Feuille de TD n° 12

Théorème du rang, Factorisation de polynômes, racines

8 décembre 2021

■ *Pour commencer ...*

Exercice 1. Soit E un $\mathbb{K}$-espace vectoriel. Soit $u \in \mathcal{L}(E)$.

1. Montrer que $\mathrm{Ker}\,(u) \subset \mathrm{Ker}\,(u^2)$ et $\mathrm{Im}\,u^2 \subset \mathrm{Im}\,u$.
2. Montrer l'équivalence
$$\mathrm{Ker}\,(u^2) = \mathrm{Ker}\,(u) \Longleftrightarrow \mathrm{Ker}\,(u) \cap \mathrm{Im}\,u = \{0\}.$$
3. Montrer l'équivalence
$$\mathrm{Im}\,u^2 = \mathrm{Im}\,u \Longleftrightarrow \mathrm{Ker}\,(u) + \mathrm{Im}\,u = E.$$
4. Supposons que E est de dimension finie. Montrer que
$$\mathrm{Ker}\,(u) \oplus \mathrm{Im}\,u = E \Longleftrightarrow \mathrm{Ker}\,(u^2) = \mathrm{Ker}\,(u) \Longleftrightarrow \mathrm{Im}\,u^2 = \mathrm{Im}\,u.$$

---

1. Si $u(x) = 0$ alors $u(u(x)) = 0$. De plus, si $y = u^2(x)$ alors $y = u(u(x))$.
2. Supposons que $\mathrm{Ker}\,(u^2) = \mathrm{Ker}\,(u)$. Soit $y \in \mathrm{Ker}\,(u) \cap \mathrm{Im}\,u$, il existe $x \in E$ tel que $y = u(x)$ et $u(y) = 0$. Donc $u^2(x) = 0$ et $x \in \mathrm{Ker}\,(u^2) = \mathrm{Ker}\,(u)$. D'où $y = u(x) = 0$.
Réciproquement, supposons que $\mathrm{Ker}\,(u) \cap \mathrm{Im}\,u = \{0\}$. Soit $x \in \mathrm{Ker}\,(u^2)$. Alors $u(x) \in \mathrm{Ker}\,(u) \cap \mathrm{Im}\,u$ donc $u(x) = 0$ et $x \in \mathrm{Ker}\,(u)$.
3. Supposons que $\mathrm{Im}\,u^2 = \mathrm{Im}\,u$. Soit $y \in E$. Alors $u(y) \in \mathrm{Im}\,u = \mathrm{Im}\,u^2$. Donc il existe $x \in E$ tel que $u(y) = u(u(x))$, c'est-à-dire $u(y - u(x)) = 0$. On a donc $y = y - u(x) + u(x)$ avec $y - u(x) \in \mathrm{Ker}\,(u)$ et $u(x) \in \mathrm{Im}\,u$.
Réciproquement, supposons que $\mathrm{Ker}\,(u) + \mathrm{Im}\,u = E$. Soit $y \in \mathrm{Im}\,u$: $y = u(x)$ avec $x \in E$. Alors $x = a + b$ avec $a \in \mathrm{Ker}\,(u)$ et $b \in \mathrm{Im}\,u$, ce qui donne $y = u(x) = u(b)$. D'où $y \in \mathrm{Im}\,u^2$.
4. On a montré que si $\mathrm{Ker}\,(u) \oplus \mathrm{Im}\,u = E$ alors $\mathrm{Ker}\,(u^2) = \mathrm{Ker}\,(u)$ et $\mathrm{Im}\,u = \mathrm{Im}\,u^2$. En dimension finie, le théorème du rang nous donne
$$\dim \mathrm{Ker}\,(u) + \dim \mathrm{Im}\,u = \dim \mathrm{Ker}\,(u^2) + \dim \mathrm{Im}\,u^2 = \dim E.$$
On a donc $\dim \mathrm{Ker}\,(u) = \dim \mathrm{Ker}\,(u^2)$ si et seulement si $\dim \mathrm{Im}\,u = \dim \mathrm{Im}\,u^2$, ce qui prouve l'équivalence $\mathrm{Ker}\,(u^2) = \mathrm{Ker}\,(u) \Longleftrightarrow \mathrm{Im}\,u = \mathrm{Im}\,u^2$, d'après la question 1.

