CHAPITRE 0

RAPPELS : ESPACES VECTORIELS ET APPLICATIONS LINÉAIRES

Ce chapitre 0 est constitué de **rappels** : espaces vectoriels, familles génératrices, familles libres, bases et dimension, applications linéaires et matrices, transposée d'une matrice, théorème du rang, formules de changement de base, matrices équivalentes, matrices semblables. Ces notions ont été introduites en L1 et ne seront pas traitées en cours, mais le lecteur pourra se reporter, si nécessaire, à ce chapitre 0 pour un rappel de ces notions ou résultats. On suppose également connue la théorie du pivot pour la résolution des systèmes linéaires $AX = Y$; ceci équivaut à faire des opérations sur les lignes de la matrice A et on verra dans le chapitre 1 comment faire des opérations sur les *colonnes* (ce qui est plus pratique pour la recherche de vecteurs propres).

On a indiqué par des symboles les définitions, exemples et résultats fondamentaux. Par ailleurs, des *compléments de cours*, pour les étudiants intéressés, sont donnés dans un appendice à la fin du chapitre ; ces passages n'interviendront pas dans les évaluations.

0.1. Espaces vectoriels : définition et exemples

0.1.1. Trois exemples importants. — (1) Un exemple d'espace vectoriel sur $\mathbb{R}$ est l'espace de dimension 3

$$\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}.$$

Dans ce cas, l'espace vectoriel nous est donné comme un ensemble de n-uplets (ici $n = 3$) de « coordonnées ».

Deux autres exemples sont les suivants.

(2) Soient $a, b \in \mathbb{R}$; l'ensemble $\mathscr{S}(a, b)$ des suites $(u_n)_{n\in\mathbb{N}}$ de nombres réels vérifiant la relation de récurrence linéaire

$$(*) \qquad u_{n+2} = au_{n+1} + bu_n$$

est un $\mathbb{R}$-espace vectoriel, qui est de dimension 2, car toute suite vérifiant $(*)$ est déterminée par ses termes initiaux u_0 et u_1, qui peuvent être choisis arbitrairement.

(3) Soient $a, b \in \mathbb{R}$ et $t_0 \in \mathbb{R}$; l'ensemble $\mathscr{S}(a, b)$ des fonctions $f : \mathbb{R} \to \mathbb{R}$ de classe C^∞, vérifiant l'équation différentielle linéaire :

$$(E) \qquad \forall t \in \mathbb{R}, \qquad f''(t) = af'(t) + bf(t)$$

est un $\mathbb{R}$-espace vectoriel, qui est de dimension 2, car toute solution f de (E) est déterminée par les « conditions initiales » $f(t_0)$ et $f'(t_0)$, qui peuvent être choisies arbitrairement.

Dans ces deux cas, le choix de « coordonnées » sur l'espace $\mathscr{S}(a, b)$ n'est pas évident ... Une des forces de l'algèbre linéaire est qu'elle permet de décrire simplement tous les éléments de $\mathscr{S}(a, b)$, une fois qu'on a choisi une base appropriée de cet espace ...

Rappelons que la notion d'espace vectoriel sur un corps k est définie pour tout corps k, par exemple, $k = \mathbb{Q}$ ou $\mathbb{C}$, ou un corps fini $\mathbb{F}_q$ à q éléments (q étant une puissance d'un nombre premier p), ou le corps des fractions rationnelles $\mathbb{R}(X)$, etc.

[0] version du 23/1/2013

***Définition 0.1.2* (Espaces vectoriels).** — Soit k un corps. Un k-espace vectoriel V est un *groupe abélien* $(V, +)$ (c.-à-d., un ensemble muni d'une loi de groupe + commutative) muni d'une « opération » $(t, v) \mapsto t \cdot v$ de k sur V vérifiant les deux conditions suivantes :

(i) $1 \cdot v = v$ et $t \cdot (t' \cdot v) = (tt') \cdot v$

(ii) $(t + t') \cdot v = t \cdot v + t' \cdot v, \qquad t \cdot (v + v') = t \cdot v + t \cdot v'.$

On peut mémoriser la condition (i) en disant que 1 agit par l'identité et que l'opération est « associative », et la condition (ii) en disant que l'action de k sur V est « compatible avec l'addition » (dans k et dans V).

***Remarque 0.1.3* (Vecteur nul).** — Étant un groupe abélien, V est muni d'un élément zéro, qu'on notera provisoirement 0_V ou $\overrightarrow{0}$. Par exemple, dans $V = \mathbb{R}^3$, 0_V est le vecteur nul

$$\overrightarrow{0} = (0, 0, 0).$$

Notons 0 l'élément zéro du corps k. Alors la condition (ii) entraîne, pour tout $v \in V$,

$$0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v, \qquad \text{d'où } 0 \cdot v = 0_V = \overrightarrow{0}.$$

Par conséquent, le vecteur nul $0_V = \overrightarrow{0}$ sera noté simplement (par abus de notation) 0. Ainsi, on note $\{0\}$ l'espace vectoriel nul. Par exemple, dans $\mathbb{R}^2$ l'espace des solutions du système

$$\begin{cases} x - y = 0 \\ x + y = 0 \end{cases}$$

est l'espace vectoriel nul $\{0\} = \{(0, 0)\}$.

***Terminologie 0.1.4*.** — On dira que k est (relativement à V) le « *corps des scalaires* », et que les éléments de k sont les scalaires (ceux de V étant les vecteurs).

***Exemples 0.1.5*.** — 1) Pour tout $n \in \mathbb{N}^*$, $k^n = \{(x_1, \ldots, x_n) \mid x_i \in k\}$ est un k-espace vectoriel.

2) L'ensemble $M_{m,n}(k)$ des matrices à m lignes et n colonnes à coefficients dans k est un k-espace vectoriel. Lorsque $m = n$, on le note simplement $M_n(k)$.

3) L'anneau de polynômes $k[X]$ est un k-espace vectoriel.

***Définition 0.1.6* (Sous-espaces vectoriels).** — Soit V un k-espace vectoriel. Un *sous-espace vectoriel* (pour abréger, on dira « sev ») W de V est un sous-ensemble de V qui est un sous-groupe (en particulier, $0 \in W$) et qui est stable par l'opération de k. Ceci équivaut à dire que $W \neq \varnothing$ et que, pour tous $w, w' \in W$ et $t \in k$, on a $t \cdot w + w' \in W$.

***Exemples*.** — (1) Le plan « horizontal »

$$P = \{(x, y, 0) \mid x, y \in \mathbb{R}\},$$

donné par l'équation $z = 0$, est un sous-espace vectoriel de $\mathbb{R}^3$.

(2) L'ensemble des matrices $(a_{ij})_{1 \leq i,j \leq 3} \in M_3(k)$ qui sont triangulaires supérieures, i.e. telles que $a_{21} = a_{31} = a_{32} = 0$, est un sous-espace vectoriel de $M_3(k)$.

(3) L'ensemble $k_n[X]$ des polynômes en X de degré $\leq n$ est un sous-espace vectoriel de $k[X]$.

Le lemme suivant permet de construire de nombreux espaces vectoriels de fonctions :

***Lemme 0.1.7*.** — *Soient V un k-espace vectoriel et X un ensemble. Alors l'ensemble* $\mathrm{Hom}(X, V)$ *de toutes les applications $X \to V$ est muni d'une structure de k-espace vectoriel, définie comme suit : si $f, g \in \mathrm{Hom}(X, V)$ et $t \in k$, on définit l'application $t \cdot f + g : X \to V$ par :*

$$(t \cdot f + g)(x) = tf(x) + g(x),$$

pour tout $x \in X$.

Démonstration. Soient $f, g \in \mathrm{Hom}(X, V)$ et $t, t' \in k$; il faut voir que les conditions (i) et (ii) de 0.1.2 sont vérifiées. Ceci est facile : pour tout $x \in X$, on a $(1 \cdot f)(x) = 1f(x) = f(x)$ donc $1 \cdot f = f$, et

$$\big(t \cdot (t' \cdot f)\big)(x) = t\big((t' \cdot f)(x)\big) = t(t' f(x)) = (tt')f(x) = \big((tt') \cdot f\big)(x),$$

donc $t \cdot (t' \cdot f) = (tt') \cdot f$. On vérifie de même la condition (ii).

Exemples 0.1.7.1. — (1) L'ensemble $k^{\mathbb{N}}$ de toutes les suites $(u_n)_{n\in\mathbb{N}}$ d'éléments de k muni de l'addition et de l'opération de k définies « terme à terme », c.-à-d.,

$$(u_n)_{n\in\mathbb{N}} + (v_n)_{n\in\mathbb{N}} = (u_n + v_n)_{n\in\mathbb{N}}, \qquad t \cdot (u_n)_{n\in\mathbb{N}} = (t \cdot u_n)_{n\in\mathbb{N}},$$

est un k-espace vectoriel. En effet, ceci coïncide avec la structure définie plus haut si on regarde une suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de k comme l'application $\mathbb{N} \to k$, $n \mapsto u_n$.

(2) Soit I un intervalle de $\mathbb{R}$. Alors l'ensemble $\mathrm{Fonc}(\mathrm{I},\mathbb{R})$ de toutes les fonctions $I \to \mathbb{R}$ est un $\mathbb{R}$-espace vectoriel. Pour les applications à l'analyse, il est plus intéressant de constater que si $t \in \mathbb{R}$ et si $f, g : I \to \mathbb{R}$ sont continues, resp. de classe C^1, resp. C^2, …, resp. C^∞, alors $t \cdot f + g$ est encore continue (i.e. de classe C^0), resp. C^1, …, resp. C^∞. Par conséquent, pour tout $d \in \mathbb{N} \cup \{\infty\}$, l'ensemble $\mathscr{C}^d(I,\mathbb{R})$ des fonctions $f : I \to \mathbb{R}$ de classe C^d est un $\mathbb{R}$-espace vectoriel.

***Définition 0.1.8* (Applications linéaires et endomorphismes).** — Soient k un corps, V, W deux k-espaces vectoriels. On dit qu'une application $\phi : V \to W$ est une *application linéaire* (ou « homomorphisme d'espaces vectoriels ») si elle préserve l'addition et l'opération des scalaires, c.-à-d., si pour tout $v, v' \in V$ et $t \in k$ on a :

$$\phi(v + v') = \phi(v) + \phi(v'), \qquad \phi(t \cdot v) = t \cdot \phi(v).$$

Notons qu'on peut regrouper ces deux conditions en une seule condition :

$$\text{(AL)} \qquad \phi(t \cdot v + v') = t \cdot \phi(v) + \phi(v')$$

et bien sûr cette condition implique (et est impliquée par) la suivante :

$$\phi(t \cdot v + t' \cdot v') = t \cdot \phi(v) + t' \cdot \phi(v').$$

Si $W = V$, on dit alors que ϕ est un *endomorphisme* de V.

Exemples 0.1.9. — a) Soit $V = \mathbb{R}[X]$; l'application d qui à tout polynôme $P = a_n X^n + \cdots + a_1 X + a_0$ associe le polynôme dérivé $P' = n a_n X^{n-1} + \cdots + a_1$ est une application linéaire de V dans V.

b) Soit $V = \mathscr{C}^0([0,1],\mathbb{R})$ le $\mathbb{R}$-espace vectoriel des fonctions continues $f : [0,1] \to \mathbb{R}$. Alors l'application

$$V \to \mathbb{R}, \qquad f \mapsto \int_0^1 f(x)dx$$

est linéaire. Par contre, l'application $f \mapsto \int_0^1 f^2(x)dx$ ne l'est pas.

