Planche 4

Une histoire de familles (suite)

Exercice 35 ().
Soit E un espace vectoriel et $f : E \to E$ une application linéaire. On dit que $\lambda \in \mathbb{R}$ est une *valeur propre* de f s'il existe $x \in E$ avec $x \neq 0$ tel que $f(x) = \lambda x$. Un tel x est alors appelé *vecteur propre* associé à la valeur propre λ.
On note alors

$$E_\lambda = \left\{x \in E \mid f(x) = \lambda x\right\}$$

l'ensemble des vecteurs propres associés à la valeur propre λ.

1. Dans la définition de valeur propre, que se passerait-il si on enlevait la condition $x \neq 0$?
2. E_λ est-il un espace vectoriel ?
3. Si f est une transformation de $\mathbb{R}^2$ vers $\mathbb{R}^2$ (ou $\mathbb{R}^3$ vers $\mathbb{R}^3$), donner une interprétation géométrique de la notion de vecteur propre.

Exercice 36 ().
On pose l'ensemble de polynômes suivants $H = \{a_2X^2 - a_1X \mid a_1, a_2 \in \mathbb{R}\}$.

1. Déterminer deux polynômes $P_1(X)$ et $P_2(X)$ tels que $H = \text{Vect}(P_1, P_2)$ et en déduire que H est un espace vectoriel.
2. La famille $(X^2 - X, X)$ est-elle génératrice de H ?
3. La famille $(1, 1 - X, 1 + X^2)$ est-elle génératrice de H ?
4. Décrivez du mieux possible l'espace vectoriel suivant :

$$\text{Vect}(1 - X^2, 1 + X^2)$$

Exercice 37 ().
Démontrer que le noyau d'une application linéaire est un espace vectoriel.

Correction

Soient E et F deux espaces vectoriel, et $u : E \to F$ une application linéaire. Démontrons que $\ker u$ est un espace vectoriel.
D'une part, par définition $\ker u \subset E$. D'autre part, $0 \in \ker u$ puisque $u(0) = 0$ (car u est linéaire), et donc $\ker u$ n'est pas vide.
Enfin, démontrons que $\ker u$ est stable par combinaisons linéaires. Soient donc $x, y \in \ker u$ et $\lambda \in \mathbb{R}$, et montrons que $\lambda x + y \in \ker u$. On a :

$$\begin{aligned} u(\lambda x + y) &= \lambda u(x) + u(y) && \textit{car } u \textit{ est linéaire} \\ &= \lambda \times 0 + 0 && \textit{car } x \in \ker u \textit{ et } y \in \ker u \\ &= 0 \end{aligned}$$

Ainsi on a bien $\lambda x + y \in \ker u$. Finalement, $\ker u$ est un sous-espace vectoriel de E et donc *c'est un espace vectoriel.*

Exercice 38 ().
Soit E un espace vectoriel et soient $(e_1, \dots, e_p)$ et $(f_1, \dots, f_n)$ deux familles de vecteurs de E, avec $p \geq 1$ et $n \geq 1$ des entiers.
Démontrer que :

$$\mathrm{Vect}(e_1, \dots, e_p) \subset \mathrm{Vect}(f_1, \dots, f_n) \quad \Longleftrightarrow \quad e_1, \dots, e_p \in \mathrm{Vect}(f_1, \dots, f_n)$$

Exercice 39 ().
En cryptographie, un chiffrement d'un message en un message codé peut dans certains cas être représenté par une application linéaire $c : E \to F$, E représentant alors l'espace vectoriel des messages non chiffrés et F l'espace vectoriel contenant les messages chiffrés. *(On passera pour l'instant sous silence ce que sont précisément E et F)*

1. Pour que le déchiffrement puisse se faire, il ne faut pas que deux messages initialement différents donnent la même version chiffrée, sinon on ne saurait pas quel est le message initial. Parmi les formulations suivantes, énoncées pour toute paire de messages $(m_1, m_2) \in E \times E$, laquelle ou lesquelles traduisent mathématiquement cette contrainte ?

   (a) Si $m_1 \neq m_2$ alors $c(m_1) \neq c(m_2)$

   (b) Si $m_1 = m_2$ alors $c(m_1) = c(m_2)$

   (c) Si $c(m_1) \neq c(m_2)$ alors $m_1 \neq m_2$

   (d) Si $c(m_1) = c(m_2)$ alors $m_1 = m_2$

2. Lorsque cette contrainte est vérifiée, c est une application linéaire dite *injective*. Démontrer que c est injective si et seulement si $\ker c = \{0\}$.

