# éléments de mathématiques

## I Equation caractéristique

Soient E un K-espace vectoriel, f un endomorphisme de E et $P \in K[X]$. ($K = \mathbb{R}$ ou $\mathbb{C}$ en général)
On notera Id pour l'endomorphisme identité de E.

Quelques rappels sur les polynômes d'endomorphismes :
Rappelons que l'on peut considérer l'endomorphisme $P(f)$ en convenant que :
$f^0 = Id$, $f^1 = f$, $f^2 = fof$, $f^3 = fofof$ et plus généralement $f^n = fofo\ldots of$ (n fois)

Ainsi, si $P(x) = 2x^2 - 4$, on a alors $P(f) = 2f^2 - 4\,Id$
Si $P, Q \in K[X]$ alors on a : **$PQ(f) = P(f) \circ Q(f)$**
En effet :
● Si P est un monôme : on peut écrire $P(x) = a x^n$ et $Q(x) = b_0 + b_1 x + \ldots + b_m x^m$ où $a, b_i \in K$ et $n, m \in \mathbb{N}$
D'où $[PQ](x) = P(x)Q(x) = ab_0 x^n + ab_1 x^{n+1} + \ldots + ab_m x^{n+m}$
donc $PQ(f) = ab_0 f^n + ab_1 f^{n+1} + \ldots + ab_m f^{n+m}$
Or $P(f) \circ Q(f) = a f^n (b_0 Id + b_1 f + \ldots + b_m f^m) = ab_0 f^n + ab_1 f^{n+1} + \ldots + ab_m f^{n+m}$ par linéarité des $f^i$.
Donc on a bien : $PQ(f) = P(f) \circ Q(f)$
● Si $P = P_1 + P_2 + \ldots + P_n$ où les $P_i$ sont des monômes alors on a :
$P(f) \circ Q(f) = (P_1(f) + P_2(f) + \ldots + P_n(f)) \circ Q(f) = P_1(f) \circ Q(f) + P_2(f) \circ Q(f) + \ldots + P_n(f) \circ Q(f)$
$= P_1 Q(f) + P_2 Q(f) + \ldots + P_n Q(f) = (P_1 Q + P_2 Q + \ldots + P_n Q)(f) = PQ(f)$

**Théorème de décomposition des noyaux** : Soient $P_1 ; P_2 ; \ldots ; P_n$ des polynômes premiers entre eux deux à deux. On a : $\ker(P_1 P_2 \ldots P_n(f)) = \ker(P_1(f)) \oplus \ker(P_2(f)) \ldots \oplus \ker(P_n(f))$
En effet : pour n = 2 :
● $P_1$ et $P_2$ étant premiers entre eux le théorème de Bezout permet d'affirmer qu'il existe des polynômes $A_1$ et $A_2$ tels que $A_1 P_1 + A_2 P_2 = 1$
D'où $A_1 P_1(f) + A_2 P_2(f) = Id$ et donc $A_1 P_1(f)(x) + A_2 P_2(f)(x) = x$
Notons alors $x_1 = A_1 P_1(f)(x)$ et $x_2 = A_2 P_2(f)(x)$ donc $x = x_1 + x_2$
Si $x \in \ker(P_1 P_2(f))$ alors on a : $P_2(f)(x_1) = P_2(f) \circ A_1 P_1(x) = A_1 P_1 P_2(f)(x) = 0$
et donc $x_1 \in \ker(P_2(f))$.
De même $x_2 \in \ker(P_1(f))$
D'où $\ker(P_1 P_2(f)) \subset \ker(P_1(f)) + \ker(P_2(f))$
● Inversement : si $x \in \ker(P_2(f))$, alors $P_1 P_2(f)(x) = 0$ et donc $\ker(P_2(f)) \subset \ker(P_1 P_2(f))$ et par suite $\ker(P_1(f)) + \ker(P_2(f)) \subset \ker(P_1 P_2(f))$
Donc $\ker(P_1 P_2(f)) = \ker(P_1(f)) + \ker(P_2(f))$
● La somme $\ker(P_1(f)) + \ker(P_2(f))$ est directe car si $x \in \ker(P_1(f)) \cap \ker(P_2(f))$ alors $x_1 = x_2 = 0 = x$
D'où $\ker(P_1 P_2(f)) = \ker(P_1(f)) \oplus \ker(P_2(f))$
● Supposons l'égalité établie pour n, alors puisque $P_1 P_2 \ldots P_n$ et $P_{n+1}$ sont premiers entre eux on peut écrire : $\ker(P_1 P_2 \ldots P_{n+1}(f)) = \ker(P_1 P_2 \ldots P_n(f)) \oplus \ker(P_{n+1}(f)) = \ker(P_1(f)) \oplus \ldots \oplus \ker(P_{n+1}(f))$
et l'égalité est établie au rang n + 1 : le théorème est donc démontré par récurrence.

