Feuille de TD n° 11

Applications linéaires, PGCD et PPCM de polynômes

1er décembre 2021

Pour commencer . . .

Exercice 1.
Soit $P \in \mathbb{K}[X]$ de degré $n > 0$.
On définit la fonction $\phi : \mathbb{K}[X] \to \mathbb{K}_{n-1}[X]$, telle que $\phi(Q)$ est le reste de la dlvision euclidienne de Q par P.

1. Montrer que ϕ est une application linéaire.
2. Est-ce que ϕ est injective ? Déterminer $Ker(\phi)$.
3. Est-ce que ϕ est surjective ? Déterminer $Im(\phi)$.
4. Quelle différence y a-t-il avec la division euclidienne d'entiers ?
5. Soient $a, b \in \mathbb{K}$ distincts. Montrer qu'il existe une unique application linéaire $\psi : \mathbb{K}[X] \to \mathbb{K}[X]$ telle que

$$\psi(1) = 1\,,\ \psi(X) = X\,,\ \text{ et }\ Q(a) = Q(b) = 0 \text{ implique } \psi(Q) = 0\,,\ \text{pour tout } Q \in \mathbb{K}[X].$$

1. Pour $Q = 0$, on a $\phi(Q) = 0$.
Soient $Q_1, Q_2 \in \mathbb{K}[X]$. Soit $\lambda \in \mathbb{K}$. On écrit $Q_1(X) = B_1(X)P(X) + \phi(Q_1)(X)$ et $Q_2(X) = B_2(X)P(X) + \phi(Q_2)(X)$, avec $\deg(\phi(Q_1)), \deg(\phi(Q_2)) < n = \deg(P)$.
Alors, on a
$$Q_1 + \lambda Q_2 = (B_1 + \lambda B_2)P + (\phi(Q_1) + \lambda\phi(Q_2)).$$
Comme on a $\deg(\phi(Q_1) + \lambda\phi(Q_2)) < n$, on en déduit que le reste de la division euclidienne de $Q_1 + \lambda Q_2$ par P est $\phi(Q_1) + \lambda\phi(Q_2)$.
On a ainsi $\phi(Q_1 + \lambda Q_2) = \phi(Q_1) + \lambda\phi(Q_2)$.
Ainsi, ϕ est une application linéaire.
2. On a $\dim(\mathbb{K}[X]) = +\infty$ et $\dim(\mathbb{K}_{n-1}[X]) = n$, donc ϕ ne peut pas être injective.
D'après le cours, on a $\phi(Q) = 0$ si et seulement si $P \mid Q$.
On a donc $Ker(\phi) = P.\mathbb{K}[X]$. (ensemble des multiples de P)
3. Soit $R \in \mathbb{K}_{n-1}[X]$. On a alors $R = 0.P + R$, avec $\deg(R) < n$. Donc, on a $\phi(R) = R$.
L'application ϕ est surjective.
4. Pour la division euclidienne d'entiers, il est faux en général de dire que le reste de la somme $q_1 + q_2$ est égal à la somme des restes. (Ex : $8 = 2.3 + 2$, $11 = 3.3 + 2$, $19 = 6.3 + 1$, le reste de la division euclidienne de 19 par 3 est 1 et non $2 + 2 = 4$)
5. On pose, et on prend $\psi : \mathbb{K}[X] \to \mathbb{K}[X]$ telle que $\psi(Q)$ est le reste de la division euclidienne de Q par $P(X) = (X - a)(X - b)$.
Alors, on a bien $\psi(1) = 1$, $\psi(X) = X$.
De plus, on a : $\psi(Q) = 0$ si et seulement si $Q \in Ker(\psi)$ si et seulement si $(X-a)(X-b) \mid Q$.
Si $(X - a)(X - b) \mid Q$ on a alors $Q(X) = S(X)(X - a)(X - b)$, donc $Q(a) = Q(b) = 0$.
Réciproquement, si $Q(a) = Q(b) = 0$, on a $(X - a) \mid Q$ donc $Q(X) = (X - a)S_1(X)$.
Comme $Q(b) = 0$ on a $S_1(b) = 0$ donc $S_1(X) = (X-b)S_2(X)$, donc $(X-a)(X-b) \mid Q$.