Correction

1. *La phrase a) désigne le fait que si deux messages sont différents, leurs versions chiffrées sont également différentes. Ce qui est bien ce qui est demandé dans l'énoncé.*

   La phrase b) désigne le fait que si deux messages sont identiques alors leurs versions chiffrées est identique. C'est exact mais ce n'est pas une contrainte de l'énoncé c'est quelque-chose de naturellement vraie (une application, qu'elle soit linéaire ou pas, ne peut pas envoyer un même objet sur deux images différentes. À moins d'être une variable aléatoire mais c'est une autre histoire...)

   La phrase c) désigne le fait que si deux chiffrements sont différents, leurs versions non chiffrées sont également différentes. Ce n'est pas la contrainte de l'énoncé, même si c'est aussi également vrai (cela traduit la même chose que la b)).

   La phrase d) désigne le fait que si deux chiffrements sont égaux, alors la seule possibilité est que les messages initiaux soient les mêmes. Ce qui est bien ce qu'on veut pour pouvoir retrouver le message initial à partir de sa version chiffrée. Cette phrase est en fait une autre manière d'exprimer la phrase a).

2. *Il s'agit de démontrer une équivalence ("si et seulement si"), on va donc procéder par double implication.*

   Supposons d'abord que c est injective, et montrons que $\ker c = \{0\}$. D'une part $\{0\} \subset \ker c$ puisque $c(0) = 0$ (car c est linéaire). D'autre part, si $x \in \ker c$ alors $c(x) = 0$ et donc $c(x) = c(0)$. D'après la phrase d) de la question précédent, on a alors $x = 0$. Donc $\ker c \subset \{0\}$ et on en conclut par double inclusion que

$$\ker c = \{0\}$$

Réciproquement, supposons que $\ker c = \{0\}$ *et démontrons que* c *est injective. Démontrons pour cela la phrase d) de la question précédente. Soient* $m_1, m_2 \in E$ *tels que* $c(m_1) = c(m_2)$*, et démontrons que* $m_1 = m_2$*.*
On a par linéarité :

$$c(m_1 - m_2) = c(m_1) - c(m_2) = 0$$

Donc $m_1 - m_2 \in \ker c$*. Mezalor puisque* $\ker c = \{0\}$ *on a* $m_1 - m_2 = 0$ *et donc* $m_1 = m_2$*. Ainsi* c *est bien injective.*

Exercice 40 ().
Soit E un espace vectoriel. Soit v une application linéaire de E vers E.
Montrer que si $x \in \ker(v \circ v) \setminus \ker v$, alors $(x, v(x))$ est une famille libre.
(Rappel : La notation $\setminus$ *signifie "privé de", c'est-à-dire que* $x \in \ker v \circ v$ *mais* $x \notin \ker v$*)*

Correction

Soit $x \in \ker v^2 \setminus \ker v$*. Soit* $\lambda, \mu \in \mathbb{R}$ *tels que*

$$\lambda x + \mu v(x) = 0$$

Alors

$$v(\lambda x + \mu v(x)) = v(0) = 0$$

et donc

$$\lambda v(x) + \mu v^2(x) = 0$$

Or $x \in \ker v^2$ *donc* $\lambda v(x) = 0$*. Et comme* $x \notin \ker v$*,* $\lambda = 0$*.*
Ainsi, en réinjectant dans la première égalité, on a $\mu v(x) = 0$*. Et comme* x *n'appartient toujours pas à* $\ker v$*,* $\mu = 0$*.*
Ainsi, $(x, v(x))$ *est libre.*

Exercice 41 ().
Dans chacun des cas suivants, déterminer si la famille donnée est libre ou liée et reformuler si possible cette question en rapport avec le noyau d'une certaine matrice.