Objectif : On veut résoudre l'équation : $P(f)(x) = 0$

Définition : L'équation $P(x) = 0$ s'appelle l'équation caractéristique pour l'équation $P(f)(x) = 0$.

On cherche en générale les solutions de l'équation $P(f)(x) = 0$ sous la forme de vecteur propre de f.

Théorème :
1° ) Si r est une racine de P et que $x_r$ est un vecteur propre de f associé à r, alors $x_r$ est solution de l'équation $P(f)(x) = 0$.
2° ) Si P est scindé en racines simples alors l'ensemble des solutions de $P(f)(x) = 0$ est l'espace vectoriel engendré par les vecteurs propres associés à chaque racine de P.
3° ) Plus généralement, si P est scindé alors l'ensemble des solutions de $P(f)(x) = 0$ est l'espace vectoriel engendré par les espaces caractéristiques associés à chaque racine de P.

Preuve : 1° ) On a $f(x_r) = r x_r$ et on peut écrire $P(x) = Q(x)(x - r)$ où $Q \in K[X]$.
Donc $P(f)(x_r) = Q(f) \circ (f(x_r) - r x_r) = Q(f)(r x_r - r x_r\ 0) = Q(f)(0) = 0$.
2° ) On peut écrire $P = a P_1 P_2 \dots P_n$ où $a \in K$ et $P_i(x) = x - a_i$ pour $1 \le i \le n$ et $a_p \neq a_q$ si $1 \le p \neq q \le n$
Les polynômes $P_i$ , $1 \le i \le n$, sont premiers entre eux deux à deux, donc d'après le théorème de décomposition des noyaux on a : $\ker(P(f)) = \ker(P_1(f)) \oplus \ker(P_2(f)) \dots \oplus \ker(P_n(f))$.
$\ker(P_i(f))$ n'étant autre que l'espace propre de $P_i(f)$ associé à $a_i$, on a donc bien le résultat annoncé.
3° ) Même chose que pour 2° ) sauf que $P_i(x) = (x - a_i)^{n_i}$ et donc $\ker(P_i(f))$ est l'espace caractéristique associé à la racine $a_i$.

Remarque : ceci n'est autre qu'une généralisation du théorème bien connu des collégiens : "un produit de facteur est nul si et seulement si un de ses facteurs est nul".

**Exemples classiques**

1° ) équation différentielle
On veut résoudre par exemple $y'' + y' - 2y = 0$.
On prend :

- $E = C^2(\mathbb{R})$ l'espace vectoriel des fonctions réelles deux fois continûment dérivables.
- $f$ est l'endomorphisme de dérivation sur E : $f(y) = y'$
- $P(x) = x^2 + x - 2 = (x - 1)(x + 2)$ donc P est scindé en racine simple.

Soit $r \in \mathbb{R}$ et $x_r$ est la solution de $f(y) = r y$
On a donc : $y' = r y$ donc $x_r$ est la fonction $x \mapsto a e^{rx}$ où $a \in \mathbb{R}$.
Ainsi, les fonctions $x_1 : x \mapsto a e^{x}$ et $x_{-2} : x \mapsto b e^{-2x}$ engendrent les solutions de l'équation différentielle puisque $1$ et $-2$ sont les racines de P.

