Algèbre linéaire et bilinéaire

(version du 21 février 2020)

Bernard Le Stum

Il existe [...] un certain ordre de considérations Métaphysiques qui planent sur tous les calculs, et qui souvent les rendent inutiles, Évariste Galois.

Réalisé en LaTeX à partir du modèle Legrand Orange Book

Table des matières

Introduction

Dans cette introduction, nous allons déconstruire la définition formelle d'un espace vectoriel de manière à faire apparaître de nombreuses structures algébriques que l'on peut ensuite illustrer par des exemples venant de toutes les mathématiques. En particulier, nous oublions totalement l'aspect concret ou intuitif de la notion d'espace vectoriel pour nous concentrer sur sa définition.

Qu'est-ce qu'un *espace vectoriel* ? C'est un *ensemble* E muni d'une *loi interne*

$$E \times E \to E, \quad (x,y) \mapsto x+y,$$

et d'une *loi externe*

$$K \times E \to E, \quad (a,x) \mapsto ax,$$

satisfaisant les propriétés suivantes :

1. (E est un *groupe abélien* [1])
   (a) $\forall x,y,z \in E, \quad (x+y)+z = x+(y+z)$,
   (b) $\exists 0_E \in E, \forall x \in E, \quad 0_E + x = x$,
   (c) $\forall x \in E, \exists -x \in E, \quad x+(-x) = 0_E$,
   (d) $\forall x,y \in E, \quad x+y = y+x$,
2. (K *opère* sur E)
   (a) $\forall a,b \in K, \forall x \in E, \quad (ab)x = a(bx)$,
   (b) $\forall x \in E, \quad 1_K x = x$,
3. (l'opération est *distributive*)
   (a) $\forall a \in K, \forall x,y \in E, \quad a(x+y) = ax+ay$,
   (b) $\forall a,b \in K, \forall x \in E, \quad (a+b)x = ax+bx$.

On peut remarquer que les propriétés (a) et (b) des conditions 1. et 2. respectivement sont analogues. Il s'agit de l'*associativité* (a) et de la propriété de l'*élément neutre* (b) (le *zéro* pour l'addition et le *un* pour la multiplication). Les propriétés (c) et (d) de la condition 1. expriment respectivement l'existence d'*éléments symétriques* (il s'agit de l'*opposé* pour l'addition) ainsi que la *commutativité*.

1. Nous employons le mot abélien comme synonyme de commutatif lorsque le groupe est noté additivement.

Avant d'aller plus loin, il est bon de rappeler que K désigne un *corps* (dont l'archétype pour nous est le corps $\mathbb{R}$ des réels), c'est à dire un ensemble muni de deux lois internes

$$K \times K \to K, \quad (a,b) \mapsto a+b, \quad \text{et} \quad K \times K \to K, \quad (a,b) \mapsto ab,$$

satisfaisant les propriétés suivantes :

1. (K est un groupe abélien)
   (a) $\forall a,b,c \in K, \quad (a+b)+c = a+(b+c)$,
   (b) $\exists 0_K \in K, \forall a \in K, \quad 0_K + a = a$,
   (c) $\forall a \in K, \exists -a \in K, \quad a+(-a) = 0_K$,
   (d) $\forall a,b \in K, \quad a+b = b+a$,
2. ($K \setminus \{0_K\}$ est un groupe commutatif)
   (a) $\forall a,b,c \in K, \quad (ab)c = a(bc)$,
   (b) $\exists 1_K \in K \setminus \{0_K\}, \forall a \in K, \quad 1_K a = a$,
   (c) $\forall a \in K \setminus \{0_K\}, \exists a^{-1} \in K, \quad aa^{-1} = 1_K$,
   (d) $\forall a,b \in K, \quad ab = ba$,
3. (la multiplication est distributive sur l'addition)
   (a) $\forall a,b,c \in K, \quad a(b+c) = ab+ac$.

Dans les conditions 1. et 2., on trouve successivement l'associativité (a), l'existence d'un élément neutre (b) (zéro ou un selon le cas), l'existence des symétriques (c) (opposé ou *inverse* selon le cas) ainsi que la commutativité (d). Si on supprime la condition 2.(c) de l'existence de l'inverse et qu'on ne requiert plus que $1_K \neq 0_K$, on obtient la notion d'*anneau commutatif*. Un exemple typique est l'anneau $\mathbb{Z}$ des entiers relatifs. Si on supprime aussi la condition 2.(d) de la commutativité, on obtient un *anneau* (pas nécessairement commutatif) mais il faut alors rajouter en 2.(b) la condition $a1_K = a$ qui n'est alors plus automatique, ainsi que dans le 3., la condition $(a+b)c = ac+bc$. Un exemple typique d'anneau non commutatif est l'anneau des matrices carrées sur un corps.

On définit un *module* M exactement comme un espace vectoriel E mais en remplaçant le corps K par un anneau quelconque A. Par exemple, on peut remarquer que si M est un groupe abélien, on a toujours

1. ($\mathbb{Z}$ *opère* sur M)
   (a) $\forall m,n \in \mathbb{Z}, \forall x \in M, \quad (mn)x = m(nx)$,
   (b) $\forall x \in M, \quad 1_{\mathbb{Z}} x = x$,
2. (l'opération est *distributive*)
   (a) $\forall m \in \mathbb{Z}, \forall x,y \in E, \quad m(x+y) = mx+my$,
   (b) $\forall m,n \in \mathbb{Z}, \forall x \in E, \quad (m+n)x = mx+nx$.

Autrement dit, un groupe abélien est automatiquement un module sur $\mathbb{Z}$ si bien que la notion de module est une généralisation commune de celles d'espace vectoriel (anneau = corps) et de groupe abélien (anneau = $\mathbb{Z}$).

Il est aisé de formaliser les différentes propriétés rencontrées ci-dessus. Un ensemble G muni d'une loi interne

$$G \times G \to G, \quad (g,h) \mapsto g*h$$

est parfois appelé un *magma*. La loi est dite *associative* si

$$\forall g,h,k \in G, \quad (g*h)*k = g*(h*k)$$

et on dit alors parfois que G est un *semi-groupe* (ou magma associatif). Si de plus, il existe $e \in G$ (on écrira e_G si nécessaire) tel que

$$\forall g \in G, \quad e*g = g*e = g,$$

alors il est unique. On dit que c'est l'*élément neutre* et que G est un *monoïde*. Un exemple typique de monoïde s'obtient de la façon suivante : on se donne un ensemble X quelconque et on considère l'ensemble $\mathscr{F}(X)$ de toutes les applications $f : X \to X$ et la loi de composition des applications. On a bien

1. $\forall f,g,h : X \to X, \quad (f \circ g) \circ h = f \circ (g \circ h)$,
2. $\forall f : X \to X, \quad \mathrm{Id}_X \circ f = f \circ \mathrm{Id}_X = f$.

Un exemple plus simple est donné par l'ensemble $\mathbb{N}$ des entiers naturels muni de l'addition (ou de la multiplication d'ailleurs).

Si G est un monoïde, on dit que $g' \in G$ est un *symétrique* pour $g \in G$ si

$$g * g' = g' * g = e,$$

et que G est un *groupe* si tout élément possède un symétrique. Enfin, on dit que G est *commutatif* (ou *abélien*) si

$$\forall g,h \in G, \quad g * h = h * g.$$

Dans le cas d'une loi externe

$$G \times X \to X, \quad (g,x) \mapsto g * x,$$

ou G est un monoïde, on dit que G *opère* (ou *agit*) sur X si la loi est associative :

$$\forall g,h \in G, x \in X \quad (g * h) * x = g * (h * x)$$

et si l'opération de e est neutre :

$$\forall x \in X, \quad e * x = x,$$

Nous n'en dirons pas plus ici. L'exemple classique d'une opération est donné par celle du *groupe symétrique* $\mathscr{S}_3$ sur un *triangle équilatéral* (ou plus généralement le *groupe diédral* opérant sur un *polygone régulier*).

L'interprétation de la notion d'*application linéaire* en terme de matrice démontre immédiatement sa puissance. La définition formelle est cependant très élémentaire : c'est une application $u : E \to F$ entre deux espaces vectoriels sur K qui satisfait

1. $\forall x,y \in E, \quad u(x+y) = u(x) + u(y)$ (u est un *morphisme* de groupes abéliens),
2. $\forall a \in K, \forall x \in E, \quad u(ax) = au(x)$ (u est compatible avec l'opération de K).

On définit exactement de la même manière la notion d'application linéaire (ou de *morphisme*) entre deux modules. Nous allons de nouveau déconstruire cette définition.

D'une part, on dit qu'une application $f : G \to H$ entre deux groupes est un *morphisme* (ou *homomorphisme*) si

$$\forall g,h \in G, \quad f(g * h) = f(g) * f(h).$$

C'est une généralisation de la condition 1. L'exemple typique est l'exponentielle qui est un morphisme entre $\mathbb{R}$ muni de l'addition, et $\mathbb{R}_{>0}$ muni de la multiplication (ou le logarithme dans l'autre sens). Lorsque G et H sont seulement des monoïdes, dans la définition d'un *morphisme*, il faut rajouter la condition

$$f(e_G) = e_H,$$

qui n'est plus alors automatique. On peut ensuite définir un *morphisme* entre deux corps, ou plus généralement deux anneaux, comme une application qui est simultanément un morphisme de groupes abéliens (additifs) et un morphisme de monoïdes multiplicatifs. D'autre part, si un monoïde G opère sur deux ensembles X et Y, une application $f : X \to Y$ sera dite *compatible* avec l'opération si

$$\forall g \in G, \forall x \in X, \quad f(g * x) = g * f(x).$$

C'est une généralisation de la condition 2.

Jusqu'ici, nous avons laissé de coté la notion de distributivité qui spécifie l'interaction entre l'addition et la multiplication. Pour mieux comprendre comment cela fonctionne, il est bon de rappeler qu'il revient au même de se donner une application $\varphi : X \times Y \to Z$ ou une application $\Phi : X \mapsto \mathscr{F}(Y,Z)$ à valeurs dans l'ensemble des applications de Y dans Z. Cette correspondance est donnée par $\varphi(x,y) = \Phi(x)(y)$. En particulier, une loi externe $G \times X \to X$, notée multiplicativement pour simplifier (on ne met pas de $*$), correspond à une application

$$G \to \mathscr{F}(X), \quad g \mapsto (h \mapsto gh).$$

C'est une opération si et seulement ci cette dernière application est un morphisme de monoïdes. Supposons maintenant que le monoïde G opère sur un groupe abélien M. On peut alors requérir que l'image de l'application $G \to \mathscr{F}(M)$ soit en fait contenue dans l'ensemble $\mathrm{End}(M)$ des morphismes de groupes abéliens de M dans lui même (endomorphismes). Cela signifie que

$$\forall g \in G, \forall x, y \in M, \quad g(x+y) = gx + gy.$$

Supposons maintenant que ce soit un anneau A qui opère (par multiplication) sur le groupe abélien M. Remarquons qu'il existe une addition sur $\mathscr{F}(M)$ qui en fait un groupe abélien. On peut alors demander que l'application $A \to \mathscr{F}(M)$ soit un morphisme de groupes abéliens (et donc d'anneaux), cela signifie que

$$\forall a, b \in A, \forall x \in M, \quad (a+b)x = ax + bx,$$

et on retrouve la distributivité de l'autre coté. Ce sera en fait cette approche que nous suivrons pour définir la notion d'espace vectoriel (et plus généralement de module).

Pour conclure, on rappellera qu'un *sous-espace* d'un espace vectoriel E sur un corps K est une partie F de E qui satisfait les propriétés suivantes :

1. (a) $0_E \in F$,
   (b) $\forall x, y \in F, \quad x + y \in F$,
2. $\forall a \in K, \forall x \in F, \quad ax \in F$.

Ici encore, on voit immédiatement comment définir les notions de *sous-groupe*, de *sous-monoïde* (analogue des conditions de 1)) ou de *sous-anneau* (conditions de 1) satisfaites pour les deux lois). De même, si un monoïde G opère sur un ensemble X, on peut dire ce qu'est une partie *stable* sous l'opération de G (analogue de la condition 2)). Les détails sont laissés au lecteur.

La stratégie utilisée dans ce cours pour étudier les espaces vectoriels s'applique aussi bien à toutes les autres structures algébriques (groupes, anneaux, modules, ensembles à opérateurs, etc.). Cela pourra sembler un peu formel et trop abstrait au début, voire inutile pour ceux qui souhaitent simplement maîtriser quelques outils d'algèbre linéaire. Que ceux-ci se rassurent, au fur et à mesure que le cours se déroule, nous serons de plus en plus spécifiques et conséquemment plus concrets dans un certain sens. Nous démontrerons des théorèmes utiles.

Un grand merci aux étudiant(e)s qui ont participé à cet enseignement pour leurs retours sur les versions préliminaires de ce cours.

Première partie

1. Structures algébriques

1.1 Ensemble

Nous ne faisons qu'effleurer la *Théorie des Ensembles* et nous renvoyons le lecteur intéressé vers l'ouvrage éponyme de Jean-Louis Krivine ([Kri07]) par exemple. Ici, nous voulons surtout rappeler le vocabulaire et fixer les notations.

Ensemble, élément

Définition 1.1.1 Un *ensemble* est une « collection » X d'objets x, appelés les *éléments* de X, qui satisfont tous une même *propriété* $\mathscr{P}$ (par exemple, celle d'appartenir à X). C'est un nouvel objet.

On dit alors que x *appartient* à X, et on écrit $x \in X$, ou que x *satisfait* la propriété $\mathscr{P}$, et on écrit $\mathscr{P}(x)$.

Exemple On *définit* par récurrence l'*entier naturel* $n := \{0, 1, \dots, n-1\}$ (c'est donc aussi un ensemble) et l'*ensemble des entiers naturels* $\mathbb{N} := \{0, 1, 2, \dots\}$ (c'est donc aussi un objet).

La théorie des ensembles permet de concrétiser la logique (mathématique) :

Mathématiques	$\longleftrightarrow$	Logique
Objet	$\longleftrightarrow$	Concept
Ensemble	$\longleftrightarrow$	Propriété
$\{x \,/\, \mathscr{P}(x)\}$	$\longleftrightarrow$	$x \in X$
Égalité	$\longleftrightarrow$	Équivalence
Inclusion	$\longleftrightarrow$	Implication
Complémentaire	$\longleftrightarrow$	Négation
Intersection	$\longleftrightarrow$	Conjonction
Union	$\longleftrightarrow$	Disjonction
Vide	$\longleftrightarrow$	Impossible
Disjoint	$\longleftrightarrow$	Incompatible

On décrit un ensemble X en donnant *une* liste des ses éléments (en *extension*) ou en donnant *une* propriété qui le caractérise (en *compréhension*).

Exemple 1. $\{1,-1\}$ (extension) $=\{x\in\mathbb{Z}\ /\ x^2=1\}$ (compréhension).
2. La diagonale du plan :

$$\Delta := \{(t,t),\quad t\in\mathbb{R}\} \text{ (extension) } = \{(x,y)\in\mathbb{R}^2\ /\ y=x\} \text{ (compréhension).}$$

Produit, famille

Définition 1.1.2 Soit S un ensemble. Pour chaque $s\in S$, soit X_s un ensemble. Si on se donne pour tout $s\in S$, un élément $x_s\in X_s$, on dit que $(x_s)_{s\in S}$ est une *famille* indexée par S. Le *produit* des ensembles X_s est l'ensemble

$$\prod_{s\in S} X_s := \{(x_s)_{s\in S},\quad x_s\in X_s\}$$

de toutes ces familles.

Souvent, tous les X_s sont égaux au même ensemble X et on écrit alors

$$X^S := \{(x_s)_{s\in S},\quad x_s\in X\}.$$

On parle alors de *puissance* (au lieu de produit) et on dit que $(x_s)_{s\in S}$ est une famille d'éléments de X. Au lieu de famille, on dit *n-uple* (*singleton*, *couple*, *triplet*) si $S=n$, *suite* si $S=\mathbb{N}$ et *matrice* si $S=m\times n$ (rappelons qu'on peut voir un entier naturel comme un ensemble).

Exemple 1. Comme on compte traditionnellement à partir de 1, on fera souvent l'abus d'écriture $n=\{1,\dots,n\}$ (au lieu de $n=\{0,\dots,n-1\}$). Par exemple, pour les n-uples, on écrira plutôt $(x_1,\dots,x_n)$ et on note leur ensemble $X_1\times\cdots\times X_n$.
2. De même, une matrice est une famille indexée par $n\times m$: c'est donc (en numérotant à partir de 1) un objet de la forme

$$\begin{bmatrix} x_{1,1} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots \\ x_{n,1} & \cdots & x_{n,m} \end{bmatrix}.$$

Leur ensemble se note aussi $\mathrm{M}_{n\times m}(X)$ (ou $\mathrm{M}_n(X)$ lorsque $m=n$).

Remarque Ne pas confondre *ensemble* et *famille*. On a

$$\{a,a\}=\{a\} \quad \text{et} \quad \{a,b\}=\{b,a\}$$

mais les égalités analogues sont *fausses* pour les familles (l'ordre compte et on peut répéter). Cependant, on peut jongler entre ces deux notions : si on se donne un ensemble X, il suffit de prendre $S:=X$ et de considérer la famille $(x)_{x\in X}$; et réciproquement, si on se donne une famille d'éléments $(x_s)_{s\in S}$ d'un ensemble X, on peut regarder l'ensemble $\{x_s, s\in S\}\subset X$.

C'est plus anecdotique mais on peut aussi définir l'*union disjointe* (appelée aussi *somme* ou *coproduit*) d'une famille d'ensembles :

$$\sqcup_{s\in S}X_s = \{(s,x_s),\quad s\in S, x_s\in X_s\}.$$

Application

Définition 1.1.3 Une *application* est une « méthode » f qui permet d'associer à tout élément x d'un ensemble (*de départ, source*) X, un élément $f(x)$ d'un autre ensemble (*d'arrivée, but*) Y. On dit aussi parfois *opérateur* sur X lorsque $X = Y$.

On écrit

$$f : \quad \begin{array}{ccc} X & \longrightarrow & Y \\ x & \longrightarrow & f(x), \end{array}$$

et on dit que $f(x)$ est l'*image* de x ou que x est un *antécédent* de $f(x)$.

On désignera par

$$\mathscr{F}(X,Y) := \{f : X \to Y\}$$

l'ensemble de toutes les applications de X vers Y. On écrira simplement $\mathscr{F}(X)$ lorsque $X = Y$.

Remarque Rigoureusement parlant, l'application f est le triplet (X,Y,Γ) ou

$$\Gamma := \{(x,y) \ / \ y = f(x)\} \subset X \times Y$$

est le *graphe* de f.

Si $f : X \to Y$ est une application, on posera pour $A \subset X$ et $B \subset Y$,

$$f(A) := \{f(x), \quad x \in A\} \subset Y \quad \text{et} \quad f^{-1}(B) := \{x \in X \ / \ f(x) \in B\} \subset X.$$

Exemple Si

$$f : \mathbb{R}^2 \to \mathbb{R}^2, \quad (x,y) \mapsto (x-y, x+y)$$

et Δ désigne la diagonale, on a

$$f(\Delta) = \{0\} \times \mathbb{R} \quad \text{et} \quad f^{-1}(\Delta) = \mathbb{R} \times \{0\}.$$

injection, surjection, bijection

Nous utiliserons librement les quantificateurs $\forall$ (« quel que soit » ou par abus « quels que soient ») ainsi que $\exists$ (« il existe ») et par abus $\exists!$ (« il existe un unique »), voire $\nexists$ (« il n'existe pas »).

Définition 1.1.4 Une application $f : X \to Y$ est

1. *injective* si $\quad \forall x_1 \neq x_2 \in X, \quad f(x_1) \neq f(x_2)$,
2. *surjective* si $\quad \forall y \in Y, \quad \exists x \in X, \quad f(x) = y$,
3. *bijective* si $\quad \forall y \in Y, \quad \exists! x \in X, \quad f(x) = y$.

On notera $\mathscr{S}(X,Y)$ l'ensemble de toutes les bijections de X vers Y, et $\mathscr{S}(X)$ lorsque $X = Y$.

Remarque
1. On a bijective $\Leftrightarrow$ injective et surjective.
2. Les trois conditions sont équivalentes si $\mathrm{card}(X)$ et $\mathrm{card}(Y)$ sont égaux et finis (voir ci-dessous).
3. f bijective $\Leftrightarrow$ il existe une (unique) application $f^{-1} : Y \to X$ (la *réciproque*) telle que

$$y = f(x) \Leftrightarrow f^{-1}(y) = x.$$

4. On a toujours $f(\{x\}) = \{f(x)\}$ et, si f est bijective, $f^{-1}(\{y\}) = \{f^{-1}(y)\}$.

Exemple
1. Il existe une bijection (que l'on utilise usuellement comme une identification)

$$n := \{0, 1, \ldots, n-1\} \simeq \{1, \ldots, n\}, \quad i \mapsto i+1.$$

2. Si X et Y sont deux ensembles, il existe une bijection (une symétrie)

$$X \times Y \simeq Y \times X, \quad (x,y) \mapsto (y,x).$$

3. Il existe une bijection, dite de *transposition*,

$$\mathrm{M}_{n\times m}(X) \simeq \mathrm{M}_{m\times n}(X), \quad [x_{i,j}] \mapsto [x_{j,i}].$$

4. Si X et Y sont deux ensembles, il existe une bijection $\mathscr{F}(X,Y) \simeq Y^X$ donnée par

Application	$\longleftrightarrow$	Famille
$f : X \to Y$	$\longleftrightarrow$	$(y_x)_{x\in X}$
	$f(x) = y_x$	

Nous n'hésiterons pas à utiliser cette bijection pour appliquer à $\mathscr{F}(X,Y)$ certains résultats concernant les produits (et donc les puissances). On peut vraiment penser à une application comme à une famille et réciproquement. La différence est plutôt d'ordre psychologique, une application étant dynamique et une famille étant statique.

Cardinal

Définition 1.1.5 Le *cardinal* d'un ensemble X est le « nombre d'éléments » de cet ensemble : c'est l'ensemble X vu à bijection près. On le notera ultérieurement $\mathrm{card}(X)$, mais on utilise ici la notation $|X|$ plus pratique.

Par définition, on a donc $|X| = |Y|$ si et seulement si il existe une bijection $X \simeq Y$. On écrira $|X| \leq |Y|$ s'il existe seulement une injection $X \hookrightarrow Y$. Si $(X_s)_{s\in S}$ est une famille d'ensembles, on pose

$$\prod_{s\in S} |X_s| := \left|\prod_{s\in S} X_s\right| \quad \text{et} \quad \sum_{s\in S} |x_s| := \left|\bigsqcup_{s\in S} X_s\right|$$

(et on écrira aussi $|Y|^{|X|} := \left|Y^X\right|$).

