EPITA

ÉCOLE D'INGENIEURS EN INFORMATIQUE

Algèbre linéaire sur un corps $\mathbb{K}$

Uli Fahrenberg *d'après* Bashar Dudin

Résumé

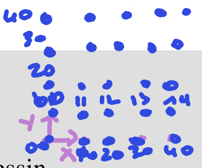
Cette feuille de travaux dirigés vise à vous donner un aperçu du comportement que vous pouvez attendre de l'algèbre linéaire sur un corps quelconque. En particulier, on s'attardera sur les questions d'algèbre linéaire sur un corps fini.

Table des matières

1 Applications linéaires sur un corps fini

On souhaite dans cette section vous familiariser avec les calculs et représentations des espaces vectoriels sur un corps fini. On se limite en un premier temps à la dimension 2 car c'est probablement le lieu où, dans le cas réel, votre imagination peut vous égarer.

det $\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{A} = ad - bc$ $\qquad A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$



Question 1-1

1. Représenter dans un plan le $\mathbb{F}_5$-espace vectoriel $\mathbb{F}_5^2$.
2. Calculer le nombre de droites dans $\mathbb{F}_5^2$. Représenter celles-ci géométriquement sur votre dessin.
3. Calculer le nombre d'endomorphismes de $\mathbb{F}_5^2$. $= \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\quad \overset{e_1}{(1,0)}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a\ b) = f(e_1)$

   $= 5^4 \leftarrow 625$
4. On considère l'endormorphisme φ de $\mathbb{F}_5^2$ donné dans la base canonique par la matrice

   $u = u_1(1,0) + u_2(0,1)$

   $= u_1(3(1,1)+3(1,-1)) + u_2[2(1,1)+2(1,-1)]$

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

   $(1,0)\cdot M = (1\,1)$, $(0,1)\cdot M = (1,1)$ $\quad$ Im M = Vect(1,1)

   ker M = $\{u : uM = 0\}$

   Diagonaliser φ.

   $= (\underbrace{3u_1+3u_2}_{u_1'})(1,1) + (\underbrace{3u_1+2u_2}_{u_2'})(1,-1)$
5. Que se passe-t-il si l'on considère l'endomorphisme ψ donné par la même matrice M dans les bases canoniques, mais sur $\mathbb{F}_2^2$?

$u.M = 0$

$\forall i \ \langle u | C_i \rangle = 0$

$\Rightarrow u \perp (1,1)$

$\Rightarrow u \in D_{1,-1}$

$(1,0) = \frac{1}{2}(1,1) + \frac{1}{2}(1,-1)$

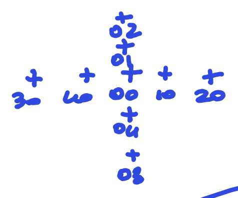
$= 3.(1,1) + 3(1,-1)$

$(0,1) = \frac{1}{2}(1,1) - \frac{1}{2}(1,-1)$

$= 3(1,1) + 2(1,-1)$

$(1\,1)M = (2,2) = 2.(1,1) \to$ 2 est VP pour le VP $(1,1)$

$(1,-1)M = (0,0) = 0.(1,-1)$ $\quad$ 0 VP pour VP $(1,-1)$



ker M = $D_{1,-1}$

$u = u_1(1,0) + u_2(0,1)$

$= u_1'(1,1) + u_2'(1,-1)$

P: $B_c \to B$, det = 2 $\qquad P^{-1} = \frac{1}{2}\begin{pmatrix} 2 & 2 \\ 2 & 3 \end{pmatrix}$

$M = \begin{pmatrix} 3 & 3 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = M$ ok

$(u_1, u_2)\begin{pmatrix} 3 & 3 \\ 3 & 2 \end{pmatrix} = (u_1', u_2')$

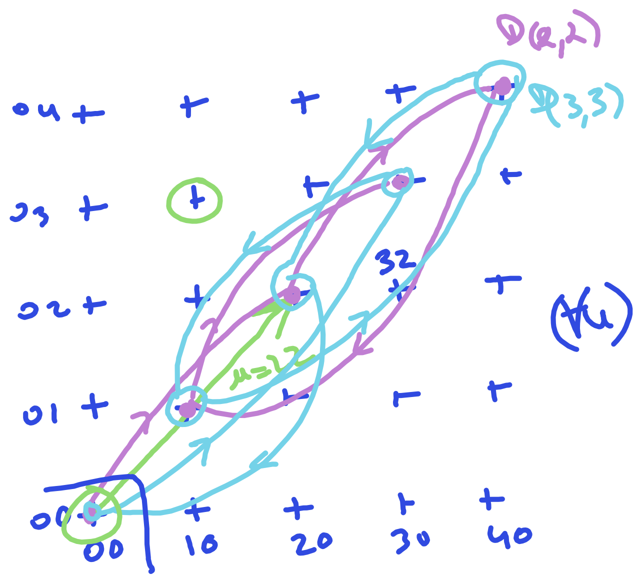
uM base canonique

convertir u écrit dans base c.