Exercice 2.
1. Calculer $pgcd(X^2, (X-1)^3)$, $pgcd(X^2-1, X^3-1)$, $pgcd(X^4-1, X^6-1)$, $pgcd(X^4 - 2X^2 + 3, X^2 + X)$.
2. Factoriser dans $\mathbb{R}[X]$: $X^2 - 1$, $X^3 - 1$, $X^2 - 5X + 2$,$X^2 + 1$, $X^4 + 1$.
3. Factoriser dans $\mathbb{C}[X]$: $X^3 - 1$, $X^n - 1$ $n \geq 1$, $X^2 - 5X + 2$, $X^2 + 1$, $X^n - z$ $n \geq 1$ $z = r.e^{it}$.

1. $pgcd(X^2, (X-1)^3) = 1$, $pgcd(X^2 - 1, X^3 - 1) = (X - 1)$.
$pgcd(X^4 - 2X^2 + 3, X^2 + X) = X + 1$ car $X^2 + X = X(X + 1)$, et X ne divise pas $X^4 - 2X^2 + 3$ mais $(-1)^4 - 2.(-1)^2 + 3 = 0$ donc $X + 1 \mid X^4 - 2X^2 + 3$.
$pgcd(X^4 - 1, X^6 - 1) = X^2 - 1$ car $X^4 - 1 = (X - 1)(X + 1)(X^2 + 1)$ et $X^6 - 1 = (X^3-1)(X^3+1) = (X-1)(X^2+X+1)(X+1)(X^2-X+1)$, et $pgcd(X^2+1, X^2+X+1) = pgcd(X^2 + 1, X^2 - X + 1) = 1$.
2. $X^2-1 = (X-1)(X+1)$. $X^3-1 = (X-1)(1+X+X^2)$. $X^2-5X+2 = (X-\frac{5+\sqrt{17}}{2})(X-\frac{5-\sqrt{17}}{2})$. $X^2 + 1 = X^2 + 1$ (polynôme irréductible). $X^4 + 1 = X^4 + 2X^2 + 1 - 2X^2 = (X^2 + 1)^2 - 2X^2 = (X^2 + 1 - \sqrt{2}X)(X^2 + 1 + \sqrt{2}X)$, et ces deux polynômes sont irréductibles dans $\mathbb{R}[X]$.
3. $X^3 - 1 = (X - 1)(X - j)(X - j^2)$. $X^n - 1 = \Pi_{k=1}^{n}(X - e^{2i\pi\frac{k}{n}})$. $X^2 - 5X + 2 = (X - \frac{5+\sqrt{17}}{2})(X - \frac{5-\sqrt{17}}{2})$. $X^2+1 = (X-i)(X+i)$. $X^n - z = \Pi_{k=1}^{n}(X - r^{\frac{1}{n}}e^{2i\pi\frac{k}{n}+\frac{t}{n}})$.

Exercice 3. Soient $P, Q \in \mathbb{Q}[X]$. Montrer que dans $\mathbb{Q}[X]$, dans $\mathbb{R}[X]$, et dans $\mathbb{C}[X]$, le polynôme $pgcd(P, Q)$ reste identique.
En déduire que si P divise Q dans $\mathbb{C}[X]$, alors P divise Q dans $\mathbb{Q}[X]$.
Si P divise Q, comment trouver le polynôme R tel que $Q = PR$?

Soient R_1, R_2, R_3 les *pgcd* de P, Q dans $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$.
On a alors $R_1 = U_1P + V_1Q$ (dans $\mathbb{Q}[X]$), $R_2 = U_2P + V_2Q$ (dans $\mathbb{R}[X]$), $R_3 = U_3P + V_3Q$ (dans $\mathbb{C}[X]$).
Comme on sait que R_1 divise P et Q dans $\mathbb{Q}[X]$, alors R_1 divise P et Q dans $\mathbb{R}[X]$.
On a donc $R_1 \mid U_2P + V_2Q = R_2$. Comme R_1 est unitaire et non-nul, on en déduit par propriété de minimalité du *pgcd* dans $\mathbb{R}[X]$ que $R_1 = R_2$.
Comme on sait que R_1 divise P et Q dans $\mathbb{Q}[X]$, alors R_1 divise P et Q dans $\mathbb{C}[X]$.
On a donc $R_1 \mid U_3P + V_3Q = R_3$. Comme R_1 est unitaire et non-nul, on en déduit par propriété de minimalité du *pgcd* dans $\mathbb{C}[X]$ que $R_1 = R_3$.
On a $P \mid Q$ si et seulement si $pgcd(P, Q) = P$, ce qui conclut.
Si $Q = PR$, on a $Q = PR + 0$. Le polynôme R s'obtient en faisant la division euclidienne de Q par P.