2° ) Suites récurrentes
On veut trouver les suites réelles $(a_n)_{n \in \mathbb{N}}$ telles que : $\forall n \in \mathbb{N},\ a_{n+2} + a_{n+1} - 2 a_n = 0$
On prend :

- E l'espace vectoriel des suites réelles.
- f l'endomorphisme sur E défini par : $f((a_n)_{n \in \mathbb{N}}) = (a_{n+1})_{n \in \mathbb{N}}$
- $P(x) = x^2 + x - 2 = (x - 1)(x + 2)$ donc P est scindé en racine simple.

Si $r = 1$, $x_1$ est la suite constante $a_n = d$ pour tout $n \in \mathbb{N}$ et $d \in \mathbb{R}$.
Si $r \in \mathbb{R}/\{1\}$ alors $x_r$ est la solution de $f((a_n)_{n \in \mathbb{N}}) = r (a_n)_{n \in \mathbb{N}}$ donc de $(a_{n+1})_{n \in \mathbb{N}} = (r a_n)_{n \in \mathbb{N}}$
donc de $a_{n+1} = r a_n$ donc $x_r$ est la suite géométrique $a_n = c r^n$ pour $n \in \mathbb{N}$ et $c \in \mathbb{R}$.
Ainsi, $a_n = d$ et $b_n = c(-2)^n$ pour $n \in \mathbb{N}$ sont engendrent les solutions de $a_{n+2} + a_{n+1} - 2 a_n = 0$.

## II approximation de e

Inégalités d'E. DUPUY : Pour tout entier naturel n on a : $(1 + \frac{1}{n})^n \le e \le (1 + \frac{1}{n-1})^n$

Preuve : Par passage au logarithme népérien, il suffit de prouver que :

$$n \ln(1 + \frac{1}{n}) \le 1 \le n \ln(1 + \frac{1}{n-1})$$

Or : $n \ln(1 + \frac{1}{n}) \le n \times \frac{1}{n} = 1$ de part l'inégalité classique $\ln(1 + x) \le x$ pour $x > -1$.

D'autre part : $n \ln(1 + \frac{1}{n-1}) = n \ln(\frac{n}{n-1}) = -n \ln(\frac{n-1}{n}) = -n \ln(1 - \frac{1}{n}) \ge -n \times -\frac{1}{n} = 1$

CQFD

Application : pour n = 10 000, on obtient que $2{,}7181 \le e \le 2{,}7184$

## III L'hypothèse du continu

Voici une raison qui laisse clairement à penser que l'hypothèse du continu est vraie : nous allons construire une famille croissante (partiellement) d'ensemble dont la croissance est très progressive et nous allons montrer que ces ensembles sont soit dénombrables, soit continus. Il ne semble donc pas y avoir de place pour des ensembles intermédiaires.

Notons $E = \{0;1\}^{\mathbb{N}}$ qui est équipotent à [0;1[ de part l'écriture binaire des nombres réels.

Pour tout $X=(x_n)_{n\in\mathbb{N}}$ de E, on note : $S_n(X)=\sum_{k=0}^{n} x_k$ et $M_n(X) = \frac{S_n(X)}{n}$

Considérons l'ensemble des suites croissantes d'entiers naturels $\mathfrak{A} = \{( S_n(X))_{n\in\mathbb{N}} \mid X\in E\}$.

Pour tout $A=(a_n)_{n\in\mathbb{N}}$ de $\mathfrak{A}$, notons F(A) l'ensemble des éléments X de E tels que : $\forall\, n\in\mathbb{N}, S_n(X) \le a_n$,

Donc $F(A) = \{ X\in E \mid \forall\, n\in \mathbb{N}, S_n(X) \le a_n \}$

La famille d'ensemble $\{F(A)\}_{A\in\mathfrak{A}}$ est croissante pour des suites comparables ($A<B \Leftrightarrow \forall n, a_n<b_n$), allant d'un singleton à l'ensemble E tout entier.

Observons les 4 cas suivants :

1 – A=0 (cad $\forall n, a_n=0$) : F(A)=0 donc F(A) est un ensemble fini car il ne contient qu'un élément.

