Représentation matricielle des applications linéaires

Table des matières

Contextualisation

On a déjà avancé lors des fiches de TD précédentes que l'algèbre linéaire propose des modèles d'utilité notoire dans l'analyse des différents problèmes d'ingénierie informatique. Cette promesse ne ferait sens si l'ont n'était pas en mesure de stocker, d'une manière ou d'une autre, l'information portée par une application linéaire en machine. On sous-entend donc qu'on serait en mesure de réduire l'information portée par une application linéaire à une information de taille finie. Pouvoir effectuer ce type de réduction en dimension infinie n'est pas possible en général, ou du moins en dehors de certains contextes que vous aurez l'occasion d'étudier, comme par exemple en mathématiques du signal. En ***dimension finie***, cependant, cette réduction est toujours possible. On peut donc dans ce cas, stocker l'ensemble de l'information que porte une application linéaire f dans un tableau de valeurs. On a autant de manière de faire cette réduction que de bases dans les espaces vectoriels de départ et d'arrivée de f, en général une infinité. On étudie dans cette fiche comment penser ces différentes réductions et les rapports qui les lient.

Convention 1. Soit $n \in \mathbb{N}^*$. On note $e_1, \dots, e_n$ les éléments de la base canonique de $\mathbb{R}^n$. Précisément pour $i \in \{1, \dots, n\}$, e_i est l'élément ayant toutes ses coordonnées à 0 sauf la i-ème qui est à 1.

1 Caractérisation d'une application linéaire par l'image d'une base

1.1 Résumé

Soient E et F deux $\mathbb{R}$-espaces vectoriels. Pour connaître les valeurs que prend une application linéaire $f : E \to F$ en ***tout*** élément de E il faut et il suffit de connaître les valeurs que prend cette application linéaire sur ***une*** quelconque base de E. Cette section est consacrée à travailler ce seul point.

1.2 Exercices

Exercice 1.1

Soit $f : \mathbb{R}^3 \to \mathbb{R}^2$ une application linéaire telle que

$$\begin{aligned} f(e_1) &= (2, 1) \\ f(e_2) &= (-1, 1) \\ f(e_3) &= (1, 7). \end{aligned}$$

1. Est-ce que f peut prendre la valeur $(3, 1)$ en $(1, -1, 0)$?
2. Quelle est la valeur que prend f en $(1, 2, 3)$?
3. Plus généralement quelle valeur prend f en un point $(x, y, z) \in \mathbb{R}^3$ en fonction des coordonnées x, y et z ?

Exercice 1.2

Soit $f : \mathbb{R}^3 \to \mathbb{R}^2$ une application linéaire telle que

$$\begin{aligned} f\big((1, 0, 1)\big) &= (2, 1) \\ f\big((0, 1, 0)\big) &= (-1, 1) \\ f\big((1, 1, 1)\big) &= (1, 2). \end{aligned}$$

1. Quelle est la valeur que prend f en $(2, 1, 2)$?
2. Quelle est la valeur que prend f en $(1, 0, 2)$? Quel est le soucis ?

Exercice 1.3

Lors d'une de vos séances de TD, votre enseignant vous décrit une application linéaire $f : \mathbb{R}^3 \to \mathbb{R}^3$ donnée par

$$\begin{aligned} f\big((1,2,1)\big) &= (1,1,1) \\ f\big((-1,1,1)\big) &= (-1,1,1) \\ f\big((0,3,2)\big) &= (0,0,1). \end{aligned}$$

Pourquoi a-t-il fait une *erreur de typo* ?

Exercice 1.4

Soient f et g deux applications linéaires différentes de $\mathbb{R}^2$ dans un espace vectoriel F. Est-ce que f et g peuvent prendre les mêmes valeurs sur tous les éléments

1. d'une droite vectorielle de $\mathbb{R}^2$?
2. de la droite affine $y = 2x + 1$?
3. du disque de rayon 1, centré en l'origine ?
4. des vecteurs dans $\mathbb{N}^2$?