Exercice 2. Soit $n \in \mathbb{N}^*$. On définit
$$\phi : \begin{array}{ccc} \mathbb{R}_n[X] & \longrightarrow & \mathbb{R}_n[X] \\ P & \longmapsto & P(X+1) - P(X) \end{array}.$$

1. Calculer le degré de $\phi(P)$ en fonction de celui de P.
2. En déduire $\mathrm{Ker}\,(\phi)$.
3. Déterminer $\mathrm{Im}\,\phi$.

---

1. Si P est constant, alors $\phi(P) = 0$. Si $P = \sum_{k=0}^{d} a_k X^k$, avec $d \geq 1$, $a_d \neq 0$ et donc $\deg P = d$, on a
$$\phi(P) = \sum_{k=0}^{d} \left(\sum_{i=k}^{d} \binom{i}{k} a_i - a_k \right) X^k.$$
Le coefficient de X^d est donc 0 et le coefficient de X^{d-1} est $da_d \neq 0$. Donc $\deg \phi(P) = \deg P - 1$.
2. On en déduit que $\phi(P) = 0$ si et seulement si P est constant, donc $\mathrm{Ker}\,(\phi)$ est le sous-espace des polynômes constants.
3. On déduit également de la question 1 que $\mathrm{Im}\,\phi \subset \mathbb{R}_{n-1}[X]$. Or le théorème du rang donne
$$\dim \mathrm{Im}\,\phi = \dim \mathbb{R}_n[X] - \dim \mathrm{Ker}\,(\phi) = n = \dim \mathbb{R}_{n-1}[X],$$
donc $\mathrm{Im}\,\phi = \mathbb{R}_{n-1}[X]$.

Exercice 3. Soit E un $\mathbb{K}$-espace vectoriel et soit $u \in \mathcal{L}(E)$ tel que $u^2 + u - 2\mathrm{Id}_E = 0$.

1. Montrer que u est inversible et calculer u^{-1}.
2. Montrer que $\mathrm{Ker}\,(u - \mathrm{Id}_E)$ et $\mathrm{Ker}\,(u + 2\mathrm{Id}_E)$ sont en somme directe.
3. Montrer que $(u - \mathrm{Id}_E) \circ (u + 2\mathrm{Id}_E) = (u + 2\mathrm{Id}_E) \circ (u - \mathrm{Id}_E) = 0$.
4. En écrivant $x = \frac{1}{3}(u(x) + 2x) - \frac{1}{3}(u(x) - x)$, montrer que $\mathrm{Ker}\,(u - \mathrm{Id}_E) \oplus \mathrm{Ker}\,(u + 2\mathrm{Id}_E) = E$.

1. On a $\frac{1}{2}u^2 + \frac{1}{2}u = \mathrm{Id}_E$, donc $u \circ \left(\frac{u+\mathrm{Id}_E}{2}\right) = \left(\frac{u+\mathrm{Id}_E}{2}\right) \circ u = \mathrm{Id}_E$. Donc u est inversible et $u^{-1} = \frac{u+\mathrm{Id}_E}{2}$.
2. Si $x \in E$ vérifie : $u(x) = x$ et $u(x) = -2x$, alors $3x = 0$ et donc $x = 0$.
3. On a $(u - \mathrm{Id}_E)(u + 2\mathrm{Id}_E) = u^2 + 2u - u - 2\mathrm{Id}_E = 0$. De même pour l'autre composition.
4. On a montré que $\mathrm{Im}\,(u + 2\mathrm{Id}_E) \subset \mathrm{Ker}\,(u - \mathrm{Id}_E)$ et $\mathrm{Im}\,(u - \mathrm{Id}_E) \subset \mathrm{Ker}\,(u + 2\mathrm{Id}_E)$, donc pour tout $x \in E$, $u(x) + 2x \in \mathrm{Ker}\,(u - \mathrm{Id}_E)$ et $u(x) - x \in \mathrm{Ker}\,(u + 2\mathrm{Id}_E)$.

