# Algèbre linéaire, TD1, 15/1/2021

Bonjour !

- Rappels sur l'arithmétique des polynômes
- Algèbre $\mathcal{L}(E)$ quand $E$ est de dim finie
- Exos du poly.

Fixons $\mathbb{K}$ un corps.
$\mathbb{K}[X]$ anneau de polynômes, même une $\mathbb{K}$-algèbre
Déf formelle : un polynôme est une suite (de coeffs) dans $\mathbb{K}$ nulle presque partout.

Propriétés des anneaux :
intègre
commutatif

euclidien — déf : $\exists$ "valuation" qui permet de faire une sorte de div. eucl.
$\Downarrow$ pas compliqué
principal — déf : tout idéal est engendré par un élément
$\Downarrow$ compliqué
factoriel — déf : $\exists$ irréductibles tq tout élément de l'anneau s'écrit de façon unique comme un invasible fois un produit d'irréductibles

inversible

$\mathbb{K}[X]$ est euclidien.

Notions apparaissant en arithmétique :
nombres premiers dans $\mathbb{Z}$ $\rightsquigarrow$ se généralise en "irréductibles"
idéaux premiers

Théorème de Bézout
Algorithme d'Euclide
pgcd

Pour A factoriel, on peut définir le pgcd de 2 éléments (à inversible près)
Pour A principal, on dispose du théorème de Bézout,
Pour A euclidien, on dispose de l'algorithme d'Euclide pour calculer le pgcd.

Dans $\mathbb{K}[X]$, les inversibles sont les polynômes constants non nuls.
les irréductibles ~~sont~~ dépendent fortement de $\mathbb{K}$, pas forcément faciles à décrire.

* Pour $\mathbb{C}[X]$, quels sont les polynômes qui ne s'écrivent pas comme produit de 2 polynômes non constants ? Ce sont exactement ceux de degré 1 (car ceux de degré $\geq 2$ ont au moins 1 racine, disons $\lambda \in \mathbb{C}$, et $(X-\lambda)$ peut être mis en facteur).

Rem : Idem sur un corps algébriquement clos.

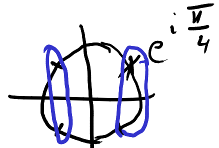
Fondamental

* Pour $\mathbb{R}[X]$, les irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif

Rem : Si P de degré $\geq 2$ a une racine, alors P n'est pas irréductible.
càd P irréductible de degré $\geq 2$ implique que P n'a pas de racine.

* Pour $P \in \mathbb{R}[X]$ de degré $\geq 3$ impair, on sait que P a une racine réelle donc P est réductible.
* Pour $P \in \mathbb{R}[X]$ de degré pair, s'il n'y a aucune racine réelle, on peut écrire la décomposition dans $\mathbb{C}[X]$ puis regrouper les termes $(X-\lambda)(X-\bar{\lambda})$, qui sont de discriminant négatif.

Ex $P = X^4 + 1 \in \mathbb{R}[X]$. Décomposition en irréductibles ?
Indication : passage par les complexes.




une racine va avec son conjugué.

$$X^4-\underbrace{(-1)}_{=e^{i\pi}} = X^4+1 = (X^2-i)(X^2+i)$$
$$= \left(X-e^{i\frac{\pi}{4}}\right)\left(X-e^{-i\frac{5\pi}{4}}\right)(X-\dots)\dots$$
$$= \prod_{\lambda \text{ racine } 4^e \text{ de } -1}(X-\lambda)$$

vont ensemble

ensemble

$$= \left(X-e^{i\frac{\pi}{4}}\right)\left(X-e^{i\frac{3\pi}{4}}\right)\left(X-e^{i\frac{5\pi}{4}}\right)\left(X-e^{i\frac{7\pi}{4}}\right)$$ décomp dans $\mathbb{C}[X]$

$$(X-\lambda)(X-\overline{\lambda})$$
$$= X^2-\lambda X-\overline{\lambda}X+\lambda\overline{\lambda}$$
$$= X^2-X(2\operatorname{Re}\lambda)+|\lambda|^2$$
$\in \mathbb{R}[X]$.
de discriminant négatif,

$$= \left(X-e^{i\frac{\pi}{4}}\right)\left(X-\overline{e^{i\frac{\pi}{4}}}\right)\left(X-e^{i\frac{3\pi}{4}}\right)\left(X-\overline{e^{i\frac{3\pi}{4}}}\right)$$
?
$$= (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$$ décomp. dans $\mathbb{R}[X]$

**Prop** Si $\lambda \in \mathbb{C}$ est racine de $P\in\mathbb{R}[X]$, alors $\overline{\lambda}$ aussi est racine de $P$.