1. La famille $(X^2 + 1, X^2 + X, X^2 + X + 1)$.
2. La famille $\big(1, X - 1, (X - 1)^2\big)$.
3. La famille $\big(X - 1, X^2 + 1, X(X + 1)\big)$.
4. La famille formée par les vecteurs

$$v_1 = \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

5. La famille formée par les vecteurs

$$w_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \quad w_2 = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}, \quad w_3 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

Correction

1. *Il s'agit de déterminer les solutions* $\lambda_1, \lambda_2, \lambda_3$ *de l'équation*

$$\lambda_1(X^2+1) + \lambda_2(X^2+X) + \lambda_3(X^2+X+1) = 0$$

En regroupant les termes en X^2*,* X *et constants cette équiation est équivalent à :*

$$(\lambda_1+\lambda_2+\lambda_3)X^2 + (\lambda_2+\lambda_3)X + (\lambda_1+\lambda_3) = 0$$

En identifiant les coefficients à gauche et à droite on obtient le système suivants :

$$\begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ \qquad\ \ \lambda_2 + \lambda_3 = 0 \\ \lambda_1 \qquad\ \ + \lambda_3 = 0 \end{cases}$$

Ce qui revient à déterminer le noyau de la matrice

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

On échelonne le système en effectuant $L_3 \leftarrow L_3 - L_1$ *puis* $L_3 \leftarrow L_3 + L_2$*, puis on résout en remontant et on obtient* $\lambda_3 = 0$*,* $\lambda_2 = 0$ *et* $\lambda_1 = 0$.
Ainsi, la famille est libre.

2. *On procède de la même manière que précédemment, la matrice dont on cherche le noyau est alors (si on a ordonné dans le sens termes constants, puis en* X *puis en* X^2*) :*

$$\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

qui est échelonné donc le système sera d'autant plus simple à résoudre et fournira de même une seule solution nulle, et donc la famille est libre.

3. *Ici, soit on procède de la même manière que précédemment, soit on remarque que :*

$$X^2 + 1 = X(X+1) - (X-1)$$

et donc la famille est liée puisqu'un des polynôme s'exprimer comme une combinaison linéaire des autres.

4. *On cherche à résoudre l'équation*

$$\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = 0$$

Ce qui aboutit immédiatement au système linéaire suivant :

$$\begin{cases} 2\lambda_1 \qquad\ \ + \lambda_3 = 0 \\ -\lambda_1 - \lambda_2 \qquad\ = 0 \\ \qquad\ \ \lambda_2 - \lambda_3 = 0 \end{cases}$$

En effectuant $L_2 \leftarrow 2L_2 + L_1$ on obtient :

$$\begin{cases} 2\lambda_1 & & + \lambda_3 = 0 \\ & -2\lambda_2 & + \lambda_3 = 0 \\ & \lambda_2 & - \lambda_3 = 0 \end{cases}$$

puis en effectuant $L_3 \leftarrow 2L_3 + L_2$ on obtient :

$$\begin{cases} 2\lambda_1 & & + \lambda_3 = 0 \\ & -2\lambda_2 & + \lambda_3 = 0 \\ & & - \lambda_3 = 0 \end{cases}$$

En remontant, on a alors $\lambda_3 = 0$, $\lambda_2 = 0$ et $\lambda_1 = 0$. La famille est donc libre.

5. *On remarque que $w_1 = w_2 + w_3$ donc la famille est liée.*

Exercice 42 ().
On considère un espace vectoriel E et une application linéaire $f : E \to E$. On rappelle que id_E désigne l'application identité de E vers E, qui ne modifie pas les vecteurs de E ($\mathrm{id}_E(x) = x$). On rappelle aussi que si $\lambda \in \mathbb{R}$, on note $f - \lambda \mathrm{id}_E$ l'application linéaire définie par :

$$(f - \lambda \mathrm{id}_E)(x) = f(x) - \lambda x$$

On pose $\lambda_1 \in \mathbb{R}$ et $\lambda_2 \in \mathbb{R}$ deux nombres réels différents.
Démontrer que si $x_1 \in \ker(f - \lambda_1 \mathrm{id}_E)$ et si $x_2 \in \ker(f - \lambda_2 \mathrm{id}_E)$, avec x_1 et x_2 non nuls, alors (x_1, x_2) est une famille libre.

Correction

Soient $x_1 \in \ker(f - \lambda_1 id_E)$ *et* $x_2 \in \ker(f - \lambda_2 id_E)$ *(avec* $\lambda_1 \neq \lambda_2$*). On sait alors que*

$$f(x_1) = \lambda_1 x_1 \qquad f(x_2) = \lambda_2 x_2$$

Démontrons que (x_1, x_2) *est libre. Soient donc* $\alpha, \beta \in \mathbb{R}$ *tels que*

$$\alpha x_1 + \beta x_2 = 0$$

Démontrons que $\alpha = \beta = 0$.
En appliquant f *à l'équation de départ on obtient :*