2 Matrice d'une application linéaire dans des bases données

2.1 Résumé

La section précédente nous a permis de constater que l'ensemble de l'information portée par une application linéaire peut être représentée par les valeurs que prend cette application linéaire sur une base du $\mathbb{R}$-espace vectoriel de départ. Dans le cas d'espaces vectoriels au départ et à l'arrivée qui sont de dimensions finies, et pour peu qu'on choisisse également une base de l'espace vectoriel d'arrivée on peut représenter une application linéaire par un tableau à 2 dimensions : si $f : E \to F$ est une application linéaire entre deux $\mathbb{R}$-espaces vectoriels de dimensions finies, et si $B = (b_i)_{i=1}^n$ et $C = (c_j)_{j=1}^m$ sont respectivement des bases de E et F alors toute l'information de f est contenue dans le tableau des coefficients des $f(b_i)$ dans la base c_j. Ce tableau 2 dimensionnel dépend du choix de bases au départ et à l'arrivée, il changera si on fait différents choix de bases. On l'appelle ***matrice de f dans les bases B et C***.

Associer à une application f en dimension finie une matrice dans des bases données n'est pas uniquement une manière de *stocker* l'information portée par f, on peut en réalité s'abstraire complétement de f pour ne travailler qu'avec sa matrice. On pourrait résumer la majeure partie des problématiques d'algèbre linéaire à celle-ci : ***comment choisir la base adaptée à l'application linéaire qu'on étudie ?***

Hypothèse 2.1. On se limite dans la suite au cas des $\mathbb{R}$-espaces vectoriels de dimensions finies.

2.2 Exercices

Exercice 2.5

Décrire les matrices des applications linéaires suivantes dans les bases indiquées :

1. l'application linéaire $f : \mathbb{R}^2 \to \mathbb{R}^2$ donnée, pour tout $(x,y) \in \mathbb{R}^2$, par $f(x,y) = (2x+y, x-y)$
   (a) dans la base canonique de $\mathbb{R}^2$ au départ et à l'arrivée
   (b) dans la base canonique au départ et $\big((1,1),(1,-1)\big)$ à l'arrivée
   (c) dans la base $\big((1,1),(1,-1)\big)$ au départ et la base canonique à l'arrivée
   (d) dans la base $\big((1,-1),(1,1)\big)$ au départ et la base canonique à l'arrivée
   (e) dans la base $\big((1,1),(1,-1)\big)$ au départ et $\big((0,1),(1,1)\big)$ à l'arrivée ;

★ 2. l'application linéaire $g : \mathbb{R}^3 \to \mathbb{R}^2$ donnée, pour tout (x,y,z) par $f(x,y,z) = (3x-y+z, y-2z)$

   (a) dans les bases canoniques de $\mathbb{R}^3$ et $\mathbb{R}^2$
   (b) dans la base $(0,1,1)$, $(1,0,1)$ et $(1,1,0)$ au départ et la base $(1,-1)$ et $(1,1)$ à l'arrivée
3. l'application linéaire de $h : \mathbb{R}^4 \to \mathbb{R}$ donnée, pour tout (x_1, x_2, x_3, x_4) par
$$h(x_1, \ldots, x_4) = x_2 - 2x_2 + 3x_4$$
   (a) dans les bases canonique au départ et à l'arrivée
   (b) dans la base canonique au départ et la base 2 à l'arrivée ;

★ 4. l'application linéaire de $\ell : \mathbb{R}^n \to \mathbb{R}^m$ donnée, pour tout $(x_1, \ldots, x_n)$ par
$$\ell(x_1, \ldots, x_n) = (\sum_{j=0}^{n} a_{0,j} x_j, \ldots, \sum_{j=0}^{n} a_{m,j} x_j)$$
   pour des coefficients réels $(a_{i,j})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$;
5. l'application linéaire $\ell : \mathbb{R}_3[X] \to \mathbb{R}_3[X]$ donnée par la dérivée de polynôme
   (a) dans la base canonique $(1, X, X^2, X^3)$ ad départ et à l'arrivée
   (b) dans la base $(1, X+1, X^2-1, X^3+X)$ au départ et la base canonique à l'arrivée
   (c) dans la base canonique au départ et la base $(1, X+1, X^2-1, X^3+X)$ à l'arrivée.

Exercice 2.6

On consdière la matrice
$$\begin{pmatrix} 1 & 2 \\ -1 & 1 \\ 0 & 1 \end{pmatrix}$$
comme
- la matrice de l'application linéaire f dans les bases canoniques
- la matrice de l'application linéaire g dans la base $\big((1,1),(1,-1)\big)$ au départ et la base canonique à l'arrivée.