***Définition 0.1.10* (Isomorphismes).** — Soient V, W deux k-espaces vectoriels, et $\phi : V \to W$ une application linéaire. Suivant des principes généraux, on dit que ϕ est un *isomorphisme* (d'espaces vectoriels) si elle est *bijective* et si l'application inverse $\psi = \phi^{-1}$ est linéaire.

En fait, la seconde condition est automatiquement vérifiée. En effet, soient $w, w' \in W$ et $t \in k$; comme ϕ est bijective il existe $v, v' \in V$ uniques tels que $\phi(v) = w$ et $\phi(v') = w'$. Alors

$$\phi(t \cdot v + v') = t \cdot \phi(v) + \phi(v') = t \cdot w + w',$$

donc appliquant ψ à cette égalité on obtient

$$\psi(t \cdot w + w') = t \cdot v + v' = t \cdot \psi(v) + \psi(v').$$

Donc : *toute application linéaire bijective est un isomorphisme.*

Exemple 0.1.11. — On rappelle que l'ensemble $k^{\mathbb{N}}$ de toutes les suites d'éléments de k est un k-espace vectoriel (cf. 0.1.7.1). Soient $a, b \in k$ et soit $\mathscr{S}(a,b)$ le sous-ensemble de $k^{\mathbb{N}}$ formé des suites $(u_n)_{n\in\mathbb{N}}$ vérifiant la relation de récurrence linéaire :

$$(*) \qquad u_{n+2} = a u_{n+1} + b u_n.$$

Alors $\mathscr{S}(a,b)$ est un sous-espace vectoriel de $k^{\mathbb{N}}$ (le vérifier !). De plus, l'application $\phi : \mathscr{S}(a,b) \to k^2$ qui à toute suite $(u_n)_{n\in\mathbb{N}}$ associe le couple (u_0, u_1), est linéaire (le vérifier !) ; elle est surjective (car on peut choisir arbitrairement u_0 et u_1), et injective (car les u_n sont déterminés à partir de u_0 et u_1 par la formule $(*)$). Donc ϕ est bijective, donc c'est un isomorphisme d'espaces vectoriels :

$$\phi : \mathscr{S}(a,b) \xrightarrow{\sim} k^2.$$

Exercices 0.1.12. — 1) Soit $k = \mathbb{R}$. Est-ce que l'ensemble des suites $(u_n)_{n\in\mathbb{N}}$ vérifiant la relation de récurrence

$$u_{n+2} = u_{n+1} + u_n^2$$

est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$?

2) Soient $k = \mathbb{C}$ et $\mathscr{S}(-1,-1)$ l'espace des suites de nombres complexes $(u_n)_{n\in\mathbb{N}}$ vérifiant la relation de récurrence linéaire

$$u_{n+2} = -u_{n+1} - u_n.$$

Soit $(w_n)_{n\in\mathbb{N}}$ l'élément de $\mathscr{S}(-1,-1)$ défini par $w_0 = 2$ et $w_1 = 1$. Pouvez-vous calculer w_{2010} et w_{2011} ? (Cf. la Feuille d'exercices 1.)

0.2. Familles génératrices, familles libres, bases et dimension

Définitions 0.2.1 **(Sous-espace engendré. Familles génératrices).** — Soit V un k-espace vectoriel.

(1) Soit S un sous-ensemble (fini ou infini) de V. On note $\boxed{\mathrm{Vect}(S)}$ l'ensemble de toutes les combinaisons linéaires *finies*

$$\sigma = t_1v_1 + \cdots + t_rv_r, \qquad \text{pour } r \in \mathbb{N}^* \text{ (variable)},\ v_i \in S,\ t_i \in k,$$

c'est un sous-espace vectoriel de V, car si $\sigma' = t_1'v_1' + \cdots + t_p'v_p'$ est une autre combinaison linéaire de ce type et si $\lambda \in k$, alors

$$\lambda\sigma + \sigma' = \lambda t_1v_1 + \cdots + \lambda t_rv_r + t_1'v_1' + \cdots + t_p'v_p'$$

est encore une combinaison linéaire du même type. De plus, si E est un sous-espace vectoriel de V contenant S, alors il contient toute combinaison linéaire σ comme ci-dessus, i.e. il contient $\mathrm{Vect}(S)$. Donc : $\boxed{\mathrm{Vect}(S) \text{ est le plus petit sous-espace vectoriel de } V \text{ contenant } S.}$ On l'appelle le sous-espace vectoriel *engendré* par S.

Dans la suite, on utilisera principalement ceci dans le cas où S est une famille *finie* de vecteurs $v_1, \dots, v_n$; dans ce cas, on a simplement :

$$\mathrm{Vect}(v_1, \dots, v_n) = \{t_1v_1 + \cdots + t_nv_n \mid t_1, \dots, t_n \in k\}.$$

(2) On dit que la famille $\mathscr{F} = (v_1, \dots, v_n)$ est une *famille génératrice* de V si $\mathrm{Vect}(\mathscr{F}) = V$, c.-à-d., si tout élément de V s'écrit comme combinaison linéaire de $v_1, \dots, v_n$. Dans ce cas, on dit aussi que les vecteurs $v_1, \dots, v_n$ *engendrent* V.

Il résulte de la définition que : *toute famille contenant une famille génératrice est génératrice.*

Exemple 0.2.2. — Pour tout $n \in \mathbb{N}$, l'espace k^n est engendré par les vecteurs

$$e_1 = (1, 0, \dots, 0), \quad e_2 = (0, 1, 0, \dots, 0), \quad \cdots, \quad e_n = (0, \dots, 0, 1).$$

Définition 0.2.3 **(Familles libres ou liées).** — Soient V un k-espace vectoriel et $\mathscr{F} = (v_1, \dots, v_n)$ une famille d'éléments de V. On dit que $v_1, \dots, v_n$ sont *linéairement indépendants*, et que $\mathscr{F}$ est une *famille libre*, s'il n'existe pas de relation linéaire non triviale entre les v_i, c.-à-d., si la condition suivante est vérifiée :

(FL) pour *tous* $t_1, \dots, t_n \in k$, si $t_1v_1 + \cdots + t_nv_n = 0$, *alors* $t_1 = 0 = \cdots = t_n$.

Il résulte de la définition que : *toute sous-famille d'une famille libre est libre.*

Au contraire, on dit que $v_1, \dots, v_n$ sont *linéairement dépendants*, et que $\mathscr{F}$ est une *famille liée*, s'il existe une relation linéaire non triviale entre les v_i, c.-à-d., s'il existe des scalaires non tous nuls $t_1, \dots, t_n$, tels que $t_1v_1 + \cdots + t_nv_n = 0$. Dans ce cas, si par exemple $t_i \neq 0$, on peut exprimer v_i en fonction des v_j, pour $j \neq i$:

$$v_i = -\sum_{j\neq i} \frac{t_j}{t_i}\, v_j.$$

Il résulte de la définition que : *toute famille contenant une famille liée est liée.*

Exemple 0.2.4. — Dans k^n, la famille $(e_1, \dots, e_n)$ (cf. 0.2.2) est libre. En effet, *pour tous* $t_1, \dots, t_n \in k$ on a

$$t_1e_1 + \cdots + t_ne_n = (t_1, \dots, t_n),$$

donc si la somme de gauche est nulle, alors $t_1 = 0 = \cdots = t_n$.

***Définition 0.2.5* (Bases).** — Soient V un k-espace vectoriel. On dit qu'une famille $\mathscr{B} = (v_1, \dots, v_n)$ est une *base* de V si tout élément v de V *s'écrit de façon unique comme combinaison linéaire des* v_i, c.-à-d., si pour tout $v \in V$, *il existe un unique n-uplet* $(t_1, \dots, t_n) \in k^n$ *tel que* $v = t_1 v_1 + \cdots + t_n v_n$. Ceci équivaut à dire que la famille $\mathscr{B}$ est à la fois génératrice et libre.

Exemples 0.2.6. — 1) Lorsque $V = k^n$, la famille $(e_1, \dots, e_n)$ (cf. 0.2.2) est une base, appelée la *base canonique de k^n.*

2) Soit $M_{m,n}(k)$ le k-espace vectoriel des matrices à m lignes et n colonnes à coefficients dans k. On note E_{ij} la « *matrice élémentaire* » dont tous les coefficients sont nuls, sauf celui d'indice (i,j) (c.-à-d., celui situé sur la ligne i et la colonne j), qui vaut 1. Alors, toute matrice $A \in M_{m,n}(k)$ *s'écrit de façon unique* comme combinaison linéaire des E_{ij} :

$$A = \sum_{\substack{i=1,\dots,m \\ j=1,\dots,n}} a_{ij}\, E_{ij},$$

où a_{ij} est le coefficient d'indice (i,j) de A. Donc la famille $(E_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$ est une *base* de $M_{m,n}(k)$.

3) La famille $(1, X, \dots, X^d)$ est une base de l'espace vectoriel $k_d[X]$ des polynômes de degré $\leq d$. En effet, tout polynôme $P \in k_d[X]$ s'écrit de façon unique

$$P = a_0 + \cdots + a_d X^d, \qquad \text{avec} \quad a_i \in k.$$

Définition 0.2.7. — Soit V un k-espace vectoriel. Disons provisoirement que V est *finiment engendré* (ou « de type fini », cf. le cours LM 125) s'il est engendré par un nombre fini de vecteurs $v_1, \dots, v_p$.

Remarque : il existe des k-espaces vectoriels qui ne sont pas finiment engendrés, par exemple, l'espace vectoriel $k[X]$ (cf. Exercice 10 de la Feuille 1), mais dans ce cours on s'intéressera à ceux qui le sont.

Rappelons le résultat suivant, déjà vu en LM 125 :

***Théorème 0.2.8* (Dimension d'un espace vectoriel).** — *Soit V un k-espace vectoriel finiment engendré.*

(i) *Il existe des bases de V, et toutes ont même cardinal n ; cet entier s'appelle la dimension de V sur k et se note* $\dim_k V$ *ou simplement* $\dim V$.

(ii) *De toute famille génératrice $\mathscr{F}$ on peut extraire une base, en particulier $\mathscr{F}$ est de cardinal $\geq n$; de plus si* $\operatorname{card}(\mathscr{F}) = n$ *alors $\mathscr{F}$ est une base de V.*

(iii) *Toute famille libre est de cardinal $\leq n$, et toute famille libre de cardinal n est une base de V.*

(iv) « Théorème de la base incomplète » *: Toute famille libre peut être complétée en une base de V.*

(v) *Tout sous-espace W de V est de dimension finie $\leq \dim_k V$; de plus si $\dim_k W = \dim_k V$, alors $W = V$. En d'autres termes, tout sous-espace vectoriel distinct de V est de dimension $< \dim_k V$.*

Démonstration. Ceci a été vu en L1. Pour être complet, on redonne la démonstration dans un appendice à la fin de ce chapitre, où on introduira aussi les notions de familles génératrices ou libres dans un espace vectoriel arbitraire (i.e. qui n'est pas nécessairement finiment engendré).

Terminologie 0.2.9. — En raison du théorème précédent, on dira désormais « k-espace vectoriel *de dimension finie* » au lieu de « k-espace vectoriel finiment engendré », et si $n = \dim_k V$, on dira que V est de dimension n.

D'après les exemples de 0.2.6, k^n est de dimension n, $M_{m,n}(k)$ de dimension mn, et $k_d[X]$ de dimension $d+1$.