On identifie $n \in \mathbb{N}$ avec son cardinal (on omet les barres de part et d'autre) et on écrit parfois $\aleph_0 := |\mathbb{N}|$. On dit que X est *fini* si $|X| = n \in \mathbb{N}$ et on écrit alors $|X| < +\infty$. Sinon, on dit que X est *infini*. On dit aussi que X est *dénombrable* si $|X| = \aleph_0$.

Remarque 1. On peut montrer que $|X| \leq |Y|$ si et seulement si $X = \emptyset$ ou bien il existe une surjection $Y \twoheadrightarrow X$.

2. On dispose aussi du *théorème de Cantor-Bernstein* :

$$|X| = |Y| \Leftrightarrow (|X| \leq |Y| \text{ et } |Y| \leq |X|).$$

3. On peut montrer que $|X| < 2^{|X|}$ et qu'il existe donc une infinité de cardinaux infinis.
4. Comme exemple, on peut voir que $|\mathbb{N}| = |\mathbb{Q}| < |\mathbb{R}| = |\mathbb{C}|$.
5. Dans le cas des opérations finies sur les cardinaux finis, on retrouve l'arithmétique habituelle des entiers naturels (ordre, multiplication, addition).
6. La définition de l'ordre, du produit et de la somme des cardinaux a vraiment un sens : elle ne dépend pas du choix des ensembles mais seulement de leur cardinal.

Composition, identité

Définition 1.1.6 L'*identité* de X est l'application $\mathrm{Id}_X : X \to X$ définie par $\mathrm{Id}_X(x) = x$. La *composée* des applications $f : X \to Y$ et $g : Y \to Z$ est l'application $g \circ f : X \to Z$ donnée par

$$(g \circ f)(x) = g(f(x)).$$

Remarque 1. Si $Y \subset X$, on considérera aussi l'*application d'inclusion* $Y \hookrightarrow X, y \mapsto y$ (à ne pas confondre avec l'identité lorsque $Y \neq X$).
2. On appelle parfois *projection* (ou *projecteur*) une application $p : X \to X$ telle que $p \circ p = p$ et *symétrie* (ou *involution*) une application $s : X \to X$ telle que $s \circ s = \mathrm{Id}_X$.
3. Lorsque $h : g \circ f$, nous dirons aussi que le *diagramme*

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "h"'] & Y \arrow[d, "g"] \\ & Z \end{tikzcd}$$

est *commutatif*. Cela s'étend à des diagrammes plus complexes comme nous le verrons plus tard.

Proposition 1.1.7 1. Étant donnés $f : X \to Y$, $g : Y \to Z$ et $h : Z \to W$, on a $(h \circ g) \circ f = h \circ (g \circ f)$.
2. Si $f : X \to Y$, on a $f \circ \mathrm{Id}_X = \mathrm{Id}_Y \circ f = f$.
3. $f : X \to Y$ est bijective si et seulement si il existe $g : Y \to X$ telle que $g \circ f = \mathrm{Id}_X$ et $f \circ g = \mathrm{Id}_Y$ (et on a alors $g = f^{-1}$).

Démonstration. Exercice. ■

Propriété universelle du produit

Nous voyons maintenant notre première *propriété universelle* :

Proposition 1.1.8 Soient $(X_s)_{s \in S}$ une famille d'ensembles, $X := \prod_{s \in S} X_s$, et pour tout $s \in S$,

$$p_s : X \to X_s, \quad x := (x_t)_{t \in S} \mapsto x_s.$$

Soient Y un ensemble quelconque et pour tout $s \in S$, $f_s : Y \to X_s$ une application. Alors, il existe une unique application $f : Y \to X$ telle que pour tout $s \in S$, on ait $f_s = p_s \circ f$.

Démonstration. Exercice. ■

On résume cette propriété dans le diagramme commutatif

$$\begin{tikzcd} Y \arrow[r, dashed, "\exists! f"] \arrow[dr, "f_s"'] & X \arrow[d, "p_s"] \\ & X_s. \end{tikzcd}$$

Définition 1.1.9 On dit que p_s est la *projection* de X sur X_s et que f_s est la s-ème *composante* de f.

Remarque 1. Dans le cas d'un produit fini $X_1 \times \cdots \times X_n$, on a

$$p_i(x_1, \ldots, x_n) = x_i \quad \text{et} \quad f(y) = (f_1(y), \ldots, f_n(y)).$$

2. Les résultats sur les produits s'appliquent toujours aux puissances dont les éléments peuvent s'interpréter comme des applications : si X et Y sont deux ensembles, ce sont les applications d'*évaluation*
$$p_x : \mathscr{F}(X,Y) \to Y, \quad f \mapsto f(x),$$
qui jouent le rôle des projections.
3. Si on se donne une famille d'applications $f_s : X_s \to Y_s$, on pourra considérer l'application
$$\prod_{s\in S} f_s : \prod_{s\in S} X_s \to \prod_{s\in S} Y_s, \quad (x_s)_{s\in S} \mapsto (f_s(x_s))_{s\in S}.$$

Loi de composition

Définition 1.1.10 Une *loi (de composition)* est une application $\Phi : X \times Y \to Z$. On dit loi de composition *interne* sur X si $X = Y = Z$ (et *externe* sur Y si $Y = Z$). Une loi de composition s'appelle aussi parfois une *opération* (mais nous donnerons à ce mot une définition plus restrictive).

En pratique, on fait souvent disparaître Φ des notations et on écrit par exemple $xy := \Phi(x,y)$. Notons aussi qu'il revient au même de se donner une loi de composition $X \times Y \to Z$ ou une application $\rho : X \mapsto \mathscr{F}(Y,Z)$, l'équivalence étant donnée par $\rho(x)(y) = xy$. Nous utiliserons alternativement les deux approches.

C'est la donnée d'un certain nombre d'opérations, satisfaisant un certain nombre de propriétés, qui constitue ce qu'on appelle une *structure algébrique*. Nous allons en passer un certain nombre en revue.

1.2 Monoïde, groupe

Nous introduisons la notion de monoïde à cause de son ubiquité en mathématiques mais nous ne considérerons ensuite que des structures plus riches. Pour la notion de groupe on peut se référer à l'ouvrage de Felix Ulmer ([Ulm12]) par exemple.

Définition 1.2.1 Un *monoïde* est un ensemble G muni d'une loi de composition interne
$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & gh \end{array}$$
qui
1. est *associative* : $\forall g,h,k \in G, \quad (gh)k = g(hk)$
2. admet *élément neutre* : $\exists 1 \in G, \quad g1 = 1g = g$.

On définit alors (par récurrence) le *produit*
$$\prod_{i=1}^n g_i := g_1 \cdots g_n$$
et la *puissance*
$$g^n := \underbrace{g \cdots g}_{n \text{ fois}}.$$

Remarque 1. Rappelons que la notation gh (ainsi que 1) qui rappelle la multiplication est arbitraire. Parfois la loi sera une loi de composition (et l'unité devient alors l'identité) ou d'addition (et l'unité devient alors le zéro).
2. On écrira parfois 1_G pour l'unité de G afin de la différentier de l'unité d'un autre monoïde.

3. Le produit de n éléments est plus précisément défini par récurrence en stipulant que le produit vide vaut 1. La puissance est un cas particulier du produit si bien que l'on a toujours $g^0 = 1$.
4. On rencontre aussi les structures plus pauvres que celle de monoïde comme celles de *magma* (aucune condition) et de *semi-groupe* (seulement la première condition).

Exemple 1. Si X est un ensemble, alors l'ensemble $G := \mathscr{F}(X)$ des opérateurs sur X est un monoïde pour $\circ$ (avec Id_X comme élément neutre).
2. Si G est un monoïde et X est un ensemble quelconque, alors l'ensemble $\mathscr{F}(X,G)$ de toutes les applications de X vers G est un monoïde pour la loi

$$\forall x \in X, \quad (fg)(x) := f(x)g(x)$$

avec $\forall x \in X, 1(x) = 1$ (attention : dans le cas $X = G$, on voit donc que $\mathscr{F}(G)$ est muni de deux lois distinctes).
3. Si $(G_s)_{s\in S}$ est une famille de monoïdes, alors $\prod_{s\in S} G_s$ est un monoïde pour la loi (dite *terme à terme*)

$$(g_s)_{s\in S}(h_s)_{s\in S} = (g_s h_s)_{s\in S}$$

avec $1 = (1_s)_{s\in S}$. C'est en quelque sorte une généralisation du cas précédent.
4. Si A est un *anneau* (voir plus bas), alors $\mathrm{M}_n(A)$ est un monoïde pour la loi

$$[a_{i,j}][b_{i,j}] = \left[\sum_k a_{i,k} b_{k,j}\right]$$

avec la *matrice unité* I comme unité (on dispose aussi de la multiplication terme à terme que l'on n'utilisera *jamais*).
5. Les ensembles de nombres comme $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Z}/n\mathbb{Z}, \ldots$ sont des monoïdes pour la multiplication mais aussi pour l'addition (avec 0 comme élément neutre).

On utilisera souvent la *notation de Minkowski* : si $A, B \subset G$ monoïde, alors

$$AB := \{gh, \quad g \in A, h \in B\}$$

(c'est l'image de $A \times B$ par la loi de G). Lorsque $A = \{g\}$ ou $B = \{h\}$, on écrira gB ou Ah si bien que

$$gB := \{gh, \quad h \in B\} \quad \text{et} \quad Ah := \{gh, \quad g \in A\}.$$

Définition 1.2.2 Un *morphisme* de monoïdes $f : G \to H$ est une application telle que
1. $\forall g, h \in G, \quad f(gh) = f(g)f(h)$
2. $f(1_G) = 1_H$.

Un *isomorphisme* est un morphisme bijectif.

On note $\mathrm{Hom}(G,H)$ l'ensemble des morphismes de monoïdes, $\mathrm{End}(G) := \mathrm{Hom}(G,G)$ et $\mathrm{Aut}(G) := \mathrm{End}(G) \cap \mathscr{S}(G)$. S'il existe un isomorphisme entre G et H, on écrira $G \simeq H$.

Remarque 1. De manière équivalente, un morphisme de monoïdes est un morphisme qui préserve les produits

$$f\left(\prod_{i=1}^n g_i\right) = \prod_{i=1}^n f(g_i)$$

(avec la convention usuelle que le produit vide vaut 1).

2. La notion de *morphisme* est très générale et, si on veut enlever toute ambiguïté on indiquera par un indice la catégorie d'objets dans laquelle on les considère. Autrement dit, on pourra écrire $\mathrm{Hom}_{\mathrm{Mon}}(G,H)$ pour préciser qu'on considère les morphismes *de monoïdes*, et pas des morphismes relatifs à une autre structure que pourraient porter G et H.
3. Attention, les formules peuvent prendre une forme très différente en fonction de la notation des lois. Par exemple, un morphisme $\varphi : \mathscr{F}(X) \to \mathbb{N}$ (avec composition à gauche et addition à droite) doit satisfaire

$$\varphi(g \circ f) = \varphi(g) + \varphi(f) \quad \text{et} \quad \varphi(\mathrm{Id}_X) = 0.$$

Proposition 1.2.3
1. Si $f : G \to H$ et $g : H \to K$ sont deux morphismes de monoïdes, alors $g \circ f$ aussi.
2. Si $f : G \to H$ est un isomorphisme de monoïdes, alors f^{-1} aussi.

Démonstration.
1. Exercice.
2. Rappelons la définition de l'application réciproque : $f(x) = y \Leftrightarrow x = f^{-1}(y)$. Comme f est un morphisme de monoïdes, si $g,h \in H$, on a

$$f(f^{-1}(g)f^{-1}(h)) = f(f^{-1}(g))f(f^{-1}(h)) = gh$$

et donc $f^{-1}(g)f^{-1}(h) = f^{-1}(gh)$. De même, comme $f(1) = 1$, on aura $1 = f^{-1}(1)$. ■

Définition 1.2.4 Un monoïde H est un *sous-monoïde* d'un monoïde G s'il est contenu dans G et si l'inclusion est un morphisme.

Si c'est le cas, alors la loi de H est induite par la loi de G et l'unité de H est l'unité de G. Réciproquement, si H est une partie d'un monoïde G telle que
1. $1 \in H$,
2. $\forall g,h \in H, \quad gh \in H$,

alors la loi de G induit sur H une structure de sous-monoïde. Notons, que la seconde condition s'écrit aussi $HH \subset H$. Alternativement, on peut demander que tous les produits (y compris le produit vide) d'éléments de H restent dans H.

Proposition 1.2.5 Soit $f : G \to H$ un morphisme de monoïdes.
1. Si G' est un sous-monoïde de G, alors $f(G')$ est un sous-monoïde de H.
2. Si H' est un sous-monoïde de H, alors $f^{-1}(H')$ est un sous-monoïde de G.

Démonstration. Exercice. ■

Définition 1.2.6 Soit $f : G \to H$ un morphisme de monoïdes. Alors,
1. l'*image* de f est $\operatorname{im} f := f(G) \subset H$,
2. le *noyau* de f est $\ker f := f^{-1}(\{1_H\}) \subset G$.

Remarque
1. On voit donc que si $f : G \to H$ un morphisme de monoïdes, alors $\operatorname{im} f$ est un sous-monoïde de H et $\ker f$ est un sous-monoïde de G.
2. La notion d'image a un sens pour n'importe quelle application $f : X \to Y$ en posant

$$\operatorname{im} f := f(X) \subset Y,$$

mais celle de noyau est typique des structures algébriques.

Définition 1.2.7 Soit G un monoïde. On dit que $g,h \in G$ *commutent* si $gh = hg$. On dit que G est *commutatif* si tous ses éléments commutent.

Exemple 1. Les ensembles de nombres comme ci-dessus, avec la multiplication *ou* avec l'addition (voir plus bas), sont des monoïdes commutatifs.
2. Le *groupe symétrique* $\mathscr{S}_n$ (voir plus bas) pour $n > 2$ n'est pas commutatif. Le monoïde $\mathrm{M}_n(A)$ pour $n > 1$ et $A \neq \{0\}$ n'est pas commutatif.

Si on utilise la notation additive (et 0 pour l'élément neutre), on dira que le monoïde est *abélien* au lieu de commutatif. En d'autres termes, M est un monoïde abélien s'il est muni d'une loi

$$\begin{aligned} M \times M &\longrightarrow M \\ (x,y) &\longmapsto x+y \end{aligned}$$

telle que
1. $\forall x,y,z \in M, \quad (x+y)+z = x+(y+z)$,
2. $\exists 0 \in M, \forall x \in M, \quad 0+x = x$,
3. $\forall x,y \in M, \quad x+y = y+x$.

On considère alors les notions de *somme*

$$\sum_{i=1}^{n} x_i := x_1 + \cdots + x_n,$$

ainsi que de *multiple*

$$nx := \underbrace{x+\cdots+x}_{n \text{ fois}}$$

(au lieu de produit et puissance).

Définition 1.2.8 Soit G un monoïde. On dit que g^{-1} est un *inverse* pour $g \in G$ si $gg^{-1} = g^{-1}g = 1$. On dit que G est un *groupe* si tous ses éléments sont inversibles.

On note $G^{\times}$ l'ensemble de tous les éléments inversibles d'un monoïde G. C'est un sous-monoïde qui est un *groupe*. On écrit parfois $g/h := gh^{-1}$ (attention tout de même si G n'est pas commutatif).

Si M est un monoïde abélien, on parle d'*opposé* et on écrit $-x$ si bien que la condition devient $x+(-x) = 0$. On écrit alors $x - y := x + (-y)$.

Exemple 1. Si X est un ensemble, alors $\mathscr{S}(X) = \mathscr{F}(X)^{\times}$ est un groupe pour $\circ$.
2. $\mathscr{S}_n := \mathscr{S}(\{1,\ldots,n\})$ est appelé le *groupe symétrique* et ses éléments sont les *permutations*.
3. $\mathbb{Z}$ est un groupe abélien pour $+$ mais pas $\mathbb{N}$.
4. $\mathbb{Z}^{\times} = \{-1,1\}$ est un groupe pour la multiplication mais pas $\mathbb{Z}$.
5. Si A est un anneau, alors $\mathrm{GL}_n(A) := \mathrm{M}_n(A)^{\times}$ est le groupe des matrices inversibles.
6. Si M et N sont deux groupes abéliens, alors $\mathrm{Hom}(M,N)$ est un sous-groupe (abélien) de $\mathscr{F}(M,N)$ (qui est lui même un groupe abélien). Attention : la structure de groupe est induite par celle de N seulement.

Remarque 1. On devrait dire *monoïde inversif* au lieu de groupe. En effet, un groupe est tout simplement un monoïde qui satisfait une propriété en sus.
2. On dira *(iso-) morphisme de groupes* pour (iso-) morphisme de monoïdes $f : G \to H$ entre deux groupes. Notons que la seconde condition $f(1_G) = 1_H$ est alors conséquence de la première et que l'on a toujours $f(g^{-1}) = f(g)^{-1}$.
3. De même, un *sous-groupe* H d'un groupe G est un sous-monoïde qui est lui-même un groupe : il faut donc penser à s'assurer que si $h \in H$, on a bien $h^{-1} \in H$.

4. On dit qu'un monoïde G est *intègre* si

$$\forall g,h,h' \in G, \quad gh = gh' \Rightarrow h = h' \quad \text{et} \quad \forall g,g',h \in G, \quad gh = g'h \Rightarrow g = g'.$$

Un groupe est toujours intègre. Notons que dans un monoïde abélien M, la condition s'écrit

$$\forall x,y,z \in M, \quad x+y = x+z \Rightarrow y = z.$$

La notion suivante est très importante mais nous la rencontrerons très peu dans cet ouvrage :

Définition 1.2.9 Si G est un monoïde, alors un *G-ensemble* est un ensemble X muni d'un morphisme de monoïdes

$$\begin{aligned} G &\longrightarrow \mathscr{F}(X) \\ g &\longmapsto (x \mapsto gx). \end{aligned}$$

On dit aussi que G *opère* sur X.

Alternativement, cela revient a donner une loi de composition externe

$$\begin{aligned} G \times X &\longrightarrow X \\ (g,x) &\longmapsto gx \end{aligned}$$

telle que

1. $\forall g,h \in G, \forall x \in X, \quad (gh)x = g(hx)$
2. $\forall x \in G, \quad 1x = x.$

Définition 1.2.10 Un *morphisme de G-ensembles* est une application $f : X \to Y$ telle que

$$\forall g \in G, \forall x \in X, \quad f(gx) = gf(x).$$

On dit aussi que l'application $f : X \to Y$ est *compatible* avec les opérations.

1.3 Anneau, corps

La notion d'anneau formalise l'idée d'un d'ensemble de nombres. Nous resterons extrêmement succin et le lecteur qui souhaite en savoir plus pourra regarder l'ouvrage de Rémi Goblot ([Gob01]) par exemple.

Définition 1.3.1 Un *anneau (associatif unitaire)* est un groupe abélien A muni d'un morphisme de groupes abéliens

$$\begin{aligned} A &\longrightarrow \mathrm{End}_{\mathrm{Ab}}(A) \subset \mathscr{S}(A) \\ a &\longmapsto (b \mapsto ab). \end{aligned}$$

telle que la loi induite fasse de A un monoïde. On dit que l'anneau est *commutatif* si la multiplication aussi est commutative.

Alternativement, cela revient à munir A de deux lois internes

$$\begin{aligned} A \times A &\longrightarrow A \\ (a,b) &\longmapsto a+b \end{aligned} \qquad \text{et} \qquad \begin{aligned} A \times A &\longrightarrow A \\ (a,b) &\longmapsto ab \end{aligned}$$

satisfaisant les propriétés suivantes

1. (a) $\forall a,b,c \in A, \quad (a+b)+c = a+(b+c),$
   (b) $\exists 0 \in A, \forall a \in A, \quad 0+a = a,$

   (c) $\forall a \in A, \exists -a \in A, \quad a + (-a) = 0$,
   (d) $\forall a, b \in A, \quad a + b = b + a$,
2. (a) $\forall a, b, c \in A, \quad (ab)c = a(bc)$,
   (b) $\exists 1 \in A, \forall a \in A, \quad a1 = 1a = a$,
3. et la *distributivité* :

$$\forall a, b, c \in A, \quad a(b+c) = ab + ac \quad \text{et} \quad (b+c)a = ba + ca.$$

Exemple 1. $\mathbb{Z}$ est un anneau commutatif.
2. Si M est un groupe abélien, alors $\mathrm{End}(M)$ est un anneau (non commutatif en général) pour $+$ et $\circ$.
3. Si A est un anneau et X un ensemble, alors $\mathscr{F}(X, A)$ est aussi un anneau.
4. Si $(A_s)_{s \in S}$ est une famille d'anneaux, alors $\prod_{s \in S} A_s$ est aussi un anneau.
5. Si A est un anneau, alors $\mathrm{M}_n(A)$ est aussi un anneau (pour l'addition terme à terme et la multiplication des matrices) mais il n'est pas commutatif (si $A \neq \{0\}$).

Définition 1.3.2 1. Un *morphisme d'anneaux* $f : A \to B$ est une application qui est un morphisme simultanément pour les deux lois. On dit *isomorphisme d'anneau* s'il est bijectif.
2. Un *sous-anneau* B d'un anneau A est un anneau qui est contenu dans A et tel que l'inclusion soit un morphisme d'anneaux.

Remarque 1. Si $f : A \to B$ et $g : B \to C$ sont deux morphismes d'anneaux, alors $g \circ f$ aussi.
2. Si $f : A \to B$ est un isomorphisme d'anneaux, alors f^{-1} aussi.
3. Un isomorphisme d'anneaux est une application qui est un isomorphisme pour les deux lois.
4. Un sous-anneau est une partie qui est à la fois un sous-groupe pour l'addition et un sous-monoïde pour la multiplication.
5. On dit qu'un anneau A est *intègre* si $A \setminus \{0\}$ est un sous-monoïde. C'est alors automatiquement un sous-monoïde intègre.

Définition 1.3.3 Un *corps* est un anneau commutatif K tel que $K \setminus \{0\}$ soit un groupe. Un morphisme d'anneaux entre deux corps s'appelle une *extension de corps*.

Exemple 1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ si p est premier, $K(T)$ si K est un corps.
2. Les anneaux $\mathbb{Z}$ et $\mathbb{D}$ des entiers naturels et des nombres décimaux sont des anneaux commutatifs intègres qui ne sont *pas* des corps. De même, si n n'est pas premier, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps (même pas intègre). Si K et L sont des corps, alors $K \times L$ est un anneau qui n'est *pas* un corps (pas intègre). L'anneau nul $\{0\}$ n'est *pas* un corps (pas intègre non plus).