$$f(\alpha x_1 + \beta x_2) = f(0)$$

Par linéarité de f*, on a :*

$$\alpha f(x_1) + \beta f(x_2) = 0$$

Et donc

$$\alpha \lambda_1 x_1 + \beta \lambda_2 x_2 = 0$$

En multipliant l'équation initiale par λ_1 *on a aussi :*

$$\alpha \lambda_1 x_1 + \beta \lambda_1 x_2 = 0$$

Ainsi,

$$\alpha \lambda_1 x_1 + \beta \lambda_2 x_2 = \alpha \lambda_1 x_1 + \beta \lambda_1 x_2$$

et donc

$$\beta\lambda_2 x_2 = \beta\lambda_1 x_2$$

ou encore $\beta(\lambda_2 - \lambda_1)x_2 = 0$. *Mais* $x_2 \neq 0$ *et* $\lambda_2 - \lambda_1 \neq 0$ *par hypothèse, donc nécessairement* $\beta = 0$.
Mezalor, en revenant à l'équation initiale et en y injectant cette valeur de β*, on obtient :*

$$\alpha x_1 = 0$$

Puisque $x_1 \neq 0$ *par hypothèse, on obtient* $\alpha = 0$. *Ainsi,* $\alpha = \beta = 0$ *et donc la famille est libre.*

Exercice 43 ().
Un *endomorphisme* est une application linéaire qui va d'un espace vectoriel vers lui-même. Autrement dit, f est un endomorphisme d'un espace vectoriel E si $f : E \to E$ est une application linéaire.
Lorsque c'est le cas, on définit alors pour tout entier $n \geq 1$ l'application f^n définit par :

$$\text{pour tout } x \in E,\ f^n(x) = \underbrace{f \circ \cdots \circ f}_{n \text{ fois}}(x) = \underbrace{f\big(f(\ldots f(x))\big)}_{f \text{ appliqué } n \text{ fois}}$$

1. Expliquer pourquoi on ne peut en général par définir f^n si f n'est pas un endomorphisme.
2. Si f est la rotation de centre $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ et d'angle θ dans $\mathbb{R}^2$, que représente f^2 ? f^3 ? f^n pour un entier quelconque $n \geq 1$?
3. Soit f un endomorphisme d'un espace vectoriel E quelconque.
   (a) Démontrer que
   $$\ker f^n \subset \ker f^{n+1}$$
   (b) Démontrer que
   $$\operatorname{Im} f^n \supset \operatorname{Im} f^{n+1}$$

Correction

1. *Si* $f : E \to F$*, pour pouvoir écrire* $f(f(x))$*, il faut que* $f(x)$ *soit dans l'espace de définition de* f*, c'est-à-dire* E*. Il faut donc que* $\operatorname{Im} f \subset E$*, ce qui est en particulier vrai lorsque* $F = E$ *mais faux dans beaucoup d'autres cas.*
2. *Si* f *est la rotation de centre* $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ *et d'angle* θ *dans* $\mathbb{R}^2$*,* f^2 *représente le fait de refaire cette rotation après l'avoir déjà fait une fois. On va donc obtenir en tout une rotation d'angle* 2θ*. Plus généralement, pour un entier quelconque* $n \geq 1$*,* f^n *représente la rotation d'angle* $n\theta$*.*
3. *Soit* f *un endomorphisme d'un espace vectoriel* E *quelconque.*
   (a) *Soit* $x \in \ker f^n$*. On sait alors que* $f^n(x) = 0$*. Montrons que* $x \in \ker f^{n+1}$*, c'est-à-dire que* $f^{n+1}(x) = 0$*.*
   Or on a :
   $$\begin{aligned} f^{n+1}(x) &= f(f^n(x)) & \\ &= f(0) & \textit{car } x \in \ker f^n \\ &= 0 & \textit{car } f \textit{ est linéaire} \end{aligned}$$

Et c'est ce qu'il fallait démontrer. On a donc l'inclusion cherchée.

(b)

(c) *Soit $y \in \operatorname{Im} f^{n+1}$. On sait alors qu'il existe $x \in E$ tel que $y = f^{n+1}(x)$. Montrons que $y \in \operatorname{Im} f^n$, c'est-à-dire qu'il existe $z \in E$ tel que $y = f^n(z)$.*
Or on a $y = f^n(f(x))$ donc choisir $z = f(x)$ convient, on a donc $y \in Imf^n$. On a ainsi l'inclusion cherchée.