***Définition 0.2.10* (Coordonnées relativement à une base).** — Soit V un k-espace vectoriel de dimension n et soit $\mathscr{B} = (v_1, \dots, v_n)$ une base de V. Alors tout $v \in V$ s'écrit de façon unique

$$v = x_1 v_1 + \cdots + x_n v_n;$$

on dit que $(x_1, \dots, x_n)$ sont les *coordonnées de v par rapport à la base* $\mathscr{B} = (v_1, \dots, v_n)$. Donc la donnée de $\mathscr{B}$ fournit un isomorphisme de k-espaces vectoriels

$$\phi_{\mathscr{B}} : \quad k^n \xrightarrow{\sim} V, \qquad (x_1, \dots, x_n) \mapsto x_1 v_1 + \cdots + x_n v_n.$$

Remarque 0.2.11. — Remarquons qu'une base de V est un n-uplet *ordonné* ; par exemple, si $\mathscr{B} = (v_1, v_2)$ est une base de V, alors $\mathscr{C} = (v_2, v_1)$ est une base de V distincte de $\mathscr{B}$: l'image de $(1,2) \in \mathbb{R}^2$ par $\phi_{\mathscr{B}}$ est le vecteur $v_1 + 2v_2$, tandis que son image par $\phi_{\mathscr{C}}$ est le vecteur $v_2 + 2v_1 \neq v_1 + 2v_2$.

Proposition 0.2.12. — *Soit $f : V \to W$ une application linéaire.*

a) *Si f est injective et si $\mathscr{F} = (v_1, \dots, v_n)$ est une famille libre de V, alors $f(\mathscr{F})$ est libre.*

b) *Si f est surjective et si $\mathscr{F} = (v_1, \dots, v_n)$ est une famille génératrice de V, alors $f(\mathscr{F})$ engendre W.*

c) *Si f est bijective et si $\mathscr{B} = (v_1, \dots, v_n)$ est une base de V, alors $f(\mathscr{B})$ est une base de W, d'où $\dim W = n = \dim V$.*

Démonstration. a) Supposons f injective et soit $\mathscr{F} = (v_1, \dots, v_n)$ une famille libre de V. Supposons qu'il existe une relation linéaire dans W :

$$t_1 f(v_1) + \cdots + t_n f(v_n) = 0,$$

avec $t_i \in k$. Alors $0 = f(t_1v_1 + \cdots + t_nv_n)$ d'où, puisque f est injective, $t_1v_1 + \cdots + t_nv_n = 0$, donc comme $\mathscr{F}$ est libre, $t_i = 0$ pour $i = 1, \dots, n$. Ceci montre que $f(\mathscr{F})$ est libre.

b) Supposons f surjective et soit $\mathscr{F} = (v_1, \dots, v_n)$ une famille génératrice de V. Soit $w \in W$; comme f est surjective, il existe $v \in V$ tel que $f(v) = w$. Comme $\mathscr{F}$ engendre V, il existe $t_1, \dots, t_n \in k$ tels que $v = t_1v_1 + \cdots + t_nv_n$, d'où

$$w = t_1 f(v_1) + \cdots + t_n f(v_n).$$

Ceci montre que $f(\mathscr{F})$ engendre W.

c) Supposons f bijective et soit $\mathscr{B} = (v_1, \dots, v_n)$ une base de V. D'après a) et b), $f(\mathscr{B})$ est une famille libre et génératrice de W, donc une base de W ; alors $\dim W = n = \dim V$.

Corollaire 0.2.13. — (i) *Tout k-espace vectoriel V de dimension finie est isomorphe (de façon non canonique) à k^n, pour un unique n, égal à $\dim_k V$.*

(ii) *Deux k-espaces vectoriels de dimension finie V et W sont isomorphes si et seulement si ils ont la même dimension.*

Démonstration. (i) Si V est de dimension n alors, par le choix d'une base, il est isomorphe à k^n. (Cet isomorphisme est « non canonique » car il dépend du choix de la base.) Réciproquement, si $V \simeq k^m$, alors d'après la proposition précédente, on a $\dim V = \dim k^m = m$, donc $m = n$. En particulier, $k^m \not\simeq k^n$ si $m \neq n$.

(ii) Si $V \simeq W$, alors $\dim_k V = \dim_k W$, d'après la proposition précédente. Réciproquement, si $\dim_k V = \dim_k W = n$, alors V et W sont tous deux isomorphes à k^n.

Exemples 0.2.14. — 1) La droite d'équation $x_1 + x_2 = 0$ dans $\mathbb{R}^2$ admet pour base le vecteur $e_1 - e_2$, mais on peut tout aussi bien choisir le vecteur $e_2 - e_1$.

2) Le plan d'équation $x_1 + x_2 + x_3 = 0$ dans $\mathbb{R}^3$ admet pour base $(e_1 - e_2, e_2 - e_3)$, mais on peut aussi choisir $(e_1 - e_3, e_1 - e_3)$, ou $(e_1 - e_2, e_1 + e_2 - 2e_3)$, ou $(e_1 - (e_1 + e_2 + e_3)/3, e_1 + e_2 - 2(e_1 + e_2 + e_3)/3)$, etc.

Exemple 0.2.15. — Reprenons l'espace $\mathscr{S}(a, b)$ des suites $(u_n)_{n\in\mathbb{N}}$ d'éléments de k vérifiant la relation de récurrence linéaire $u_{n+2} = au_{n+1} + bu_n$. On a vu (cf. 0.1.11) qu'il est isomorphe à k^2, par l'application $(u_n)_{n\in\mathbb{N}} \mapsto (u_0, u_1)$, donc est de dimension 2. Supposons que le polynôme $P = X^2 - aX - b$ ait deux racines distinctes $\lambda \neq \mu$ dans k. Considérons les éléments $\mathbf{u} = (u_n)_{n\in\mathbb{N}}$ et $\mathbf{v} = (v_n)_{n\in\mathbb{N}}$ de $\mathscr{S}(a, b)$ définis par

$$u_0 = 1 = v_0, \qquad u_1 = \lambda, \quad v_1 = \mu.$$

Alors la famille $(\mathbf{u}, \mathbf{v})$ est libre (car si $s\mathbf{u} + t\mathbf{v} = 0$, on obtient $s + t = 0 = s\lambda + t\mu$, donc $t = -s$ et $s(\lambda - \mu) = 0$, d'où $s = 0$), donc est une base de $\mathscr{S}(a, b)$. Par conséquent, tout élément $\mathbf{w} = (w_n)_{n\in\mathbb{N}}$ de $\mathscr{S}(a, b)$ s'écrit de façon unique

$$\mathbf{w} = s\mathbf{u} + t\mathbf{v},$$

et s, t sont déterminés par les conditions $s + t = w_0$ et $s\lambda + t\mu = w_1$. Ceci permet-il de calculer w_{2010} et w_{2011} dans l'exercice 0.1.12 ?

0.3. Noyau, image, et théorème du rang

***Définition 0.3.1* (Noyau, image et rang).** — Soit $f : V \to W$ une application linéaire. D'une part, on définit son noyau

$$\operatorname{Ker}(f) = \{v \in V \mid f(v) = 0\},$$

c'est un sous-espace vectoriel de V. Noter que f est *injective* si et seulement si $\operatorname{Ker}(f) = \{0\}$: en effet, on a $f(v) = f(v') \iff f(v - v') = 0$.

D'autre part, on définit son image

$$\operatorname{Im}(f) = f(V) = \{f(v) \mid v \in V\} \subseteq W,$$

c'est un sous-espace vectoriel de V. Alors f est *surjective* si et seulement si $\operatorname{Im}(f) = W$.

Lorsque $\operatorname{Im}(f)$ est *de dimension finie* r (ce qui est le cas si W ou V est de dimension finie, cf. ci-dessous), l'entier $r = \dim \operatorname{Im}(f)$ est appelé le **rang** de f et est noté $\operatorname{rg}(f)$ ou $\operatorname{rang}(f)$.

***Théorème 0.3.2* (Théorème du rang).** — *Soit $f : V \to W$ une application linéaire, avec V de dimension finie n. Alors*

$$n = \dim V = \dim \operatorname{Ker}(f) + \operatorname{rg}(f).$$

(En particulier, f est surjective si et seulement si W est de dimension $\operatorname{rg}(f) = n - \dim \operatorname{Ker}(f)$.)

Démonstration. Comme V est de dimension finie n, alors $\operatorname{Ker}(f)$ est de dimension finie $d \leq n$; soit $\mathscr{K} = (e_1, \dots, e_d)$ une base de $\operatorname{Ker}(f)$.

<u>1ère méthode</u> (la plus courte). Complétons $\mathscr{K}$ en une base $\mathscr{B} = (e_1, \dots, e_d, e_{d+1}, \dots, e_n)$ de V. Alors $\operatorname{Im}(f) = f(V)$ est engendré par $f(\mathscr{B})$ (cf. Prop. 0.2.12), donc par $f(e_{d+1}), \dots, f(e_n)$ puisque $f(e_i) = 0$ pour $i \leq d$. Montrons que ces vecteurs sont linéairement indépendants : supposons qu'on ait une relation de dépendance linéaire

$$0 = t_1 f(e_{d+1}) + \cdots + t_{n-d} f(e_n) = f(t_1 e_{d+1} + \cdots + t_{n-d} e_n)$$

alors le vecteur $t_1 e_{d+1} + \cdots + t_{n-d} e_n$ appartient à $\operatorname{Ker}(f)$, donc est combinaison linéaire de $e_1, \dots, e_d$, d'où une égalité

$$t_1 e_{d+1} + \cdots + t_{n-d} e_n - s_1 e_1 - \cdots - s_d e_d = 0.$$

Comme $(e_1, \dots, e_n)$ est une base de V, ceci implique $t_i = 0 = s_j$ pour tous i, j. Ceci montre que les vecteurs $f(e_{d+1}), \dots, f(e_n)$ sont linéairement indépendants, donc forment une base de $f(V)$, d'où $\dim f(V) = n - d$ et donc $\operatorname{rg}(f) = \dim f(V) = n - \dim \operatorname{Ker}(f)$.

<u>2ème méthode</u>. Soit toujours $\mathscr{K} = (e_1, \dots, e_d)$ une base de $\operatorname{Ker}(f)$, donnons une autre démonstration, qui sera utile plus loin (cf. 0.5.10). [1] Comme $\operatorname{Im}(f) = f(V)$ est engendré par n éléments (les images d'une base de V), $\operatorname{Im}(f)$ est de dimension finie $r \leq n$. Soit $(w_1, \dots, w_r)$ une base de $\operatorname{Im}(f)$ et pour $i = 1, \dots, r$, soit v_i un élément de V tel que $f(v_i) = w_i$. Alors la famille

$$\mathscr{B} = (e_1, \dots, e_d, v_1, \dots, v_r)$$

est une *base* de V. En effet, elle est *génératrice* : soit $v \in V$ arbitraire, son image $f(v)$ s'écrit $f(v) = t_1 w_1 + \cdots + t_r w_r$, d'où $f(v - t_1 v_1 - \cdots - t_r v_r) = 0$, donc $v - t_1 v_1 - \cdots - t_r v_r$ appartient à $\operatorname{Ker}(f)$, donc s'écrit $s_1 e_1 + \cdots + s_p e_p$, d'où

$$v = t_1 v_1 + \cdots + t_r v_r + s_1 e_1 + \cdots + s_p e_p.$$

Ceci montre que $\mathscr{B}$ est génératrice. Elle est aussi *libre* : si

$$0 = t_1 v_1 + \cdots + t_r v_r + s_1 e_1 + \cdots + s_p e_p$$

alors $0 = f(0) = t_1 w_1 + \cdots + t_r w_r$, donc chaque t_i est nul (puisque $(w_1, \dots, w_r)$ est libre), d'où $0 = s_1 e_1 + \cdots + s_p e_p$, donc chaque s_j est nul (puisque $(e_1, \dots, e_p)$ est libre). Ceci montre que $\mathscr{B}$ est aussi libre, donc est une base de V. Donc $\dim V = d + r = \dim \operatorname{Ker}(f) + \operatorname{rg}(f)$.