Définition 1.3.4 La *caractéristique* d'un anneau A, notée $\mathrm{Car}(A)$, est le plus petit $p \in \mathbb{N} \setminus \{0\}$ tel que

$$p1_A := \underbrace{1_A + \cdots + 1_A}_{p \text{ fois}} = 0_A$$

s'il existe, et 0 sinon.

Remarque 1. De manière plus sophistiquée, il existe un unique morphisme d'anneaux $\mathbb{Z} \to A$ et son noyau est (l'idéal principal) $p\mathbb{Z} := \{pn, \quad n \in \mathbb{Z}\}$.
2. Dire que $\mathrm{Car}(A) = 0$ signifie essentiellement que A contient $\mathbb{Z}$ et, dans le cas d'un corps K, que K contient $\mathbb{Q}$.
3. Dire que $\mathrm{Car}(A) \neq 2$ signifie que $1_A \neq -1_A$. Lorsque A est un anneau intègre (par exemple un corps), c'est équivalent à dire que l'on a jamais $-a = a$ dans A si $a \neq 0$.

1.4 Module, espace vectoriel

La notion de module généralise simultanément celles de groupe abélien et d'espace vectoriel. Nous nous limiterons très vite à ce dernier cas mais le lecteur qui voudrait mieux comprendre l'utilité de cette notion pourra consulter l'ouvrage de Daniel Guin ([Gui13]) par exemple.

On fixe un anneau A (que l'on peut supposer commutatif – par exemple $A = K$, un corps, ou $A = \mathbb{Z}$).

Définition 1.4.1 Un *A-module (à gauche)* est un groupe abélien M muni d'un morphisme d'anneaux

$$\begin{aligned} A &\longrightarrow \mathrm{End}_{\mathrm{Ab}}(M) \\ a &\longmapsto (x \mapsto ax). \end{aligned}$$

Cela veut donc dire que M est muni d'une loi interne et d'une loi externe

$$\begin{aligned} M \times M &\longrightarrow M \\ (x,y) &\longmapsto x+y \end{aligned} \qquad \text{et} \qquad \begin{aligned} A \times M &\longrightarrow M \\ (a,x) &\longmapsto ax, \end{aligned}$$

et que l'on a les propriétés suivantes

1. (a) $\forall x,y,z \in M, \quad (x+y)+z = x+(y+z)$,
   (b) $\exists 0 \in M, \forall x \in M, \quad 0+x = x$,
   (c) $\forall x \in M, \exists -x \in M, \quad x+(-x) = 0$,
   (d) $\forall x,y \in M, \quad x+y = y+x$,
2. (a) $\forall a,b \in A, \forall x \in M, \quad (ab)x = a(bx)$,
   (b) $\forall x \in M, \quad 1x = x$,
   (c) $\forall a \in A, \forall x,y \in M, \quad a(x+y) = ax+ay$,
   (d) $\forall a,b \in A, \forall x \in M, \quad (a+b)x = ax+bx$.

Exemple 1. Un $\mathbb{Z}$-module est tout simplement un groupe abélien : l'opération de $\mathbb{Z}$ est automatiquement l'action naturelle donnée par

$$nx = \underbrace{x+\cdots+x}_{n \text{ fois}} \quad \text{et} \quad (-n)x = \underbrace{-x-\cdots-x}_{n \text{ fois}} \quad \text{pour } n \in \mathbb{N}.$$

2. Si K est un corps, un K-module est un *K-espace vectoriel*.
3. Un $K[T]$-module est essentiellement un K-espace vectoriel E muni d'un opérateur linéaire u : l'opération est alors donnée par $Px := P(u)(x)$ (voir plus loin).
4. $\{0\}$ et A sont toujours des A-module.
5. Si M est un A-module et X un ensemble, alors $\mathscr{F}(X,M)$ est aussi un A-module.
6. Si $(M_s)_{s\in S}$ est une famille de A-modules, alors $\prod_{s\in S} M_s$ est aussi un A-module (pour les lois terme à terme).
7. $\mathrm{M}_{n\times m}(A)$ est un A-module.

On utilisera parfois la notation de Minkowski dans ce contexte si bien que si $X,Y \subset M$ et $S \subset A$, on écrira

$$X+Y := \{x+y, \quad x \in X, y \in Y\} \quad \text{et} \quad SX = \{ax, \quad a \in S, x \in X\}.$$

Définition 1.4.2 Une *application A-linéaire* $u : M \to N$ entre deux A-modules est un morphisme de groupes abéliens qui est *compatible* avec la multiplication par les éléments de A.

En d'autres termes, on a

1. $\forall x,y \in M, \quad u(x+y) = u(x)+u(y)$,

2. $\forall a \in A, \forall x \in M, \quad u(ax) = au(x)$.

Alternativement, on peut demander que u préserve toutes les *combinaisons linéaires* :

$$\forall x_1, \ldots, x_n \in M, \forall a_1, \ldots, a_n \in A, \quad u\left(\sum_{i=1}^{n} a_i x_i\right) = \sum_{i=1}^{n} a_i u(x_i)$$

(la combinaison linéaire vide étant nulle par définition).

On dira aussi *morphisme de A-modules*, et on parlera donc d'*endomorphisme* (cas $M = N$), d'*isomorphisme* (cas u bijectif) ou d'*automorphisme* (les deux). On notera $\mathrm{L}(M,N)$ l'ensemble de toutes les applications linéaires de M vers N, $\mathrm{L}(M) := \mathrm{L}(M,M)$ et $\mathrm{GL}(M) = \mathrm{L}(M) \cap \mathscr{S}(M)$. S'il existe un isomorphisme entre deux A-modules M et N, on écrira encore $M \simeq N$. On indiquera A en indice si nécessaire.

Proposition 1.4.3
1. Si $u : M \to N$ et $v : N \to P$ sont deux applications A-linéaires, alors $v \circ u$ aussi.
2. Si $u : M \to N$ est un isomorphisme de A-modules, alors u^{-1} aussi.

Démonstration. Exercice. ∎

Définition 1.4.4 Un *sous-module* N d'un A-module M est un A-module N qui est contenu dans M et tel que l'inclusion $N \hookrightarrow M$ soit linéaire. Lorsque $M = A$, on dit *idéal*.

En d'autres termes, on demande que N soit une partie de M (muni de la structure induite) telle que

1. $0 \in N$
2. $\forall x, y \in N, \quad x + y \in N$,
3. $\forall a \in A, \forall x \in N, \quad ax \in N$.

Les deux dernières conditions s'écrivent aussi $N + N \subset N$ et $AN \subset N$. Alternativement, on peut demander que toute *combinaison linéaire* $\sum_{i=1}^{n} a_i x_i$ d'éléments $x_1, \ldots, x_n \in N$ avec *coefficients* $a_1, \ldots, a_n \in A$, soit encore dans N (la combinaison linéaire vide étant nulle par définition).

Exemple
1. Si M et N sont des A-modules, alors $\mathrm{L}(M,N)$ est un sous-module de $\mathscr{F}(M,N)$.
2. On dispose d'un isomorphisme de A-modules $\mathrm{M}_{n\times m}(A) \simeq \mathrm{L}(A^m, A^n)$ et on identifie parfois les deux.
3. La transposition $[a_{i,j}] \mapsto [a_{j,i}]$ est un isomorphisme $\mathrm{M}_{n\times m}(A) \simeq \mathrm{M}_{m\times n}(A)$ de A-modules.
4. Lorsque l'anneau A est un corps K, un sous-module est un *sous-espace vectoriel*. Lorsque $A = \mathbb{Z}$, un sous-module est un sous-groupe.
5. Un anneau commutatif est un corps si et seulement si il a exactement deux idéaux : $\{0\}$ et lui même (analogue à la définition d'un nombre premier).
6. Si $a \in A$, alors $(a) := Aa := \{ca, \quad c \in A\}$ est un idéal de A (dit *principal*).
7. Les idéaux de $K[T]$ sont tous principaux : ce sont donc les parties de la forme
$$(P) := \{PQ, \quad Q \in K[T]\}$$
formées des multiples de $P \in K[T]$. Et un tel P est unique si on requiert qu'il soit unitaire.
8. Les idéaux de $\mathbb{Z}$ aussi sont tous principaux (correspondant aux entiers naturels).
9. Nous avons mentionné ci-dessus qu'un $K[T]$-module est donné par un K-espace vectoriel E ainsi qu'un endomorphisme $u \in L(E)$. Alors, les sous-modules correspondent aux sous-espaces vectoriels F de E qui sont stables par u (tel que $u(F) \subset F$).

Tous les résultats à venir dans le chapitre 2 et la première moitié du chapitre 3 qui seront énoncés pour des espaces vectoriels sur un corps sont en fait encore valides pour des modules sur un anneau quelconque. La majeure partie des notions et résultats étudiés ensuite ont aussi un analogue pour les modules bien que certaines subtilités apparaissent.

1.5 Algèbre

Nous ne parlerons pas ici de la notion générale d'algèbre mais seulement de celle d'*algèbre associative unitaire* que nous abrégerons en disant tout simplement « algèbre ».

On fixe un corps K (ou plus généralement un anneau *commutatif* et il faut alors lire module au lieu d'espace vectoriel).

Définition 1.5.1 Une *K-algèbre (associative unitaire)* est un anneau L muni d'un morphisme d'anneau $K \to L$.

Cela signifie en fait que L est est muni d'une structure de K-espace vectoriel telle que

$$\forall a \in K, \forall u, v \in L, \quad (au)v = a(uv) = u(av)$$

(le morphisme d'anneaux $K \to L$ étant nécessairement donné par $a \mapsto a1_L$).

En d'autres termes, on dispose de trois lois

$$\begin{array}{ccc} L \times L \longrightarrow L & L \times L \longrightarrow L & K \times L \longrightarrow L \\ (x,y) \longmapsto x+y \quad , & (x,y) \longmapsto xy \quad \text{et} & (a,x) \longmapsto ax \end{array}$$

avec les propriétés suivantes

1. (a) $\forall u, v, c \in L, \quad (u+v)+c = u+(v+c)$,
   (b) $\exists 0 \in L, \forall u \in L, \quad 0+u = u$,
   (c) $\forall u \in L, \exists -u \in L, \quad u+(-u) = 0$,
   (d) $\forall u, v \in L, \quad u+v = v+u$,
2. (a) $\forall a, b \in K, \forall u \in L, \quad (ab)u = a(bu)$.
   (b) $\forall u \in L, \quad 1_K u = u$,
   (c) $\forall a \in K, \forall u, v \in L, \quad a(u+v) = au+av$,
   (d) $\forall a, b \in K, \forall u \in L, \quad (a+b)u = au+bu$,
3. (a) $\forall u, v, w \in L, \quad (uv)w = u(vw)$,
   (b) $\exists 1_L \in L, \forall u \in L, \quad u1_L = 1_L u = u$,
   (c) $\forall a \in K, \forall u, v \in L, \quad (au)v = a(uv) = u(av)$,
   (d) $\forall u, v, w \in L, \quad u(v+w) = uv+uw \quad$ et $\quad (v+w)u = vu+wu$.

Remarque On définit plus généralement une K-algèbre comme étant un K-espace vectoriel L muni d'une application *bilinéaire* (voir plus bas) $L \times L \to L$. On dit alors que L est *associative unitaire* si L est un monoïde (et donc un anneau) pour cette nouvelle loi.

Exemple
1. Les polynômes sur K forment une K-algèbre *commutative* $K[T]$.
2. Si E est un espace vectoriel, alors $\mathrm{L}(E)$ est une K-algèbre (pour $+, \circ, \cdot$).
3. Les matrices $n \times n$ à coefficients dans K forment une K-algèbre $\mathrm{M}_n(K)$.
4. Un produit d'algèbres $\prod_{s \in S} L_s$ est une algèbre et de même pour $\mathscr{F}(X, L)$ si X est un ensemble et L une algèbre.
5. Le corps $\mathbb{C}$ est une algèbre sur $\mathbb{R}$.

Définition 1.5.2
1. Un *morphisme de K-algèbres* est une application qui est simultanément un morphisme d'anneaux et d'espaces vectoriels. C'est un *isomorphisme* s'il est bijectif.
2. Une *sous-algèbre* d'une K-algèbre A est une K-algèbre qui est contenue dans A et telle que l'inclusion soit un morphisme de K-algèbres.

Exemple
1. Si X est un espace topologique et K un corps valué (comme $\mathbb{R}$ ou $\mathbb{C}$), alors l'ensemble $\mathscr{C}(X, K)$ des fonctions continues à valeur dans K est une sous-algèbre de $\mathscr{F}(X, K)$.

2. On dispose d'un isomorphisme de K-algèbres (non commutatives si $n > 1$) $\mathrm{M}_n(K) \simeq \mathrm{L}(K^n)$ et on identifie parfois les deux.
3. La transposition $\mathrm{M}_n(A) \to \mathrm{M}_n(A)$ n'est *pas* un automorphisme de K-algèbre (ce n'est pas un morphisme d'anneaux).

Nous pouvons énoncer une nouvelle propriété universelle (principe de substitution) :

Proposition 1.5.3 Si L est une K-algèbre et $u \in L$, il existe un unique morphisme de K-algèbres $\Phi_u : K[T] \to L$ tel que $\Phi_u(T) = u$. Si $P = \sum_{i=0}^d a_i T^i \in K[T]$, on aura $\Phi_u(P) = P(u) := \sum_{i=0}^d a_i u^i$.

Démonstration. On aura nécessairement

$$\Phi_u(P) = \Phi_u\left(\sum_{i=0}^d a_i T^i\right) = \sum_{i=0}^d a_i \Phi_u(T)^i = \sum_{i=0}^d a_i u^i =: P(u).$$

Réciproquement, il faut montrer qu'on obtient bien ainsi un morphisme d'algèbres (exercice) :
1. $\forall P, Q \in K[T], (P+Q)(u) = P(u) + Q(u)$,
2. $\forall a \in K, \forall P \in K[T], (aP)(u) = aP(u)$,
3. $\forall P, Q \in K[T], (PQ)(u) = P(u)Q(u)$,
4. $1(u) = 1_L$. ■

Exemple 1. Si u est un endomorphisme d'un k-espace vectoriel E et $P = T - a \in K[T]$, alors $P(u) = u - a\mathrm{Id}_E$ si bien que $P(u)(x) = u(x) - a$ si $x \in E$.
2. Si A est une matrice carrée et χ est son *polynôme caractéristique* (voir plus loin), alors le théorème de Cayley-Hamilton stipule que $\chi(A) = 0$ (matrice nulle).

Remarque 1. Dans le cas particulier ou $L = K[T]$ et $u = T$, l'unique morphisme $K[T] \to L$ qui envoie T sur u est l'identité. Autrement dit, on a $P(T) = P$, ce qui justifie a posteriori l'utilisation de la variable muette T (si on l'avait notée X, on aurait $P(X) = P$).
2. Comme $K[T]$ est un anneau commutatif, on voit que si $P, Q \in K[T]$ et $u \in L$, alors $P(u)$ commute avec $Q(u)$. Dans le cas particulier ou $L = L(E)$, cela s'écrit $P(u) \circ Q(u) = Q(u) \circ P(u)$ ou encore, si $x \in E$,

$$P(u)(Q(u)(x)) = Q(u)(P(u)(x)),$$

ce qui n'a rien d'évident.

1.6 Opérations élémentaires

On fixe un corps de base K (mais les définitions font sens sur n'importe quel anneau).

Définition 1.6.1 Si X est un ensemble, la *k-ème ligne* (resp. *l-ème colonne*) d'une matrice $A := [x_{i,j}] \in M_{n\times m}(X)$ est la matrice $[x_{k,1} \cdots x_{k,m}] \in M_{1\times m}(X)$

$$\left(\text{resp.}\quad \begin{bmatrix} x_{1,l} \\ \vdots \\ x_{n,l} \end{bmatrix} \in M_{n\times 1}(X)\right).$$

Remarque 1. La l-ème colonne de la transposée de A est la transposée de la l-ème ligne de A. Et réciproquement.
2. Dans tout ce qui suit, on pourra remplacer partout ligne par colonne, quitte à échanger aussi gauche et droite (car la transposée d'un produit est le produit des transposées dans l'ordre inverse).

Définition 1.6.2 Une *opération élémentaire* sur les lignes d'une matrice $A \in M_{n\times m}(K)$ est une transformation du type suivant

1. *Échange* : on échange la ligne k et la ligne l,
2. *Dilatation* : on multiplie la ligne k par une constante non nulle a,
3. *Transvection* : on ajoute à la ligne k un multiple par une constante a d'une *autre* ligne l.

Définition 1.6.3 Une *matrice élémentaire* est une matrice obtenue en effectuant une opération élémentaire sur I.

Proposition 1.6.4

1. Une matrice élémentaire est inversible et son inverse est une matrice élémentaire du même type.
2. Faire une opération élémentaire sur les lignes d'une matrice revient à multiplier à gauche par la matrice élémentaire correspondante.

Démonstration. Exercice. ■

Définition 1.6.5 Une matrice est *échelonnée* si le nombre de zéros précédent le premier coefficient non nul (appelé *pivot*) augmente *strictement* à chaque ligne. Elle est *échelonnée réduite* si les pivots valent tous 1 et que les autres coefficients sur la même colonne sont nuls.

Théoreme 1.6.6 — du pivot de Gauss (-Jordan). Il existe toujours une suite finie d'opérations élémentaires sur les lignes d'une matrice qui la transforme en une matrice échelonnée (réduite).

Démonstration. Il s'agit de l'algorithme du Pivot de Gauss. ■

Exemple

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 & 2 \\ 0 & 3 & 0 & 0 & 3 \end{pmatrix} \to \begin{pmatrix} 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 3 & 0 & 0 & 3 \end{pmatrix} \to$$
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 3 & 0 & 0 & 3 \end{pmatrix} \to \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Corollaire 1.6.7 Une matrice est inversible si et seulement si c'est un produit de matrices élémentaires. Si A est une matrice quelconque, il existe une matrice inversible P telle que PA soit échelonnée (réduite).

Démonstration. Exercice. ■

En pratique, on voit qu'une matrice A est inversible si et seulement si il existe une suite d'opérations élémentaires sur les lignes qui aboutit à la matrice unité I. Cela s'écrit $PA = I$ et on a donc $A^{-1} = P$, c'est à dire $A^{-1} = PI$. Autrement dit, on obtient A^{-1} en faisant la *même* suite d'opérations élémentaires sur I.

1.7 Exercices

Exercice 1.1 Étant données $f : X \to Y$ et $g : Y \to Z$, montrer que
1. Si f et g sont injectives (resp. surjectives), alors $g \circ f$ aussi.
2. Si $g \circ f$ est injective (resp. surjective), alors f aussi (resp. g aussi).

Exercice 1.2 Montrer que si $f : \mathbb{R}^2 \to \mathbb{R}^2, (x,y) \mapsto (x-y, x+y)$ et Δ désigne la diagonale, on a

$$f(\Delta) = \{0\} \times \mathbb{R} \quad \text{et} \quad f^{-1}(\Delta) = \mathbb{R} \times \{0\}.$$

Exercice 1.3 Étant donné $f : X \to Y$, montrer que l'on a toujours :

$A \subset B \Rightarrow f(A) \subset f(B)$	$C \subset D \Rightarrow f^{-1}(C) \subset f^{-1}(D)$
$f(A \cap B) \subset f(A) \cap f(B)$	$f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$
$f(A \cup B) = f(A) \cup f(B)$	$f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$
$A \subset f^{-1}(f(A))$	$f(f^{-1}(C)) \subset C$

et donner des contre exemples lorsque l'égalité ou l'équivalence n'est pas satisfaite.

Exercice 1.4 Montrer que si $f : X \to Y$ et $g : Y \to Z$, on a toujours :

$(g \circ f)(A) = g(f(A))$	$(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$

Exercice 1.5
1. Montrer que l'on a toujours

$$(|Y_1| \times |Y_2|)^{|X|} = |Y_1|^{|X|} \times |Y_2|^{|X|} \quad \text{et} \quad |Y|^{|X_1| \times |X_2|} = (|Y|^{|X_1|})^{|X_2|}.$$

2. Montrer que $|Y|^{|X_1|+|X_2|} = |Y|^{|X_1|} \times |Y|^{|X_2|}$.
3. Montrer que $|Y|^0 = 1$, $|Y|^1 = |Y|$ et $|Y|^{n+1} = |Y|^n \times |Y|$.

Exercice 1.6 Soient $X := \{a, b\}$ et $G := \mathscr{F}(X)$ l'ensemble des application de X dans lui même. On désigne par 1 l'identité de X, s la permutation des deux éléments de X et p, q les deux autres éléments de G. Établir un tableau représentant la loi de composition sur G et vérifier que G est bien un monoïde. Est-il commutatif ? Est-ce un groupe ? Sinon, expliciter $G^\times$.

Exercice 1.7 Soient G et H deux monoïdes. Montrer que si H est commutatif, alors $\mathrm{Hom}(G, H)$ est un sous-monoïde de $\mathscr{F}(G, H)$, mais que c'est faux par exemple si G est le groupe additif du corps $\mathbb{F}_2$ à 2 éléments et H est le groupe des permutations $\mathscr{S}_3$ de l'ensemble $\{1, 2, 3\}$.

Exercice 1.8 Soient G et H deux monoïdes et $f : G \to H$ une application satisfaisant $f(gh) = f(g)f(h)$. Montrer que si H est un groupe, alors f est un morphisme, mais que c'est faux par exemple pour l'application nulle du monoïde *multiplicatif* $\mathbb{N}$ dans lui même.

Exercice 1.9 Montrer que si M est un groupe abélien (noté additivement), alors l'ensemble $\mathrm{End}(M)$ des endomorphismes de M est un anneau pour $+$ et $\circ$. Montrer qu'il n'est pas commutatif si, par exemple, $M = \mathbb{Z}^2$.

Exercice 1.10 Soient $(G_s)_{s \in S}$ une famille de monoïdes et $G := \prod_{s \in S} G_s$ (muni de sa loi de monoïde). Montrer que si H est un monoïde quelconque, alors une application $f : H \to G$ est un morphisme si et seulement si ses composantes f_s le sont. En déduire que toutes les projections $p_s : G \to G_s$ sont des morphismes.

Exercice 1.11 Montrer qu'un groupe est toujours un *monoïde intègre*. Montrer qu'il existe des monoïdes qui ne sont pas intègres. Montrer que si A est un *anneau intègre*, alors $A \setminus \{0\}$ est un monoïde intègre.

Exercice 1.12

1. Montrer que si G est un monoïde et $g \in G$, il existe un unique morphisme $\varphi : \mathbb{N} \to G$ (ou $\mathbb{N}$ est muni de l'addition) tel que $\varphi(1) = g$ (on a en fait $\varphi(n) = g^n$).
2. Montrer que si G est un groupe et $g \in G$, il existe un unique morphisme $\varphi : \mathbb{Z} \to G$ tel que $\varphi(1) = g$ (on étend alors la notation précédente).
3. En déduire que si A est un anneau, alors il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z} \to A$ (attention, on regarde un groupe *additif* maintenant).
4. En déduire qu'un groupe abélien possède une unique structure de $\mathbb{Z}$-module.