M dans la base $\{(1,1), (1,-1)\} = B$

et u écrit dans la base B

$u \neq (0,0) : D_u = \text{Vect}(u) = \{a.u : a \in \mathbb{F}_5\}$



→ 4 vecteurs directeurs : (1,1) (2,2) (3,3) (4,4)

$(\forall u)$ $5.u = (0,0)$

$\forall u$ $|D_u| \le 5$

si $u \neq (0,0)$. $\Downarrow$ p.ex : $u_1 \neq 0$

$a.u = b.u$ → en particulier on a $a.u_1 = b.u_1$

⇒ $(a-b).u_1 = 0$

→ intégrité de $\mathbb{F}_5$ ⇒ $a-b=0$ ou ~~$u_1 = 0$~~

⇒ $a=b$

• chq droite contient exactement 5 élts dont 4 non-nuls.

• mq il n'y a qu'une seule dte qui passe par (0,0) et $u \neq 0$

① il y en a une $D_u = \{a.u : a \in \mathbb{F}_5\}$

② Soit D_v qui passe par u, montrer que $D_v = D_u$

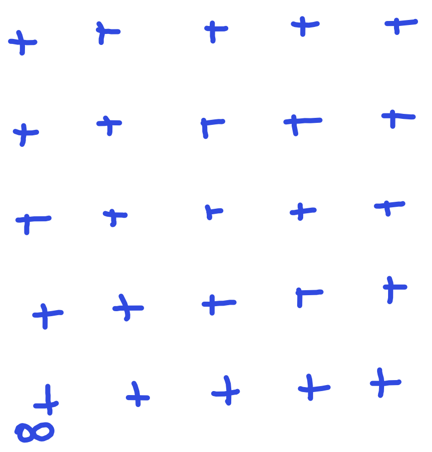
⇒ $\exists a$ tq $u = a.v$ $\quad \forall b \in \mathbb{F}_5$ $b.u = (a.b).v \in D_v$

⇒ $D_u \subseteq D_v$

or $|D_u| = |D_v| = 5$ donc $D_u = D_v$

⇒ $v \in D_u$

Cl : $\forall u \neq (0,0)$, u appartient à une unique dte, définie par 4 vecteurs ≠ nuls.



$M = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

$(1,1)M = (2,2)$ vrai aussi ds $\mathbb{F}_2$

$\boxed{=(0,0)}$

$(1,-1)M = (0,0)$ mais $1 = -1$ ds $\mathbb{F}_2$

$trM = 2 = 0$

si M est diag. $= \lambda_2 + \lambda_1$

$\lambda_1 = 0$ que vaudrait λ_2 ? $= 0$

⇒ si M était diagonalisable ses 2 vp seraient 0 et donc M serait nulle

Or M n'est pas nulle

⇒ M n'est pas diagonalisable ds $\mathbb{F}_2^2$

si $P = \dots + \underbrace{a_i}_{=1} x^{2i+1} + \dots$

$\partial P = \dots + \underbrace{(2i+1)}_{=1} x^2$

$\partial x^i = i x^{i-1} = 0$ si i est pair

$\partial P = 0$ si P est une somme de monomes de deg pair

$\ker P = \{P : P = \sum a_i X^{2i}\}$

Question 1-2 On s'intéresse à deux exemples d'applications linéaires sur le $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_2[X]$.

1. Décrire le noyau de l'endomorphisme linéaire donné par la dérivée d'un polynôme.
2. Montrer que l'application $P \mapsto P^2$ est un endomorphisme linéaire sur $\mathbb{F}_2[X]$.