**Rem** : Bcp plus compliqué pour les corps en général.
Les polynômes de degrés 1 sont toujours irréductibles.

**Rappel** Th de division euclidienne dans $\mathbb{K}[X]$

**Th** : Pour $P$ et $Q$ dans $\mathbb{K}[X]$, avec $Q$ non nul
$\exists!(G,R)\in(\mathbb{K}[X])^2$, $P=QG+R$ avec $\deg(R)<\deg(Q)$.

---

**Algèbres**
* $\mathbb{K}[X]$
* Pour $E$ un $\mathbb{K}$-ev, $L(E)$ est une algèbre.
* ~~$GL_n(\mathbb{R})$~~ $M_n(\mathbb{K})$

**Prop** : Pour $E$ de dim finie, $L(E)$ est aussi de dim finie.

**Preuve** : Disons $n=\dim E$. **Mq** $\dim L(E)=n^2$

On se fixe une base de $E$.

$$\begin{array}{rcl} L(E) & \to & M_n(\mathbb{K}) \quad \text{iso.} \\ f & \mapsto & \underbrace{\mathcal{M}_\beta(f)}_{\dim n^2} \end{array}$$

On en déduit que $L(E)$ est de dim $n^2$.

---

## Exos du poly

**Exo 1** $E = \mathbb{K}[X]$ espace vectoriel

$D$ opérateur de dérivation formelle

1) Mq si $\mathbb{K}$ est de caractéristique nulle, alors $D$ n'a pas de polynôme annulateur non nul.

2) Que se passe-t-il en caractéristique positive ?

**Dérivation de polynômes**

On sait dériver les fonctions, donc notamment les fonctions polynômes.

$(x \mapsto x^n)' = (x \mapsto n x^{n-1})$ pour $n \in \mathbb{N}^*$

La dérivée formelle d'un monôme $X^n$ ($n \in \mathbb{N}^*$) est $n X^{n-1}$.

de $X^0$ est $0$.

La dérivée formelle est linéaire.

$D : \mathbb{K}[X] \to \mathbb{K}[X]$ appl. lin.

1) Dire que $D$ n'a pas de polynôme annulateur non nul est équivalent à

$\operatorname{Ker}(ev_D) = \{0\}$ où $ev_D : \mathbb{K}[X] \to \mathcal{L}(\mathbb{K}[X]) = E$

$P \mapsto P(D)$

Indication : Par l'absurde.

B) * Supposons qu'on a $P$ non nul polynôme annulateur de $D$. En utilisant le degré de $P$, trouver une contradiction pour arriver au fait que $P$ ne peut pas être annulateur.

A) * Pour $P = X^2$, quels polynômes sont annulés par $P(D)$ ?

Chercher aussi l'exo 4.2 (du poly envoyé)

Pause jusqu'à 10h50. (je suis de retour ~~dès 10h40~~)

Indication A) Pour $P = X^2$, $P(D) = D \circ D$

Les polynômes annulés (càd envoyés sur le polynôme nul) par $D \circ D$ sont les polynômes de degré $\leq 1$.

Si $\mathbb{K}$ est de carac $0$, $n(n-1)$ est toujours non nul.
Si $\mathbb{K}$ est de carac $\neq 0$, alors $\varphi(n(n-1))$ peut être nul.

Rem $(D \circ D)(X^n) = D(nX^{n-1}) = \underbrace{n(n-1)}_{\neq 0} X^{n-2}$ pour $n \geq 2$.

B) Supposons qu'il existe $P \neq 0$ dans $\mathbb{K}[X]$ polynôme annulateur de $D$.

Disons $\deg P = n \in \mathbb{N}^*$.

Dire que $P$ est annulateur dit que $P(D) = 0 \in \mathcal{L}(\mathbb{K}[X])$.

On écrit $P = \sum_{i=0}^{n} a_i X^i$.

D'où $P(D) = a_0 \, Id + \sum_{i=1}^{n} a_i D^i$ (où $D^i = D \circ \dots \circ D$)

Pour $f = X^n$, $P(D)(f) = a_0 X^n + \sum_{i=1}^{n} a_i \underbrace{D^i(X^n)}$ $= n! \neq 0$ si car $\mathbb{K} = 0$.

$= a_0 X^n + \sum_{i=1}^{n-1} \dots X^{n-i} + a_n n! X^0$

$\boxed{= n(n-1)\dots(n-i+1) X^{n-i} \quad (\text{ici } n-i \geq 0)}$ $\neq 0$

Dire que $P$ est de degré $n$ impose $a_n \neq 0$.

Et $a_n \neq 0$ implique qu'on a un terme non nul dans $P(D)(f)$, terme constant $a_n n!$.

Contradiction avec le fait que $P$ soit annulateur de $D$.

<u>Conclusion</u> Pour $\mathbb{K}$ de caractéristique nulle, on a que la dérivation formelle n'a pas de polynôme annulateur non nul.