Exercice 1.13

1. Soient $\varphi : A' \to A$ un morphisme d'anneaux et M un A-module. Montrer que la loi $a'x := \varphi(a')x$ fait de M un A'-module.
2. En déduire que si A' est un sous-anneau de A, alors tout A-module M est automatiquement un A'-module (restriction à A').

Exercice 1.14 Montrer que si A est un anneau et M est un A-module, on a

$$\forall x \in M, \quad 0_A x = 0_M \quad \text{et} \quad \forall a \in A, \quad a0_M = 0_M.$$

Exercice 1.15 Montrer que si A est un anneau et $a \in A$, alors $(a) := Aa := \{ca, \quad c \in A\}$ est un idéal de A (dit *principal*).

Exercice 1.16 Montrer qu'un anneau commutatif est un corps si et seulement si il a exactement deux idéaux : $\{0\}$ et lui même.

Exercice 1.17

1. Utiliser la division euclidienne pour montrer que tous les idéaux de $\mathbb{Z}$ sont de la forme (n) pour un unique $n \in \mathbb{N}$.
2. Utiliser la division euclidienne pour montrer que, si K est un corps, les idéaux de $K[T]$ sont de la forme (P) pour un unique P unitaire.

Exercice 1.18 Vérifier que si E est un espace vectoriel sur un corps K, alors $\mathrm{L}(E)$ est une K-algèbre pour $(+, \circ, \cdot)$ (on fera simplement la liste des propriétés).

Exercice 1.19 Montrer que si K est un corps et $a \in K$, il existe un unique morphisme d'algèbres φ_a de $K[T]$ dans lui même qui envoie T sur $T - a$. Expliciter $\varphi_1(1)$, $\varphi_1(T)$, $\varphi_1(T^2)$.

Exercice 1.20 Soit K un corps.

1. Montrer que si E est un $K[T]$-module, alors l'application $u : E \to E, x \mapsto Tx$ est linéaire et que $Px = P(u)(x)$ pour $P \in K[T]$ et $x \in E$.
2. Réciproquement, montrer que si E est un espace vectoriel sur K et $u \in \mathrm{L}(E)$, la loi $Px := P(u)(x)$ fait de E un $K[T]$-module.
3. Montrer qu'un sous-espace vectoriel F de E est un sous-module si et seulement si $u(F) \subset F$.

Exercice 1.21 Démontrer toutes les propositions du cours laissées en exercice.

Exercice 1.22 — TP. Soient $M := \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ et $I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Calculer

$$M^2 - (a+d)M + (ad-bc)I.$$

En déduire que si $ad-bc$ est inversible, alors M aussi, et exprimer dans ce cas M^{-1} en fonction de M et de ses coefficients. Calculer M^{-1}.

Exercice 1.23 — TP. On considère les matrices

$$\begin{bmatrix} 1 & a & a^2 & a^3 \\ 0 & 1 & a & a^2 \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1+a & 1 & 1 \\ 1 & 1 & 1+b & 1 \\ 1 & 1 & 1 & 1+c \end{bmatrix} \in \mathbb{Q}^4.$$

Calculer leurs inverses. Est-ce toujours possible ? Était-ce prévisible ?

Exercice 1.24 — TP. Effectuez l'algorithme du pivot de Gauss sur les matrices

$$\begin{bmatrix} 3 & 2 & -3 \\ 5 & -1 & -2 \\ 1 & 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & -1 \\ -1 & -4 & 5 \\ 11 & -5 & 2 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} -2 & -3 & 3 \\ -3 & 3 & 5 \\ -5 & -2 & 4 \end{bmatrix} \in \mathrm{M}_3(\mathbb{Q}),$$

en indiquant toutes les étapes. Même question avec

$$\begin{bmatrix} -1 & -1 & -4 & -2 \\ 4 & 5 & 18 & 11 \\ 3 & 6 & 17 & 7 \\ -5 & -3 & -14 & 11 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} -3 & 4 & -5 & 1 \\ 1 & -1 & 1 & -1 \\ -2 & 5 & 4 & -5 \\ 9 & 0 & 1 & -4 \end{bmatrix} \in \mathrm{M}_4(\mathbb{Q}).$$

Parmi toutes ces matrices, lesquelles sont inversibles ?

2. Algèbre linéaire

On fixe un corps de base K, appelé par la suite le corps des *scalaires* (penser à $K = \mathbb{R}$). Tous les espaces vectoriels sont des K-espaces vectoriels et toutes les applications linéaires sont K-linéaires.

Remarque Tous les résultats qui suivent sont en fait valides pour des modules sur un anneau quelconque. En d'autres termes, on peut remplacer le corps K par n'importe quel anneau A et les K-espaces vectoriels $E, F, \ldots$ par des A-modules $M, N, \ldots$ En prenant $A = \mathbb{Z}$, on voit que l'on peut aussi remplacer partout « espace vectoriel » par « groupe abélien » et « application linéaire » par « morphisme de groupes ».

2.1 Espace vectoriel

On commence par rappeler les notions de base introduites plus généralement pour les modules dans la section 1.4.

Définition 2.1.1 Un espace vectoriel est un groupe abélien E muni d'un endomorphisme d'anneaux

$$\begin{aligned} K &\longrightarrow \mathrm{End}_{\mathrm{Ab}}(E) \\ a &\longmapsto (x \mapsto ax). \end{aligned}$$

Cela veut donc dire que E est muni d'une loi interne et d'une loi externe satisfaisant les propriétés suivantes

1. $\forall x, y, z \in E, \quad (x + y) + z = x + (y + z)$,
2. $\exists 0_E \in E, \forall x \in E, \quad 0_E + x = x$,
3. $\forall x \in E, \exists -x \in E, \quad x + (-x) = 0_E$,
4. $\forall x, y \in E, \quad x + y = y + x$,
5. $\forall a, b \in K, \forall x \in E, \quad (ab)x = a(bx)$,
6. $\forall x \in E, \quad 1_K x = x$,
7. $\forall a \in K, \forall x, y \in E, \quad a(x + y) = ax + ay$,
8. $\forall a, b \in K, \forall x \in E, \quad (a + b)x = ax + bx$.

Définition 2.1.2 Une *application linéaire* $u : E \to F$ entre deux espace vectoriels est un morphisme de groupes abéliens qui est *compatible* avec la multiplication par les éléments de K.

Cela veut donc dire que l'on a

1. $\forall x, y \in E, \quad u(x+y) = u(x) + u(y)$,
2. $\forall a \in K, \forall x \in E, \quad u(ax) = au(x)$.

On parlera d'*endomorphisme* ou d'*opérateur linéaire* si $E = F$, d'*isomorphisme* si u est bijectif et d'*automorphisme* si u est à la fois un endomorphisme et un isomorphisme. On notera $\mathrm{L}(E,F)$ l'ensemble de toutes les applications linéaires de E vers F, $\mathrm{L}(E) := \mathrm{L}(E,E)$ et $\mathrm{GL}(E) = \mathrm{L}(E) \cap \mathscr{S}(E)$. S'il existe un isomorphisme entre deux K-espace vectoriels E et F, on écrira encore $E \simeq F$.

Proposition 2.1.3
1. Si $u : E \to F$ et $v : F \to G$ sont deux applications linéaires, alors $v \circ u$ aussi.
2. Si $u : E \to F$ est un isomorphisme d'espace vectoriels, alors u^{-1} aussi.

Démonstration. Exercice. ■

Définition 2.1.4 Un *sous-espace vectoriel* F d'un espace vectoriel E est un espace vectoriel F qui est contenu dans E et tel que l'inclusion $F \hookrightarrow E$ soit linéaire.

En d'autres termes, on veut que F soit une partie de E telle que

1. $0 \in F$
2. $\forall x, y \in F, \quad x + y \in F$,
3. $\forall a \in K, \forall x \in F, \quad ax \in F$.

2.2 Image, noyau

Nous allons maintenant étudier les notions d'image et de noyau dans le cadre de l'algèbre linéaire.

Proposition 2.2.1 Soit $u : E \to F$ une application linéaire.
1. Si E' est un sous-espace vectoriel de E, alors $u(E')$ est un sous-espace vectoriel de F.
2. Si F' est un sous-espace vectoriel de F, alors $u^{-1}(F')$ est un sous-espace vectoriel de E.

Démonstration. Exercice. ■

On rappelle maintenant la définition 1.2.6 :

Définition 2.2.2 Soit $u : E \to F$ une application linéaire.
1. L'*image* de u est $\mathrm{im}\, u := u(E) \subset F$.
2. Le *noyau* de u est $\ker u := u^{-1}(\{0_F\}) \subset E$.

Corollaire 2.2.3 Soit $u : E \to F$ une application linéaire. Alors,
1. $\mathrm{im}\, u$ est un sous-espace vectoriel de F.
2. $\ker u$ est un sous-espace vectoriel de E.

Démonstration. ■

Proposition 2.2.4 Soit $u : E \to F$ une application linéaire. Alors,
1. u surjective $\Leftrightarrow \mathrm{im}\, u = F$
2. u injective $\Leftrightarrow \ker u = \{0_E\}$

Démonstration. 1. Exercice.

2. Comme $u(0)=0$, on sait déjà que $\{0\}\subset \ker u$. Si $x\in\ker u$, alors $u(x)=0=u(0)$. Donc, si u est injective, on a $x=0$. Réciproquement, si $u(x)=u(y)$ alors $u(x-y)=u(x)-u(y)=0$ si bien que $x-y\in\ker u$. Donc, si on suppose que $\ker u=\{0\}$, on voit que $x-y=0$ si bien que $x=y$. ■

Remarque L'analogue de ce résultat est faux pour les monoïdes en général mais il est toujours valide pour les groupes ou les anneaux par exemple (et bien sûr aussi pour les A-modules). La première assertion est même valide pour n'importe quelle application entre deux ensembles.

Rappelons qu'on utilise la notation de Minkowski : si E est un espace vectoriel et $A,B\subset E$, alors

$$A+B=\{x+y,\quad x\in A \text{ et } y\in B\}.$$

Lemme 2.2.5 Soit $u:E\to F$ une application linéaire.

1. Si E' est un sous-espace vectoriel de E, alors $u^{-1}(u(E'))=E'+\ker u$.
2. Si F' est un sous-espace vectoriel de F, alors $u(u^{-1}(F'))=F'\cap\operatorname{im} u$.

Démonstration. 1. On dispose de la suite d'équivalences

$$\begin{aligned}
x\in u^{-1}(u(E')) &\Leftrightarrow u(x)\in u(E')\\
&\Leftrightarrow \exists y\in E',\quad u(x)=u(y)\\
&\Leftrightarrow \exists y\in E',\quad u(x-y)=0\\
&\Leftrightarrow \exists y\in E',\quad x-y\in\ker u\\
&\Leftrightarrow \exists y\in E', z\in\ker u,\quad x-y=z\\
&\Leftrightarrow \exists y\in E', z\in\ker u,\quad x=y+z\\
&\Leftrightarrow x\in E'+\ker u.
\end{aligned}$$

2. De même, on dispose de la suite d'équivalences

$$\begin{aligned}
y\in u(u^{-1}(F')) &\Leftrightarrow \exists x\in u^{-1}(F'),\quad y=u(x)\\
&\Leftrightarrow \exists x\in E,\quad u(x)\in F' \text{ et } y=u(x)\\
&\Leftrightarrow y\in F' \text{ et } \exists x\in E,\quad y=u(x)\\
&\Leftrightarrow y\in F'\cap\operatorname{im} u.
\end{aligned}$$

■

Proposition 2.2.6 Soit $u:E\to F$ une application linéaire. Alors, u et u^{-1} induisent des bijections réciproques

$$\begin{gathered}
\{\text{Sous espaces vectoriels de } E \text{ contenant } \ker u\}\\
u\downarrow\uparrow u^{-1}\\
\{\text{Sous espaces vectoriels de } F \text{ contenus dans } \operatorname{im} u\}
\end{gathered}$$

Démonstration. On montre d'abord que les flèches sont bien définies. On sait que si E' est un sous-espace vectoriel de E alors $u(E')$ est un sous-espace vectoriel de F, et comme $E'\subset E$, on aura $u(E')\subset u(E)=\operatorname{im} u$. De même, on sait que si F' est un sous-espace vectoriel de F alors $u^{-1}(F')$ est un sous-espace vectoriel de E, et comme $\{0_F\}\subset F'$, on aura $\ker u=u^{-1}(\{0_F\})\subset u^{-1}(F')$. Pour conclure, il suffit de montrer que si $\ker u\subset E'$, alors $u^{-1}(u(E'))=E'$ et si $F'\subset\operatorname{im} u$, alors $u(u^{-1}(F'))=F'$. Cela résulte du lemme 2.2.5 : en effet, si $\ker u\subset E'$, on a $E'+\ker u=E'$ et si $F'\subset\operatorname{im} u$, on a $F'\cap\operatorname{im} u=F'$. ■

2.3 Produit

Proposition 2.3.1 Soient $(E_s)_{s\in S}$ une famille d'espaces vectoriels et

$$E := \prod_{s\in S} E_s := \{(x_s)_{s\in S}, \quad x_s \in E_s\}.$$

Il existe alors une unique structure d'espace vectoriel sur E telle que toutes les projections $p_s : E \to E_s$ soient linéaires.

On rappelle que si $x = (x_s)_{s\in S}$, alors $p_s(x) = x_s$.

Démonstration. L'unicité est immédiate car la condition signifie que l'on a

$$(x_s)_{s\in S} + (y_s)_{s\in S} = (x_s + y_s)_{s\in S} \quad \text{et} \quad a(x_s)_{s\in S} = (ax_s)_{s\in S}.$$

On vérifie que cela définit bien une structure d'espace vectoriel (exercice). ■

Remarque
1. Si $E_1,\dots,E_n$ sont des espaces vectoriels, alors $E_1 \times \cdots \times E_n$ sera donc muni de l'addition et de la multiplication terme à terme :

$$(x_1,\dots,x_n) + (y_1,\dots,y_n) := (x_1 + y_1,\dots,x_n + y_n)$$

et

$$a(x_1,\dots,x_n) := (ax_1,\dots,ax_n).$$

2. Si E est un espace vectoriel et S un ensemble quelconque, alors

$$E^S := \{(x_s)_{s\in S}, \quad x_s \in E\}$$

est naturellement un espace vectoriel.
3. En faisant l'intersection des deux cas précédents, on trouve

$$E^n := E^{\{1,\dots,n\}} = \underbrace{E \times \cdots \times E}_{n \text{ fois}}.$$

Exemple
1. $K^0 = \{0\}, K^1 = K, K^2 = K \times K, \dots, K^n = K \times \cdots \times K, \dots$
2. Dans K^n, si on pose $\mathbb{1}_i := (0,\dots,1,\dots,0)$ avec 1 à la i-ème place, on a (vérifier)

$$(x_1,\dots,x_n) = x_1\mathbb{1}_1 + \cdots + x_n\mathbb{1}_n.$$

3. $K^{\mathbb{N}} := \{(x_i)_{i\in\mathbb{N}}, \quad x_i \in K\}$ est l'espace des suites d'éléments de K.
4. Si K est un corps valué comme $\mathbb{R}$ ou $\mathbb{C}$, alors les suites bornées forment un sous-espace vectoriel $\ell_\infty(K) \subset K^{\mathbb{N}}$ (plus précisément, la condition est

$$(x_i)_{i\in\mathbf{N}} \in \ell_\infty(K) \Leftrightarrow \exists M \in \mathbb{R}_{\geq 0}, \forall i \in \mathbb{N}, |x_i| \leq M).$$

Proposition 2.3.2 Soient $(E_s)_{s\in S}$ une famille d'espaces vectoriels et $E := \prod_{s\in S} E_s$. Si F est un espace vectoriel, alors une application $u : F \to E$ est linéaire si et seulement si ses composantes u_s le sont.

On rappelle que les composantes de u sont les applications composées $u_s := p_s \circ u$.

Démonstration. Il suffit d'écrire les conditions (exercice). ■

Remarque Comme conséquence de la proposition, on voit que si on se donne une famille d'applications linéaires $u_s : E_s \to F_s$, alors l'application produit

$$\prod_{s\in S} u_s : \prod_{s\in S} E_s \to \prod_{s\in S} F_s, \quad (x_s)_{s\in S} \mapsto (u_s(x_s))_{s\in S}$$

est aussi linéaire. Dans le cas d'un nombre fini, on écrit

$$u_1 \times \cdots \times u_n : E_1 \times \cdots \times E_n \to F_1 \times \cdots \times F_n, \quad (x_1, \ldots, x_n) \mapsto (u_1(x_1), \ldots, u_n(x_n)).$$

Proposition 2.3.3 Si E est un espace vectoriel et X un ensemble quelconque, alors il existe une unique structure d'espace vectoriel sur l'ensemble $\mathscr{F}(X,E)$ de toutes les applications de X vers E, telle que toutes les applications d'évaluation $f \mapsto f(x)$ soient linéaires.

Démonstration. On peut identifier $\mathscr{F}(X,E)$ avec E^X en faisant correspondre $f : X \to E$ et $(y_x)_{x\in X}$ lorsque $f(x) = y_x$. Les applications d'évaluations correspondent alors aux projections. ■

Remarque 1. Si E est un espace vectoriel et X un ensemble, alors $\mathscr{F}(X,E)$ est muni de

$$(f+g)(x) := f(x) + g(x) \quad \text{et} \quad (af)(x) := af(x).$$

2. Il suit que si $h : Y \to X$ est n'importe quelle application, on aura

$$(f+g)\circ h = f\circ h + g\circ h \quad \text{et} \quad (af)\circ h = a(f\circ h)$$

par *définition* (on ne demande pas que les applications soient linéaires) : tout se passe bien par composition à droite.

Exemple Si E est un espace vectoriel normé (voir plus loin) et X est un espace topologique, alors les applications continues $f : X \to E$ forment un sous-espace vectoriel $\mathscr{C}(X,E) \subset \mathscr{F}(X,E)$.

Proposition 2.3.4 Si E et F sont des espace vectoriels, alors l'ensemble $\mathrm{L}(E,F)$ des applications linéaires de E vers F est un sous-espace vectoriel de $\mathscr{F}(E,F)$.

Démonstration. On montre tout d'abord que si $f, g : E \to F$ sont linéaires, alors $f+g$ aussi. En effet, si $x, y \in E$, on a par définition de la somme de deux applications et linéarité de f et g,

$$(f+g)(x+y) = f(x+y) + g(x+y) = f(x) + f(y) + g(x) + g(y)$$

et, toujours par définition de la somme de deux applications,

$$(f+g)(x) + (f+g)(y) = f(x) + g(x) + f(y) + g(y).$$

On vérifie de même que si $x \in E$ et $a \in K$, alors $(f+g)(ax) = a(f+g)(x)$ (exercice). On montre ensuite que si $f : E \to F$ est linéaire et $a \in K$, alors af est linéaire (exercice). ■

Remarque L'application d'évaluation en 1 est un isomorphisme

$$\begin{aligned} \mathrm{L}(K,E) &\xrightarrow{\simeq} E \\ u &\longmapsto u(1). \end{aligned}$$

La réciproque envoie $x \in E$ sur l'application $i_x : a \mapsto ax$. On *identifiera* souvent ces deux espaces. En particulier, on a $\mathrm{L}(K) \simeq K$ (un endomorphisme de K est la multiplication par une constante).

Proposition 2.3.5 On a un isomorphisme d'espace vectoriels

$$\begin{array}{ccc} \mathrm{L}(K^m, K^n) & \xrightarrow{\simeq} & \mathrm{M}_{n\times m}(K) \\ u & \longleftrightarrow & A \end{array}$$

donné par

$$A = [a_{i,j}] \Leftrightarrow u(x_1, \dots, x_m) = (a_{1,1}x_1 + \cdots + a_{1,m}x_m, \dots, a_{n,1}x_1 + \cdots + a_{n,m}x_m).$$

On écrira $A = \mathrm{Mat}(u)$, ou $A = [u]$ pour faire plus court.

Démonstration. Exercice. ■

Remarque 1. On utilisera aussi la suite d'isomorphismes $K^n \simeq \mathrm{L}(K, K^n) \simeq \mathrm{M}_{n\times 1}(K)$ pour voir les vecteurs de K^n comme des *vecteurs colonnes* et on écrira :

$$[x] := [i_x] := \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

si $x = (x_1, \dots, x_n)$. En particulier, on identifiera K et $\mathrm{M}_1(K)$ (scalaires et matrices à un seul coefficient).

2. Donnons nous deux matrices $A' \in \mathrm{M}_{n'\times m'}(K)$ et $A'' \in \mathrm{M}_{n''\times m''}(K)$ correspondant à des applications linéaires $u' : K^{m'} \to K^{n'}$ et $u'' : K^{m''} \to K^{n''}$ respectivement. Alors, si on pose $m = m' + m''$ et $n = n' + n''$, la matrice de $u = u' \times u'' : K^m \to K^n$ est *diagonale par blocs* :

$$A = \begin{bmatrix} A' & 0 \\ 0 & A'' \end{bmatrix}.$$

On dispose d'une loi de composition

$$\begin{array}{ccc} \mathrm{M}_{n\times m}(K) \times \mathrm{M}_{m\times l}(K) & \longrightarrow & \mathrm{M}_{n\times l}(K) \\ (A, B) & \longmapsto & AB \end{array}$$

via la formule

$$[a_{i,j}][b_{j,k}] = \left[\sum_{j=1}^{m} a_{i,j}b_{j,k}\right].$$

Proposition 2.3.6 Si on se donne deux applications linéaires

$$K^l \xrightarrow{v} K^m \xrightarrow{u} K^n,$$

alors on a $[u \circ v] = [u][v]$.

Démonstration. Exercice. ■

Remarque 1. L'*image* (resp. le *noyau*) d'une matrice $A \in \mathrm{M}_{n\times m}(K)$ est l'image (resp. le noyau) de l'application $u \in L(K^m, K^n)$ correspondant. Plus généralement, nous appliquerons systématiquement aux matrices le vocabulaire des applications linéaires.