Exercice 4.

1. Montrer qu'un polynôme de $\mathbb{K}[X]$, de degré 3, qui n'a pas de racines dans $\mathbb{Q}$, est irréductible dans $\mathbb{K}[X]$.
2. Soit $n \in \mathbb{N}$. Est-ce que le polynôme X^2+X+1 divise $X^{3n+8}+X^{3n+4}+X^{3n}$ dans $\mathbb{Q}[X]$?
3. Résoudre l'équation $P(X^2) = (X^2+1)P(X)$, d'inconnue $P \in \mathbb{K}[X]$.

1. Soit $P \in \mathbb{K}[X]$ avec $\deg(P) = 3$ et P sans racines.
   On suppose par l'absurde que P est réductible dans $\mathbb{K}[X]$.
   On aurait alors $P = Q_1Q_2$ avec Q_1 et Q_2 des polynômes non-constants.
   On aurait alors $\deg(P) = 3 = \deg(Q_1) + \deg(Q_2)$, donc $\deg(Q_1) = 1$ et $\deg(Q_2) = 2$ ou $\deg(Q_1) = 2$ ou $\deg(Q_2) = 1$.
   Or, un polynôme de degré 1 est de la forme $aX + b$ avec $a \neq 0$, et admet comme racine $\frac{-b}{a}$. Ainsi, Q_1 ou Q_2 a une racine dans $\mathbb{K}$, donc P a une racine dans $\mathbb{K}$, contradiction.
   Donc P est irréductible dans $\mathbb{K}$.
2. On a $X^{3n+8} + X^{3n+4} + X^{3n} = X^{3n}(X^8 + X^4 + 1)$.
   On se place dans $\mathbb{C}[X]$. On a alors $X^2 + X + 1 = (X - j)(X - j^2)$. On a $j^3 = 1$ et $j^2 + j + 1 = 0$. Cela donne $j^8 + j^4 + 1 = j^2 + j + 1 = 0$, et $j^{16} + j^8 + 1 = j + j^2 + 1 = 0$.
   Donc, $X^2 + X + 1$ divise $X^8 + X^4 + 1$ dans $\mathbb{C}$. Donc, d'après l'exercice précédent, $X^2 + X + 1$ divise $X^8 + X^4 + 1$ dans $\mathbb{Q}$.
   Ainsi, $X^2 + X + 1$ divise bien $X^{3n+8} + X^{3n+4} + X^{3n}$.
3. Supposons que le polynôme P est une solution non nulle de l'équation. Le polynôme $P(X^2)$ est de degré $2\deg(P)$ et le polynôme $(X^2+1)P(X)$ est de degré $\deg(P)+2$. Donc un polynôme solution de cette équation doit vérifier l'équation $2\deg(P) = \deg(P) + 2$. Donc c'est un polynôme de degré 2. Donc $P = aX^2 + bX + c$ doit vérifier :

$$aX^4 + bX^2 + c = (X^2+1)(aX^2 + bX + c) = aX^4 + bX^3 + (a+c)X^2 + bX + c.$$

Donc (a, b, c) doivent vérifier :

$$\begin{cases} b &= 0 \\ a &= -c \end{cases}$$

Donc P est de la forme $a(X^2 - 1)$. Or tous les polynômes de cette forme vérifient l'équation souhaitée.

Exercice 5.

1. Soit $P \in \mathbb{C}[X]$ vérifiant $P(X^2) = P(X-1)P(X+1)$.
   (a) Soit $z \in \mathbb{C}$ une racine de P. Démontrer que P possède alors une racine w telle que $|w| > |z|$.
   (b) En déduire les polynômes $P \in \mathbb{C}[X]$ solutions de l'équation.
2. Soit $P \in \mathbb{R}[X]\backslash\{0\}$ vérifiant $P(X^2) = P(X)P(X-1)$.
   (a) Démontrer que si z est racine de P, alors $z = j$ ou $z = j^2$, où $j = e^{2i\frac{\pi}{3}}$.
   (b) En déduire les polynômes $P \in \mathbb{R}[X]$ solutions.