***Proposition 0.3.3*.** — *Soit V un k-espace vectoriel de dimension n et soit $u \in \operatorname{End}_k(V)$ ou, plus généralement, soit $u : V \to W$ une application linéaire, où $\dim W = n = \dim V$. Alors les conditions suivantes sont équivalentes :*

(i) *u est bijectif ;*

(ii) *u est injectif ;*

(iii) *u est surjectif.*

---

[1] Cette démonstration a l'avantage suivant. Elle montre que si une base $(w_1, \dots, w_r)$ de $\operatorname{Im}(f)$ est donnée à l'avance et si $v_1, \dots, v_r \in V$ vérifient $f(v_i) = w_i$ pour $i = 1, \dots, r$, alors $(e_1, \dots, e_d, v_1, \dots, v_r)$ est une base de V.

En effet, il est clair que (i) implique (ii) et (iii). Réciproquement, si u est injectif, i.e. $\mathrm{Ker}(u) = \{0\}$ (resp. surjectif, i.e. $\mathrm{Im}(u) = W$), il résulte du théorème du rang que u est aussi surjectif (resp. injectif), donc bijectif.

0.4. Applications linéaires et matrices

***Définition 0.4.1* (Espaces d'applications linéaires).** — Soient V, W deux k-espaces vectoriels. On note $\mathrm{Hom}_k(V, W)$ ou $\mathscr{L}(V, W)$ l'ensemble des applications linéaires de V dans W. C'est un k-espace vectoriel : plus précisément, c'est un sous-espace vectoriel du k-espace vectoriel $\mathrm{Fonc}(V, W)$ de toutes les fonctions $V \to W$ (cf. 0.1.7). Rappelons que si $t \in k$ et $\phi, \psi \in \mathrm{Fonc}(V, W)$ alors les fonctions $\phi + \psi$ et $t \cdot \phi$ sont définies comme suit : pour tout $v \in V$,

$$(*) \qquad (\phi + \psi)(v) = \phi(v) + \psi(v) \qquad \text{et} \qquad (t \cdot \phi)(v) = t \cdot \phi(v).$$

Il s'agit de voir que si $\phi, \psi : V \to W$ sont des applications *linéaires*, alors il en est de même de $\phi + \psi$ et de $t \cdot \phi$. Ceci se vérifie facilement : si $v, v' \in V$ et $s \in k$, alors

$$\begin{aligned}
(\phi + \psi)(s \cdot v + v') &= \phi(s \cdot v + v') + \psi(s \cdot v + v') && \text{(par définition)} \\
&= s \cdot \phi(v) + \phi(v') + s \cdot \psi(v) + \psi(v') && \text{(car } \phi, \psi \text{ linéaires)} \\
&= s \cdot (\phi + \psi)(v) + (\phi + \psi)(v') && \text{(par définition)}
\end{aligned}$$

et de même

$$(t \cdot \phi)(s \cdot v + v') = t \cdot \phi(s \cdot v + v') = ts \cdot \phi(v) + t \cdot \phi(v') = s \cdot (t \cdot \phi)(v) + (t \cdot \phi)(v').$$

Donc $\mathrm{Hom}_k(V, W) = \mathscr{L}(V, W)$ est bien un k-espace vectoriel ; on dit que c'est l'espace des applications linéaires de V dans W.

Supposons V *de dimension finie* n et soit $(e_1, \dots, e_n)$ une *base* de V (par exemple, $V = k^n$ et $(e_1, \dots, e_n)$ la base canonique). Soit $\phi \in \mathrm{Hom}_k(V, W)$, posons $w_i = \phi(e_i)$ pour $i = 1, \dots, n$; alors tout $v \in V$ s'écrit de façon unique $v = x_1 e_1 + \cdots + x_n e_n$ et l'on a

$$(*) \qquad \phi(v) = x_1 w_1 + \cdots + x_n w_n$$

donc ϕ est déterminée par la donnée des n vecteurs $w_1, \dots, w_n \in W$. Réciproquement, pour tout n-uplet $(w_1, \dots, w_n) \in W^n$, l'application $\phi : V \to W$ définie par la formule $(*)$ est linéaire. On a donc obtenu la

Proposition 0.4.2. — *Si $\mathscr{B} = (e_1, \dots, e_n)$ est une base de V, se donner une application linéaire $\phi : V \to W$* « est la même chose » *que se donner un n-uplet $(w_1, \dots, w_n) \in W$.*

Supposons de plus que W soit *de dimension finie* m et soit $\mathscr{C} = (f_1, \dots, f_m)$ une base de W. Alors, chaque $w_j = \phi(e_j)$ s'écrit de façon unique

$$w_j = a_{1j} f_1 + \cdots + a_{mj} f_m,$$

ce qu'on représente par le vecteur *colonne* (d'où le choix de l'indice j pour paramétrer ces colonnes) :

$$w_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

et donc ϕ est déterminée par la matrice suivante :

$$\mathrm{Mat}_{\mathscr{C},\mathscr{B}}(\phi) = \mathrm{Mat}_{(f_i),(e_j)}(\phi) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{n2} & \cdots & a_{mn} \end{pmatrix}$$

qui exprime les vecteurs $\phi(e_j)$ (les colonnes) en fonction de $f_1, \dots, f_m$. Noter que la dimension n de l'espace de *départ* V est le nombre de *colonnes*, et la dimension m de l'espace d'*arrivée* W est le nombre de *lignes*.

Réciproquement, pour toute matrice A comme ci-dessus, ses colonnes définissent de façon unique n vecteurs $w_1, \dots, w_n$ de W, à savoir

$$w_j = a_{1j} f_1 + \cdots + a_{mj} f_m,$$

et ce n-uplet $(w_1, \dots, w_n) \in W^n$ définit une application linéaire $\phi : V \to W$ dont la matrice associée est A. On obtient donc une *bijection* :

$$\mathrm{Hom}_k(V, W) \longleftrightarrow M_{m,n}(k).$$

De plus, on voit facilement que si A (resp. B) est la matrice associée à ϕ (resp. ψ), alors $tA + B$ est la matrice associée à $t\phi + \psi$, donc la bijection ci-dessus est un *isomorphisme d'espaces vectoriels.*

***Théorème 0.4.3* (Applications linéaires et matrices).** — *Soient $\mathscr{B} = (e_1, \dots, e_n)$ une base de V, et $\mathscr{C} = (f_1, \dots, f_m)$ une base de W. Si ϕ est une application linéaire $V \to W$, on note $\mathrm{Mat}_{\mathscr{C},\mathscr{B}}(\phi)$ sa matrice dans les bases : $\mathscr{B}$ « au départ » et $\mathscr{C}$ « à l'arrivée ».* [2]

(1) *L'application $\phi \mapsto \mathrm{Mat}_{\mathscr{C},\mathscr{B}}(\phi)$ est un isomorphisme d'espaces vectoriels :*

$$\mathrm{Hom}_k(V, W) \xrightarrow{\sim} M_{m,n}(k).$$

Donc le « slogan » à retenir est : « Des bases de V et W étant choisies, une application linéaire $V \to W$ est la même chose qu'une matrice à m lignes et n colonnes » .

(2) *Cet isomorphisme transforme la composition des applications linéaires en le produit des matrices : si U est un k-espace vectoriel de base $\mathscr{A} = (d_1, \dots, d_p)$ et si $\theta \in \mathrm{Hom}_k(U, V)$ et $\phi \in \mathrm{Hom}_k(V, W)$, on peut former la composée $\phi \circ \theta$:*

$$U \xrightarrow{\theta} V \xrightarrow{\phi} W,$$

et l'on a :

$$\boxed{\mathrm{Mat}_{\mathscr{C},\mathscr{A}}(\phi \circ \theta) = \mathrm{Mat}_{\mathscr{C},\mathscr{B}}(\phi) \cdot \mathrm{Mat}_{\mathscr{B},\mathscr{A}}(\theta).}$$

Démonstration. — On a déjà vu l'assertion (1), montrons l'assertion (2). Notons

$$A = \mathrm{Mat}_{\mathscr{C},\mathscr{B}}(\phi) = (a_{ij})_{\substack{j=1,\dots,n \\ i=1,\dots,m}} \qquad B = \mathrm{Mat}_{\mathscr{B},\mathscr{A}}(\theta) = (b_{j\ell})_{\substack{\ell=1,\dots,p \\ j=1,\dots,n}}$$

alors, pour tout $\ell = 1, \dots, p$, on a :

$$(\phi \circ \theta)(d_\ell) = \phi\big(\sum_{j=1}^n b_{j\ell}\, e_j\big) = \sum_{j=1}^n b_{j\ell}\, \phi(e_j) = \sum_{j=1}^n \sum_{i=1}^m b_{j\ell}\, a_{ij} f_i = \sum_{i=1}^m \big(\sum_{j=1}^n a_{ij} b_{j\ell}\big) f_i.$$

Donc le coefficient d'indice (i, ℓ) de $M = \mathrm{Mat}_{(f_i),(d_\ell)}(\phi \circ \theta)$ est $\sum_{j=1}^n a_{ij} b_{j\ell}$; ceci montre que $M = AB$. □

***Remarque 0.4.4*.** — Soit $A = (a_{ij}) \in M_{m,n}(k)$ et soient $(e_1, \dots, e_n)$ et $(f_1, \dots, f_m)$ les bases canoniques de k^n et k^m. Alors par l'isomorphisme précédent, A correspond à l'application linéaire $u : k^n \to k^m$ telle que, pour tout $j = 1, \dots, n$,

$$u(e_j) = \sum_{i=1}^m a_{ij}\, f_i.$$

On identifiera, chaque fois que ce sera utile, A à l'application linéaire $u : k^n \to k^m$ ainsi définie (i.e. la i-ième colonne de A est l'image du i-ième vecteur de la base canonique de k^n.

***Corollaire 0.4.5*.** — *Soient $A \in M_{m,n}(k)$, $B \in M_{n,p}(k)$ et $u : k^n \to k^m$, $v : k^p \to k^n$ les applications linéaires associées. Alors AB est la matrice de $u \circ v : k^p \to k^m$.*

***Remarque 0.4.6*.** — Soient $B \in M_{m,n}(k)$ et $A \in M_{n,p}(k)$. Si l'on note $A_1, \dots, A_p \in k^n$ les colonnes de A, alors les colonnes de BA sont les vecteurs $BA_1, \dots, BA_p \in k^m$. [3]

En effet, ceci se voit directement sur la formule du produit matriciel : $(BA)_{ij} = \sum_{\ell=1}^n b_{i\ell}\, a_{\ell j}$. Ou bien, on peut raisonner comme suit : soit $(e_1, \dots, e_p)$ la base canonique de k^p, alors A correspond à l'application linéaire qui envoie chaque e_j sur le vecteur $Ae_j = A_j \in k^n$, et BA correspond à l'application linéaire qui envoie chaque e_j sur le vecteur $B(Ae_j) = BA_j \in k^n$.

***Remarque 0.4.7*.** — On ne peut effectuer le produit AB de deux matrices $A \in M_{m,n}(k)$ et $B \in M_{q,p}(k)$ que si $n = q$, c.-à-d., si le nombre de colonnes de A égale le nombre de lignes de B.