2. Pour calculer le noyau et l'image d'une matrice A, on peut utiliser la méthode suivante : on effectue une suite d'opérations élémentaires sur les *colonnes*
$$\begin{bmatrix} A \\ I \end{bmatrix} \longrightarrow \begin{bmatrix} C_1 & \cdots & C_r & 0 & \cdots & 0 \\ \star & \cdots & \star & D_1 & \cdots & D_t \end{bmatrix}.$$
Alors, $\{C_1,\ldots,C_r\}$ sera une *base* de $\operatorname{im}A$ et $\{D_1,\ldots,D_t\}$ sera une *base* de $\ker A$ (voir plus loin pour les bases).
3. On peut justifier la méthode ci-dessus comme suit : faire une suite d'opérations sur les colonnes revient à multiplier à droite par une matrice inversible P (celle obtenue en faisant les mêmes opérations sur I). On aura donc
$$\begin{bmatrix} A \\ I \end{bmatrix} P = \begin{bmatrix} C_1 & \cdots & C_r & 0 & \cdots & 0 \\ \star & \cdots & \star & D_1 & \cdots & D_t \end{bmatrix},$$
c'est à dire
$$AP = [C_1 \cdots C_r\, 0 \cdots 0] \quad \text{et} \quad P\ (= IP) = [\star \cdots \star\ D_1 \cdots D_t]$$
si bien que
$$A[\star \cdots \star\ D_1 \cdots D_t] = [C_1 \cdots C_r\, 0 \cdots 0].$$
Autrement dit, on aura $A\star = C_1, \ldots, A\star = C_r$ (image) et $AD_1 = \cdots = AD_t = 0$ (noyau). C'est le *théorème du rang* (voir plus loin) qui nous permet de conclure qu'il s'agit bien d'une base dans chaque cas.

Exemple Pour
$$A := \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 6 \\ 3 & 8 & 15 & 16 \end{bmatrix},$$
on fait
$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 6 \\ 3 & 8 & 15 & 16 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 3 & 2 \\ 3 & 2 & 6 & 4 \\ 1 & -2 & -3 & -4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 1 & -2 & 3 & 0 \\ 0 & 1 & -3 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$
si bien que $\{(1,1,3),(0,1,2)\}$ est une base de $\operatorname{im}A$ et $\{(3,-3,1,0),(0,-2,0,1)\}$ est une base de $\ker A$.

2.4 Dual (début)

Définition 2.4.1 Une *forme linéaire* sur un espace vectoriel E est une application linéaire $\varphi : E \to K$. L'*espace dual* de E est l'espace vectoriel ${}^tE := \mathrm{L}(E,K)$ de toutes les formes linéaires sur E. Un *hyperplan* de E est un sous-espace qui est le noyau d'une forme linéaire non nulle φ.

Dans la littérature, on voit souvent la notation E^* pour le dual.

Exemple 1. Comme corollaire de la proposition 2.3.5, on dispose d'un isomorphisme

$$ {}^tK^n \simeq \mathrm{M}_{1\times n}(K), \quad \varphi \mapsto [\varphi] $$

donné par

$$ \varphi(x_1,\ldots,x_n) = a_1x_1+\cdots+a_nx_n \Leftrightarrow [\varphi] = [a_1\cdots a_n] $$

Une forme linéaire sur K^n sera donc vue comme un *vecteur ligne*.

2. Les projections $p_i : K^n \to K$ sont des formes linéaires et toute forme linéaire sur K^n s'écrit de manière unique

$$ \varphi = a_1p_1+\cdots+a_np_n \quad \text{avec } a_1,\ldots,a_n \in K. $$

Plus précisément, on a

$$ \varphi = \varphi(\mathbb{1}_1)p_1+\cdots+\varphi(\mathbb{1}_n)p_n. $$

3. On dispose du *diagramme commutatif* suivant :

$$ \begin{tikzcd} {}^tK^n \times K^n \arrow[r] \arrow[d, "\simeq"] & K \arrow[d, "\simeq"] \\ \mathrm{M}_{1\times n}(K)\times \mathrm{M}_{n\times 1}(K) \arrow[r, "\times"] & \mathrm{M}_1(K) \end{tikzcd} $$

avec $(\varphi,x)\mapsto\varphi(x)$ en haut et

$$ \left([a_1\cdots a_n], \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}\right) \mapsto [a_1x_1+\cdots a_nx_n] $$

en bas. En d'autres termes, on a $[\varphi(x)] = [\varphi][x]$.

4. Un hyperplan de K^n est une partie de la forme

$$ H := \{(x_1,\ldots,x_n)\in K^n \ / \ a_1x_1+\cdots+a_nx_n = 0\} $$

avec $a_1,\ldots,a_n\in K$ non tous nuls.

5. On dispose d'un isomorphisme d'espaces vectoriels

$$ \begin{array}{ccc} K^n & \xrightarrow{\simeq} & {}^tK^n \\ (a_1,\ldots,a_n) & \longmapsto & a_1p_1+\cdots+a_np_n \\ (\varphi(\mathbb{1}_i),\ldots,\varphi(\mathbb{1}_n)) & \longleftarrow\!\shortmid & \varphi \end{array} $$

que l'on utilisera parfois (mais prudemment) pour identifier ${}^tK^n$ avec K^n.

Remarque 1. Bien que ${}^tK^n$ soit isomorphe à K^n, il est faux en général que ${}^tE$ soit isomorphe à E. En fait, le *théorème d'Erdos-Kaplansky* nous dit que si E est de dimension infinie, alors $\dim{}^tE > \dim E$ (voir plus loin pour la notion de dimension).

2. Sur un anneau quelconque, il faut renforcer l'hypothèse *non nulle* en *surjective* dans la définition d'un hyperplan (sur un corps, les deux conditions sont équivalentes).

Proposition 2.4.2 Soit E un espace vectoriel.

1. Si $x\in E$, l'application d'évaluation

$$ p_x : {}^tE \to K, \quad \varphi\mapsto\varphi(x) $$

est une forme linéaire sur ${}^tE$.

2. L'application (dite canonique)

$$E \to {}^{tt}E, \quad x \mapsto p_x$$

est linéaire.

Démonstration. 1. Résulte facilement du corollaire 2.3.3 (exercice).
2. Résulte immédiatement de la linéarité de φ (exercice). ■

Définition 2.4.3 Soit $u : E \to F$ une application linéaire. Alors, l'*application duale* de u est l'application

$$\begin{array}{rrcl} {}^t u : & {}^t F & \longrightarrow & {}^t E \\ & \psi & \longmapsto & \psi \circ u. \end{array}$$

En d'autres termes, on a donc ${}^t u(\psi) := \psi \circ u$.

Proposition 2.4.4 1. Si $u : E \to F$ est une application linéaire, alors ${}^t u : {}^t F \to {}^t E$ aussi.
2. Si E et F sont deux espaces vectoriels alors l'application

$$\begin{array}{rcl} \mathrm{L}(E,F) & \longrightarrow & \mathrm{L}({}^t F, {}^t E) \\ u & \longmapsto & {}^t u \end{array} \tag{2.1}$$

est linéaire.
3. Si $u : E \to F$ et $v : F \to G$ sont deux applications linéaires, alors ${}^t(v \circ u) = {}^t u \circ {}^t v$.

Démonstration. 1. Si $\psi_1, \psi_2 \in {}^t F$, on a par définition de la somme de deux applications

$${}^t u(\psi_1 + \psi_2) = (\psi_1 + \psi_2) \circ u = \psi_1 \circ u + \psi_2 \circ u = {}^t u(\psi_1) + {}^t u(\psi_2),$$

et de même, si $a \in K$ et $\psi \in {}^t F$, alors ${}^t u(a\psi) = a^t u(\psi)$.
2. Si $u_1, u_2 : E \to F$ sont deux applications linéaires et $\psi \in {}^t F$, on a

$${}^t(u_1 + u_2)(\psi) = \psi \circ (u_1 + u_2) = \psi \circ u_1 + \psi \circ u_2 = {}^t u_1(\psi) + {}^t u_2(\psi) = ({}^t u_1 + {}^t u_2)(\psi)$$

car ψ est linéaire et il suit que ${}^t(u_1 + u_2) = {}^t u_1 + {}^t u_2$. On montre de même que si $u : E \to F$ est linéaire et $a \in K$, alors ${}^t(au) = a^t u$.
3. Si $\psi \in {}^t F$, on a

$${}^t(v \circ u)(\psi) = \psi \circ v \circ u = ({}^t u({}^t v(\psi)) = ({}^t u \circ {}^t v)(\psi). \quad ■$$

Exemple Si on identifie ${}^t K^n$ avec K^n et ${}^t K^m$ avec K^m, alors l'application (2.1) correspond à la transposition des matrices

$$\begin{array}{rcl} \mathrm{M}_{n\times m}(K) & \longrightarrow & \mathrm{M}_{m\times n}(K) \\ A & \longmapsto & {}^t A. \end{array}$$

Autrement dit, la matrice du dual de u sera la transposée de la matrice de u (on reparlera de ça plus tard).

2.5 Orthogonal

Définition 2.5.1 Soit E un espace vectoriel. La partie *orthogonale* à $U \subset {}^tE$ est

$$U^\circ = \{x \in E \ / \ \forall \varphi \in U, \quad \varphi(x) = 0\} \subset E.$$

Dans la littérature, on voit souvent la notation $U^\perp$ que nous préférons éviter pour l'instant afin de prévenir les risques d'ambiguïté.

Exemple
1. Une partie H de E est un hyperplan si et seulement si $H = \{\varphi\}^\circ$ avec φ non nulle.
2. En général, $U^\circ = \cap_{\varphi \in U} \ker \varphi$ est toujours une intersection d'hyperplans.
3. Considérons un système linéaire homogène à m équations et n inconnues :

$$\mathscr{S} := \left\{ \begin{array}{rcl} a_{1,1}x_1 \cdots + a_{1,m}x_m & = & 0 \\ & \vdots & \\ a_{n,1}x_1 \cdots + a_{n,m}x_n & = & 0. \end{array} \right.$$

Posons alors $U = \{\varphi_1, \ldots, \varphi_n\}$ avec

$$\forall i = 1, \ldots, n, \quad \varphi_i(x_1, \ldots, x_m) = a_{i,1}x_1 \cdots + a_{i,m}x_m.$$

Alors U° est l'ensemble $\mathrm{Sol}(\mathscr{S})$ des solutions de $\mathscr{S}$.

Remarque
1. On peut aussi considérer la partie *orthogonale* à $X \subset E$ qui est par définition

$$^\circ X = \{\varphi \in {}^tE \ / \ \forall x \in X, \quad \varphi(x) = 0\} = \{\varphi \in {}^tE, \quad X \subset \ker \varphi\} \subset {}^tE$$

Les énoncés concernant l'opération $U \mapsto U^\circ$ ont souvent des analogues pour l'opération $X \mapsto {}^\circ X$. Mais ces derniers sont habituellement plus faciles à démontrer.
2. On dit aussi que $U \subset {}^tE$ et $X \subset E$ sont *orthogonaux*, et on écrira $U \circ X$ si nécessaire, si

$$\forall \varphi \in U, \forall x \in X, \quad \varphi(x) = 0.$$

Autrement dit, on a

$$U \circ X \Leftrightarrow U \subset {}^\circ X \Leftrightarrow X \subset U^\circ.$$

Exemple Si on identifie K^n et ${}^tK^n$ comme ci-dessus, on voit que $(x_1, \ldots, x_n)$ et $(y_1, \ldots, y_n)$ sont orthogonaux si et seulement si $x_1y_1 + \cdots + x_ny_n = 0$. On retrouve ainsi la notion classique de produit scalaire (on y reviendra plus tard).

Proposition 2.5.2 Soit E un espace vectoriel.
1. Si $U \subset {}^tE$, alors U° est un sous-espace vectoriel de E et $U \subset {}^\circ(U^\circ)$.
2. Si $U_1, U_2 \subset {}^tE$, alors
   (a) $U_1 \subset U_2 \Rightarrow U_2^\circ \subset U_1^\circ$ et
   (b) $(U_1 \cup U_2)^\circ = U_1^\circ \cap U_2^\circ$.

Démonstration.
1. Soient $x, y \in U^\circ$ et $a, b \in K$. Si $\varphi \in U$, on a par linéarité

$$\varphi(ax + by) = a\varphi(x) + b\varphi(y) = 0$$

et donc $ax + by \in U^\circ$. Comme $0 \in U^\circ$, cela montre que U° est un sous-espace vectoriel. De plus si $x \in U$ et $\varphi \in U^\circ$, alors $\varphi(x) = 0$ par définition, et cela prouve que $U \subset {}^\circ(U^\circ)$.
2. (a) Donnons nous $x \in U_2^\circ$. Soit $\varphi \in U_1$. Si on suppose que $U_1 \subset U_2$, on a aussi $\varphi \in U_2$ et donc $\varphi(x) = 0$. Cela montre que $x \in U_1^\circ$.

(b) En appliquant ce dernier résultats aux inclusions $U_1, U_2 \subset U_1 \cup U_2$, on obtient immédiatement l'inclusion $(U_1 \cup U_2)^\circ \subset U_1^\circ \cap U_2^\circ$. Inversement, donnons nous $x \in U_1^\circ \cap U_2^\circ$. Si $\varphi \in U_1 \cup U_2$, on a soit $\varphi \in U_1$ et alors nécessairement, $\varphi(x) = 0$ car $x \in U_1^\circ$, ou alors $\varphi \in U_2$ et on obtient la même conclusion. On voit donc que $x \in (U_1 \cup U_2)^\circ$ comme annoncé. ■

Remarque On démontre de la même manière que

1. Si $X \subset E$, alors ${}^\circ X$ est un sous-espace vectoriel de ${}^tE$ et $X \subset ({}^\circ X)^\circ$.
2. Si $X_1, X_2 \subset E$, alors
   (a) $X_1 \subset X_2 \Rightarrow {}^\circ X_2 \subset {}^\circ X_1$ et
   (b) ${}^\circ(X_1 \cup X_2) = {}^\circ X_1 \cap {}^\circ X_2$.

En fait, pour cette variante de l'orthogonalité, on peut démontrer quelques propriétés de plus comme nous l'allons voir maintenant.

Proposition 2.5.3 Si E est un espace vectoriel, on a ${}^\circ E = \{0_{{}^tE}\}$ et ${}^\circ\{0_E\} = {}^tE$.

Démonstration. Pour la première assertion, on voit que

$$\varphi \in {}^\circ E \Leftrightarrow \forall x \in E, \varphi(x) = 0 \Leftrightarrow \varphi = 0.$$

En ce qui concerne la seconde, il suffit de rappeler que si $\varphi \in {}^tE$, alors φ est linéaire si bien que $\varphi(0) = 0$. On a donc $\varphi \in {}^\circ\{0\}$. ■

Proposition 2.5.4 Si $u : E \to F$ est une application linéaire, on a

$${}^\circ\mathrm{im}\, u = \ker {}^tu.$$

Démonstration. Nous avons tout simplement la suite d'équivalences

$$\begin{aligned}
\psi \in {}^\circ\mathrm{im}\, u &\Leftrightarrow \forall y \in \mathrm{im}\, u, \quad \psi(y) = 0\\
&\Leftrightarrow \forall x \in E, \quad \psi(u(x)) = 0\\
&\Leftrightarrow \psi \circ u = 0\\
&\Leftrightarrow {}^tu(\psi) = 0\\
&\Leftrightarrow \psi \in \ker {}^tu.
\end{aligned}$$

■

Corollaire 2.5.5 Si $u : E \to F$ est une application linéaire surjective, alors ${}^tu$ est injective.

Démonstration. En effet, si $\mathrm{im}\, u = F$, alors $\ker {}^tu = {}^\circ F = \{0\}$ grâce à la proposition 2.5.3. ■

Corollaire 2.5.6 Si $\iota : F \hookrightarrow E$ est l'inclusion d'un sous-espace vectoriel, on a

$${}^\circ F = \ker {}^t\iota.$$

Démonstration. ■

2.6 Quotient

On rappelle qu'on utilise la notation de Minkowski si bien que, si F est un sous-espace vectoriel d'un espace vectoriel E, alors
$$x+F := \{x+y, \quad y \in F\}$$
désigne le *sous-espace affine* parallèle à F et passant par l'*extrémité* de x (faire un dessin), c'est à dire le translaté de F par x.

Lemme 2.6.1 Soient F un sous-espace vectoriel d'un espace vectoriel E et $x_1, x_2 \in E$. On a alors
$$x_1 + F = x_2 + F \Leftrightarrow x_2 - x_1 \in F.$$

Démonstration. Si $x_1 + F = x_2 + F$, alors il existe $y \in F$ tel que $x_1 + y = x_2 + 0$ et on a donc $x_2 - x_1 = y \in F$. Réciproquement, si on suppose que $y := x_2 - x_1 \in F$ et si $z \in F$, on a
$$x_2 + z = x_1 + (y+z) \in x_1 + F,$$
si bien que $x_2 + F \subset x_1 + F$ et l'autre inclusion s'obtient par symétrie. ■

Définition 2.6.2 Si F est un sous-espace vectoriel d'un espace vectoriel E, le *quotient* de E par F est l'ensemble
$$E/F := \{x+F, \quad x \in E\}$$
de tous les sous-espaces affines parallèles à F.

Remarque On définit plus généralement le *quotient* d'un ensemble par une *relation d'équivalence* (hors programme). Dans notre cas, la relation serait $x_1 \equiv x_2 \Leftrightarrow x_2 - x_1 \in F$.

Proposition 2.6.3 Si F est un sous-espace vectoriel d'un espace vectoriel E, alors il existe une unique structure d'espace vectoriel sur E/F telle que la *projection* (ou *application quotient*)
$$\begin{aligned} E &\xrightarrow{\pi} E/F \\ x &\longmapsto x+F. \end{aligned}$$
soit linéaire. Celle-ci est surjective et on a $\ker \pi = F$.

Démonstration. Par définition, on doit avoir
$$\forall x, y \in E, \quad (x+F) + (y+F) = (x+y) + F$$
et
$$\forall x \in E, \forall a \in K, \quad a(x+F) = ax + F$$
(attention : la seconde formule n'est pas tout à fait compatible avec la notation de Minkowski qui donnerait $ax + aF$). On vérifie immédiatement qu'on obtient ainsi un espace vectoriel, que π est linéaire et que $\ker \pi = F$ (exercice).

Il faut tout de même s'assurer que les lois sont bien définies. Montrons le pour la seconde, l'argument étant le même dans les deux cas (exercice). On suppose donc que $x_1 + F = x_2 + F$ et on doit montrer que $ax_1 + F = ax_2 + F$. Grâce au lemme 2.6.1, il suffit de remarquer que si $x_2 - x_1 \in F$, alors $ax_2 - ax_1 = a(x_2 - x_1) \in F$. ■

Remarque 1. Nous avons donc $0_{E/F}\ (= 0_E + F) = F$.

2. Cette proposition montre que tout sous-espace vectoriel est le noyau d'une application linéaire (on connaissait déjà la réciproque).
3. Notons que $E/E = \{E\} = \{0_{E/E}\}$ est l'espace nul et que $E/\{0_E\} = \{\{x\}, x \in E\} \simeq E$ peut facilement être identifié avec E.
4. Lorsque l'espace F est fixé, on écrira parfois $\overline{x} := x + F$. Dans ce cas, les lois sont donc données par $\overline{x} + \overline{y} = \overline{x+y}$ et $a\overline{x} = \overline{ax}$. Comme $F = \ker \pi$ et que $\pi(x) = \overline{x}$, aura
$$x \in F \Leftrightarrow \overline{x} = \overline{0}.$$
5. Si au lieu de travailler sur K, nous travaillons sur $\mathbb{Z}$, nous obtenons la notion de *quotient d'un groupe abélien par un sous-groupe*, par exemple $\mathbb{Z}/n\mathbb{Z}$.
6. Attention : on peut généraliser la notion de quotient au cas des groupes qui ne sont pas nécessairement commutatifs (on utilise alors la notation multiplicative) mais il faut alors faire attention aux classes à droites et aux classes à gauche. En particulier, le quotient ne sera lui même un groupe que si le sous-groupe est *distingué*.
7. Si I est un idéal (c'est à dire un sous-module) d'un anneau commutatif, alors il existe en fait une unique structure d'anneau sur A/I qui fait de la projection un morphisme d'anneaux. Par exemple, cela fait de $\mathbb{Z}/n\mathbb{Z}$ ou de $K[T]/(P)$ un anneau et pas seulement un groupe abélien.

Nous pouvons énoncer la propriété universelle du quotient :

Théoreme 2.6.4 Soient F un sous-espace vectoriel d'un espace vectoriel E et $\pi : E \to E/F$ la projection. Alors, pour une application linéaire $u : E \to E'$, les conditions suivantes sont équivalentes :
1. $F \subset \ker u$,
2. il existe une application $\overline{u} : E/F \to E'$ telle que $u = \overline{u} \circ \pi$.

Celle ci est alors unique et linéaire et on a $\ker \overline{u} = \ker u/F$:

$$\begin{tikzcd}
F \arrow[r, hook] & \ker u \arrow[r, hook] \arrow[d] & E \arrow[r, "u"] \arrow[d, "\pi"] & E' \\
& \ker u/F \arrow[r, hook] & E/F \arrow[ur, "\overline{u}"] &
\end{tikzcd}$$

Démonstration. L'unicité est immédiate et $\overline{u}$ sera donné par la formule $\overline{u}(\overline{x}) = u(x)$. La linéarité de $\overline{u}$ résulte alors de celle de u et on aura bien sûr $F \subset \ker u$ et $\ker \overline{u} = \ker u/F$ (exercice).

Il reste à s'assurer que l'application est bien définie lorsque $F \subset \ker u$. Or, si $\overline{x}_1 = \overline{x}_2$, le lemme 2.6.1 nous dit que $x_2 - x_1 \in F \subset \ker u$ et on aura donc $u(x_2 - x_1) = 0$ si bien que $u(x_1) = u(x_2)$. ∎

Corollaire 2.6.5 — Théorème de Noether. Si $u : E \to E'$ est une application linéaire, alors
$$E/\ker u \simeq \operatorname{im} u.$$

Démonstration. C'est le cas $F = \ker u$ du théorème. On aura donc $\ker \overline{u} = \{\overline{0}\}$ si bien que $\overline{u}$ est injective. D'autre part, on a $\operatorname{im} \overline{u} = \operatorname{im} u$ car la projection $E \to E/F$ est surjective. ∎

Exemple 1. Considérons K^m comme contenu dans K^n en identifiant
$$(x_1, \ldots, x_m) \leftrightarrow (x_1, \ldots, x_m, 0, \ldots, 0)$$
(penser au plan horizontal dans l'espace) et K^{n-m} comme contenu dans K^n en identifiant
$$(x_1, \ldots, x_{n-m}) \leftrightarrow (0, \ldots, 0, x_1, \ldots, x_{n-m})$$

(penser à la droite verticale). On a alors un isomorphisme

$$\begin{tikzcd} K^{n-m} \arrow[r, hook] \arrow[rr, bend left, "\simeq"] & K^n \arrow[r, two heads] & K^n/K^m \end{tikzcd}$$

(on associerait donc à un point de la droite verticale le plan horizontal passant par ce point). On remarquera l'analogie entre cet isomorphisme et la formule $e^{n-m} = e^n/e^m$.