1. (a) Soit z une racine de P. L'équation vérifiée par P s'écrit aussi $P\big((X+1)^2\big) = P(X)P(X+2)$, et donc $(z+1)^2$ est aussi racine de P. De même, $(z-1)^2$ est aussi racine de P.
   On va prouver qu'au moins un des deux nombres complexes $(z+1)^2$ ou $(z-1)^2$ est de module supérieur strict à z. En effet, on a $(z+1)^2 - (z-1)^2 = 4z$, et donc

$$4|z| \leq |z+1|^2 + |z-1|^2.$$

   Ainsi, l'un de ces deux nombres complexes est de module supérieur ou égal à $2|z|$.
   Si $|z| \neq 0$, le résultat est prouvé.
   Sinon, si $z = 0$, on a $(z+1)^2 = 1 > 0$.
   (b) Si P admet une racine (complexe), alors il en admet d'après la question précédente une infinité. C'est donc le polynôme nul. Les polynômes qui sont solutions de l'équation ne peuvent donc être que des polynômes constants, et les seuls polynômes constants solutions sont les polynômes $P(X) = 0$ et $P(X) = 1$.
2. (a) En raisonnant comme dans le premier cas, on voit que si z est racine de P, alors z^2 et $(z+1)^2$ sont aussi solutions. Par récurrence, z^{2^n} et $(z+1)^{2^n}$ seront racines pour tout entier n.
   Puisque le polynôme n'admet qu'un nombre fini de racines, les suites $(z^{2^n})_n$ et $\big((z+1)^{2^n}\big)_n$ ne peuvent prendre qu'un nombre fini de valeurs.

i. la première condition nous dit qu'on a nécessairement $z = 0$ ou $|z| = 1$, donc $z = 0$ ou $z = e^{i\theta}$.

ii. La seconde condition nous dit que $z = -1$ ou $|z + 1| = 1$.

Si $z = 1$, alors $(z + 1)^2 = 4$ est racine et P est nul car possède une infinité de racines.
Si $z = 0$, alors $(z + 1)^2 = 1$ est encore racine et donc P est nul d'après le point précédent.
Ceci montre que toutes les racines sont de modules 1. Donc, si $z = e^{i\theta}$ avec $\theta \in]-\pi, \pi[$, alors $1 + e^{i\theta} = 2\cos\theta/2 e^{i\theta/2}$ est de modules 1, d'où $\cos\theta/2 = 1/2$ car $\theta/2 \in]-\pi/2, \pi/2[$. C'est-à-dire $\theta = \pm 2\pi/3$ et $z = j$ ou $z = j^2$.

(b) Puisque P est à coefficients réels, j et j^2, qui sont des complexes conjugués, doivent être des racines de même multiplicité. On doit donc avoir $P(X) = \lambda(X - j)^n(X - j^2)^n = \lambda(X^2 + X + 1)^n$. Par identification des coefficients dominants, on trouve $\lambda = 1$. Réciproquement, on vérifie facilement que les polynômes $P(X) = (X^2 + X + 1)^n$ sont solutions de l'équation.

■ *Un peu de Géométrie . . .*

Exercice 6.
Soit f l'endomorphisme de $\mathbb{R}^3$ dont la matrice dans la base canonique est donnée par

$$M = \begin{pmatrix} 1 & 1 & -1 \\ -3 & -3 & 3 \\ -2 & -2 & 2 \end{pmatrix}.$$

1. Déterminer une base et une équation cartésienne de $\mathrm{Ker} f$.
2. Déterminer une base et un système d'équations cartésiennes de $\mathrm{Im} f$.
3. Déterminer une base de $\mathrm{Ker}\,(f) \cap \mathrm{Im}\, f$ et en déduire une base de $\mathbb{R}^3$ dans laquelle la matrice de f n'a qu'un coefficient non nul.
4. En déduire une matrice P telle que

$$P^{-1}MP = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

---

1. Soit $(x, y, z) \in \mathbb{R}^3$. On a

$$(x, y, z) \in \mathrm{Ker}\,(f) \iff \begin{cases} x & +y & -z & = 0 \\ -3x & -3y & +3z & = 0 \\ -2x & -2y & +2z & = 0 \end{cases} \iff x + y - z = 0.$$

Donc une équation cartésienne du noyau de f est $x + y - z = 0$ et $\mathrm{Ker}\,(f) = \mathrm{Vect}\,(1, -1, 0), (1, 0, 1)$. Le noyau est donc de dimension 2.