Exercice 44 ().
Soit E un espace vectoriel, soient $n \geq 1$ un entier et $(e_1, \dots, e_n)$ une famille génératrice de E. Soit $u : E \to F$ une application linéaire.
Montrer que $\big(u(e_1), \dots u(e_n)\big)$ est une famille génératrice de $\operatorname{Im} u$. Est-ce également une famille génératrice de F ? (Si oui, le démontrer, si non donner un contre-exemple)

Correction

Il s'agit de démontrer que

$$\operatorname{Im} u = \operatorname{Vect}\big(u(e_1), \dots u(e_n)\big)$$

D'une part, $u(e_1), \dots u(e_n) \in Imu$ et par stabilité par combinaison linéaire, on a immédiatement l'inclusion :

$$\operatorname{Vect}\big(u(e_1), \dots u(e_n)\big) \subset \operatorname{Im} u$$

Réciproquement, soit $y \in \operatorname{Im} u$ et montrons que $y \in \operatorname{Vect}\big(u(e_1), \dots u(e_n)\big)$.
Soit $x \in E$ tel que $y = u(x)$. Comme $(e_1, \dots, e_n)$ est une famille génératrice de E, on peut poser $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ tels que $x = \sum_{i=1}^{n} \lambda_i e_i$. On a alors :

$$\begin{aligned} y &= u\Big(\sum_{i=1}^{n} \lambda_i e_i\Big) \\ &= \sum_{i=1}^{n} \lambda_i u(e_i) && \textit{par linéarité de } u \end{aligned}$$

Ainsi $y \in \operatorname{Vect}\big(u(e_1), \dots u(e_n)\big)$. On a donc l'inclusion :

$$\operatorname{Im} u \subset \operatorname{Vect}\big(u(e_1), \dots u(e_n)\big)$$

et donc par double inclusion on conclut que $\big(u(e_1), \dots u(e_n)\big)$ est bien génératrice de $\operatorname{Im}(u)$.

Exercice 45 ().
Un signal radio peut être affecté par des interférences, ou bien de manière général contenir deux signaux (ou plus) de sources différentes que l'on souhaite séparer (enlever le bruit de fond, isoler différentes voix dans une conversation...).
Dans cet exercice, on modélise le signal total reçu par un vecteur s_{total} et on suppose qu'il est la somme de deux vecteurs s_1 et s_2 représentant deux signaux de sources différentes (source 1 et source 2) à séparer :

$$s_{\text{total}} = s_1 + s_2$$

On note E_1 l'espace vectoriel des signaux possibles provenant de la source 1 et E_2 l'espace vectoriel des signaux possibles provenant de la source 2.

Concrètement, on dispose seulement du signal total s_{total}.

1. Montrer que s'il existe un signal $s \neq 0$ pouvant provenir de E_1 comme de E_2, alors on ne peut pas espérer déterminer s_1 et s_2 (et donc on ne peut pas séparer les signaux).
2. Au contraire, montrer que si le seul signal commun à E_1 et E_2 est le signal nul, alors il n'y aura qu'une possibilité pour s_1 et s_2.

Correction

1. S'il existe un tel signal $s \in E_1 \cap E_2$, alors on aurait aussi

$$s_{total} = s_1 - s + s + s_2$$

Comme $s_1 - s \in E_1$ par stabilité (et car $s \in E_1$) et $s + s_2 \in E_2$ pour les mêmes raisons, cela donnerait une autre possibilité d'obtenir s_{total}. On ne saurait donc pas identifier de manière sûre s_1 et s_2.

2. Supposons par l'absurde qu'il y ait deux possibilités distinctes de décomposer le signal total :

$$s_{total} = s_1 + s_2$$

$$s_{total} = t_1 + t_2$$

avec $s_1, t_1 \in E_1$ et $s_2, t_2 \in E_2$. Alors on aurait $s_1 + s_2 = t_1 + t_2$ et donc

$$s_1 - t_1 = t_2 - s_2$$

Or pas stabilité $s_1 - t_1 \in E_1$ et $t_2 - s_2 \in E_2$. Puisque ces deux quantités sont égales, on a :

$$s_1 - t_1 \in E_1 \cap E_2 \qquad \text{et} \qquad s_2 - t_2 \in E_1 \cap E_2$$

Si le seul signal commun à E_1 et E_2 est le signal nul alors $s_1 - t_1 = 0$ et $s_2 - t_2 = 0$, et donc :

$$s_1 = t_1 \qquad \text{et} \qquad s_2 = t_2$$

ce qui contredit le fait que les deux décompositions soient différentes. Il n'y a donc qu'une décomposition possible.