EPITA

ÉCOLE D'INGENIEURS EN INFORMATIQUE

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

Uli Fahrenberg *d'après* E

**Résumé**

Cette feuille de travaux dirigés vise à vous donner un aperçu du comportement que vous pouvez attendre en 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 1

2 Se donner une sous-espace vectoriel 3

## 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.

**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 $\mathbb{F}_5^2$. $=$ appl. linéaire $\mathbb{F}_5^2 \to \mathbb{F}_5^2$ $=$ une matrice $2\times 2$ à coefficients de $\mathbb{F}_5$
4. On considère l'endomorphisme $\varphi$ de $\mathbb{F}_5^2$ donné dans la base canonique par la matrice

$625 = 5^4$

j'ai 5 choix pour a, pour b, pour c et pour d

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

image de $(1,0) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où $a,b,c,d \in \mathbb{F}_5$

Diagonaliser $\varphi$.

5. Que se passe-t-il si l'on considère l'endomorphisme $\psi$ donné par la même matrice $M$ dans les bases canoniques, mais sur $\mathbb{F}_2^2$ ?

$\mathrm{tr}\, M = 2 = 0$ si $M$ était diagonalisable alors $\exists$ VP $= 0$

$\Rightarrow M = 0$ faux $\Rightarrow M$ n'est pas diagonalisable sur $\mathbb{F}_2^2$

polynôme caractéristique
$\det(M - X \cdot \mathrm{Id})$

$$= \begin{pmatrix} 1-x & 1 \\ 1 & 1-x \end{pmatrix}$$

$$= (1-x)^2 - 1$$

$$= \cancel{1} \underbrace{-2x}_{=0} + x^2 \cancel{-1}$$

$$= x^2 \text{ de } \mathbb{F}_2[x]$$

$$\neq x$$

$$(1,0)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a\ b)$$

$$(0,1)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (c\ d)$$

$\Rightarrow$ Pté : il y a exactement autant de matrices que d'applications linéaires

$\Leftrightarrow$ Chq matrice représente une application linéaire $\neq$ !

$M = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ ds $\mathbb{F}_5^2$ diagonaliser $M$

$$\begin{array}{cc} C_1 & C_2 \\ \left(\begin{array}{c|c} 1 & 1 \\ 1 & 1 \end{array}\right) \end{array} \begin{array}{l} \text{image de }(1,0) \\ \text{image de }(0,1) \end{array}$$

Soit $u \in \mathbb{F}_5^2$ $\quad u \cdot M = (u_1\ u_2)\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

$$= (\underbrace{u_1 \cdot 1 + u_2 \cdot 1}_{\langle u | C_1 \rangle},\ \underbrace{u_1 \cdot 1 + u_2 \cdot 1}_{\langle u | C_2 \rangle})$$

$\boxed{C_i = i^{\text{ème}} \text{ colonne de } M}$

produit scalaire

$u = (1,-1) \to uM = (0,0)$

$uM = 0 = 0 \cdot u$

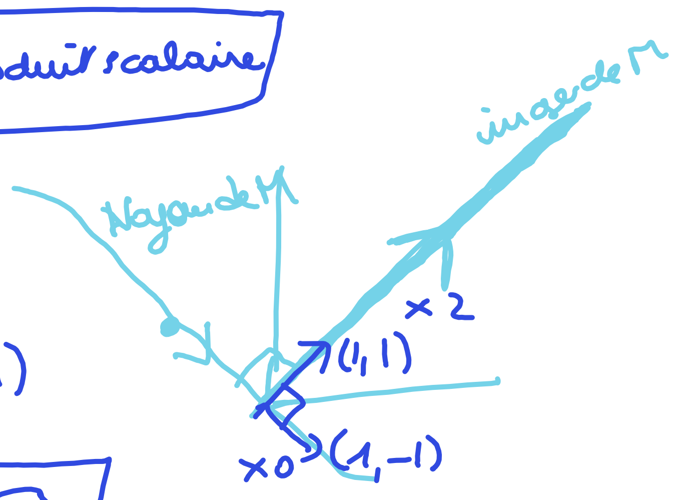
$uM = 0$ ssi $\langle u | \binom{1}{1} \rangle = 0$