2. Rappelons que si $P \in K[T]$, alors on désigne par (P) l'ensemble des multiples de P (c'est un idéal et donc un espace vectoriel). Si $\deg P = d$, on dispose d'un isomorphisme d'espaces vectoriels

$$\begin{tikzcd} K[T]_{<d} \arrow[r, hook] \arrow[rr, bend left, "\simeq"] & K[T] \arrow[r, two heads] & K[T]/(P) \\ R \arrow[rr, mapsto] & & R+(P), \end{tikzcd}$$

la réciproque étant donné par le reste dans la division euclidienne par P.

Remarque 1. Il suit qu'un sous-espace vectoriel H d'un espace vectoriel E est un hyperplan si et seulement si $E/H \simeq K$.

2. Comme nous l'avons déjà dit, on peut travailler avec des groupes abéliens par exemple, à la place des espaces vectoriels. Si on applique le théorème de Noether au morphisme de groupes abéliens $\mathbb{R} \to \mathbb{C}^\times, \theta \mapsto e^{i\theta}$, on obtient un isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \simeq S_1$ (le cercle) dont l'inverse est exactement l'application qui associe son argument à un nombre complexe de module 1.

Proposition 2.6.6 Si F est un sous-espace vectoriel de E, alors

$$^t(E/F) \simeq {}^\circ F.$$

Démonstration. Comme la projection $\pi : E \to E/F$ est une application linéaire surjective, il résulte du corollaire 2.5.5 que l'on dispose d'une application linéaire injective ${}^t\pi : {}^t(E/F) \hookrightarrow {}^tE$. Et on a

$$\begin{aligned} \psi \in \operatorname{im}{}^t\pi &\Leftrightarrow \exists \overline{\psi} \in {}^t(E/F), \quad \psi = {}^t\pi(\overline{\psi}) \\ &\Leftrightarrow \exists \overline{\psi} \in E/F \to K, \quad \psi = \overline{\psi} \circ \pi \\ &\Leftrightarrow F \subset \ker \psi \\ &\Leftrightarrow \psi \in {}^\circ F \end{aligned}$$

(en appliquant le théorème à ψ). ■

Proposition 2.6.7 Soient $u : E \to F$ une application linéaire et $E' \subset E$, $F' \subset F$ des sous-espaces tels que $u(E') \subset F'$. Il existe alors des applications linéaires (uniques) $u' : E' \to F'$ et $u'' : E/E' \to F/F'$ telles que $u'(x) = u(x)$ si $x \in E'$ et $u''(\bar{x}) = \overline{u(x)}$ si $x \in E$:

$$\begin{tikzcd} E' \arrow[r, hook] \arrow[d, "u'"] & E \arrow[r, two heads] \arrow[d, "u"] & E/E' \arrow[d, "u''"] \\ F' \arrow[r, hook] & F \arrow[r, two heads] & F/F'. \end{tikzcd}$$

Démonstration. L'unicité est claire dans les deux cas et l'existence de u' est immédiate. Pour obtenir u'', on applique le théorème à l'application composée

$$E \to F \to F/F', \quad x \mapsto \overline{u(x)}.$$

Il faut montrer que son noyau contient E' mais si $x \in E'$, on a $u(x) \in F'$ et donc $\overline{u(x)} = \overline{0}$. ■

Remarque On peut montrer les résultats suivants (*lemme du serpent*) :

1. u injective $\Rightarrow u'$ injective,
2. u', u'' injectives $\Rightarrow u$ injective,
3. u injective et u' surjective $\Rightarrow u''$ injective
4. u'' injective et u surjective $\Rightarrow u'$ surjective
5. u', u'' surjectives $\Rightarrow u$ surjective
6. u surjective $\Rightarrow u''$ surjective.

On voit en particulier que si u' et u'' sont bijectives, alors u aussi.

Exemple

1. Considérons la situation suivante

$$\begin{tikzcd}
K^{m'} \arrow[r, hook] \arrow[d, "u'"] & K^m \arrow[r, two heads] \arrow[d, "u"] & K^m/K^{m'} \arrow[d, "u''"] & K^{m-m'} \arrow[l, "\simeq"'] \arrow[d] \\
K^{n'} \arrow[r, hook] & K^n \arrow[r, two heads] & K^n/K^{n'} & K^{n-n'}. \arrow[l, "\simeq"']
\end{tikzcd}$$

   On dispose alors des matrices A, A' et A'' de u, u' et u'' (en utilisant l'identification de droite pour u'') et on a
$$A = \begin{bmatrix} A' & \star \\ 0 & A'' \end{bmatrix}$$
   qui est une *matrice triangulaire par blocs*. Si A' et A'' sont des matrices inversibles, alors A aussi comme conséquence de la remarque (nous verrons plus tard que la réciproque est vraie).
2. Par récurrence, on voit qu'une matrice triangulaire
$$\begin{bmatrix} a_1 & \star & \cdots & \star \\ 0 & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \star \\ 0 & \cdots & 0 & a_n \end{bmatrix}$$
   est inversible si (et seulement si) $a_1, \ldots, a_n \neq 0$.

2.7 Exercices

Exercice 2.1 Montrer que l'ensemble $l_\infty(\mathbb{R})$ des suites réelles bornées est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$ et que l'ensemble $\mathscr{C}(I,\mathbb{R})$ des fonctions continues sur un intervalle I à valeur dans $\mathbb{R}$ est un sous-espace vectoriel de $\mathscr{F}(I,\mathbb{R})$.

Exercice 2.2 Dire dans chaque cas si ces fonctions forment un sous-espace vectoriel de l'espace $\mathscr{F}(\mathbb{R})$ des applications de $\mathbb{R}$ dans lui même.

1. Les fonctions dérivables.
2. Les fonctions paires.
3. Les fonctions croissantes.
4. Les fonctions monotones.

Exercice 2.3 Démontrer les propositions 2.1.3 et 2.2.1.

Exercice 2.4 Démontrer les propositions 2.3.5 et 2.3.6.

Exercice 2.5 : Montrer qu'un espace vectoriel E est une *droite* (c'est à dire, isomorphe à K) si et seulement si E a exactement deux sous-espaces vectoriels.

Exercice 2.6 Montrer que si E est un espace vectoriel, alors l'application d'évaluation

$$\begin{aligned} \mathrm{L}(K,E) &\longrightarrow E \\ u &\longmapsto u(1) \end{aligned}$$

est un isomorphisme dont on déterminera l'inverse. En déduire un isomorphisme $\mathrm{M}_{n\times 1}(K) \simeq K^n$ que l'on explicitera.

Exercice 2.7 Montrer (en calculant le second membre) que si on pose $\mathbf{1}_1 := (1,0,0)$, $\mathbf{1}_2 := (0,1,0)$ et $\mathbf{1}_3 := (0,0,1)$, on a

$$(x,y,z) = x\mathbf{1}_1 + y\mathbf{1}_2 + z\mathbf{1}_3.$$

Généraliser.

Exercice 2.8 Montrer que si $u \in \mathrm{L}(K^m,K^n)$ et $v \in \mathrm{L}(K^l,K^m)$, alors $[u\circ v] = [u][v]$.

Exercice 2.9

1. Montrer que si $\varphi \in {}^tK^n$, on a

$$\varphi = \varphi(\mathbb{1}_1)p_1 + \cdots + \varphi(\mathbb{1}_n)p_n$$

ou les p_i désignent les projections sur les axes. En déduire un isomorphisme entre K^n et ${}^tK^n$.

2. Montrer que pour tout $i \in \mathbb{N}$, l'application « i-ème coefficient »

$$p_i : K[T] \to K, \quad \sum_j c_jT^j \mapsto c_i$$

est une forme linéaire sur $K[T]$. En déduire un isomorphisme entre $K^{\mathbb{N}}$ et ${}^tK[T]$.

Exercice 2.10 Montrer que si A est la matrice d'une application linéaire $u : K^m \to K^n$ (dans les bases usuelles), alors la matrice du dual de u est la transposée de A (en identifiant K^n et K^m avec leurs espaces duaux comme ci-dessus).

Exercice 2.11 On se donne pour tout $i = 1, \dots, n$, une forme linéaire

$$\varphi_i := a_{i,1}p_1 + \cdots + a_{i,m}p_m$$

sur K^m et on pose $U := \{\varphi_1, \dots, \varphi_n\}$. Montrer que l'orthogonal U° de U est l'ensemble des solutions du système linéaire homogène

$$\mathscr{S} := \left\{ \begin{array}{c} a_{1,1}x_1 + \cdots a_{1,m}x_m = 0 \\ \vdots \\ a_{n,1}x_1 + \cdots a_{n,m}x_m = 0. \end{array} \right.$$

Exercice 2.12 On désigne par I l'idéal principal de $K[T]$ engendré par T^d. Montrer que

$$\varphi \in {}^\circ I \Leftrightarrow \forall i \geq d, \varphi(T^i) = 0.$$

En déduire un isomorphisme entre K^d et ${}^\circ I$.

Exercice 2.13 Montrer que le noyau de la forme linéaire $\varphi : \mathbb{R}^2 \to \mathbb{R}, (x, y) \mapsto x - y$ est la diagonale $\Delta := \{(t,t), t \in \mathbb{R}\} \subset \mathbb{R}^2\}$. En déduire un isomorphisme $\mathbb{R}^2/\Delta \simeq \mathbb{R}$. Interprétation géométrique.

Exercice 2.14 Établir un isomorphisme $K^{n-m} \simeq K^n/K^m$ lorsque $m \leq n$ (on voit K^m comme sous-espace de K^n en identifiant $(x_1, \dots, x_m)$ et $(x_1, \dots, x_m, 0, \dots, 0)$).

Exercice 2.15 On rappelle que les multiples d'un polynôme P forment un sous-espace vectoriel F de l'espace E de tous les polynômes sur K. Montrer que E/F est isomorphe à l'espace E_n des polynômes de degré strictement plus petit que $n = \deg P$.

Exercice 2.16 On rappelle qu'une suite $(x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ *tend vers* 0 si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, |x_n| \leq \varepsilon$$

et qu'elle de *de Cauchy* si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall m, n \geq N, |x_n - x_m| \leq \varepsilon.$$

Montrer que les suites de Cauchy forment un sous-espace vectoriel A de l'espace de toutes les suites et que les suites qui tendent vers 0 forment un sous-espace vectoriel I de A. Établir un isomorphisme $A/I \simeq \mathbb{R}$ (c'est même un isomorphisme d'anneaux).

Exercice 2.17 Soit F un sous-espace vectoriel d'un espace vectoriel E. Établir une bijection entre l'ensemble de tous les sous-espaces vectoriels de E/F et celui des sous-espaces vectoriels de E contenant F.

Exercice 2.18 Montrer qu'un sous-espace vectoriel H d'un espace vectoriel E est un hyperplan si et seulement si E/H est une droite, si et seulement si H est maximum parmi les sous-espaces vectoriels de E distinct de E.

Exercice 2.19 Soient $u : E \to F$ une application linéaire, $E' \subset E$, $F' \subset F$ des sous-espaces tels que $u(E') \subset F'$ et $u' : E' \to F'$ et $u'' : E/E' \to F/F'$ les applications induites. Montrer que

1. u injective (resp. surjective) $\Rightarrow u'$ injective (resp. u'' surjective),
2. u', u'' injectives (resp. surjectives) $\Rightarrow u$ injective (resp. surjective).

3. Somme directe, base

On fixe toujours un corps des scalaires K.

Remarque Tout ce qui précède le théorème de la base incomplète (section 3.4) est encore valable pour des A-modules où A est un anneau quelconque, et en particulier pour des groupes abéliens (cas $A = \mathbb{Z}$). Par contre, ce qui suit l'énoncé de ce théorème est faux sur un anneau quelconque, même si on se limite aux modules libres (c'est à dire qui admettent une base) sur un anneau commutatif.

3.1 Somme directe (externe)

Définition 3.1.1 Soit $(E_s)_{s\in S}$ une famille d'espaces vectoriels. Alors, le *support* de $x := (x_s)_{s\in S} \in \prod_{s\in S} E_s$ est

$$\mathrm{supp}(x) = \{s \in S \;/\; x_s \neq 0\}.$$

La *somme directe (externe)* de la famille est

$$\bigoplus_{s\in S} E_s = \{x \;/\; |\mathrm{supp}(x)| < +\infty\} \subset \prod_{s\in S} E_s.$$

Lorsque tous les E_s sont égaux à un même espace E, on écrira $E^{(S)}$.

Remarque
1. On dit aussi que les éléments de $\bigoplus_{s\in S} E_s$ sont les familles *presque toujours nulles* (c'est à dire toujours sauf un nombre fini).
2. Lorsque S est fini, il n'y a pas de différence entre somme directe (externe) et produit :
$$E_1 \oplus \cdots \oplus E_n = E_1 \times \cdots \times E_n.$$
On utilise alors plutôt la notation du produit, réservant la notation de somme directe pour les sommes directes internes (voir plus bas). Mais ce n'est pas le cas en général.
3. Si E est un espace vectoriel et X est un ensemble quelconque, on peut considérer le *support* de f
$$\mathrm{supp}(f) = \{x \in X \;/\; f(x) \neq 0\},$$

et l'ensemble
$$\mathscr{F}_{\mathrm{f}}(X,E) = \{f : X \to E \ / \ |\mathrm{supp}(f)| < +\infty\}$$
des applications à support fini (c'est à dire *presque toujours nulles*). On a bien sûr $\mathscr{F}_{\mathrm{f}}(X,E) \simeq E^{(X)}$.

Lemme 3.1.2 Si $x, y \in \prod_{s\in S} E_s$, alors
$$\mathrm{supp}(x+y) \subset \mathrm{supp}(x) \cup \mathrm{supp}(y)$$
et si $x \in \prod_{s\in S} E_s$ et $a \in K$, alors
$$\mathrm{supp}(ax) \subset \mathrm{supp}(x).$$

Démonstration. On écrit $x := (x_s)_{s\in S}$ et $y := (y_s)_{s\in S}$. Si $x_s = y_s = 0$, alors $x_s + y_s = 0$ et la première assertion en découle. La seconde se démontre de la même manière (exercice). ■

Proposition 3.1.3 Si $(E_s)_{s\in S}$ est une famille d'espaces vectoriels, alors $\bigoplus_{s\in S} E_s$ est un sous-espace vectoriel de $\prod_{s\in S} E_s$.

Démonstration. Résulte immédiatement du lemme 3.1.2 (exercice). ■

Remarque 1. Si $E := \oplus_{s\in S} E_s$, on dispose encore de projections (composée de l'inclusion et des projections habituelles), que l'on notera toujours
$$p_s : E \to E_s,$$
et qui sont linéaires.

2. Si E est un espace vectoriel et X est un ensemble quelconque, alors $\mathscr{F}_{\mathrm{f}}(X,E)$ est un sous-espace vectoriel de $\mathscr{F}(X,E)$ et les applications d'évaluation
$$p_x : \mathscr{F}_{\mathrm{f}}(X,E) \to E, \quad f \mapsto f(x)$$
sont linéaires.

De même que les projections sont associées aux produits, ce sont les injections qui sont liées aux sommes directes :

Proposition 3.1.4 Si $E := \oplus_{s\in S} E_s$, alors il existe pour tout $s \in S$ une unique application (linéaire injective) $i_s : E_s \hookrightarrow E$ telle que pour tout $t \in S$, on ait
$$p_t \circ i_s = \begin{cases} \mathrm{Id}_{E_s} & \text{si } s = t \\ 0 & \text{sinon.} \end{cases}$$
On aura alors
$$\sum_{s\in S} i_s \circ p_s = \mathrm{Id}_E.$$

Démonstration. La propriété universelle du produit nous dit qu'il existe une telle application i_s à valeurs dans le produit, et il faut juste s'assurer qu'on tombe dans la somme directe. Or, si $x_s \in E_s$, on aura $\mathrm{supp}(i_s(x_s)) = \{s\}$ qui est bien fini.

Pour démontrer la dernière assertion, il suffit de remarquer que pour tout $t \in S$, on a bien, pour $x \in E$,
$$p_t\left(\sum_{s\in S}(i_s \circ p_s)(x)\right) = \sum_{s\in S}(p_t \circ i_s \circ p_s)(x) = p_t(x).$$
En effet, il suit alors que $\sum_{s\in S}(i_s \circ p_s)(x) = x$. ■

Remarque Comme toujours, nous en déduisons que si E est un espace vectoriel et X un ensemble quelconque, alors il existe pour tout $x \in X$ une unique application (injective)

$$i_x : E \hookrightarrow \mathscr{F}_{\mathrm{f}}(X,E)$$

telle que

$$\forall x,y \in X, \quad p_y \circ i_x = \begin{cases} \mathrm{Id} & \text{si } x = y \\ 0 & \text{sinon.} \end{cases}$$

Exemple

1. Si E_1 et E_2 sont deux espaces vectoriels et $E := E_1 \times E_2$, on dispose du diagramme

$$\begin{tikzcd} E_1 \arrow[r, shift left, "i_1"] & E \arrow[l, shift left, "p_1"] \arrow[r, shift left, "p_2"] & E_2 \arrow[l, shift left, "i_2"] \end{tikzcd} \tag{3.1}$$

avec

$$i_1(x_1) = (x_1,0), \quad p_1(x_1,x_2) = x_1, \quad i_2(x_2) = (0,x_2) \quad \text{et} \quad p_2(x_1,x_2) = (x_1,x_2),$$

et des formules

$$p_1 \circ i_1 = \mathrm{Id}, \quad p_2 \circ i_2 = \mathrm{Id}, \quad p_1 \circ i_2 = 0, \quad p_2 \circ i_1 = 0 \quad \text{et} \quad i_1 \circ p_1 + i_2 \circ p_2 = \mathrm{Id}. \tag{3.2}$$

2. Réciproquement, si on se donne un diagramme (3.1) satisfaisant les conditions (3.2), alors on a un isomorphisme

$$\begin{array}{rcl} E_1 \times E_2 & \xrightarrow{\simeq} & E \\ (x_1,x_2) & \longmapsto & i_1(x_1) + i_2(x_2) \\ x & \longleftarrow & (p_1(x), p_2(x)) \end{array}$$

3. Si on se donne un ensemble S, on peut considérer les différentes inclusion $i_s : K \to K^{(S)}$ pour $s \in S$. On pose alors $\mathbb{1}_s := i_s(1) \in K^{(S)}$ si bien que pour tout $a \in K$, $i_s(a) = a\mathbb{1}_s$. On aura donc

$$(a_s)_{s\in S} = \sum_{s \in S} a_s \mathbb{1}_s.$$

4. Alternativement, si on se donne un ensemble X, on peut considérer dans $\mathscr{F}_{\mathrm{f}}(X,K)$ les applications indicatrices (notées de la même façon)

$$\forall x,y \in X, \quad \mathbb{1}_x(y) = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{sinon,} \end{cases}$$

et on aura toujours $f = \sum_{x \in X} f(x) \mathbb{1}_x$.

On passe maintenant à la propriété universelle des sommes directes.

Proposition 3.1.5 Si on se donne pour pour tout $s \in S$, une application linéaire $u_s : E_s \to F$, alors il existe une unique application linéaire $u : \oplus_{s \in S} E_s \to F$ telle que pour tout $s \in S$, on ait $u_s = u \circ i_s$:

$$\begin{tikzcd} E_s \arrow[d, hook, "i_s"'] \arrow[dr, "u_s"] & \\ \oplus_{s\in S} E_s \arrow[r, dashed, "\exists ! u"] & F. \end{tikzcd}$$

Démonstration. On aura nécessairement

$$u(x) = u\left(\sum_{s\in S} i_s(x_s)\right) = \sum_{s\in S}(u\circ i_s)(x_s) = \sum_{s\in S} u_s(x_s),$$

d'où l'unicité. Et on vérifie que l'application ainsi définie répond bien à la question (exercice). ∎

Remarque 1. Dans la situation ci-dessus, on dit parfois que les applications i_s sont les *injections* et que les u_s sont les *applications partielles (à l'origine)*. Une application linéaire définie sur une somme directe est déterminée par ses applications partielles.

2. Les injections sont donc les applications partielles correspondant au cas $u = \mathrm{Id}$.
3. Par un calcul direct, ou en utilisant la propriété universelle, on montre facilement que si E, F et G sont trois espaces vectoriels, on a
   (a) $E\times F \simeq F\times E$ (commutativité),
   (b) $(E\times F)\times G \simeq E\times(F\times G)$ (associativité),
   (c) $E\times\{0\}\simeq E$ (neutre)
   Ceci se généralise à des sommes directes quelconques.
4. Comme conséquence de la propriété universelle, si on se donne une famille d'applications linéaires $u_s : E_s \to F_s$, on dispose alors d'une application linéaire

$$\oplus_{s\in S}u_s : \oplus_{s\in S}E_s \to \oplus_{s\in S}E_s, \quad (x_s)_{s\in S} \mapsto (u_s(x_s))_{s\in S}.$$

   C'est l'application induite par $\prod_{s\in S} u_s$.

Exemple 1. Dans le cas d'un nombre fini d'espaces vectoriels $E_1,\ldots,E_n$, les injections sont les applications

$$E_i \to E_1\times\cdots\times E_n, \quad x_i \mapsto (0,\ldots,0,x_i,0\ldots,0),$$

et les applications partielles associées à $u : E_1\times\cdots\times E_n \to F$ sont les applications

$$u_i : E_i \mapsto F, x_i \mapsto u(0,\ldots,0,x_i,0\ldots,0).$$

On a donc $u(x_1,\ldots,x_n) = u_1(x_1) + u_n(x_n)$.