En raison de son importance, répétons le théorème 0.4.3 et le corollaire 0.4.5 dans le cas particulier où *l'espace de départ est le même que celui d'arrivée*, c.-à-d., le cas où l'on considère des *endomorphismes* d'un espace V de dimension finie n, ou des matrices *carrées de taille* n.

---

[2] L'ordre est choisi afin d'avoir, pour la composition des appplications, la formule qui figure dans le point (2) du théorème.
[3] Cette remarque sera utile pour la construction du déterminant, voir Chap. 2.

***Proposition 0.4.8* (Endomorphismes de $V \simeq k^n$).** — *Le k-espace vectoriel $M_n(k)$ est un anneau (non commutatif si $n \geq 2$), c.-à-d., la multiplication des matrices carrées est associative : $A(BC) = (AB)C$, distributive à gauche et à droite par rapport à l'addition : $(A+B)C = AC+BC$ et $A(B+C) = AB+AC$, et la matrice identité I_n est élément neutre. De plus, $M_n(k)$ est une k-*algèbre*, c.-à-d.,*[4] *pour $A, B \in M_n(k)$ et $t \in k$, on a $t \cdot (AB) = (t \cdot A)B = A(t \cdot B)$, où $\cdot$ désigne la loi externe.*

De même, si V est un k-espace vectoriel de dimension n, l'espace des endomorphismes $\mathrm{End}_k(V)$ est une k-algèbre (la multiplication étant la composition des endomorphismes). De plus, si l'on choisit une base $\mathscr{B} = (e_1, \ldots, e_n)$ de V, l'application

$$\mathrm{End}_k(V) \to M_n(k), \qquad u \mapsto \mathrm{Mat}_{\mathscr{B}}(u)$$

est un isomorphisme d'anneaux et de k-espaces vectoriels, c.-à-d., un isomorphisme de k-algèbres.

***Définition 0.4.9* (Noyau, image et rang d'une matrice).** — Soit $A \in M_{m,n}(k)$, on définit son noyau $\mathrm{Ker}(A)$, son image $\mathrm{Im}(A)$, et son rang, noté $\mathrm{rang}(A)$ ou $\mathrm{rg}(A)$, comme le noyau, l'image et le rang de l'application linéaire $u : k^n \to k^m$ associée. On a $\mathrm{rang}(u) \leq n$ (d'après le théorème du rang), et $\mathrm{rang}(u) \leq m$ (puisque $\mathrm{Im}(u)$ est un sous-espace de k^m), donc $\mathrm{rang}(u) \leq \mathrm{Min}(m, n)$.

Or, l'image de u est le sous-espace de k^m engendré par les vecteurs colonnes $C_1, \ldots, C_n$ de A, donc par définition $\mathrm{rang}(A)$ est le nombre maximum de *colonnes* de A linéairement indépendantes, et l'on a $\mathrm{rang}(A) \leq \mathrm{Min}(m, n)$.

On verra plus bas que $\mathrm{rang}(A)$ est aussi le nombre maximum de *lignes* linéairement indépendantes, et l'on donnera des moyens algorithmiques pour calculer $\mathrm{rang}(A)$.

***Définition 0.4.10* (Transposée d'une matrice).** — Soit dans $M_{m,n}(k)$:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Sa *transposée*, notée ${}^t A$, est la matrice de $M_{n,m}(k)$ suivante :

$${}^t A = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}$$

c.-à-d., la j-ème colonne de A est devenue la j-ème ligne de ${}^t A$, c.-à-d., $({}^t A)_{ji} = a_{ij}$. On a évidemment

$$(\star) \qquad \boxed{{}^t({}^t A) = A.}$$

***Proposition 0.4.11*.** — *L'application $A \mapsto {}^t A$ est linéaire : si $A, A' \in M_{m,n}(k)$ et $s \in k$,*

$${}^t(s \cdot A + A') = s \cdot {}^t A + {}^t A'.$$

De plus, si $B \in M_{n,p}(k)$, alors $BA \in M_{m,p}(k)$ et l'on a dans $M_{p,m}(k)$ l'égalité :

$$(\star\star) \qquad \boxed{{}^t(AB) = {}^t B \, {}^t A.}$$

Démonstration. Écrivons $A = (a_{ij})$ et $A' = (a'_{ij})$. Alors $sA + A' \in M_{m,n}(k)$ est la matrice $(sa_{ij} + a'_{ij})$, et sa transposée est la matrice $C \in M_{n,m}(k)$ telle que, pour tout (j, i),

$$C_{ji} = (sA + A')_{ij} = sa_{ij} + a'_{ij} = s({}^t A)_{ji} + ({}^t A')_{ji},$$

donc $C = s \cdot {}^t A + {}^t A'$. Puis, si l'on pose $B = (b_{j\ell}) \in M_{n,p}(k)$, alors pour tout couple (i, ℓ) on a

$$\big({}^t(AB)\big)_{\ell i} = (AB)_{i\ell} = \sum_{r=1}^{n} a_{ir} b_{r\ell} = \sum_{r=1}^{n} ({}^t B)_{\ell r} \cdot ({}^t A)_{ri} = \big({}^t B \, {}^t A\big)_{\ell i}$$

ce qui montre que ${}^t(AB) = {}^t B \, {}^t A$. $\square$

---

[4] cf. Définition 4.2.1 dans le Chap. 3.

0.5. Changements de base

***Définition 0.5.1* (Automorphismes et matrices inversibles).** — 1) Soit V un k-espace vectoriel. On dit qu'un endomorphisme f de V est un **automorphisme** s'il possède un inverse dans $\operatorname{End}_k(V)$, i.e. s'il existe un endomorphisme g de V tel que $f \circ g = \mathrm{id}_V = g \circ f$. Ceci équivaut à dire que f est bijectif, car on a vu (cf. 0.1.10) que dans ce cas l'application inverse g est automatiquement linéaire.

2) On note $\mathrm{GL}(V)$ l'ensemble des automorphismes de V ; c'est un groupe pour la composition des endomorphismes : en effet, la composition des endomorphismes est associative, l'application identique est élément neutre, et si f, g sont inversibles, alors $f \circ g$ l'est aussi, son inverse étant $g^{-1} \circ f^{-1}$ (puisque $f \circ g \circ g^{-1} \circ f^{-1} = \mathrm{id}_V = g^{-1} \circ f^{-1} \circ f \circ g$). [5]

3) De même, on dit qu'une matrice $A \in M_n(k)$ est **inversible** s'il existe $B \in M_n(k)$ vérifiant $AB = I_n = BA$, où I_n désigne la matrice identité de taille n ; dans ce cas B est notée A^{-1}. On note $\mathrm{GL}_n(k)$ l'ensemble des matrices inversibles.

Comme la correspondance bijective $\operatorname{End}_k(k^n) \longleftrightarrow M_n(k)$ transforme la composition des endomorphismes en le produit des matrices, on voit qu'une matrice A est inversible si et seulement si l'endomorphisme correspondant u de k^n est bijectif, et dans ce cas A^{-1} est la matrice de u^{-1} ; de plus $\mathrm{GL}_n(k)$ est un groupe pour la multiplication des matrices : la matrice I_n est élément neutre, et si A, B sont inversibles, alors AB l'est aussi, son inverse étant $B^{-1}A^{-1}$.

La proposition suivante est importante et très utile :

Proposition 0.5.2. — (i) *Soit V un k-espace vectoriel* de dimension finie *et soient $u, v \in \operatorname{End}_k(V)$ tels que $u \circ v = \mathrm{id}_V$. Alors u et v sont bijectifs et $u = v^{-1}$.*

(i′) *Soient $A, B \in M_n(k)$ telles que $AB = I_n$. Alors on a aussi $BA = I_n$ et donc A et B sont inversibles et inverses l'une de l'autre.*

(ii) *Si A est inversible alors ${}^tA$ est inversible et l'on a $({}^tA)^{-1} = {}^t(A^{-1})$.*

Démonstration. (i) Pour tout $x \in V$, on a $x = u(v(x))$, donc u est surjectif, et v est injectif. Donc, d'après la proposition 0.3.3, u et v sont bijectifs ; alors en multipliant l'égalité $u \circ v = \mathrm{id}_V$ à gauche par u^{-1} (ou bien à droite par v^{-1}), on obtient que $v = u^{-1}$.

(i′) Notons u (resp. v) l'endomorphisme de k^n correspondant à A (resp. B). Comme $AB = I_n$ équivaut à $u \circ v = \mathrm{id}_V$ alors, d'après (i), u et v sont bijectifs et inverses l'un de l'autre, donc il en est de même de A et B et l'on a $B = A^{-1}$ et $BA = I_n$.

(ii) Supposons A inversible, alors il existe $B \in M_n(k)$ telle que $AB = I_n = BA$. Prenant la transposée de ces matrices, on obtient, puisque ${}^tI_n = I_n$:

$$ {}^tB\,{}^tA = {}^t(AB) = I_n = {}^t(BA) = {}^tA\,{}^tB. $$

Ceci montre que ${}^tA$ est inversible, d'inverse ${}^tB = {}^t(A^{-1})$.

Remarque 0.5.3. — 1) Soit $V = \mathbb{R}[X]$, soit I l'opérateur « d'intégration », qui envoie chaque monôme X^n sur $X^{n+1}/(n+1)$, et soit D l'opérateur de dérivation, qui envoie chaque polynôme P sur le polynôme dérivé P'. Alors $D \circ I = \mathrm{id}_V$, donc D est surjectif et I injectif, mais D n'est pas injectif car $D(1) = 0$, et I n'est pas surjectif car son image est formée des polynômes de terme constant nul.

2) De même, soit V l'espace des suites $(u_n)_{n\in\mathbb{N}}$ et soient I (resp. D) l'opérateur qui envoie toute suite $(u_n)_{n\in\mathbb{N}}$ sur

$$ (0, u_0, u_1, u_2, \dots) \qquad \text{resp.} \qquad (u_1, u_2, u_3, \dots). $$

Alors $D \circ I = \mathrm{id}_V$, donc D est surjectif et I injectif, mais D n'est pas injectif car D annule la suite telle que $u_0 = 1$ et $u_i = 0$ pour $i \geq 1$, et I n'est pas surjectif car son image est formée des suites de terme u_0 nul.

Ces deux exemples montrent que si V est un espace vectoriel qui n'est pas de dimension finie et si $u, v \in \operatorname{End}_k(V)$ vérifient $u \circ v = \mathrm{id}_V$, alors u et v ne sont pas nécessairement bijectifs.

Lemme 0.5.4. — *Soient f un endomorphisme d'un espace vectoriel V de dimension finie, $\mathscr{B} = (v_1, \dots, v_n)$ une base de V, posons $w_i = f(v_i)$. Si $(w_1, \dots, w_n)$ est une base de V, alors f est bijective, et son inverse est l'endomorphisme g de V défini par $g(w_i) = v_i$ pour $i = 1, \dots, n$.*

---

[5] Attention ! Noter l'inversion de l'ordre des facteurs : $(f \circ g)^{-1}$ égale $g^{-1} \circ f^{-1}$, tandis que $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$!

Démonstration. On suppose que $\mathscr{C} = (w_1, \dots, w_n)$ est une base de V. Alors f est surjectif, car pour tout $w \in V$ il existe $t_1, \dots, t_n \in k$ tels que

$$w = t_1 w_1 + \cdots + t_n w_n = f(t_1 v_1 + \cdots + t_n v_n).$$

Donc, d'après la proposition 0.3.3, f est bijectif. (On peut aussi voir directement que f est injectif : soit $v \in \operatorname{Ker}(f)$, il existe $t_1, \dots, t_n \in k$ tels que $v = x_1 v_1 + \cdots + x_n v_n$, alors $0 = f(v) = x_1 w_1 + \cdots + x_n w_n$ donc, puisque $(w_1, \dots, w_n)$ est libre, $t_1 = 0 = \cdots = t_n$, d'où $v = 0$.)