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

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

$(1,4) = \boxed{(1,-1) \text{ est } \vec{VP} \text{ pour la VP } 0}$

$\boxed{\langle u | v \rangle = \sum u_i v_i \quad \text{produit scalaire}}$




$u = (1,1) \quad uM = (1\ 1)\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

$= (2\ 2) = 2 \cdot (1,1)$

$= 2u$

$\boxed{(1,1) \text{ est } \vec{VP} \text{ pour la valeur propre } 2}$

$0 + 2 = 2 (= \mathrm{tr} M)$

$$\begin{array}{ccc} P^{-1} & & P \end{array}$$

$\boxed{(u_1, u_2) \to (u'_1, u'_2)}$ $\qquad (u'_1, u'_2) \mapsto (u_1, u_2)$

$u\, M = u \begin{pmatrix} 3 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & \cancel{-1}\ 4 \end{pmatrix}$

u écrit dans la base canonique $u = (u_1, u_2) = u_1 (1\,0) + u_2 (0\,1)$

$\big|$ u est écrit ds la base $\underline{(1\,1)}\ \underline{(1\,-1)} = B'$

u écrit ds B'

$\boxed{u = u'_1 (1\,1) + u'_2 (1,-1)}$

$3 \cdot (1\,1) + 3 (1,-1)$

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

$= 1/2 \qquad -1/2 = -3 = +2$

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

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

$= u'_1\,(1\,1) + u'_2\,(1,-1)$

$\Rightarrow \begin{cases} u'_1 = 3u_1 + 3u_2 \\ u'_2 = 3u_1 + 2u_2 \end{cases}$

$(u_1\ u_2) \overbrace{\begin{pmatrix} 3 & 3 \\ 3 & 2 \end{pmatrix}}^{P^{-1}} = (u'_1, u'_2) = (\underbrace{3u_1 + 3u_2}_{\langle u | C_1 \rangle},\ \underbrace{3u_1 + 2u_2}_{= \langle u | C_2 \rangle})$

$\begin{matrix} (1\,1) \\ (1\,1) \end{matrix} \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$