2. Il revient au même de se donner les applications partielles $u_1 : E_1 \to F$ et $u_2 : E_2 \to F$ ou bien l'application globale $u : E_1\times E_2 \to F$:

$$\begin{tikzcd}
 & E_1 \arrow[d, hook, "i_1"'] \arrow[ddr, bend left, "u_1"] & \\
E_2 \arrow[r, hook, "i_2"] \arrow[drr, bend right, "u_2"'] & E_1\times E_2 \arrow[dr, dashed, "\exists! u"] & \\
 & & F
\end{tikzcd}$$

On termine avec la propriété universelle de $K^{(S)}$:

Corollaire 3.1.6 Si on se donne un ensemble S et une application $f : S\to E$ ou E est un espace vectoriel, il existe une unique application linéaire $\tilde f : K^{(S)} \to E$ telle que, pour tout $s\in S$, on ait $\tilde f(\mathbb{1}_s) = f(s)$:

$$\begin{tikzcd}
s \arrow[d, mapsto] \\
\mathbb{1}_s
\end{tikzcd}
\qquad
\begin{tikzcd}
S \arrow[d, hook] \arrow[dr, "f"] & \\
K^{(S)} \arrow[r, dashed, "\exists!\tilde f"] & E.
\end{tikzcd}$$

Démonstration. On doit avoir

$$\tilde{f}((a_s)_{s\in S}) = \tilde{f}\left(\sum_{s\in S} a_s \mathbb{1}_s\right) = \sum_{s\in S} a_s \tilde{f}(\mathbb{1}_s) = \sum_{s\in S} a_s f(s).$$

En particulier, les applications partielles doivent être données par

$$\tilde{f}_s : K \to E, \quad a \mapsto af(s)$$

qui sont bien linéaires. ■

3.2 Somme directe interne

Proposition 3.2.1 Soient E un espace vectoriel et $(E_s)_{s\in S}$ une famille de sous-espaces vectoriels de E. Alors,

1. Il existe un plus grand sous-espace vectoriel de E contenu dans tous les E_s, c'est $\cap_{s\in S} E_s$.
2. Il existe un plus petit sous-espace vectoriel de E contenant tous les E_s, c'est l'image $\sum_{s\in S} E_s$ de l'application

$$\oplus_{s\in S} E_s \to E, \quad (x_s)_{s\in S} \mapsto \sum_{s\in S} x_s. \tag{3.3}$$

Démonstration. 1. Il suffit de montrer que $\cap_{s\in S} E_s$ est un sous-espace vectoriel, ce qui est immédiat (exercice).
2. On se donne un sous-espace vectoriel $F \subset E$ qui contient tous les E_s. Par construction, l'application

$$\oplus E_s \to F, \quad (x_s)_{s\in S} \mapsto \sum_{s\in S} x_s$$

a même image que celle de la proposition, qui est donc contenue dans F. Et nous savons que cette image est un sous-espace vectoriel. ■

Remarque 1. *Plus grand* (resp. *plus petit*) signifie que tous les autres sont contenus dedans (resp. le contiennent).
2. L'existence de l'application (3.3) résulte de la propriété universelle de la somme directe (et de même dans la démonstration).
3. Par définition, la *somme* des sous-espaces est donc

$$\sum_{s\in S} E_s = \left\{ \sum_{\text{finie}} x_s, \quad x_s \in E_s \right\}.$$

4. Dans le cas d'un nombre fini de sous-espaces, on écrira

$$E_1 + \cdots + E_n = \{x_1 + \cdots + x_n, \quad x_i \in E_i\}.$$

5. Attention : une union de sous-espaces vectoriels n'en est pas un en général !

Proposition 3.2.2 Si F et G sont deux sous-espaces vectoriels de E, l'application composée

$$G \overset{i}{\hookrightarrow} E \overset{\pi}{\twoheadrightarrow} E/F$$

induit un isomorphisme
$$G/(F\cap G)\simeq (F+G)/F.$$

Démonstration. Cela résulte du théorème de Noether. Vérifions que cette application a pour noyau $F\cap G$ et pour image $(F+G)/F$. Clairement, si $x\in G$, on aura $\bar{x}=0$ si et seulement si $x\in F$, ce qui signifie que $x\in F\cap G$. De même, si $y\in E$, on pourra écrire $\bar{y}=\bar{x}$ avec $x\in G$ si et seulement si $y-x\in F$, ce qui veut dire que $y\in F+G$. ■

Remarque
1. Cette proposition est habituellement appelée second théorème d'isomorphie de Noether.
2. Il y en a un troisième qui stipule que l'on a toujours $E/F\simeq (E/G)/(F/G)$ si $G\subset F\subset E$ sont des sous-espaces vectoriels.

Définition 3.2.3 Si l'application (3.3) est bijective, on dit $(E_s)_{s\in S}$ est une famille de sous-espace vectoriels *supplémentaires* dans E (ou que E est *somme directe interne* de la famille).

Remarque
1. Cela signifie donc que tout élément de E s'écrit de manière unique comme somme finie d'éléments de E_s.
2. L'application (3.3) étant linéaire, on obtient alors un *isomorphisme* $\oplus_{s\in S}E_s\simeq E$.
3. Pour mémoriser la différence entre somme directe externe et interne, on peut noter que $\mathbb{R}^2$ est somme directe *externe* de $\mathbb{R}$ par lui même ($\mathbb{R}^2=\mathbb{R}\oplus\mathbb{R}$) : c'est une opération. Par contre $\mathbb{R}^2$ est somme directe *interne* de l'axe des x par l'axe des y ($\mathbb{R}^2\simeq Ox\oplus Oy$) : c'est une propriété.

Proposition 3.2.4 Soient E un espace vectoriel et $(E_s)_{s\in S}$ une famille de sous-espaces vectoriels de E. Alors, les conditions suivantes sont équivalentes :
1. Les sous-espaces sont supplémentaires (c'est à dire $\oplus_{s\in S}E_s\simeq E$).
2. (a) $\sum_{s\in S}E_s=E$,
   (b) $\forall s\in S,\quad E_s\cap\sum_{t\neq s}E_t=\{0\}$.

Démonstration. Bien sûr la première condition n'est autre que la surjectivité de l'application (3.3), que nous désignerons ici par Φ, et il suffit donc de montrer que l'autre correspond à l'injectivité. Supposons qu'elle est satisfaite et prenons un $(x_s)_{s\in S}\in\ker\Phi$. On a donc $\sum_{s\in S}x_s=0$ si bien que pour tout $s\in S$, on a
$$x_s=-\sum_{t\neq s}x_t\in E_s\cap\sum_{t\neq s}E_t=\{0\}.$$
Inversement, si on fixe s et qu'on prend $x\in E_s\cap\sum_{t\neq s}E_t$, on pose $x_s:=-x\in E_s$ et on écrit $x=:\sum_{t\neq s}x_t$ avec $x_t\in E_t$ pour $t\neq s$. Cela définit un élément $(x_t)\in\oplus_{t\in S}E_t$ et on a $\Phi((x_t)_{t\in S})=0$ par construction. Donc si on suppose Φ injective, on voit que pour tout $t\in S$, on a $x_t=0$ et en particulier, $x=-x_s=0$. ■

Remarque
1. Comme cas particulier, on voit que si E_1 et E_2 sont deux sous-espaces vectoriels de E, on a
$$E_1\oplus E_2\simeq E\Leftrightarrow\left\{\begin{array}{l}E_1+E_2=E\\ E_1\cap E_2=\{0\}.\end{array}\right.$$
2. Attention, la seconde condition n'est *pas* aussi simple en général : il ne suffit *pas* que
$$E_1+E_2+E_3=E\quad\text{et}\quad E_1\cap E_2=E_2\cap E_3=E_1\cap E_3=\{0\}$$
pour avoir $E_1\oplus E_2\oplus E_3\simeq E$.

3. À nouveau, si E_1 et E_2 sont deux sous-espaces vectoriels de E et si on désigne par $i_1 : E_1 \hookrightarrow E$ et $i_2 : E_2 \hookrightarrow E$ les applications d'inclusion, on voit que $E_1 \oplus E_2 \simeq E$ si et seulement si il existe $p_1 : E \to E_1$ et $p_2 : E \to E_2$ telles que
$$p_1 \circ i_1 = \mathrm{Id}, \quad p_2 \circ i_2 = \mathrm{Id}, \quad p_1 \circ i_2 = 0, \quad p_2 \circ i_1 = 0 \quad \text{et} \quad i_1 \circ p_1 + i_2 \circ p_2 = \mathrm{Id}.$$
4. L'associativité de la somme directe externe permet de construire les sommes directes finies internes par récurrence : si $E_1, \dots, E_n$ sont des sous-espaces vectoriels de E et qu'on pose $F = E_1 + \cdots + E_{n-1}$, alors
$$E_1 \oplus \cdots \oplus E_n \simeq E \Leftrightarrow \begin{cases} E_1 \oplus \cdots \oplus E_{n-1} \simeq F \\ F \oplus E_n \simeq E. \end{cases}$$

Proposition 3.2.5 Deux sous-espaces vectoriels F et G sont supplémentaires dans E si et seulement si l'application composée
$$G \overset{i}{\hookrightarrow} E \overset{\pi}{\twoheadrightarrow} E/F$$
est bijective.

Démonstration. Le second théorème d'isomorphie de Noether nous dit que cette application est bijective si et seulement si $F \cap G = \{0\}$ et $(F+G)/F = E/F$. Cette dernière condition est équivalente à $F + G = E$. Les détails sont laissés en exercice. ■

Exemple 1. Si on voit K^m comme contenu dans K^n en utilisant les premières composantes et K^{n-m} comme contenu dans K^n en utilisant les dernières, on a une somme directe (interne)
$$K^m \oplus K^{n-m} \simeq K^n$$
(c'est aussi une somme directe externe).
2. Si P est un polynôme de degré d, on a une somme directe interne
$$K[T] \simeq (P) \oplus K[T]_{<d}$$
qui exprime la division euclidienne.

Remarque La proposition implique qu'un sous-espace vectoriel H d'un espace vectoriel E est un hyperplan si et seulement si c'est le supplémentaire d'une droite (d'un sous-espace isomorphe à K). Ce résultat nécessite que K soit un corps il est faux pour les A-modules en général.

Définition 3.2.6 Soit E un espace vectoriel.
1. On dit que $p \in \mathrm{L}(E)$ est une *projection* (ou un *projecteur*) si $p \circ p = p$.
2. On dit que $s \in \mathrm{L}(E)$ est une *symétrie* si $s \circ s = \mathrm{Id}_E$.

Proposition 3.2.7 Soient E un espace vectoriel et $p \in \mathrm{L}(E)$.
1. Si p est une projection, alors
$$E \simeq \ker p \oplus \operatorname{im} p.$$
2. p est une projection si et seulement si $q := \mathrm{Id}_E - p$ est une projection et on a alors
$$\ker p = \operatorname{im} q \quad \text{et} \quad \ker q = \operatorname{im} p.$$

Démonstration. Exercice. ■

Proposition 3.2.8 (Car$(K) \neq 2$) Soient E un espace vectoriel et $s \in \mathrm{L}(E)$.

1. Si s est une symétrie, alors
$$E \simeq \ker(s - \mathrm{Id}_E) \oplus \ker(s + \mathrm{Id}_E).$$
2. s est une symétrie si et seulement si $p := \frac{s+\mathrm{Id}_E}{2}$ est une projection.

Démonstration. Exercice. ■

Remarque Réciproquement, si on se donne une décomposition en somme directe $E = E_1 \oplus E_2$, on peut lui associer deux projections p_1 et p_2 de manière évidente, et donc aussi deux symétries $s_i := 2p_i - \mathrm{Id}_E$ pour $i = 1, 2$ (faire un dessin).

3.3 Base

Proposition 3.3.1 Si X est une partie d'un espace vectoriel E, il existe un plus petit sous-espace vectoriel $\mathrm{Vect}(X)$ de E contenant X.

Démonstration. Découle formellement de la proposition 3.2.1 : $\mathrm{Vect}(X)$ est l'intersection de tous les sous-espaces vectoriels contenant X. ■

Définition 3.3.2 Si X est une partie d'un espace vectoriel E, alors $\mathrm{Vect}(X)$ est le *sous-espace vectoriel de E engendré* par X.

Remarque Cette démarche est très générale et on peut définir de même le sous-monoïde ou le sous groupe engendré par une partie (bien sûr, ça fonctionne aussi pour la notion de module et en particulier celle d'idéal). Par exemple, un idéal principal est un idéal engendré par un seul élément.

Proposition 3.3.3 Si X est une partie d'un espace vectoriel E, alors $\mathrm{Vect}(X)$ est l'image de l'application
$$K^{(X)} \to E, \quad (a_x)_{x\in X} \mapsto \sum_{x\in X} a_x x. \tag{3.4}$$

Démonstration. Quasiment identique à la démonstration de la seconde assertion de la proposition 3.2.1 (exercice). ■

Exemple
1. On a $\mathrm{Vect}(\emptyset) = \{0\}$, $\mathrm{Vect}(\{x\}) = Kx := \{ax, a \in K\}$ et $\mathrm{Vect}(E) = E$.
2. En général, on a $\mathrm{Vect}(X) = \sum_{x\in X} Kx$ et donc
$$\mathrm{Vect}(\{x_1, \ldots, x_n\}) = Kx_1 + \cdots + Kx_n.$$

Remarque
1. En général, on aura
$$\mathrm{Vect}(X) = \left\{ \sum_{\text{finie}} a_x x, \quad x \in X, a_x \in K \right\}.$$
2. L'opérateur Vect est un *opérateur de clôture* :

(a) Si $X \subset E$, alors $X \subset \mathrm{Vect}(X)$,
(b) Si $X_1 \subset X_2 \subset E$, alors $\mathrm{Vect}(X_1) \subset \mathrm{Vect}(X_2)$,
(c) Si $X \subset E$, alors $\mathrm{Vect}(\mathrm{Vect}(X)) = \mathrm{Vect}(X)$.

3. Si $(X_s)_{s\in S}$ est une famille de parties de E, alors
$$\mathrm{Vect}(\cup_{s\in S} X_s) = \sum_{s\in S} \mathrm{Vect}(X_s).$$
4. On a toujours $\mathrm{Vect}(U)^\circ = U^\circ$ et ${}^\circ\mathrm{Vect}(X) = {}^\circ X$.

Il est parfois nécessaire de travailler avec des familles plutôt que des ensembles :

Définition 3.3.4 Le *sous-espace vectoriel engendré* par une *famille* $(x_s)_{s\in S} \in E^S$ est l'image $\mathrm{Vect}((x_s)_{s\in S})$ de l'application
$$K^{(S)} \to E, \quad (a_s)_{s\in S} \mapsto \sum_{s\in S} a_s x_s. \tag{3.5}$$

Proposition 3.3.5 Si $u : E \to F$ est une application linéaire et $X \subset E$, alors $\mathrm{Vect}(u(X)) = u(\mathrm{Vect}(X))$.

Démonstration. On considère l'application composée $K^{(X)} \to E \to F$ et on utilise la transitivité de l'image (il vaut mieux travailler avec des familles ici). ∎

Exemple Les colonnes d'une matrice A engendrent $\mathrm{im} A$: en effet, ce sont les images des vecteurs de la base usuelle (voir plus bas).

Définition 3.3.6 Une partie X d'un espace vectoriel E est une *partie libre* (resp. *partie génératrice*, resp. une *base*) si l'application (3.4) est injective (resp. surjective, resp. bijective). On dit que X est *liée* si elle n'est pas libre.

Remarque Notons Φ l'application (3.4) si bien que $\Phi((a_x)_{x\in X}) = \sum_{x\in X} a_x x$.

1. Rappelons que l'existence de l'application Φ résulte du corollaire 3.1.6 (propriété universelle).
2. De manière moins formelle, on voit que
   (a) X est libre lorsque $\ker\Phi = \{0\}$, c'est à dire
   $$\sum_{x\in X} a_x x = 0 \Rightarrow \forall x \in X, a_x = 0.$$
   (b) X est génératrice lorsque $\mathrm{im}\,\Phi = E$, c'est à dire
   $$\forall y \in E, \quad y = \sum_{x\in X} a_x x \quad \text{avec } a_x \in K.$$
   (c) X est une base lorsque Φ est bijective, c'est à dire
   $$\forall y \in E, \quad y = \sum_{x\in X} a_x x \quad \text{avec } a_x \in K \text{ uniques.}$$
   L'application réciproque est donc celle qui envoie un vecteur sur ses *composantes* dans la base B.
3. X est liée s'il existe un nombre fini d'éléments *non tous nuls* $a_x \in K$ tels que $\sum_{x\in X} a_x x = 0$. De manière équivalente, un des vecteurs est combinaison linéaire des autres : $x = \sum_{y\neq x} a_y y$ (faux sur un anneau quelconque).

Ici encore, on aura parfois besoin de travailler avec des familles plutôt que des ensembles.

Définition 3.3.7 Soit E un espace vectoriel.

1. Une famille $(x_s)_{s\in S} \in E^S$ est une *famille libre* (resp. *famille génératrice*, resp. une *base ordonnée*) si l'application (3.5) est injective (resp. surjective, resp. bijective). On dit que X est *famille liée* si elle n'est pas libre.
2. Des vecteurs $x_1, \ldots, x_n$ sont *linéairement indépendants* si la famille $(x_1, \ldots, x_n)$ est libre. Sinon, on dit *linéairement dépendants*.

Exemple

1. Si E est un espace vectoriel, alors $\emptyset$ est libre et E est générateur.
2. L'espace nul $\{0\}$ a pour base $\emptyset$ et l'espace K a pour base 1, ou plus généralement n'importe quel $a \in K^\times$.
3. La *base canonique* de l'espace K^n est $\{\mathbb{1}_1, \ldots, \mathbb{1}_n\}$.
4. Plus généralement, les familles $\mathbb{1}_s$ dont la seule entrée non nulle est en s, où elle vaut 1, forment la *base canonique*, de l'espace $K^{(S)}$.
5. On ne sait *pas* écrire de base de $K^{\mathbb{N}}$.
6. Les projections $p_i : K^n \to K$ forment la *base canonique* de ${}^tK^n$.
7. Les vecteurs $\{\overline{\mathbb{1}}_{n-m+1}, \ldots, \overline{\mathbb{1}}_n\}$ forment la *base canonique* de K^n/K^m.
8. Les matrices $\mathbb{1}_{i,j}$, dont les entrées sont toutes nulle sauf en (i,j) ou elles valent 1, forment la *base canonique* de $\mathrm{M}_{n\times m}(K)$.
9. Les polynômes T^d, pour $d \in \mathbb{N}$ forment la *base canonique* de $K[T]$ et les T^d, pour $d \leq n$ forment la *base canonique* de l'espace $K[T]_{\leq n}$ des polynômes de degré au plus n.
10. Soit $\mathscr{P}$ un ensemble de polynômes. Alors,
    (a) s'il existe au plus un $P \in \mathscr{P}$ de chaque degré, alors $\mathscr{P}$ est libre,
    (b) s'il existe au moins un $P \in \mathscr{P}$ de chaque degré, alors $\mathscr{P}$ est générateur,
    (c) s'il existe exactement un $P \in \mathscr{P}$ de chaque degré, alors $\mathscr{P}$ est une base.
11. La base canonique de $\mathbb{C}$ (resp. ${}^t\mathbb{C}$) comme espace vectoriel sur $\mathbb{R}$ est $\{1, i\}$ (resp. $\{\Re, \Im\}$).
12. Si D est une droite (c'est à dire isomorphe à K), alors la base canonique de $L(D)$ est Id_D.

Proposition 3.3.8 Soit X une partie d'un espace vectoriel E. On a alors

1. $\mathrm{Vect}(X) = E \Leftrightarrow X$ génératrice,
2. X base de $\mathrm{Vect}(X) \Leftrightarrow X$ libre.

Démonstration. Résulte immédiatement de la proposition 3.3.3. ■

Proposition 3.3.9 On se donne un espace vectoriel E et, pour tout $s \in S$, un sous-espace vectoriel $E_s \subset E$ et une partie $X_s \subset E$. Les conditions suivantes sont alors équivalentes

1. Les X_s sont disjoints deux à deux et $X := \cup_{s\in S} X_s$ est une base de E,
2. (a) $E \simeq \oplus_{s\in S} E_s$ et
   (b) pour tout $s \in S$, X_s est une base de E_s.

Démonstration. On considère le diagramme commutatif

$$\begin{tikzcd} \oplus_{s\in S} K^{(X_s)} \arrow[r] \arrow[d] & K^{(X)} \arrow[d] \\ \oplus_{s\in S} E_s \arrow[r] & E \end{tikzcd}$$

et on vérifie que les X_s sont disjoints deux a deux si et seulement si la flèche du haut est bijective (exercice). L'assertion résulte alors immédiatement des définitions (exercice encore). ■

Proposition 3.3.10 Soient E et F deux espace vectoriels et B une base de E. Alors, toute application $f : B \to F$ se prolonge de manière unique en une application linéaire $u : E \to F$. De plus, on a

1. u injective $\Leftrightarrow u(B)$ est une *famille* libre de F,
2. u surjective $\Leftrightarrow u(B)$ est une partie génératrice de F,
3. u bijective $\Leftrightarrow u(B)$ est une base de F.

Démonstration. L'application $f : B \to F$ s'étend de manière unique en une application linéaire $\tilde{f} : K^{(B)} \to F$ et il suffit de composer avec l'inverse de l'isomorphisme $K^{(B)} \simeq E$ pour obtenir u. Toutes les autres assertions sont triviales si on considère $\tilde{f}$ à la place de u (attention, on utilise ici la notion de famille et pas celle de partie). ∎

Remarque On peut aussi vérifier que l'on a :

1. L libre et u injective $\Rightarrow u(L)$ libre,
2. G génératrice et u surjective $\Rightarrow u(G)$ génératrice.

3.4 Théorème d'existence

Théoreme 3.4.1 — de la base incomplète. Soient E un espace vectoriel et L (resp. G) une partie libre (resp. génératrice) de E. Si $L \subset G$, il existe une base B de E telle que $L \subset B \subset G$.

Démonstration. Si $\{L_s\}_{s\in S}$ est une famille *totalement ordonnée* de parties libres de E telles que $L \subset L_s \subset G$, alors $M := \cup_{s\in S} L_s$ est une partie libre de E avec $L \subset M \subset G$ (exercice). On peut donc appliquer le *lemme de Zorn* qui nous dit qu'il existe une partie libre B de E *maximale* pour la propriété $L \subset B \subset G$. Il reste à montrer que B est une partie génératrice. Et pour cela, il suffit de montrer que $G \subset \mathrm{Vect}(B)$. Or si $x \in G \setminus B$, on peut considérer $X := B \cup \{x\}$ qui est nécessairement liée par maximalité de B. On peut donc écrire une relation $a_1x_1 + \cdots + a_nx_n + ax = 0$. On a $a \neq 0$ car B est libre et donc

$$x = -\frac{a_1}{a}x_1 - \cdots - \frac{a_n}{a}x_n \in \mathrm{Vect}(B).$$ ∎

Remarque

1. (a) $\{L_s\}_{s\in S}$ *totalement ordonnée* signifie que si $s,t \in S$, alors nécessairement $L_s \subset L_t$ ou $L_t \subset L_s$.
   (b) M *maximal* signifie que si X est une partie libre telle que $M \subset X \subset G$, alors $X = M$.
   (c) Le *lemme de Zorn* dit exactement que si toute famille totalement ordonnée de parties libres de E telles que $L \subset L_s \subset G$ a un élément maximal, alors il existe une partie libre B de E maximale pour la propriété $L \subset B \subset G$.
2. En théorie des ensembles, le théorème de la base incomplète est en fait équivalent au lemme de Zorn qui est lui même équivalent à l'*axiome du choix* (ou même au théorème de Tychonov en topologie) ou plus simplement au théorème qui dit qu'un produit d'ensembles non vides est non vide.
3. Le théorème de la base incomplète est faux pour les A-modules en général : on a utilisé le fait que si $a \neq 0$, alors a est inversible. Un module qui possède une base est dit *libre*. Par exemple, $\mathbb{Z}/2\mathbb{Z}$ n'est pas un groupe abélien libre.
4. L'existence d'une base est purement théorique et on ne peut pas toujours en exhiber une (cas de l'espace des suites $E = K^{(\mathbb{N})}$ par exemple).