Exercice 4.

1. Soit $n \in \mathbb{N}^*$, soit $x_0, \ldots, x_n$ des éléments de $\mathbb{K}$ différents deux à deux. En étudiant l'application linéaire $\varphi : \begin{array}{ccc} \mathbb{K}_n[X] & \longrightarrow & \mathbb{K}^{n+1} \\ P & \longmapsto & (P(x_0), \ldots, P(x_n)) \end{array}$, montrer que pour tout $(y_0, \ldots, y_n) \in \mathbb{K}^{n+1}$, il existe un unique polynôme L de degré inférieur ou égal à n tel que pour tout $i \in [\![0, n]\!]$, $L(x_i) = y_i$.
2. Soient a, b, c trois réels distincts et soit $(\alpha, \beta, \gamma, \delta) \in \mathbb{R}^4$. Montrer qu'il existe un unique polynôme $P \in \mathbb{R}_3[X]$ tel que $P(a) = \alpha$, $P(b) = \beta$, $P(c) = \gamma$ et $P'(c) = \delta$.

---

1. Soit $P \in \mathbb{K}_n[X]$ tel que $\varphi(P) = 0$. Alors P a $n+1$ racines distinctes et $\deg P \leq n$, ce qui implique que $P = 0$. Ainsi, φ est injective. Or $\dim \mathbb{K}_n[X] = \dim \mathbb{K}^{n+1}$, donc φ est bijective. On en déduit le résultat.
2. On définit l'application linéaire
$$\theta : \begin{array}{ccc} \mathbb{R}_3[x] & \longrightarrow & \mathbb{R}^4 \\ P & \longmapsto & (P(a), P(b), P(c), P'(c)) \end{array}.$$
Soit $P \in \mathrm{Ker}\,(\theta)$, alors $P(a) = P(b) = P(c) = 0$, donc $P = \lambda(X-a)(X-b)(X-c)$ avec $\lambda \in \mathbb{R}$, car $\deg P \leq 3$. Maintenant, $P'(c) = 0 = \lambda(c-a)(c-b)$ donc $\lambda = 0$ et $P = 0$. Ainsi θ est injective et puisque $\dim \mathbb{R}_3[X] = \dim \mathbb{R}^4$, θ est bijective.

Exercice 5. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Soit u, $v \in \mathcal{L}(E)$ deux endomorphismes de E tels que
$$E = \mathrm{Ker}\,(u) + \mathrm{Ker}\,(v) = \mathrm{Im}\, u + \mathrm{Im}\, v.$$
Montrer que les deux sommes sont directes.

On sait que si F et G sont deux sous-espaces vectoriels de E, on a $\dim(F+G) \leq \dim F + \dim G$. On en déduit que
$$\mathrm{rg}\, u + \mathrm{rg}\, v \geq \dim E \quad \text{et} \quad \dim \mathrm{Ker}\,(u) + \dim \mathrm{Ker}\,(v) \geq \dim E.$$
Or le théorème du rang donne
$$\dim \mathrm{Ker}\,(u) + \mathrm{rg}\, u + \dim \mathrm{Ker}\,(v) + \mathrm{rg}\, v = 2 \dim E.$$
On en déduit que $\mathrm{rg}\, u + \mathrm{rg}\, v = \dim E$ et $\dim \mathrm{Ker}\,(u) + \dim \mathrm{Ker}\,(v) = \dim E$, donc les sommes sont directes.

Un peu d'Algèbre . . .