$u = u'_1 \underline{(1\,1)} + u'_2 \underline{(1\,-1)}$

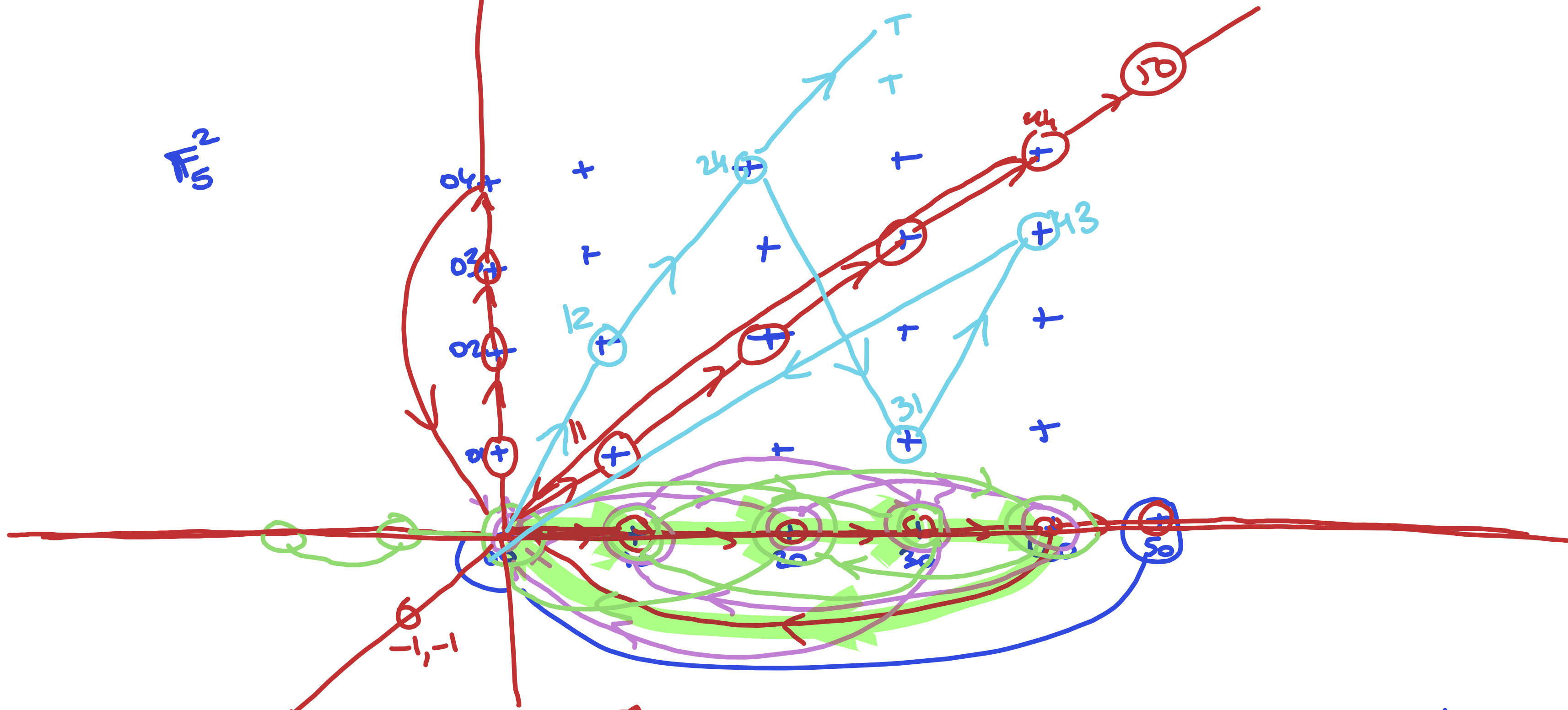
$= (\underline{u'_1 + u'_2},\ \underline{u'_1 - u'_2})$

$= (\underline{u_1}, \underline{u_2})$

$\Rightarrow \begin{cases} u_1 = u'_1 + u'_2 = \langle u' | \binom{1}{1} \rangle & = C_1 \\ u_2 = u'_1 - u'_2 = \langle u' | \binom{1}{-1} \rangle & = C_2 \end{cases}$

$(u'_1, u'_2) \overbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}^{P} = (u_1, u_2)$

$P^{-1} \cdot P = \begin{pmatrix} 3 & 3 \\ 3 & 2 \end{pmatrix} \boxed{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}} = \begin{pmatrix} 6 = 1 & 0 \\ 5 = 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$




$u \neq 0$ $\boxed{D_u = \{a.u : a \in \mathbb{F}_5\}}$

① $5.u = (0,0)$ → $|D_u| \leq 5$ car $|\mathbb{F}_5| = 5$

② si $a.u = b.u$ mq $a = b$

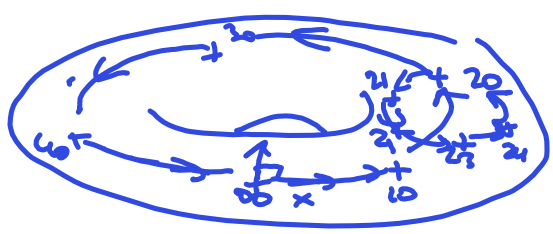
on a $u \neq 0$ donc par exemple $u_1 \neq 0$
$u = (u_1, u_2)$

$a.u = b.u \Rightarrow (a.u_1, a.u_2) = (b.u_1, b.u_2)$

$\Rightarrow a.u_1 = b.u_1$ or $u_1 \neq 0$ et $\mathbb{F}_5$ corps

$\times u_1^{-1}$ $\Rightarrow a = b$ ✓

• $\boxed{\text{THM: } \forall u \neq (0,0) \quad |D_u| = 5}$




$\Rightarrow$ $\boxed{\text{si } a \neq b \Rightarrow au \neq bv}$

$\Rightarrow$ $D_u$ contient autant de points $a.u$ que de $a$ dans $\mathbb{F}_5$, c'est-à-dire 5.