Soit g l'endomorphisme de V défini par $g(w_i) = v_i$, pour $i = 1, \dots, n$. Alors on a, d'une part, $(g \circ f)(v_i) = v_i$ pour tout i, d'où $g \circ f = \mathrm{id}_V$, et, d'autre part, $(f \circ g)(w_i) = w_i$ pour tout i, d'où $f \circ g = \mathrm{id}_V$.

***Définition 0.5.5* (Matrice de passage).** — Soient V un espace vectoriel de dimension finie, $\mathscr{B} = (e_1, \dots, e_n)$ une base de V, et $\mathscr{B}' = (v_1, \dots, v_n)$ une seconde base de V. Soit P la matrice $n \times n$ exprimant la seconde base en fonction de la première, c.-à-d., chaque v_j s'écrit de façon unique

$$v_j = p_{1j}\, e_1 + \cdots + p_{nj}\, e_n$$

et l'on forme la matrice

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1j} & \cdots & p_{1n} \\ \vdots & & \vdots & & \vdots \\ p_{i1} & \cdots & p_{ij} & \cdots & p_{in} \\ \vdots & & \vdots & & \vdots \\ p_{n1} & \cdots & p_{nj} & \cdots & p_{nn} \end{pmatrix}$$

dont les colonnes sont les vecteurs $v_1, \dots, v_n$ exprimés dans la base $(e_1, \dots, e_n)$. Alors P s'appelle la **matrice de passage** de la base $\mathscr{B} = (e_1, \dots, e_n)$ à la base $\mathscr{B}' = (v_1, \dots, v_n)$ et se note $\boxed{\mathrm{Mat}_{\mathscr{B}}(\mathscr{B}').}$

C'est une matrice **inversible** : son inverse P^{-1} est la matrice exprimant $e_1, \dots, e_n$ dans la base $(v_1, \dots, v_n)$.

Remarquons que P peut être vue comme la matrice de l'application identité id_V, exprimée dans les bases : $\mathscr{B}' = (v_1, \dots, v_n)$ au départ, et $\mathscr{B} = (e_1, \dots, e_n)$ à l'arrivée, c.-à-d.,

$$\boxed{P = \mathrm{Mat}_{\mathscr{B},\mathscr{B}'}(\mathrm{id}_V)} \qquad \text{et de même} \qquad \boxed{P^{-1} = \mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{id}_V).}$$

Conservons les notations précédentes. Tout $v \in V$ s'écrit alors de façon unique

$$v = x_1 e_1 + \cdots + x_n e_n \qquad \text{et} \qquad v = x'_1 v_1 + \cdots + x'_n v_n$$

et les x_i (resp. x'_i) s'appellent les **coordonnées** de v relativement à la base $\mathscr{B}$ (resp. $\mathscr{B}'$), cf. 0.2.10. Relativement à la base $\mathscr{B}$ (resp. $\mathscr{B}'$), on peut représenter v comme le vecteur colonne

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad \text{resp.} \qquad X' = \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$$

***Proposition 0.5.6* (Changement de coordonnées).** — *La formule de changement de coordonnées, pour le changement de base $\mathscr{B} \to \mathscr{B}'$ donné par la matrice de passage P, est donnée par :*

$$\boxed{X = PX'}$$

(noter que cette formule exprime les anciennes *coordonnées X en fonction des* nouvelles *X').*

Démonstration. En effet, écrivant $v_j = \sum_{i=1}^n p_{ij} e_i$ puis

$$v = \sum_{j=1}^n x'_j v_j = \sum_{j=1}^n \sum_{i=1}^n x'_j p_{ij} e_i = \sum_{i=1}^n \left(\sum_{j=1}^n p_{ij} x'_j \right) e_i$$

et comparant avec $v = \sum_{i=1}^n x_i e_i$, on obtient qu'on a $x_i = \sum_{j=1}^n p_{ij} x'_j$ pour $i = 1, \dots, n$, d'où $X = PX'$.

Soient $V, \mathscr{B}, \mathscr{B}'$ et P comme plus haut, et considérons maintenant une application linéaire $u : V \to W$. Soient $\mathscr{C} = (f_1, \dots, f_m)$ une base de W, et $A \in M_{m,n}(k)$ la matrice de u dans les bases $\mathscr{B}$ et $\mathscr{C}$. Alors, d'après le théorème 0.4.3, on a :

$$\mathrm{Mat}_{\mathscr{C},\mathscr{B}'}(u) = \mathrm{Mat}_{\mathscr{C},\mathscr{B}}(u) \cdot \mathrm{Mat}_{\mathscr{B},\mathscr{B}'}(\mathrm{id}_V)$$

donc la matrice de u dans les bases $\mathscr{B}'$ et $\mathscr{C}$ est AP.

Enfin, soit $\mathscr{C}' = (w_1, \dots, w_m)$ une seconde base de W et soit Q la matrice de passage de $\mathscr{C}$ à $\mathscr{C}'$; alors $Q = \mathrm{Mat}_{\mathscr{C},\mathscr{C}'}(\mathrm{id}_W)$ et $Q^{-1} = \mathrm{Mat}_{\mathscr{C}',\mathscr{C}}(\mathrm{id}_W)$, d'où :

$$\mathrm{Mat}_{\mathscr{C}',\mathscr{B}'}(u) = \mathrm{Mat}_{\mathscr{C}',\mathscr{C}}(\mathrm{id}_W) \cdot \mathrm{Mat}_{\mathscr{C},\mathscr{B}'}(u) = Q^{-1}AP.$$

On a donc obtenu le théorème suivant :

***Théorème 0.5.7* (Changement de bases pour une application linéaire)**
Soit $A \in M_{m,n}(k)$ la matrice d'une application linéaire $u : V \to W$, relativement à des bases $\mathscr{B} = (e_1, \dots, e_n)$ de V et $\mathscr{C} = (f_1, \dots, f_m)$ de W. Soit $\mathscr{B}' = (v_1, \dots, v_n)$ (resp. $\mathscr{C}' = (w_1, \dots, w_m)$) une seconde base de V (resp. de W) et soit P (resp. Q) la matrice de passage correspondante. Alors la matrice de u dans les bases $\mathscr{B}'$ et $\mathscr{C}'$ est :

$$\boxed{\mathrm{Mat}_{\mathscr{C}',\mathscr{B}'}(u) = Q^{-1}AP.}$$

Remarque 0.5.8. — Le théorème précédent est (évidemment) compatible avec la formule de changement de coordonnées 0.5.6 : si l'on désigne par X (resp. X') les coordonnées d'un vecteur $v \in V$ relativement à $\mathscr{B}$ (resp. $\mathscr{B}'$), et Y (resp. Y') les coordonnées du vecteur $u(v)$ dans la base $\mathscr{C}$ (resp. $\mathscr{C}'$), alors on a :

$$Y = AX, \qquad X = PX', \qquad Y = QY'$$

d'où $Y' = Q^{-1}Y = Q^{-1}AX = Q^{-1}APX'$. Compte-tenu de cette « compatibilité », on peut utiliser (comme moyen mnémotechnique) l'une de ces formules pour retrouver l'autre...

Remarque 0.5.9. — Même si l'on s'intéresse au départ à une *matrice* $A \in M_{m,n}(k)$, il est souvent utile de considérer A comme une application linéaire $u : k^n \to k^m$ (définie par $u(e_j) = a_{1j}f_1 + \cdots + a_{mj}f_m$, où $(e_1, \dots, e_n)$, resp. $(f_1, \dots, f_m)$, est la base canonique de k^n, resp. k^m). Par exemple, le théorème précédent donne alors le corollaire suivant :

Corollaire 0.5.10. — *Soit $A \in M_{m,n}(k)$ et soit $r = \mathrm{rang}(A)$.*
1) *Il existe des matrices inversibles $P \in \mathrm{GL}_n(k)$ et $Q \in \mathrm{GL}_m(k)$ telles que*

$$Q^{-1}AP = \begin{pmatrix} I_r & \mathbf{0}_{r,n-r} \\ \mathbf{0}_{m-r,r} & \mathbf{0}_{m-r,n-r} \end{pmatrix}$$

où I_r est la matrice identité de taille r et où $\mathbf{0}_{p,q}$ désigne la matrice nulle à p lignes et q colonnes.
2) *Réciproquement, s'il existe des matrices inversibles $P \in \mathrm{GL}_n(k)$ et $Q \in \mathrm{GL}_m(k)$ et un entier $s \in \mathbb{N}$ tels que*

$$Q^{-1}AP = \begin{pmatrix} I_s & \mathbf{0}_{s,n-s} \\ \mathbf{0}_{m-s,s} & \mathbf{0}_{m-s,n-s} \end{pmatrix}$$

alors $s = \mathrm{rang}(A)$.

Démonstration. Soient $(e_1, \dots, e_n)$ et $(f_1, \dots, f_m)$ les bases canoniques de k^n et k^m et soit u l'application linéaire $k^n \to k^m$ correspondant à A. Par définition, $r = \mathrm{rang}(A)$ est la dimension de $\mathrm{Im}(u)$. Soit donc $(w_1, \dots, w_r)$ une base de $\mathrm{Im}(u)$, on peut la compléter en une base $\mathscr{C} = (w_1, \dots, w_m)$ de k^m ; notons Q la matrice de passage de $(f_1, \dots, f_m)$ à $\mathscr{C}$.

Soient $v_1, \dots, v_r$ des éléments de k^n tels que $u(v_j) = w_j$, pour $j = 1, \dots, r$, et soit $(e_1, \dots, e_d)$ une base de $\mathrm{Ker}(u)$. D'après la démonstration (2ème méthode) du théorème du rang 0.3.2, $\mathscr{B} = (v_1, \dots, v_r, e_1, \dots, e_d)$ est une base de k^n. Alors, la matrice de u dans les bases $\mathscr{B}$ et $\mathscr{C}$ est

$$\mathrm{Mat}_{\mathscr{C},\mathscr{B}}(u) = \begin{pmatrix} I_r & \mathbf{0}_{r,n-r} \\ \mathbf{0}_{m-r,r} & \mathbf{0}_{m-r,n-r} \end{pmatrix}.$$

Or, si P désigne la matrice de passage de $(e_1, \dots, e_n)$ à $\mathscr{B}$, on a

$$\mathrm{Mat}_{\mathscr{C},\mathscr{B}}(u) = Q^{-1} \cdot \mathrm{Mat}_{(f_i),(e_j)}(u) \cdot P = Q^{-1}AP,$$

d'où l'assertion 1) du corollaire.

Réciproquement, supposons qu'il existe des matrices inversibles $P \in \mathrm{GL}_n(k)$ et $Q \in \mathrm{GL}_m(k)$ et un entier $s \in \mathbb{N}$ tels que

$$Q^{-1}AP = \begin{pmatrix} I_s & \mathbf{0}_{s,n-s} \\ \mathbf{0}_{m-s,s} & \mathbf{0}_{m-s,n-s} \end{pmatrix}.$$

Ceci signifie qu'il existe des bases $(v_1, \dots, v_n)$ de k^n et $(w_1, \dots, w_m)$ de k^m telles que $u(v_i) = w_i$ pour $i = 1, \dots, s$, et $u(v_j) = 0$ pour $j = s+1, \dots, n$. Alors $\mathrm{Im}(f) = \mathrm{Vect}(w_1, \dots, w_s)$ est de dimension s, d'où $s = \mathrm{rang}(A)$.