Exercice 6.
Calculer les *pgcd* suivants :

1. $pgcd(X^4 - 3X^3 + 5X + 2, (X-2)(X-3))$
2. $pgcd(X^n - 1, (X-1)^n)$, $n \geq 1$
3. $pgcd(X^n - nX - 1, (X^n - nX - 1)')$, $n \geq 1$
4. $pgcd((X-2)^2(X-3), ((X-2)^2(X-3))')$

---

1. 2 et 3 ne sont pas racines de $X^4 - 3X^3 + 5X + 2$, donc $pgcd(X^4 - 3X^3 + 5X + 2, (X-2)(X-3)) = 1$.
2. On a $X^n - 1 = (X-1)(1 + X + \ldots + X^{n-1})$. Donc 1 est une racine simple de $X^n - 1$. On a donc $pgcd(X^n - 1, (X-1)^n) = X - 1$.
3. On a $(X^n - nX - 1)' = n(X^{n-1} - 1)$. Soit $d = pgcd(X^n - nX - 1, (X^n - nX - 1)')$. D'après les propriétés de divisibilité du *pgcd*, on a $d \mid (X^n - nX - 1) - X(X^{n-1} - 1) = -nX - 1 + X = X(1-n) - 1$.
Si $n = 1$, on a donc $d = 1$.
Si $n \geq 2$, comme d est unitaire, on a $d = 1$ ou $d = X - \frac{1}{1-n}$.
Si $n = 2$ on a $\frac{1}{1-n} = -1$. Mais -1 n'est pas une racine de $X^{n-1} - 1 = X - 1$, donc on a $d = 1$.
Si $n > 2$, on a $\frac{1}{1-n} \in]-1, 0[$. Donc, ce nombre réel n'est pas une racine de $X^{n-1} - 1$ (sa valeur absolue ne vaut pas 1). A nouveau, on obtient que $d = 1$.
4. On a $(X-2)^2(X-3))' = 2(X-2)(X-3) + (X-2)^2 = (X-2)(2X - 6 + X - 2) = (X-2)(3X-8) = 3(X-2)(X - \frac{8}{3})$. Ainsi, on a $pgcd((X-2)^2(X-3), ((X-2)^2(X-3))') = (X-2)$.
On retrouve le résultat de cours à ce sujet.

Exercice 7.
Factoriser les polynômes suivants. Dire si le polynôme est irréductible, scindé, à racines simples.

1. $X^2 - 3X + 1$ dans $\mathbb{R}[X]$
2. $X^3 - 2X^2 + 1$ dans $\mathbb{Q}[X]$
3. $X^n - z^n$ dans $\mathbb{C}[X]$, pour $z \neq 0$ et $n \geq 1$.
4. $X^4 + 1$ dans $\mathbb{Q}[X]$, dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.
5. $X^3 + 15X - 5$ dans $\mathbb{Q}[X]$. (on pourra chercher l'ensemble des racines de ce polynôme sur $\mathbb{Q}$)