2 – A est convergente et A≠0 : alors F(A) est un ensemble qui ne contient que des éléments qui n'ont qu'un nombre de 1 fini (inférieur ou égal à la limite de A). Cet ensemble est inclus dans les *binairaux* (même chose que décimaux mais pour le binaire) : il est donc dénombrable.

3 – A tend vers l'infini : Montrons alors que F(A) a la puissance du continu.

L'idée est qu'on peut construire une injection f de E dans F(A).

Soit $Z=(z_n)_{n\in\mathbb{N}}$ l'élément de E tel que $S_n(Z)=a_n$ et donc $Z\in F(A)$.

Notons $(n_k)_{k\in\mathbb{N}}$ la sous-suite des termes de Z qui valent 1, donc $z_{n_k}=1$ pour tout k : cette sous-suite existe puisque A diverge et donc que Z contient donc une infinité de 1.

Pour tout X de E, définissons Y=f(X) par : $y_{n_k}=x_k$ pour tout k et $y_n= 0$ pour tout n ne figurant pas la suite des $(n_k)_{k\in\mathbb{N}}$.

Y est alors dans F(A) car $Y\le Z$ (Y est construite de façon à ce que tous les 0 de Z figurent dans Y).

La fonction f ainsi définie est injective car X≠X'=> f(X)≠f(X')

F(A) a donc la puissance du continu.

4 – cas particulier où A=1 (cad $\forall n, a_n=1$) : F(A)=E

Remarque : Cette *technique d'injection* faite au 3 ci-dessus s'avère efficace dans d'autres situations.

Exemple : $G = \{X\in E \mid \lim_{n\to\infty} M_n(X) = 0 \}$ et définissons f la fonction de E par :

f(X) = Y avec $y_n=0$ pour tout n sauf pour les puissances de 2 où $y_{2^n}= x_n$

On a : $M_n(Y) = \frac{1}{n}\sum_{k=0}^{\frac{\ln n}{\ln 2}} x_k \le \frac{1}{n}\sum_{k=0}^{\frac{\ln n}{\ln 2}} 1 \le \frac{1}{n}(\frac{\ln n}{\ln 2}+1)$ donc $\lim_{n\to\infty} M_n(Y) = 0$ donc $Y = f(X)\in G$

La fonction f ainsi définie est clairement une injections ( X≠X'=> f(X) ≠ f(X') ) de E dans G.

Ainsi, l'ensemble G qui est "très petit" (il est de mesure nulle car il ne contient pas de nombres normaux) a la puissance du continu.

Un critère qui semble intéressant à considérer pour savoir si un ensemble a ou n'a pas la puissance du continu est donc de savoir si on peut lui injecter E quelque part, autrement dit, s'il existe une sous-suite $(n_k)_{k\in\mathbb{N}}$ où les éléments de cet ensemble peuvent prendre n'importe quelle valeur.

Comme en informatique, nous allons utiliser le symbole * pour dire "n'importe quelle valeur" : pour rechercher par exemple tous les fichiers *pdf* commençant par *bou*, on écrit en informatique *bou*.pdf*.

Notation : Soit $\mathbf{Z}=(z_n)_{n\in\mathbb{N}}$ où $z_n\in\{0\ ;1\ ;*\}$

$\mathbf{Z}$ est le sous-ensemble de E constitué des éléments $Y=(y_n)_{n\in\mathbb{N}}$ tels que :

- $y_n=z_n$ si $x_n\in\{0\ ;1\}$
- $y_n= 0$ ou $y_n= 1$ si $z_n=*$

Si Z contient une infinité de *, on dira alors que Z est ***étoilé***.
On appelle ***le support de Z*** que l'on notera ***supp(Z)*** l'ensemble des nombres entiers n pour lesquels $z_n \neq *$ et on note ***stars(Z)*** l'ensemble des nombres entiers n pour lesquels $z_n = *$.

Si $\mathbf{Z}$ contient un nombre fini N de *, alors il contient $2^N$ éléments, sinon il a la puissance du continu.