Rappel sur la caractéristique d'un anneau unitaire

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow A \quad \text{morphisme d'anneau} \\ 1 &\longmapsto 1_A \\ n &\longmapsto n.1_A = \underbrace{1_A + \dots + 1_A}_{n \text{ fois quand } n \geq 0} \end{aligned}$$

<u>Q:</u> $\varphi$ injectif ?

$\operatorname{Ker} \varphi$ un idéal de $\mathbb{Z}$.

$= \{0\}$ ou $d\mathbb{Z}$ pour $d \in \mathbb{N}^*$.

ici on dit que $A$ est de caractéristique nulle.

$\hookrightarrow$ ici on dit que la caractéristique est $d$. et $\operatorname{Ker} \varphi = d\mathbb{Z}$

<u>Rem</u> : Si $A$ est intègre alors $d$ est premier.

(notamment pour $A$ un corps et $\operatorname{Ker} \varphi = d\mathbb{Z}$)

Pour $A = \mathbb{K}$, quand on écrit $nX^i$ avec $n \in \mathbb{Z}$,

c'est à la fois $nX^i = X^i + \dots + X^i$ (si $n \geq 0$)

et aussi $nX^i = \varphi(n).X^i$ $\leftarrow$ mult par un scalaire dans la struct. d'e.v.

(par la condition de compatibilité de la structure d'algèbre)

2) Pour $\mathbb{K}$ de caractéristique $p>0$, montrons que $D^p = 0 \in \mathcal{L}(\mathbb{K}[X])$

$D^p = D \circ D \circ \dots \circ D$

Sur $f = X^n$, $D^p(X^n) = \begin{cases} 0 & \text{si } n<p \\ p!\, X^{n-p} & \text{si } n \geq p \end{cases}$

$= 0$ car car $\mathbb{K} = p$.

rigoureusement $\varphi(p!)$ et $p! \in p\mathbb{Z} = \ker \varphi$.

On a ici que $D$ a pour polynôme annulateur $X^p$.

(On peut montrer que c'est même le polynôme minimal de $D$).

Exo 2

$E$ $\mathbb{K}$-ev de dim finie

$E = F \oplus G$ $\quad f : E \to E$ tq $F$ et $G$ stables par $f$

$f_{|F}$ et $f_{|G}$

Mq $\mu_f = \text{ppcm}(\mu_{f_{|F}}, \mu_{f_{|G}})$

Obs : $\mu_f$ annule $f_{|F}$ et $f_{|G}$

Donc $\mu_{f_{|F}}$ divise $\mu_f$ et $\mu_{f_{|G}}$ divise $\mu_f$.

Donc $\mu_f$ est un multiple commun à $\mu_{f_{|F}}$ et $\mu_{f_{|G}}$

càd $\mu_f$ ~~divise~~ est un multiple de $\text{ppcm}(\mu_{f_{|F}}, \mu_{f_{|G}})$

càd $\text{ppcm}(\mu_{f_{|F}}, \mu_{f_{|G}})$ divise $\mu_f$.

Lemme : Pour $P \in \mathbb{K}[X]$, $P(f) = 0 \iff (P(f_{|F}) = 0 \text{ et } P(f_{|G}) = 0)$

Preuve : Si $x \in E$, on a existence et unicité de $x_F$ et $x_G$ tq $x = x_F + x_G$

$P(f)(x) = 0 \iff \begin{cases} P(f)(x_F) = 0 \\ P(f)(x_G) = 0 \end{cases} \iff \begin{cases} P(f_{|F})(x_F) = 0 \\ P(f_{|G})(x_G) = 0 \end{cases}$

La condition $P(f)(x) = 0 \; \forall x \in E$ revient exactement à la condition à droite $\forall x_F \in F$ et $\forall x_G \in G$.

Raisonnement en termes d'idéaux :

$P \in (\underbrace{\mu_f}_{\text{idéal engendré}}) \iff P$ annule $f$

$\iff P(f) = 0 \in \mathcal{L}(E)$

$\iff \begin{cases} P(f_{|F}) = 0 & \in \mathcal{L}(F) \\ P(f_{|G}) = 0 & \in \mathcal{L}(G) \end{cases}$ Lemme

$\iff P$ annule $f_{|F}$ et $f_{|G}$

$\iff P \in (\mu_{f_{|F}})$ et $P \in (\mu_{f_{|G}})$

$\iff P \in (\mu_{f_{|F}}) \cap (\mu_{f_{|G}}) = (\mathrm{ppcm}(\mu_{f_{|F}}, \mu_{f_{|G}}))$

Donc $(\mu_f) = (\mathrm{ppcm}(\ldots))$

Donc $\mu_f = \mathrm{ppcm}(\mu_{f_{|F}}, \mu_{f_{|G}})$.

Rem On aurait aussi pu mq $\mathrm{ppcm}(\mu_{f_{|F}}, \mu_{f_{|G}})$ annule $f$.
(utilise la prop de somme directe)

Pour la prochaine fois, exo 4.3 à chercher, et début du 4.4