• si $v \in D_u$ mq $D_v = D_u$
$v \neq 0$

$u = a(1,1), a \in \mathbb{Z}$ $(a, a)$

$v = b(2,2), b \in \mathbb{Z}$ $(2b, 2b)$

si $v \in D_u$ alors $\exists a \in \mathbb{F}_5$ tq $v = a.u$ ($a \neq 0$ car $v \neq 0$)
$u = a^{-1}.v$

① mq $D_v \subseteq D_u$: soit $w \in D_v$ $w = b.v = b.(a.u) = (b.a).u \in D_u$, $b.a \in \mathbb{F}_5$

② mq $D_u \subseteq D_v$: soit $w \in D_u$, $\exists b$ tq $w = b.u = (b a^{-1} a).u = (b.a^{-1}).(a.u)$, $b = b.a^{-1}.a$, $a.u = v$

$= (b.a^{-1}).v$, $b.a^{-1} \in \mathbb{F}_5$, $\in D_v$

$\boxed{\text{THM2: } \forall u \neq 0 \quad \forall v \in D_u \setminus \{(0,0)\} \quad D_v = D_u}$

Rés: ① $\forall u \neq (0,0)$ $|D_u| = 5$

② $\forall u \neq (0,0)$ $\forall v \in D_u - \{(0,0)\}$ $D_v = D_u$

$\ker \partial = \{P : \partial P = 0 \text{ ds } \mathbb{F}_2[X]\}$

$P = \sum_i a_i X^i$ $\quad \partial P = \sum_{i \geq 1} i \, a_i X^{i-1} = \sum_{i \geq 1, \, i \text{ impair}} a_i X^{i-1}$

$= 0$ si $i$ est pair ($i = 1$ ds $\mathbb{F}_2$ si $i$ impair)



**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. $\partial : P \mapsto P'$
2. Montrer que l'application $P \mapsto P^2$ est un endomorphisme linéaire sur $\mathbb{F}_2[X]$.

① $(P+Q)^2 = P^2 + 2PQ + Q^2 = P^2 + Q^2$ ✓

$f(P+Q) = f(P) + f(Q)$, $2 = 0$

donc $\partial P = 0$ ssi $P$ est une somme de monome de degré pair

$\boxed{\ker \partial = \mathrm{Vect}(X^{2i}, i \geq 0)}$

② $\forall \lambda \in \mathbb{F}_2$, $\forall P \in \mathbb{F}_2[X]$: $(\lambda P)^2 = \lambda^2 . P^2 = \lambda . P^2$ ✓ ($\lambda^2 = \lambda \in \mathbb{F}_2$)

## 2 Se donner une sous-espace vectoriel

Représenter un sous-espace vectoriel d'un espace ambiant 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.

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

1. Trouver des matrices $G$ et $H$ satisfaisant :
   - i) — $G$ est une matrice dans $\mathscr{M}_{2,3}(\mathbb{K})$ d'image $V$
   - ii) — $H$ est une matrice dans $\mathscr{M}_{3,1}(\mathbb{K})$ de noyau $V$
   - iii) — $GH = 0$

   i + ii ⇒ iii
2. Proposer une interprétation « géométrique » de la dernière relation.