Quelles sont les images de $(2,-3) \in \mathbb{R}^2$ respectivement par f et g ?

Exercice 2.7

On considère à nouveau les fonctions f et g de l'exercice 2-5. On note respectivement M_f et M_g les matrices de f et g dans les bases canoniques au départ et à l'arrivée. Quelle est la matrice de $f \circ g$ dans les bases canoniques au départ et à l'arrivée ?

Exercice 2.8

On considère les matrices suivantes, supposées matrices d'applications linéaires f, g et h dans les bases canoniques au départ et à l'arrivée :
$$\begin{pmatrix} 1 & 2 & 1 \\ 1 & 0 & 2 \\ 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & -1 \\ 1 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

1. Calculer
   - le rang
   - l'image
   - et le noyau

   de chacune des applications f, g et h.
2. Répondre aux mêmes questions précédentes pour l'application linéaire ℓ dont l'application linéaire dans la base $\big((1,1),(1,-1)\big)$ au départ et à l'arrivée est
$$\begin{pmatrix} 3 & 3 \\ -1 & -1 \end{pmatrix}.$$

3. Quel est l'objectif de l'exercice ?

★ Exercice 2.9

On considère les applications linéaires f et g dont les matrices dans les bases canoniques sont respectivement

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

1. Quelle est la matrice de l'application linéaire $f \circ g$ dans les bases canoniques ? Celle de $g \circ f$?
2. Calculer la matrice de la composée de g avec elle-même 10 fois, g^{10}, dans les bases canoniques ?
3. Écrire les matrices de f et g respectivement dans la base $\big((1,1),(1,-1)\big)$ au départ et à l'arrivée.
4. Exprimer g^k et f^k pour tout $k \in \mathbb{N}$.

Exercice 2.10

On considère la suite récurrente linéaire (u_n) donnée par

— $u_0 = 1$, $u_1 = 2$,

— $\forall n \geq 0$, $u_{n+2} = 3u_{n+1} - 2u_n$.

1. Exprimer le vecteur (u_{n+2}, u_{n+1}) en fonction de (u_{n+1}, u_n) via un produit par une matrice A bien choisie.
2. Écrire la matrice de l'application linéaire associée à A dans la base $\big((0,1),(1,1)\big)$.
3. En déduire une expression explicite de u_n en terme de n.

3 *Les* matrices d'une application linéaire

3.1 Résumé

À toute application linéaire f entre deux espaces vectoriels de dimensions finies, on peut associer une représentation matricielle. Cette représentation matricielle dépend du choix de bases des espaces de départ et d'arrivée. On est donc a priori en mesure d'associer différentes matrices à f en effectuant différents choix de bases des espaces de départ et d'arrivée. On étudie cette question plus en détail dans cette section : *comment obtenir toutes les matrices qu'on pourrait associer à une application linéaire ?* Cette question est liée au fait d'être en mesure de changer le système de *coordonnées* dans lequel on travail, c'est-à-dire la base dans laquelle on travaille.

3.2 Exercices

Exercice 3.11

On note $\mathcal{B}$ la base de $\mathbb{R}^3$ donnée par $\mathcal{B} = ((1,0,1),(0,1,0),(1,1,0))$. Soit f l'application linéaire de $\mathbb{R}^3 \to \mathbb{R}^3$ donnée par

$$\begin{aligned} f(e_1) &= (1,1,1) \\ f(e_2) &= (1,0,-1) \\ f(e_3) &= (0,1,-1). \end{aligned}$$

1. Justifier le fait que f soit bijective.
2. Écrire la matrice de f dans la base canonique au départ et à l'arrivée, elle sera notée P. Comment appelle-t-on P ?
3. Exprimer les coordonnées d'un vecteur $(x,y,z) \in \mathbb{R}^3$ écrit dans la base canonique dans la base $\mathcal{B}$, à l'aide de la matrice P.
4. Quelle est la matrice de f^{-1} dans la base $\mathcal{B}$ au départ et à l'arrivée ?

