

Exercice 6 (Bonus)**.**

1. Déterminer les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathbb{U}) \subset \mathbb{U}$.
2. Déterminer les fonctions rationnelles $F \in \mathbb{C}(X)$ telles que $F(\mathbb{U}) \subset \mathbb{U}$.

---

1. Soit P un tel polynôme non constant (sinon $P = \pm 1$) de degré $n \geq 1$.
Posons $Q = X^n \bar{P}\left(\frac{1}{X}\right)$. Par hypothèse, $P(e^{i\theta})\overline{P(\mathrm{e}^{i\theta})} = 1$ donc, en multipliant par $\mathrm{e}^{i\theta}$, on a

$$P(\mathrm{e}^{i\theta})Q(\mathrm{e}^{i\theta}) = (\mathrm{e}^{i\theta})^n.$$

Donc

$$PQ = X^n$$

Donc $P \mid X^n$. P est donc de la forme $P = uX^n$ et puisque $P(\mathrm{e}^{i\theta})\overline{P(\mathrm{e}^{i\theta})} = 1$, $|u| = 1$.

2. On écrit $F = \dfrac{P}{Q}$ avec P et Q premiers et P unitaire $\deg P = d$, $\deg Q = d'$. De plus, quitte à factoriser P ou Q par X^l, on peut supposer que $X \not| P$ et $X \not| Q$.
Alors

$$\frac{P(X)}{Q(X)} \frac{X^d \overline{P}(1/X)}{X^{d'} \overline{Q}(1/X)} = X^{d-d'}$$

On en déduit $2d - 2d' = d - d'$ puis $d = d'$ et

$$P(X)\left[X^d \bar{P}(1/X)\right] = Q(X)\left[X^d \bar{Q}(1/X)\right].$$

On en déduit comme P et Q sont premiers que P divise $X^{d'}\bar{Q}(1/X)$ et Q divise $X^{d'}\bar{P}(1/X)$.
On a donc $Q = cX^n P(1/X)$ et comme $F(1) \in \mathbb{U}$, on en déduit que $c \in \mathbb{U}$.
Les fractions rationnelles sont donc de la forme $F = cX^k \dfrac{P(X)}{X^n \overline{P}(1/X)}$.
Si $|\omega| \neq 1$, alors $F(z) = \dfrac{z - \omega}{1 - \overline{\omega} z}$ vérifie la propriété (si $\omega \in \mathbb{U}$, alors $F(z) = -\omega$!).