$P \to \partial P / \partial x$

$\ker \partial = \{P : \partial P = 0\}$

$P \mapsto P^2$ de $\mathbb{F}_2[X]$

$\partial P = 0 = \sum_{i=1}^{m} a_i (i) \cdot x^{i-1}$

$P = \sum a_i x^i$

2 Se donner une sous-espace vectoriel

Représenter un sous-espace vectoriel d'un espace ambient de manière réduite est essentiel dans les problématiques computationnelles. Ainsi, on aura tendance à représenter un tel espace « matriciellement » : comme l'image ou le noyau d'une matrice. Ces deux représentations sont duales et on est en mesure de passer de l'une à l'autre.

$\iff \langle (x,y,z) | (1,1,1) \rangle = 0$

$\iff x,y,z \perp (1,1,1)$

Question 2-3 On considère le sous-espace vectoriel V de $\mathbb{K}^3$ décrit par l'equation $x+y+z=0$.

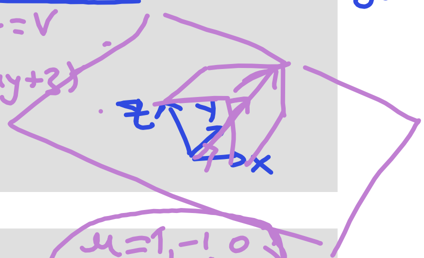
1. Trouver des matrices G et H satisfaisant :
   — G est une matrice dans $\mathscr{M}_{3,2}(\mathbb{K})$ d'image V
   — H est une matrice dans $\mathscr{M}_{1,3}(\mathbb{K})$ de noyau V
   — $HG = 0$
2. Proposer une interprétation « géométrique » de la dernière relation.

$G = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$ $\operatorname{Im} G = V$

$H = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ $(x\,y\,z)H = (x+y+z)$

GH $\forall s\ (s.G)H = 0 \Rightarrow GH = (0)$ $V = \ker H$

$\in V = \ker H$



Question 2-4 On considère le sous-espace vectoriel V de $\mathbb{K}^4$ décrit par l'equation

$$\begin{cases} x+y+z+t & = & 0 \\ x+y & = & 0 \end{cases}$$

Trouver des matrices G et H satisfaisant des propriétés similaires à ce qui est attendu à la question 2-3

$u = 1,-1,0$
$v = 0,1,-1$
$w = -1,0,1 = -(u+v)$

$\operatorname{Im} G = V$
$\ker H = V$

$(1,-1,0,0) \in V$
$(0,0,1,-1) \in V$ forme une famille libre

$G = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$ $\operatorname{Im} G = V$ car $\dim V = 2$ et $\operatorname{Im} G \subseteq V$ et $\dim \operatorname{Im} G = 2$

$u = (x,y,z,t)$

$H : \begin{cases} \langle u | 1111 \rangle = 0 \\ \langle u | 1100 \rangle = 0 \end{cases}$

$uH = (\langle u | c_1 \rangle, \langle u | c_2 \rangle, \dots) \to H = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}$ $uH = (\langle u | 1111 \rangle, \langle u | 1100 \rangle)$

$\ker H = V$ car $u \in \ker H$ ssi $\langle u | 1111 \rangle = 0$ et $\langle u | 1100 \rangle = 0$

$\forall u\ uGH = 0 \Rightarrow GH = 0$

$\in \operatorname{Im} G = V = \ker H$

$P \mapsto P^2$ est linéaire de $\mathbb{F}_2[X]$

$P = \sum_{i=0}^{d} a_i X^i$ $\quad P^2 = \left(\sum_{i=0}^{d} a_i X^i\right)^2 = \sum_{i=0}^{d} a_i^2 (X^i)^2 + \underbrace{\overbrace{2}^{=0} \sum_{i<j} a_i a_j X^i X^j}_{=0}$

x commutative

$\left(\sum_{i=1}^{n} x_i\right)^2 = \sum_{i=1}^{n} x_i^2 + 2 \sum_{i<j} x_i x_j$

$= \sum_{i=0}^{d} a_i^2 X^{2i}$

$a_i^2 = a_i$ de $\mathbb{F}_2$

$= \sum_{i=0}^{d} a_i X^{2i}$

$P \to P^2$

$P+Q = \sum_{i=0}^{D} (a_i + b_i) X^{2i}$

$P = \sum a_i X^i$ $\quad Q = \sum b_j X^j$

$f(P+Q) = (P+Q)^2 = P^2 + \underset{0}{\cancel{2PQ}} + Q^2 = f(P) + f(Q)$

$f(\lambda P) = \underbrace{\lambda^2}_{=\lambda \text{ de } \mathbb{F}_2} P^2 = \lambda . f(P)$

$\Bigg\}$ f est linéaire