Exercice 3.12

On reprend les notations de l'exercice 2-5 point (1.), pour rappel f est l'application linéaire $f : \mathbb{R}^2 \to \mathbb{R}^2$ donnée par $f(x,y) = (2x+y, x-y)$. Notre objectif est de retrouver les matrices de f dans les bases décrites dans les points (b) – (c) à partir de la matrice M dans les bases canoniques obtenues en (a). On note $\mathcal{B}$ la base $\mathcal{B} = ((1,1),(1,-1))$.

1. Quelle est la matrice de passage P de la base canonique à la base $\mathcal{B}$? Comment écrire les coordonnées d'un vecteur donné dans la base canonique dans la base $\mathcal{B}$, à l'aide de la matrice P ?
2. On note N la matrice de f dans la base canonique à l'arrivée et la base $\mathcal{B}$ au départ (matrice du point (c) 2-5. Décrire N à l'aide de P.
3. On note Q la matrice de f dans la base $\mathcal{B}$ à l'arrivée et la base canonique au départ (matrice du point (b) 2-5. Décrire Q à l'aide de P.
4. Quelle est la matrice de f dans la base $\mathcal{B}$ au départ et la base $((0,1),(1,1))$ à l'arrivée ?

A Activité libre : faire du chiffrement avec de l'algèbre linéaire

L'activité suivante ne fait pas, à proprement parler, partie de cette fiche. Elle vous suggère cependant une réflexion qui vous permettra de mettre à contribution les notions que vous venez aborder dans cette feuille, tout en vous renvoyant à la notion de chiffrement symétrique que vous avez entrevue lors du projet AFIT.

★ **Exercice 1.13**

Alice et Bob viennent de suivre le cours d'algèbre linéaire. Ils choisissent pour s'amuser d'utiliser des applications linéaires pour s'envoyer des messages chiffrés.

Voici le premier algorithme de chiffrement qu'ils conçoivent, c'est un algorithme de chiffrement symétrique[1] :

— Bob et Alice partagent de manière sécurisée la clé v, un vecteur dans $\mathbb{R}^n$
— Bob envoie à Alice une application linéaire f sur un canal pouvant éventuellement être intercepté
— quand Alice reçoit f elle regarde l'image $f(v)$ de v par f pour retrouver le message original de Bob.

Pour pouvoir envoyer f à Alice, Bob ne dipose que des structures de données que l'informatique lui permet, il utilise donc des tableaux 2D pour pouvoir envoyer ses messages à Alice. Bob va envoyer à Alice un triplet (B, C, M) où :

— $B = (w_i)_{i=1}^n$ est une base de $\mathbb{R}^n$ dont les éléments sont exprimés en coordonnées dans la base canonique
— $C = (u_j)_{j=1}^m$ est une base de $\mathbb{R}^m$ dont les éléments sont également exprimés dans la base canonique
— M est le tableau des $f(w_i)$s exprimées (en colonne) dans les coordonnées des u_j.

On suppose que la clé privée partagée par Alice et Bob est le vecteur $(1,1,1,1) \in \mathbb{R}^4$, écrit dans la base canonique[2].

1. Alice reçoit le message

$$\left[\left\{\begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\0\\0\end{pmatrix}\right\}, \left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}-1\\1\end{pmatrix}, \right\}, \begin{pmatrix}1 & 1 & 1 & 1\\0 & 1 & 0 & 1\end{pmatrix}\right].$$

Quel est le message original de Bob ?

1. Revoir le projet AFIT si vous ne vous rappelez pas de ce que c'est !
2. Cette information est superflue, si ce n'est pas précisé on est toujours dans la base canonique.

2. Que dire si Alice avait reçu le message

$$\left[\left\{\begin{pmatrix}1\\0\\1\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\\1\end{pmatrix},\begin{pmatrix}0\\0\\1\\1\end{pmatrix},\begin{pmatrix}1\\0\\2\\1\end{pmatrix}\right\},\left\{\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}-1\\1\end{pmatrix},\right\},\begin{pmatrix}1&1&1&1\\0&1&0&1\end{pmatrix}\right]?$$

3. Pensez-vous qu'il soit possible pour Eve, qui a l'habitude de surveiller les communication entre Alice et Bob, de retrouver rapidement v à partir de f ? Serait-ce plus facile si Eve a accès à $f(v)$, en plus de f ?