---

1. Le discriminant de ce polynôme vaut $5 > 0$. Donc, $X^2-3X+1 = (X-\frac{3-\sqrt{5}}{2})(X-\frac{3+\sqrt{5}}{2})$. Ce polynôme n'est pas irréductible, mais est scindé à racines simples.
2. On remarque que 1 est une racine de ce polynôme. Donc, $X^3 - 2X^2 + 1 = (X-1)(X^2 + aX + b)$.
En développant le second polynôme, on trouve alors $b = -1$ puis $a = -1$. Le discriminant de $X^2 - X - 1$ vaut -3, qui n'est pas un carré dans $\mathbb{Q}$. Ce polynôme est donc irréductible, et on a $X^3 - 2X^2 + 1 = (X-1)(X^2 - X - 1)$. Ce polynôme n'est pas irréductible et pas scindé.
3. On a $X^n - z^n = z^n(\left(\frac{X}{z}\right)^n - 1) = z^n \Pi_{i=0}^{n-1}(\frac{X}{z} - \exp(\frac{2.i.k\pi}{n})) = \Pi_{i=0}^{n-1}(X - z\exp(\frac{2.i.k\pi}{n}))$.
Ce polynôme n'est pas irréductible, mais est scindé à racines simples.
4. Dans $\mathbb{C}[X]$, on a $X^4 + 1 = X^4 - z^4$, pour $z = \exp(\frac{i\pi}{4})$.
Donc, $X^4 + 1 = X^4 - z^4 = \Pi_{i=0}^{3}(X - z.exp(\frac{2i.k.\pi}{4}) = \Pi_{i=0}^{3}(X - exp(\frac{i(2k+1)\pi}{4}))$. Ce polynôme n'est pas irréductible, mais est scindé à racines simples.
Dans $\mathbb{R}[X]$, on a $X^4 + 1 = X^4 + 2X^2 + 1 - 2X^2 = (X^2+1)^2 - 2X^2 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$.
Ces deux polynômes sont de discriminant strictement négatif, donc sont irréductibles sur $\mathbb{R}$.
Ainsi, $X^4 + 1$ n'est pas irréductible sur $\mathbb{R}$ mais n'est pas scindé non plus.
Dans $\mathbb{Q}[X]$, le polynôme $X^4 + 1$ est irréductible.
Si ce polynôme était réductible, on aurait par l'absurde $X^4 + 1 = P(X)Q(X)$ avec P, Q de degré ≥ 1. Cette factorisation se passe dans $\mathbb{Q}[X]$, donc elle est aussi vraie dans $\mathbb{R}[X]$.
On aurait donc $P(X) = X^2 \pm \sqrt{2}X + 1$ et $Q(X) = X^2 \pm \sqrt{2}X + 1$, ce qui est impossible car $P, Q \in \mathbb{Q}[X]$ et $\sqrt{2} \notin \mathbb{Q}$.
5. Montrons que ce polynôme est irréductible sur $\mathbb{Q}[X]$. Comme il est de degré 3, si $X^3 + 15X - 5$ est réductible sur $\mathbb{Q}[X]$, il se factoriserait en $P(X).Q(X)$ avec P, Q de degrés 1 et 2 (ou 2 et 1).
Donc, ce polynôme aurait une racine dans $\mathbb{Q}$.
Soit $x \in \mathbb{Q}$. On écrit $x = \frac{p}{q}$ avec $p \in \mathbb{Z}$, $q > 0$, et $pgcd(p, q) = 1$.
Si x est une racine de $X^3 + 15X - 5$, on a alors $x^3 + 15x - 5 = 0$.
Cela donne $p^3 + 15pq^2 - 5q^3 = 0$.
De $p^3 = -15q^2p + 5q^3$ on en déduit que $q \mid p^3$. Comme p et q sont premiers entre eux, on a donc $q \mid 1$, c'est-à-dire $q = 1$.
De $p^3 + 15pq^2 = 5q^3$ on en déduit que $p \mid 5q^3$. Comme p et q sont premiers entre eux, on a donc $p \mid 5$, c'est-à-dire $p = \pm 1$ ou $p = \pm 5$.
Mais $1, -1, 5, -5$ ne sont pas des racines de $X^3 + 15X - 5$.
Ce polynôme n'a donc pas de racines dans $\mathbb{Q}$, et est donc irréductible sur $\mathbb{Q}$.

Exercice 8.

1. Soit $n \geq 1$. Le polynôme $P(X) = \sum_{k=0}^{n} \frac{1}{k!} X^k$ a-t-il des racines multiples ?
2. Soit $P \in \mathbb{R}[X]$ non-nul tel que $P' \mid P$. Montrer que P ne possède qu'un seul facteur irréductible P_1.
Que peut-on dire sur $\deg(P_1)$?.
Trouver tous les polynômes $P \in \mathbb{K}[X]$ non-nuls tels que $P' \mid P$.
3. Soit $Q \in \mathbb{R}[X]$, de degré n. Montrer que $Q(X+1) = \sum_{k=0}^{n} \frac{Q^{(k)}(X)}{k!}$. (On pourra utiliser des applications linéaires, ou des bases.)