On déduit du corollaire 0.5.10 la proposition suivante.

Proposition 0.5.11. — *Soit $A \in M_{m,n}(k)$. Alors*

$$\boxed{\operatorname{rang}(A) = \operatorname{rang}({}^tA)}$$

par conséquent $\operatorname{rang}(A)$ *est aussi le nombre maximum de* lignes *de A qui sont linéairement indépendantes.*

Démonstration. D'après ce qui précède, il existe $P \in \mathrm{GL}_n(k)$ et $Q \in \mathrm{GL}_m(k)$ telles que

$$Q^{-1}AP = \begin{pmatrix} I_r & \mathbf{0}_{r,n-r} \\ \mathbf{0}_{m-r,r} & \mathbf{0}_{m-r,n-r} \end{pmatrix}.$$

où $r = \operatorname{rang}(A)$. Alors

$${}^tP\,{}^tA\,{}^tQ^{-1} = \begin{pmatrix} I_r & \mathbf{0}_{r,m-r} \\ \mathbf{0}_{n-r,r} & \mathbf{0}_{n-r,m-r} \end{pmatrix}.$$

Or, d'après la proposition 0.5.2, ${}^tP$ et ${}^tQ^{-1}$ sont inversibles, donc l'égalité ci-dessus entraîne, d'après le corollaire précédent, que $r = \operatorname{rang}({}^tA)$.

***Définition 0.5.12* (Matrices équivalentes)**. — Soient $A, B \in M_{m,n}(k)$; on dit que A et B sont *équivalentes* s'il existe des matrices inversibles $P \in \mathrm{GL}_n(k)$ et $Q \in \mathrm{GL}_m(k)$ telles que $Q^{-1}AP = B$. (D'après le corollaire 0.5.10, ceci équivaut à dire que A et B ont même rang).

Cas des endomorphismes. — Le théorème 0.5.7 traite le cas d'une application linéaire $u : V \to W$, où V, W sont *a priori* distincts. Dans ce cas, lorsque qu'on s'autorise des changements de bases arbitraires dans V et dans W, le corollaire 0.5.10 montre que le seul invariant de u est son rang, qui est un entier compris entre 0 et $\operatorname{Min}(\dim V, \dim W)$.

Mais, lorsque $V = W$ et qu'on s'intéresse à la nature géométrique d'un endomorphisme u de V, c.-à-d., lorsqu'on veut comparer $u(x)$ et x, pour x variant dans V, pour pouvoir faire la comparaison on veut exprimer x et $u(x)$ dans la même base, et c'est la raison pour laquelle, dans ce cas, on écrit la matrice de u dans une *même* base $\mathscr{B}$ au départ et à l'arrivée.

(Par exemple, si $V = W = k$, les automorphismes de k comme k-espace vectoriel sont les homothéties $h_\lambda : x \mapsto \lambda x$ avec $\lambda \neq 0$, si on prend $\{1\}$ comme base de départ et $\{\lambda\}$ comme base d'arrivée, la matrice est (1) donc on a « perdu » le rapport λ de l'homothétie ; mais si on impose de garder la même base au départ et à l'arrivée, la matrice est (λ)…)

Alors, le théorème 0.5.7 donne dans ce cas :

***Théorème 0.5.13* (Changement de base pour un endomorphisme)**

Soit A la matrice d'un endomorphisme u de V relativement à une base $\mathscr{B}$ de V. Si $\mathscr{B}'$ est une seconde base, et si P est la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$, alors la matrice de u dans la base $\mathscr{B}'$ est :

$$\boxed{\operatorname{Mat}_{\mathscr{B}'}(u) = P^{-1}AP.}$$

***Définition 0.5.14* (Matrices semblables)**. — Soit $A, B \in M_n(k)$ des matrices *carrées* de taille n. On dit que A, B sont *semblables* s'il existe une matrice inversible $P \in \mathrm{GL}_n(k)$ telle que $P^{-1}AP = B$. Dans ce cas, on dit que A, B sont dans la même *classe de similitude.*

Remarques 0.5.15. — 1) On notera que cette définition ne fait sens que pour des matrices *carrées.*

2) A et B sont semblables si et seulement si elles représentent, dans des bases différentes, le même endomorphisme de k^n.

3) Si $A, B \in M_n(k)$ sont semblables, elles sont évidemment équivalentes, mais la réciproque est loin d'être vraie : les classes de similitude forment une partition de $M_n(k)$ beaucoup plus raffinée que celle donnée par le rang (cf. le cas $n = 1$, et voir plus loin pour le cas n arbitraire).

0.6. Appendice (†) : compléments sur les familles génératrices ou libres

Dans cet appendice, on donne la définition des familles génératrices ou libres éventuellement infinies, ainsi qu'une démonstration du théorème sur la dimension (0.2.8).

***Définitions 0.6.1* (Familles génératrices)**. — Soit V un k-espace vectoriel.

1) Soit S un sous-ensemble (fini ou infini) de V. L'ensemble de toutes les combinaisons linéaires *finies*

$$t_1v_1 + \cdots + t_rv_r, \qquad \text{pour } r \in \mathbb{N}^* \text{ (variable)}, \ v_i \in S,\ t_i \in k,$$

forme un sous-espace vectoriel de V, et c'est le plus petit sous-espace vectoriel de V contenant S. On l'appelle le sous-espace *engendré* par S et on le note $\mathrm{Vect}(S)$.

En particulier, si E est un sous-ensemble *fini* $\{v_1, \dots, v_n\}$, alors $\mathrm{Vect}(E)$ est l'ensemble des combinaisons linéaires

$$t_1 v_1 + \cdots + t_n v_n, \qquad \text{où } t_1, \dots, t_n \in k.$$

2) On dit que S est un ensemble de générateurs (ou une *famille génératrice*) de V si le sous-espace engendré $\mathrm{Vect}(S)$ égale V, c.-à-d., si tout élément de V s'écrit comme combinaison linéaire des éléments de S.

Il résulte de la définition que : *toute famille contenant une famille génératrice est génératrice.*

Exemple 0.6.2. — Les monômes X^n, pour $n \in \mathbb{N}$, engendrent l'espace vectoriel $k[X]$. En effet, tout polynôme $P \in k[X]$ s'écrit comme une combinaison linéaire finie : $P = a_0 + a_1 X + \cdots + a_d X^d$.

Exercices 0.6.3. — 1) Soit $\mathbb{R}[[X]]$ l'espace des séries formelles $\sum_{i=0}^{\infty} a_i X^i$, avec $a_i \in \mathbb{R}$. Quel est le sous-espace de $\mathbb{R}[[X]]$ engendré par les monômes X^n, pour $n \in \mathbb{N}$? (Réponse : c'est $\mathbb{R}[X]$.)

2) Pouvez-vous montrer que l'espace vectoriel $\mathbb{R}[X]$ n'est *pas* finiment engendré ? (Voir Exercice 10 de la Feuille 1.)

***Définitions 0.6.4* (Familles libres ou liées)**. — Soit V un k-espace vectoriel et soit S un sous-ensemble (fini ou infini) de V. On dit que les éléments de S sont *linéairement indépendants* (ou que S est une *famille libre*) s'il n'existe pas de relation linéaire non triviale entre les éléments de S, c.-à-d., si la condition suivante est vérifiée :

$$(\mathrm{FL}) \qquad \begin{cases} \textit{pour tous } r \in \mathbb{N}^*,\ v_1, \dots, v_r \in S \textit{ deux-à-deux distincts, et } t_1, \dots, t_r \in k, \textit{ si l'on a} \\ \textit{une relation } t_1 v_1 + \cdots + t_r v_r = 0,\ \textit{ alors } t_1 = 0 = \cdots = t_r. \end{cases}$$

(Ceci prend une forme plus simple si S est un ensemble *fini* $\{v_1, \dots, v_n\}$; dans ce cas la condition s'écrit plus simplement : pour *tous* $t_1, \dots, t_n \in k$, si $t_1 v_1 + \cdots + t_n v_n = 0$, alors $t_1 = 0 = \cdots = t_n$.)

Il résulte de la définition que : *toute sous-famille d'une famille libre est libre.*

Au contraire, on dit que les éléments de S sont *linéairement dépendants* (ou que S est une *famille liée*) s'il existe une relation linéaire non triviale entre les éléments de S, c.-à-d., s'il existe un entier $r \geq 1$, des éléments $v_1, \dots, v_r \in S$ deux-à-deux distincts, et des scalaires $t_1, \dots, t_r$, non tous nuls, tels que $t_1 v_1 + \cdots + t_r v_r = 0$.

Il résulte de la définition que : *toute famille contenant une famille liée est liée.*

Exemple 0.6.5. — Dans $k[X]$, la famille des monômes $(X^n)_{n \in \mathbb{N}}$ est libre. En effet, soient $i_1 < \cdots < i_r$ dans $\mathbb{N}$ et soient $t_1, \dots, t_r \in k$ non tous nuls. Alors le polynôme

$$t_1 X^{i_1} + \cdots + t_r X^{i_r}$$

est non nul. Ceci montre que $(X^n)_{n \in \mathbb{N}}$ est une famille libre.

Remarque 0.6.6. — Soient V un k-espace vectoriel et $S = (v_i)_{i \in I}$ une famille de vecteurs indexée par un ensemble d'indice I infini. Alors S est libre si et seulement si la condition d'unicité suivante est vérifiée : (U) « si l'on a une égalité

$$\sum_{j \in J} t_j v_j = \sum_{p \in P} s_p v_p \qquad t_j \in k, \quad s_p \in k,$$

où J, P sont deux sous-ensembles finis de I, alors $\{j \in J \mid t_j \neq 0\}$ égale $\{p \in P \mid s_p \neq 0\}$ et, notant L cet ensemble, on a $t_\ell = s_\ell$ pour tout $\ell \in L$ ».

En effet, supposons cette condition vérifiée ; si l'on a une égalité $\sum_{j \in J} t_j v_j = 0$ (le terme de droite correspond à $P = \varnothing$: une somme indexée par $\varnothing$ vaut 0), alors $\{j \in J \mid t_j \neq 0\}$ égale $\varnothing$, i.e. tous les t_j sont nuls ; ceci montre que S est une famille libre.

Réciproquement, supposons que S soit une famille libre, et qu'on ait une égalité $\sum_{j \in J} t_j v_j = \sum_{p \in P} s_p v_p$ comme plus haut, alors on a :

$$0 = \sum_{j \in J - P} t_j v_j + \sum_{i \in J \cap P} (t_i - s_i) v_i - \sum_{p \in P - J} s_p v_p$$

et comme S est libre, ceci entraîne que $t_j = 0 = s_p$ pour $j \in J - P$ et $p \in P - J$, et que $t_i = s_i$ pour tout $i \in J \cap P$, donc la condition (U) est vérifiée.

***Définition 0.6.7* (Bases).** — Soient V un k-espace vectoriel et $(v_i)_{i\in I}$ une famille (finie ou infinie) de vecteurs de V. On dit que $\mathscr{B} = (v_i)_{i\in I}$ est une *base* de V si tout élément v de V *s'écrit de façon unique comme combinaison linéaire des* v_i, c.-à-d., si :

(1) $\mathscr{B}$ est une famille génératrice, i.e. pour tout $v \in V$, il existe un sous-ensemble *fini* J de I (dépendant de v) et des scalaires $t_j \in k$, pour $j \in J$, tels que $v = \sum_{j\in J} t_j v_j$.