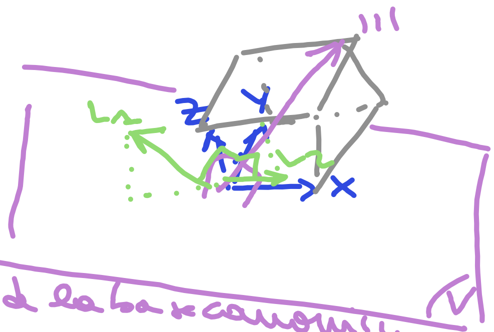
**Question 2-4** On considère le sous-espace vectoriel $V$ de $\mathbb{K}^4$ décrit par ~~l'equation~~ le système d'équations

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

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

$V = \{ (xyz) \in \mathbb{K}^3 : \underbrace{x+y+z=0}_{\langle (xyz) \mid (1,1,1) \rangle} \} =$

$(x,y,z) \in V \iff \langle (xyz) \mid (111) \rangle = 0 \iff (xyz) \perp (111)$




$G \in \mathcal{M}_{23}(\mathbb{K}) \quad \mathrm{Im}\, G =$

$M = \begin{pmatrix} \boxed{L_1} \\ \vdots \, L_i \\ \boxed{L_n} \end{pmatrix}$ ← image $(1\,0 \dots 0)$
← image $i$ème vecteur de la base canonique
← image de $(0 \dots 0\,1)$

$(0\,0 \dots 0\,1\,0 \dots 0) \begin{pmatrix} L_1 \\ \vdots \\ L_i \\ \vdots \\ L_n \end{pmatrix} = L_i$

$\uparrow i$

$\mathrm{Image}(M) = \mathrm{Vect}(L_1, \dots, L_n)$

$G = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \begin{matrix} = L_1 \\ = L_2 \end{matrix}$ $\quad (1\,0)G = (-1,1,0) \in V$
$(0,1)G = (0,1,-1) \in V$

et ils forment une base de $V$

$\mathrm{Im}\, G = V$

---

$H$ tq $V = \ker H \qquad (xyz) \in \ker H$ ssi $(xyz)H = 0$

$(xyz) \in V$ ssi $x+y+z=0$

ssi $(xyz) \underbrace{\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}}_{=_{\mathrm{def}} H} = 0$

ssi $(xyz)H = 0$

ssi $(xyz) \in \ker H$.

si on pose $H = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ alors $V = \ker H$.

$\ker H = \{ u : uH = 0 \}$

---

(iii) $GH = 0 \qquad G = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \quad H = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$

$u \in \mathbb{K}^2 \quad \underset{\in \mathrm{Im}\, G = V = \ker H}{(uG)} H = 0 \qquad \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0$

$V = \{ xyz : \underbrace{x+y+z=0}_{(xyz) \underbrace{\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}}_{H}} \}$

$G = \begin{pmatrix} L_1 \\ \vdots \\ L_m \end{pmatrix}$

$V = \{(x,y,z,t) \in \mathbb{K}^4 : \underbrace{x+y+z+t=0}_{=} \text{ et } \underbrace{x+y=0}_{=}\}$

$$(x\ y\ z\ t)\begin{pmatrix}1\\1\\1\\1\end{pmatrix} = 0 \qquad (x\ y\ z\ t)\begin{pmatrix}1\\1\\0\\0\end{pmatrix} = 0$$

on pose $H = \begin{pmatrix}1&1\\1&1\\1&0\\1&0\end{pmatrix}$

$(x,y,z,t) \in V$ ssi $(x\ y\ z\ t)\begin{pmatrix}1&1\\1&1\\1&0\\1&0\end{pmatrix} = (0,0)$

ssi $(x,y,z,t) \in \ker H$

---

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

$$\operatorname{Im} G = \operatorname{Vect}\underbrace{(\underbrace{(-1,1,0,0),\ (0,0,1,-1)}_{\in V})}_{\text{famille libre}} \subseteq \underbrace{V}_{\dim 2}$$

donc $\dim \operatorname{Im} G = 2$ or $\dim V = 2$

donc $V = \operatorname{Im} G$

---

Par construction

$GH = 0$

$$\begin{pmatrix}-1&1&0&0\\0&0&1&-1\end{pmatrix}\begin{pmatrix}1&1\\1&1\\1&0\\1&0\end{pmatrix} = \begin{pmatrix}0&0\\0&0\end{pmatrix} ✓$$