Preuve : Si $\mathbf{Z}$ contient un nombre fini N de * : Soit g la fonction qui à tout nombre entier $n\leq N$ associe le $n^e$ élément de stars($\mathbf{Z}$) dans l'ordre croissant.
Considérons la fonction f de $\{0\ ;1\}^N$ dans E définie par :
$f(x_1\ ;x_2\ ;\ldots;x_N)=Y$ tel que $y_n= z_n$ si $n \in$ supp($\mathbf{Z}$) et $y_{g(k)}= x_k$ pour $1\leq k\leq N$.
La fonction f est alors bijective de $\{0\ ;1\}^N$ dans $\mathbf{Z}$ et puisque $\{0\ ;1\}^N$ a $2^N$ éléments, il en est de même pour $\mathbf{Z}$.
Cette démonstration est encore valable lorsque $N= +\infty$, cad lorsque $\mathbf{Z}$ est étoilé, et donc f est bijective de $\{0\ ;1\}^{+\infty}= E$ dans $\mathbf{Z}$ et donc $\mathbf{Z}$ a la puissance du continu.
CQFD

Remarque : Dire qu'un ensemble est étoilé revient à dire qu'il est compatible avec la *technique de l'injection*.

Exemples d'ensembles qui contiennent un étoilé et qui ont donc la puissance du continue :

- les ensembles F(A) précédents contiennent un étoilé si la suite A diverge, les * correspondants aux rangs de la technique de l'injection.
- l'ensemble des irrationnels de [0 ;1] contient également des étoilés.

  Preuve : E est vu ici comme l'écriture binaire des nombres de [0 ;1].
  Un nombre est irrationnel ssi son écriture binaire ne se répète pas.
  Soit $X=(x_n)_{n\in\mathbb{N}}$ un nombre irrationnel et $\mathbf{Y}=(y_n)_{n\in\mathbb{N}}$ l'étoilé défini par : $y_{2n}= x_n$ et $y_{2n+1}=*$
  Soit $Z\in\mathbf{Y}$ et prouvons par l'absurde que Z est irrationnel.
  Si Z était rationnel, son écriture binaire se répèterait à partir d'un certain rang.
  Il y aurait donc une répétition d'un cycle de n termes.
  Si n est paire alors, en enlevant à Z ses termes paires, on obtient que X aurait un cycle de répétition de $\frac{n}{2}$ ce qui est absurde.
  Si n est impair, alors en considérant 2 cycles consécutifs, on obtient un cycle de 2n termes qui se répètent, ce qui est absurde d'après ce qui précède.
  Ainsi, Z est irrationnel et donc $\mathbf{Y}$ ne contient que des irrationnels et est inclus dans les irrationnels de [0 ;1]. CQFD.

Objectif suivant : L'idée serait de tenter de prouver qu'un ensemble qui ne contient pas d'étoilé est dénombrable. Alors l'hypothèse du continu serait prouvée car, un ensemble qui ne contiendrait pas d'étoilé serait dénombrable et un ensemble qui en contiendrait serait continu.
Je sais que cette quête est normalement vaine de part l'indécidabilité de l'hypothèse du continu. Cela étant, je n'arrive pas vraiment à voir le lien réel entre les axiomes de la théorie des ensembles et les démonstrations en général.

Considérons un ensemble $F \subset E$ qui ne contient pas d'étoilé.
Notons $\mathfrak{R}$ la relation d'équivalence sur E : $X\ \mathfrak{R}\ Y \Leftrightarrow x_n = y_n$ pour tout $n\in\mathbb{N}$ sauf pour un nombre fini.
F est alors partitionné en $F = \bigcup_{i\in I} \overline{f_i}$ où $f_i\in F$, $\overline{f_i}$ est la classe d'équivalence $f_i$ par $\mathfrak{R}$ et $I$ est un ensemble d'indice.
$\overline{f_i}$ est au plus dénombrable car il peut au mieux être mis en bijection avec les binairaux.
Reste à prouver que $I$ est au plus dénombrable.