(2) $\mathscr{B}$ vérifie la condition (U), i.e. si l'on a un second sous-ensemble fini P de I et des scalaires s_p, pour $p \in P$, tels que

$$v = \sum_{j\in J} t_j v_j = \sum_{p\in P} s_p v_p,$$

alors le sous-ensemble $L = \{j \in J \mid t_j \neq 0\}$ égale $\{p \in P \mid s_p \neq 0\}$ et pour tout $\ell \in L$, on a $t_\ell = s_\ell$.

D'après la remarque précédente, ceci équivaut à dire que $\mathscr{B}$ est une famille *génératrice et libre.*

Exemple 0.6.8. — La famille des monômes $(X^n)_{n\in\mathbb{N}}$ est une base de $k[X]$: en effet, tout polynôme non nul $P \in k[X]$ s'écrit de façon unique

$$P = a_0 + \cdots + a_d X^d, \qquad \text{où } a_i \in k,\ a_d \neq 0,\ d = \deg P.$$

Définitions 0.6.9. — Soient V un k-espace vectoriel, et $\mathscr{F} = (v_i)_{i\in I}$ une famille de vecteurs de V.

(i) On dit que $\mathscr{F}$ est une *famille génératrice minimale* si c'est une famille génératrice, et si « on ne peut pas la rendre plus petite », c.-à-d., si pour tout sous-ensemble $I' \neq I$, la famille $(v_i)_{i\in I'}$ n'est *pas* génératrice.

(ii) On dit que $\mathscr{F}$ est une *famille libre maximale* si c'est une famille libre, et si « on ne peut pas la rendre plus grande », c.-à-d., si pour tout $v \in V - \mathscr{F}$, la famille $\mathscr{F} \cup \{v\}$ est liée.

Proposition 0.6.10. — *Soient V un k-espace vectoriel, et $\mathscr{F} = (v_i)_{i\in I}$ une famille non vide de vecteurs de V. Les conditions suivantes sont équivalentes :*

a) $\mathscr{F}$ *est une* base *de V ;*

b) $\mathscr{F}$ *est une* famille génératrice minimale *;*

c) $\mathscr{F}$ *est une* famille libre maximale.

Démonstration. Supposons que $(v_i)_{i\in I}$ soit une base de V, c.-à-d., une famile *génératrice et libre.* Alors, pour tout $i \in I$, la famille $(v_j)_{j\in I-\{i\}}$ n'est *pas* génératrice : sinon v_i s'exprimerait comme combinaison linéaire des v_j, pour $j \neq i$, d'où une relation linéaire non triviale $v_i - (t_1 v_{j_1} + \cdots + t_r v_{j_r}) = 0$. Ceci montre que $(v_i)_{i\in I}$ est une famille génératrice minimale.

De plus, tout $v \in V$ s'écrit comme combinaison linéaire (d'un nombre fini) des v_i, donc si $v \notin \mathscr{F}$, la famille strictement plus grande $\mathscr{F} \cup \{v\}$ est liée. Ceci montre que $\mathscr{F}$ est une famille libre maximale. On a donc prouvé que a) implique b) et c).

b) $\Rightarrow$ a) Supposons que $(v_i)_{i\in I}$ soit une famille génératrice minimale et montrons qu'elle est libre. Sinon, on aurait une relation linéaire non triviale

$$t_1 v_{i_1} + \cdots + t_r v_{i_r} = 0$$

avec $r \geq 1$ et $t_p \neq 0$ pour au moins un indice p ; alors on aurait $v_{i_p} = -t_p^{-1} \sum_{q\neq p} t_q\, v_{i_q}$ et donc la famille $(v_i)_{i\in I-\{i_p\}}$ serait déjà génératrice, contredisant la minimalité. Ceci prouve b) $\Rightarrow$ a).

c) $\Rightarrow$ a) Supposons que $\mathscr{F}$ soit une famille libre maximale et montrons qu'elle est génératrice. Soit $v \in V - \mathscr{F}$, alors la famille $\mathscr{F} \cup \{v\}$ est liée, donc on a une relation linéaire

$$sv + t_1 v_{i_1} + \cdots + t_r v_{i_r} = 0$$

non triviale (c.-à-d., s et les t_p non tous nuls). On ne peut avoir $s = 0$ car sinon, les v_i étant linéairement indépendants, on aurait $t_1 = 0 = \cdots = t_r$. Donc $s \neq 0$, d'où $v = -s^{-1}(t_1 v_{i_1} + \cdots + t_r v_{i_r})$. Donc $\mathscr{F}$ est une famille libre et génératrice, donc une base de V. Ceci prouve c) $\Rightarrow$ a).

***Corollaire 0.6.11* (Existence de bases).** — *Tout k-espace vectoriel finiment engendré V possède une base. (On convient que l'ensemble vide $\varnothing$ est une base de l'espace nul* $\{0\}$.*)*

En effet, par hypothèse V est engendré par une famille *finie* $\{v_1, \ldots, v_r\}$. Celle-ci contient une sous-famille génératrice $\mathscr{B}$ de cardinal minimal, donc minimale, et d'après la proposition, $\mathscr{B}$ est une base de V.

On va voir dans un instant (cf. 0.6.13 ci-dessous) que si $(v_1, \ldots, v_n)$ est une base de V, alors *toutes les bases de V ont n éléments.* Commençons par le lemme important suivant.

Lemme 0.6.12. — *Soient V un k-espace vectoriel, $v_1, \dots, v_n \in V$, et soient $m > n$ et $u_1, \dots, u_m$ des éléments de V qui sont combinaison linéaire de $v_1, \dots, v_n$. Alors $u_1, \dots, u_m$ sont liés.*

Démonstration. On procède par récurrence sur n ; le résultat est clair si $n = 1$, supposons donc $n \geq 2$ et le résultat établi pour $n - 1$. Écrivons :

$$\begin{cases} u_1 & = & a_{11}v_1 + \cdots + a_{1n}v_n \\ u_2 & = & a_{21}v_1 + \cdots + a_{2n}v_n \\ \vdots & & \vdots \\ u_m & = & a_{m1}v_1 + \cdots + a_{mn}v_n. \end{cases}$$

Si tous les u_i sont combinaison linéaire des $n-1$ vecteurs $v_2, \dots, v_n$, alors les u_i sont liés, d'après l'hypothèse de récurrence. Sinon, quitte à renuméroter les u_i, on peut supposer que $a_{11} \neq 0$. Alors, pour $i = 2, \dots, m$, les $m - 1$ vecteurs

$$u_i' = u_i - a_{i1}a_{11}^{-1}u_1$$

sont combinaison linéaire des $n - 1$ vecteurs $v_2, \dots, v_n$, donc sont liés d'après l'hypothèse de récurrence. Donc il existe des scalaires non tous nuls $t_2, \dots, t_m$ tels que

$$0 = t_2u_2' + \cdots + t_mu_m' = t_2u_2 + \cdots + t_mu_m - \big(\sum_{i=2}^{m} t_ia_{i1}a_{11}^{-1}\big)u_1$$

et ceci montre que les u_i sont liés. Le lemme est démontré.

Le lemme précédent a les conséquences très importantes suivantes. Soit V un k-espace vectoriel engendré par un nombre fini d'éléments $x_1, \dots, x_N$. D'après le corollaire 0.6.11, V possède une base $\mathscr{B} = (v_1, \dots, v_n)$ formée de $n \leq N$ éléments. Comme $\mathscr{B}$ est une famille libre de V, il résulte du lemme précédent que :

a) toute famille génératrice de V a au moins n éléments ;

b) toute famille génératrice de V ayant n éléments est *minimale*, donc d'après 0.6.10 est une base de V.

D'autre part, comme $\mathscr{B}$ est une famille génératrice de V, il résulte du lemme précédent que :

a′) toute famille libre dans V a au plus n éléments ;

b′) toute famille libre de V ayant n éléments est *maximale*, donc d'après 0.6.10 est une base de V.

Enfin, en combinant a) et b), on voit que : *toute base de V*, étant une famille à la fois génératrice et libre, *a exactement n éléments.* On obtient donc le théorème fondamental suivant.

***Théorème 0.6.13* (Dimension d'un espace vectoriel).** — *Soit V un k-espace vectoriel finiment engendré.*

(i) *Il existe des bases de V, et toutes ont même cardinal n ; cet entier s'appelle la dimension de V sur k et se note* $\dim_k V$ *ou simplement* $\dim V$.

(ii) *De toute famille génératrice $\mathscr{F}$ on peut extraire une base, en particulier $\mathscr{F}$ est de cardinal $\geq n$; de plus si* $\mathrm{card}(\mathscr{F}) = n$ *alors $\mathscr{F}$ est une base de V.*

(iii) *Toute famille libre est de cardinal $\leq n$, et toute famille libre de cardinal n est une base de V.*

(iv) « Théorème de la base incomplète » *: Toute famille libre peut être complétée en une base de V.*

(v) *Tout sous-espace W de V est finiment engendré, et* $\dim_k W \leq \dim_k V$ *; de plus si* $\dim_k W = \dim_k V$, *alors $W = V$. En d'autres termes, tout sous-espace vectoriel distinct de V est de dimension* $< \dim_k V$.

Démonstration. On a déjà vu les assertions (i), (ii) et (iii). L'assertion (iv) résulte du fait que toute famille libre peut être agrandie en une famille libre maximale, c.-à-d., en une base de V (cf. la proposition 0.6.10).

Démontrons (v). Soit W un sous-espace vectoriel de V. D'après (iii), toute famille libre d'éléments de W est de cardinal $\leq n = \dim_k V$, donc W possède une famille *libre maximale* $\mathscr{C}$, de cardinal $m \leq n$. Alors $\mathscr{C}$ est une *base* de W, d'après la proposition 0.6.10, donc W est finiment engendré, et de dimension $m \leq n$. Si de plus $m = n$ alors, d'après (iii), $\mathscr{C}$ est une base de V (donc engendre V), d'où $W = V$. Le théorème est démontré.

Proposition 0.6.14. — *Soit $f : V \to W$ une application linéaire.*

a) *Si f est injective et si $\mathscr{F}$ est une famille libre de V, alors $f(\mathscr{F})$ est libre.*

b) *Si f est surjective et si $\mathscr{F}$ est une famille génératrice de V, alors $f(\mathscr{F})$ engendre W.*

c) *Si f est bijective et si $\mathscr{B}$ est une base de V, alors $f(\mathscr{B})$ est une base de W.*

Démonstration. a) Supposons f injective et soit $\mathscr{F}$ une famille libre de V. S'il existe une relation linéaire dans W :
$$t_1 f(x_1) + \cdots + t_n f(x_n) = 0, \qquad t_i \in k, \quad x_i \in \mathscr{F},$$
alors $0 = f(t_1 x_1 + \cdots + t_n x_n)$, donc comme f est injective $t_1 x_1 + \cdots + t_n x_n = 0$, donc comme $\mathscr{F}$ est libre, $t_i = 0$ pour $i = 1, \ldots, n$. Ceci montre que $f(\mathscr{F})$ est libre.

b) Supposons f surjective et soit $\mathscr{F}$ une famille génératrice de V. Soit $w \in W$; comme f est surjective, il existe $v \in V$ tel que $f(v) = w$. Comme $\mathscr{F}$ engendre V, il existe $x_1, \ldots, x_n \in \mathscr{F}$ et $t_1, \ldots, t_n \in k$ tels que $v = t_1 x_1 + \cdots + t_n x_n$, d'où $w = t_1 f(x_1) + \cdots + t_n f(x_n)$. Ceci montre que $f(\mathscr{F})$ engendre W.

c) Supposons f bijective et soit $\mathscr{B}$ une base de V. Alors, d'après a) et b), $f(\mathscr{B})$ est une famille libre et génératrice de W, donc une base de W.