---

1. On a $P'(X) = \sum_{k=1}^{n} \frac{k}{k!} X^{k-1} = \sum_{m=0}^{n-1} \frac{1}{m!} X^m$.
Le polynôme P a des racines multiples si et seulement si P et P' ont des racines communes.
Or, on a $P(X) - P'(X) = \frac{1}{n!} X^n$, dont la seule racine est 0. Ainsi, si x est une racine commune à P et à P', on doit avoir $\frac{x^n}{n!} P(x) - P'(x) = 0 - 0 = 0$. x doit être une racine de X^n, c'est-à-dire $x = 0$.
Comme 0 n'est pas racine du polynôme P, ce polynôme n'a donc pas de racines multiples.
2. Si P est un polynôme constant, on a $P'(X) = 0$ et cela n'est pas vrai. On a donc $\deg(P) = n > 0$.
On écrit $P = a_n P_1^{\alpha_1} \ldots P_r^{\alpha_r}$ la décomposition de P en produit de facteurs irréductibles.
D'après le cours, on a $pgcd(P', P) = P_1^{\alpha_1 - 1} \ldots P_r^{\alpha_r - 1}$.
Si $P' \mid P$ on a donc $pgcd(P', P)$ associé à P' (égaux à un scalaire près).
Comme $\deg(P) = n > 0$, on a $\deg(P') = n - 1 \geq 0$. Cela implique donc que $P_1^{\alpha_1 - 1} \ldots P_r^{\alpha_r - 1}$ est de degré $n - 1$.
Or, ce polynôme est de degré $n - \deg(P_1) - \deg(P_2) - \ldots - \deg(P_r)$.
Comme $\deg(P_1) \geq 1$, on doit donc avoir $r = 1$ et $\deg(P_1) = 1$.
Ainsi, P ne possède qu'un seul facteur irréductible, et ce facteur est de degré 1 : $P(X) = a_n(X - b)^{\alpha_1}$.

Réciproquement, si P est de cette forme, on a $P'(X) = a_n.\alpha_1(X-b)^{\alpha_1 - 1}$.
On trouve bien que P' divise P (et que P' et $pgcd(P', P)$ sont associés).

3. La fonction $f : Q \mapsto \sum_{k=0}^{n} \frac{Q^{(k)}(X)}{k!}$ est une application linéaire sur $\mathbb{R}_n[X]$ (la fonction $Q \mapsto Q'$ est une application linéaire, et f est une combinaison linéaire de composées de $Q \mapsto Q'$).
   On veut en fait montrer que pour tout $Q \in \mathbb{R}_n[X]$, on a $f(Q) = Q$, c'est-à-dire que $f = Id_{\mathbb{R}_n[X]}$.
   Pour cela, il suffit de le montrer sur une base de $\mathbb{R}_n[X]$. On prend la base canonique $(1, X, \dots, X^n)$.
   Pour $0 \leq m \leq n$, on a
   $(X+1)^m = \sum_{k=0}^{m} \binom{m}{k} 1^k X^{m-k} = \sum_{k=0}^{m} \frac{m(m-1)\dots(m-k+1)}{k!} X^{m-k}$.
   Comme on a $(X^m)^{(k)} = X^{m-k} m(m-1)\dots(m-k+1)$, on obtient $(X+1)^m = \sum_{k=0}^{m} \frac{1}{k!}(X^m)^{(k)}$.
   Comme on a $(X^m)^{(k)} = 0$ pour $k \geq m+1$, et comme $m \leq n$, on obtient $(X+1)^m = \sum_{k=0}^{n} \frac{1}{k!}(X^m)^{(k)}$.
   On a donc montré que $f(X^m) = X^m$ pour tout $0 \leq m \leq n$. Donc les applications linéaires f et Id sont égales sur une base de $\mathbb{R}_n[X]$, donc ces applications linéaires sont égales.