2. On a vu que $\mathrm{Im}\, f$ est engendré par les images par f des vecteurs d'une base. On note $\mathcal{C} = (e_1, e_2, e_3)$ la base canonique de $\mathbb{R}^3$ et on a $f(e_1) = (1, -3, -2) = f(e_2) = -f(e_3)$. On en déduit que

$$\mathrm{Im}\,(f) = \mathrm{Vect}\,(1, -3, -2).$$

Un système d'équations cartésiennes de cet espace vectoriel est

$$\begin{cases} 3x & +y & +0 & = & 0 \\ 2x & +0 & +z & = & 0 \end{cases}.$$

3. On a

$$(x, y, z) \in \mathrm{Ker}\,(f) \cap \mathrm{Im}\, f \iff \begin{cases} x + y - z & = 0 \\ 3x + y & = 0 \\ 2x + z & = 0 \end{cases} \iff \begin{cases} y & = -3x \\ z & = -2x \end{cases}.$$

Donc $\mathrm{Ker}\,(f) \cap \mathrm{Im}\, f = \mathrm{Vect}\,(1, -3, -2)$.
Prenons les vecteurs $b_1 = e_1$, $b_2 = (1, -3, -2)$ et $b_3 = (1, 0, 1)$. On a alors $f(b_1) = b_2$ et $f(b_2) = f(b_3) = 0$. De plus, la famille $\mathcal{B} = (b_1, b_2, b_3)$ est une base de $\mathbb{R}^3$. On a finalement

$$\mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

4. On sait que $\mathrm{Mat}_{\mathcal{C}}(f) = M$ et que $P^{-1}_{\mathcal{C}\to\mathcal{B}}\mathrm{Mat}_{\mathcal{C}}(f)P_{\mathcal{C}\to\mathcal{B}} = \mathrm{Mat}_{\mathcal{B}}(f)$. Donc, en choisissant

$$P = P_{\mathcal{C}\to\mathcal{B}} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & -3 & 0 \\ 0 & -2 & 1 \end{pmatrix},$$

on obtient $P^{-1}MP = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

Exercice 7.
Soit E et F deux $\mathbb{K}$-espaces vectoriels de dimensions finies, on se donne deux bases $\mathcal{B}_1$ et $\mathcal{B}_2$ de E. Soit $\mathcal{C}$ une base de F.

Soit $u \in \mathcal{L}(E, F)$ une application linéaire sur E. Si $A = \mathrm{Mat}_{\mathcal{B}_1,\mathcal{C}}(u)$ et $B = \mathrm{Mat}_{\mathcal{B}_2,\mathcal{C}}(u)$, exprimer B en fonction de A et de la matrice de passage $P_{\mathcal{B}_1\to\mathcal{B}_2}$.

On note $P = P_{\mathcal{B}_1\to\mathcal{B}_2}$. Soit $x \in E$, on note X_1 le vecteur des coordonnées de x dans $\mathcal{B}_1$ et X_2 le vecteur des coordonnées de x dans $\mathcal{B}_2$. On note aussi Y le vecteur des coordonnées de $u(x)$ dans $\mathcal{C}$. On a alors $Y = AX = BX'$.

Or, la formule de changement de base pour un vecteur donne $X = PX'$, donc $AX = APX' = BX'$. Cette relation étant vraie pour tout vecteur X', on obtient $B = AP$.

On peut aussi appliquer directement le résultat du cours :

$$B = Q^{-1}AP,$$

où $Q = P_{\mathcal{C}\to\mathcal{C}} = I_p$, *avec* $p = \dim F$. *On obtient donc* $B = AP$.