Corollaire 3.4.2 Soit E un espace vectoriel. Alors,

1. il existe une base B dans E,
2. si L est une partie libre de E, il existe une base B de E avec $L \subset B$,

3. si G est une partie génératrice de E, il existe une base B de E avec $B \subset G$.

Démonstration. ■

Corollaire 3.4.3 Si F est un sous-espace vectoriel de E, il possède un supplémentaire G.

Démonstration. Soit C une base de F. C'est une partie libre et on peut donc la prolonger en une base B de E et poser $G := \mathrm{Vect}(B \setminus C)$. On utilise alors la proposition 3.3.9. ■

Corollaire 3.4.4 Si $F \subset E$ est un sous-espace vectoriel, alors, toute application linéaire $F \to E'$ se prolonge en une application linéaire $E \to E'$.

Démonstration. ■

3.5 Dual (suite)

Lemme 3.5.1 Si $E_1, E_2 \subset E$ sont des sous-espaces vectoriels, alors

$$^\circ(E_1 \cap E_2) = {}^\circ E_1 + {}^\circ E_2.$$

On savait déjà que $^\circ(E_1 + E_2) = {}^\circ E_1 \cap {}^\circ E_2$.

Démonstration. Comme $^\circ(E_1 \cap E_2)$ est un sous-espace vectoriel qui contient à la fois $^\circ E_1$ et $^\circ E_2$, il contient nécessairement leur somme. Pour la réciproque, on choisit un supplémentaire G pour $E_1 + E_2$ dans E et un supplémentaire F_1 pour $E_1 \cap E_2$ dans E_1 si bien que $E \simeq F_1 \oplus E_2 \oplus G$ (faire un dessin). N'importe quel $\varphi \in {}^tE$ s'écrit alors (de manière unique) $\varphi = \varphi_1 + \varphi_2$ avec $\varphi_1 = 0$ sur F_1 et $\varphi_2 = 0$ sur $E_2 + G$, et on a en fait $\varphi_2 \in {}^\circ E_2$. Si on suppose que $\varphi \in {}^\circ(E_1 \cap E_2)$, on aura aussi $\varphi_1 \in {}^\circ E_1$. ■

Proposition 3.5.2 Si E est un espace vectoriel, l'application

$$\begin{array}{c} F \longmapsto {}^\circ F \\ \{\text{sous-espaces vectoriels de } E\} \to \{\text{sous-espaces vectoriels de } {}^tE\} \end{array}$$

renverse l'ordre et échange somme et intersection.

Démonstration. Résulte de la proposition en conjonction avec la remarque suivant la proposition 2.5.2. ■

Proposition 3.5.3 Si $u : E \to F$ est une application linéaire, alors

$$\mathrm{im}\,{}^tu = {}^\circ \ker u.$$

On savait déjà que $\ker {}^tu = {}^\circ \mathrm{im}\, u$.

Démonstration. On montre aisément l'inclusion (exercice). Réciproquement, si on se donne $\varphi \in {}^\circ \ker u$, on a $\ker u \subset \ker \varphi$. Donc, si on note $\pi : E \to E/\ker u$ la projection, il existe un unique

$\overline{\varphi} : E/\ker u \to K$ tel que $\overline{\varphi} \circ \pi = \varphi$. Si on désigne par $v : E/\ker u \simeq \operatorname{im} u$ l'isomorphisme de Noether, on peut alors prolonger $\overline{\varphi} \circ v^{-1} : \operatorname{im} u \to K$ en $\psi : F \to K$:

$$\begin{tikzcd}
E \arrow[r, "u"] \arrow[d, "\pi"] \arrow[rrdd, bend left, "\varphi"] & F \arrow[rdd, "\psi"] & \\
E/\ker u \arrow[r, "\simeq", "v"'] \arrow[rrd, bend right, "\overline{\varphi}"] & \operatorname{im} u \arrow[u, hook, "\iota"'] & \\
& & K
\end{tikzcd}$$

On calcule alors

$$^t u(\psi) = \psi \circ u = \psi \circ \iota \circ v \circ \pi = \overline{\varphi} \circ \pi = \varphi. \quad \blacksquare$$

Corollaire 3.5.4 Si $u : E \to F$ est une application injective, alors $^t u$ surjective.

On savait déjà que si u est surjective, alors $^t u$ est injective.

Démonstration. $\blacksquare$

Proposition 3.5.5 Si F est un sous-espace d'un espace vectoriel E, alors $(^\circ F)^\circ = F$.

Démonstration. Seule l'inclusion nécessite une démonstration. On choisit une base de E/F qui est donnée par un isomorphisme $v := K^{(S)} \simeq E/F$. On considère alors, pour $s \in S$ fixé, l'application composée

$$\varphi_s : E \xrightarrow{\pi} E/F \xrightarrow{v^{-1}} K^{(S)} \xrightarrow{p_s} K$$

qui envoie x sur la composante de $\overline{x}$. On sait que $F = \ker \pi$ et on a

$$\pi(x) = 0 \Leftrightarrow (v^{-1} \circ \pi)(x) = 0 \Leftrightarrow \forall s \in S, p_s(v^{-1} \circ \pi)(x) = 0 \Leftrightarrow \forall s \in S, \varphi_s(x) = 0,$$

si bien que $F = U^\circ$ avec $U = \{\varphi_s\}_{s \in S}$. Pour conclure, on remarque que l'on a alors $^\circ F = {}^\circ(U^\circ) \supset U$ si bien que $(^\circ F)^\circ \subset U^\circ = F$. $\blacksquare$

Remarque Cela implique que l'application $F \mapsto {}^\circ F$ de la proposition 4.4 est injective.

Corollaire 3.5.6 Une partie F d'un espace vectoriel E est un sous-espace vectoriel si et seulement si c'est une intersection d'hyperplans.

Démonstration. $\blacksquare$

Exemple Tout sous-espace vectoriel de K^n est l'ensemble des solutions d'un système linéaire homogène (et réciproquement).

Corollaire 3.5.7 Si E est un espace vectoriel, alors $(^t E)^\circ = \{0_E\}$.

Démonstration. Comme on sait que $^t E = {}^\circ\{0_E\}$, il suffit d'appliquer la proposition à $F := \{0_E\}$. $\blacksquare$

Corollaire 3.5.8 Si E est un espace vectoriel, alors l'application canonique $E \to {}^{tt}E$ est injective.

Démonstration. On rappelle que cette application canonique est l'application

$$x \mapsto (p_x : \varphi \mapsto \varphi(x)),$$

et on a $p_x = 0 \Leftrightarrow \forall \varphi \in {}^tE, \varphi(x) = 0 \Leftrightarrow x \in ({}^tE)^\circ = \{0_E\}$. ■

3.6 Exercices

Exercice 3.1 Montrer que si E, F et G sont trois espaces vectoriels, on a
1. $E \times F \simeq F \times E$ (commutativité),
2. $(E \times F) \times G \simeq E \times (F \times G)$ (associativité),
3. $E \times \{0\} \simeq E$ (neutre)

Exercice 3.2 Montrer que si E_1 et E_2 sont des sous-espaces vectoriels de E, alors $E_1 \cup E_2$ n'est pas un sous-espace vectoriel à moins que $E_1 \subset E_2$ ou que $E_2 \subset E_1$.

Exercice 3.3 Montrer qu'on peut avoir $E = E_1 + E_2 + E_3$, ainsi que

$$E_1 \cap E_2 = E_1 \cap E_3 = E_2 \cap E_3 = \{0\},$$

bien que $E \not\simeq E_1 \oplus E_2 \oplus E_3$.

Exercice 3.4 Démontrer les propositions 3.2.7 et 3.2.8

Exercice 3.5
1. Montrer que l'application de transposition $A \mapsto {}^tA$ est une symétrie vectorielle sur $\mathrm{M}_n(K)$.
2. ($\mathrm{Car}(K) \neq 2$) En déduire que les matrices symétriques (${}^tA = A$) ainsi que les matrices antisymétriques (${}^tA = -A$) forment des sous-espaces vectoriel $\mathrm{SM}_n(K)$ et $\mathrm{AM}_n(K)$ respectivement de $\mathrm{M}_n(K)$, et que

$$\mathrm{M}_n(K) \simeq \mathrm{SM}_n(K) \oplus \mathrm{AM}_n(K).$$

Exercice 3.6 Soient F, P et I les ensembles de toutes les fonctions $\mathbb{R} \to \mathbb{R}$, des fonctions paires et des fonctions impaires, respectivement. Montrer que P et I sont des sous-espaces vectoriels de F et que $F \simeq P \oplus I$ en exhibant une symétrie de F.

Exercice 3.7 Appliquer la théorie des symétries vectorielles à la conjugaison complexe σ sur $\mathbb{C}$ vu comme espace vectoriel sur $\mathbb{R}$.

Exercice 3.8 Montrer que Vect est un *opérateur de clôture* : on a toujours $X \subset \mathrm{Vect}(X) = \mathrm{Vect}(\mathrm{Vect}(X))$ et si $X_1 \subset X_2$, alors $\mathrm{Vect}(X_1) \subset \mathrm{Vect}(X_2)$.

Exercice 3.9 Montrer que l'on a toujours $\mathrm{Vect}(\cup_{s \in S} X_s) = \sum_{s \in S} \mathrm{Vect}(X_s)$.

Exercice 3.10 Montrer que l'on a toujours $\mathrm{Vect}(U)^\circ = U^\circ$ et ${}^\circ\mathrm{Vect}(X) = {}^\circ X$.

Exercice 3.11
1. Montrer que si L est une partie libre de E et $S \subset L$, alors S est aussi libre.
2. Montrer que si G est une partie génératrice de E et $G \subset S$, alors S est aussi une partie génératrice de E.
3. Montrer que si B et B' sont deux bases distinctes de E, alors $B \not\subset B'$ et $B' \not\subset B$.

Exercice 3.12
1. On rappelle que, pour tout $i = 1, \dots, n$, on pose $\mathbb{1}_i = (0, \dots, 0, 1, 0, \dots, 0)$ avec 1 à la i-ème place. Montrer que $(\mathbb{1}_1, \dots, \mathbb{1}_n)$ est une base de K^n.
2. On rappelle que, pour tout $i = 1, \dots, n$, on pose $p_i(x_1, \dots, x_n) := x_i$. Montrer que $(p_1, \dots, p_n)$ est une base de l'espace des formes linéaires sur K^n.
3. Peut-on donner une base de $\emptyset$? de $\{0\}$? de K ? de $K^{\mathbb{N}}$ (réfléchir seulement) ?
4. Donner une base de $\mathrm{M}_{n \times m}(K)$.

Exercice 3.13 Donner une base de $\mathbb{C}$ comme espace vectoriel sur $\mathbb{R}$, puis de son dual, puis du quotient $\mathbb{C}/\mathbb{R}$.

Exercice 3.14 Si X est un ensemble quelconque, on note $\mathbb{1}_x : X \to K$ l'unique application telle que

$$\mathbb{1}_x(y) = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{sinon.} \end{cases}$$

Montrer que $\{\mathbb{1}_x\}_{x\in X}$ est une base de $\mathscr{F}_f(X,K) := \{f : X \to K \ \ |\text{supp}(f)| < +\infty\}$. Interprétation en terme de familles.

Exercice 3.15

1. Établir un isomorphisme entre $K^{(\mathbb{N})}$ et $K[T]$ afin de montrer que $\{T^d\}_{d\in\mathbb{N}}$ est une base de $K[T]$.
2. Soit S un ensemble de polynômes non nuls. Montrer que si pour tout $d \in \mathbb{N}$, il existe au plus (resp. au moins, resp. exactement) un $P \in S$ avec $\deg P = d$, alors S est libre (resp. générateur, resp. une base).
3. Dire dans chaque cas si la condition nécessaire.
4. Énoncer les résultats analogues pour le sous-espace $K[T]_{\leq n}$ des polynômes de degré au plus n.

Exercice 3.16 Soit K un corps à q éléments. Combien y a-t-il d'éléments dans K^n ? Montrer qu'il existe exactement

$$(q^n - 1)(q^n - q)(q^n - q^2)\cdots(q^n - q^{r-1})$$

familles libres de r vecteurs dans K^n pour $r \leq n$. Combien y a-t-il de bases ordonnées dans K^n ? Explicitez les cas $n, q \leq 3$ (un corps a au moins 2 éléments).

Exercice 3.17 Soient B_1 et B_2 des bases de sous-espace vectoriels E_1 et E_2 de E. Montrer que $E = E_1 \oplus E_2$ si et seulement si $B_1 \cup B_2$ est une base de E et $B_1 \cap B_2$ est une base de $\{0_E\}$.

Exercice 3.18 Montrer que la famille (v_1, v_2), avec $v_1 := (1,1,1)$ et $v_2 := (1,2,3)$, est libre et compléter en une base de $\mathbb{R}^3$.

Exercice 3.19 Soient F un sous-espace vectoriel de E et $\pi : E \twoheadrightarrow E/F$ l'application quotient.

1. Montrer que si B est une base de E, il existe $L \subset B$ et une base D de E/F telle que π induise une bijection $L \simeq D$.
2. Montrer que si C est une base de F et D une base de E/F, il existe une base B de E tel que $C \subset B$ et π induit une bijection $B \setminus C \simeq D$.

Exercice 3.20 Montrer qu'une application linéaire $\alpha : E \to F$ est injective si et seulement si il existe $\beta : F \to E$ linéaire telle que $\beta \circ \alpha = \text{Id}_E$. Montrer qu'une application linéaire $\beta : E \to F$ est surjective si et seulement si il existe $\alpha : F \to E$ linéaire telle que $\beta \circ \alpha = \text{Id}_F$.

II

Seconde partie

4. Dimension

On fixe toujours un corps de scalaires K.

Remarque On pourra généraliser certaines notions et certains résultats aux modules sur un anneau mais la plupart des énoncés ne sont valides que sur un corps.

4.1 Dimension

Théoreme 4.1.1 Soit E un espace vectoriel. Si L (resp. G) une partie libre (resp. génératrice) de E, alors $\mathrm{card}(L) \leq \mathrm{card}(G)$.

Démonstration. Supposons pour commencer que $\mathrm{card}(L) = m$ et $\mathrm{card}(G) = n$ sont finis, et écrivons

$$L = \{x_1, \ldots, x_m\} \quad \text{et} \quad G = \{y_1, \ldots, y_n\}.$$

On peut toujours supposer que $y_1 = x_1, \ldots, y_r = x_r$ (avec éventuellement $r = 0$). Supposons $r < m$ et écrivons $x_{r+1} = a_1 y_1 + \cdots + a_n y_n$. Il existe nécessairement $k > r$ tel que $a_k \neq 0$ sinon on aurait

$$x_{r+1} = a_1 y_1 + \cdots + a_r y_r = a_1 x_1 + \cdots + a_r x_r,$$

ce qui est impossible car L est libre. On va remplacer y_k par x_{r+1} dans G. Plus précisément, on considère $G' := \{y'_1, \ldots, y'_n\}$ avec

$$y'_i = \begin{cases} x_i & \text{si} \quad 1 \leq i \leq r+1 \\ y_{i-1} & \text{si} \quad r+1 < i \leq k \\ y_i & \text{si} \quad k < i \leq n \end{cases}$$

On a

$$y_k = \sum_{i \neq k} -\frac{a_i}{a_k} y_i + \frac{1}{a_k} x_{r+1} \in \mathrm{Vect}(G')$$

si bien que $G \subset \mathrm{Vect}(G')$ et G' est donc aussi générateur. On peut alors remplacer G par G', et donc r par $r+1$, et ainsi de suite jusqu'à arriver à $r = m$ si bien que $m \leq n$.

Si on suppose maintenant que G est fini mais que L est infini, on arrive à une contradiction : en effet, il suffit de considérer une partie finie de L qui a plus d'éléments que G.

Il reste à traiter le cas ou G est infini. Pour tout $x \in L$, il existe une partie finie $S_x \subset G$ telle que $x \in \mathrm{Vect}(S_x)$. Maintenant, si S est une partie finie de G, on pose $L_S := \{x \in L, S_x = S\} \subset \mathrm{Vect}(S)$. Puisque S et L_S sont finis et que L_S est libre, on a $\mathrm{card}(L_S \leq \mathrm{card}(S)$. D'autre part, on a aussi $L = \cup_S L_S$. On conclut alors par la suite d'inégalités

$$\mathrm{card}(L) \leq \sum_S \mathrm{card}(L_S) \leq \sum_S \mathrm{card}(S) = \mathrm{card}(G),$$

la dernière égalité étant toujours vraie pour un ensemble infini. ■

Corollaire 4.1.2 Deux bases d'un même espace vectoriel E ont même cardinal.

Démonstration. ■

Définition 4.1.3 Soit E un espace vectoriel. Si B est une base de E, alors la *dimension* de E est

$$\dim E := \mathrm{card}(B).$$

On dit que E est une *droite* (resp. un *plan*) si $\dim E = 1$ (resp. $= 2$). Si F est un sous-espace vectoriel de E, la *codimension* de F dans E est

$$\mathrm{codim}_E(F) = \dim E/F.$$

Exemple 1. On a $\dim K^n = n$, et en particulier, $\dim K = 1$ et $\dim\{0\} = 0$. Plus généralement $\dim K^{(S)} = \mathrm{card}(S)$.
2. On a $\dim {}^t K^n = n$, $\dim K^n/K^m = n - m$ et $\dim \mathrm{M}_{n\times m}(K) = mn$.
3. On a $\dim K[T] = \mathrm{card}(\mathbb{N}) < \mathrm{card}(\mathbb{R}) = \dim K^{\mathbb{N}}$.
4. Un espace vectoriel est de dimension n si et seulement si il est isomorphe à K^n. Par exemple, E est une droite (resp. un plan) si et seulement si il est isomorphe à K (resp. K^2). Plus généralement, $\dim E = \mathrm{card}(S)$ si et seulement si $E \simeq K^{(S)}$.
5. On dira que les vecteurs de $X \subset E$ sont *colinéaires* (resp. *coplanaires*) si $\mathrm{Vect}(X)$ est contenu dans une droite (resp. un plan).

Remarque 1. Deux espaces vectoriels sont isomorphes si et seulement si ils ont même dimension :

$$E \simeq F \Leftrightarrow \dim E = \dim F$$

Attention cependant, $K[T]$ et $K^{\mathbb{N}}$, bien que tous deux de dimension infinie, ne sont pas isomorphes.
2. Un sous-espace vectoriel H de E est un hyperplan si et seulement si $\mathrm{codim}_E(H) = 1$.
3. Si A est un anneau, alors un A-module est dit de *type fini* (resp. *libre de rang fini*) s'il existe une partie génératrice (resp. une base) finie.
4. Lorsque A est commutatif, le corollaire 4.1.2 est toujours valide mais on parle alors de *rang* (au lieu de dimension).

On a la conséquence suivante du théorème 4.1.1 :

Corollaire 4.1.4 Soit E un espace vectoriel.
1. Si $L \subset E$ est une partie libre, alors $\mathrm{card}(L) \leq \dim E$.

2. Si $G \subset E$ est une partie génératrice, alors $\operatorname{card}(G) \geq \dim E$.
3. Si $B \subset E$ est une base, alors $\operatorname{card}(B) = \dim E$.

Démonstration. ■

Exemple 1. Les vecteurs $(2,3,5,7),(3,5,7,11),(5,7,11,13),(7,11,13,17),(11,13,17,19)$ sont liés dans $\mathbb{R}^4$.
2. Les polynômes X^3-1, X^3-X et X^3-X^2 n'engendrent pas $\mathbb{R}[X]_{\leq 3}$.

Proposition 4.1.5 Soient E un espace vectoriel *de dimension finie* et $X \subset E$ avec $\operatorname{card}(X) = \dim E$. On a alors

$$X \text{ libre } \Leftrightarrow X \text{ base } \Leftrightarrow X \text{ generateur.}$$

Démonstration. Grâce au théorème de la base incomplète, si X est libre (resp. générateur), il est contenu dans (resp. contient) une base B qui a même nombre d'éléments que X et on a donc $X = B$ (car ce sont des ensembles finis). . ■

Remarque 1. Ce résultat est faux en dimension infinie.
2. Inversement, si $\operatorname{card}(X) > \dim E$, alors X est lié et si $\operatorname{card}(X) < \dim E$, alors $\operatorname{Vect}(X) \neq E$ (ces résultats sont encore valides en dimension infinie par contre).

Proposition 4.1.6 Soit $u : E \to F$ une application linéaire.
1. (a) Si u est injective, alors $\dim E \leq \dim F$,
   (b) Si u est surjective, alors $\dim E \geq \dim F$,
   (c) Si u est bijective, alors $\dim E = \dim F$.
2. Si E et F sont de *même dimension finie*, on a

$$u \text{ injective } \Leftrightarrow u \text{ bijective } \Leftrightarrow u \text{ surjective.}$$

Démonstration. 1. Soit B une base de E. On a toujours $\operatorname{card}(B) \geq \operatorname{card}(u(B))$ et on sait que si u est surjective, alors $u(B)$ est générateur. Il suit que

$$\dim E = \operatorname{card}(B) \geq \operatorname{card}(u(B)) \geq \dim F.$$

Si u est injective, on a en fait $\operatorname{card}(B) = \operatorname{card}(u(B))$ et on sait aussi que $u(B)$ est libre si bien que

$$\dim E = \operatorname{card}(B) = \operatorname{card}(u(B)) \leq \dim F.$$

2. Si $\dim E = \dim F$, on obtient dans les deux cas une suite d'égalités

$$\dim E = \operatorname{card}(B) = \operatorname{card}(u(B)) = \dim F,$$

et en dimension finie, on conclut en appliquant la proposition 4.1.5 à $u(B)$. ■

Remarque 1. Comme cas particulier important, on voit que si E un espace vectoriel *de dimension finie* et $u \in \mathrm{L}(E)$, on a la suite d'équivalences de la seconde partie de la proposition 4.1.6.
2. Par contre, ce n'est plus vrai en dimension infinie.

Corollaire 4.1.7 Soient $A, B \in \mathrm{M}_n(K)$. Si $AB = I$, alors $A, B \in \mathrm{GL}_n(K)$, $A^{-1} = B$ et $B^{-1} = A$.

Démonstration. Soient $u, v \in \mathrm{L}(K^n)$ les endomorphismes correspondants à A et B respectivement. On a alors $u \circ v = \mathrm{Id}$ et il suit que v est injective et u est surjective. Ces applications sont donc toutes deux bijectives grâce à la proposition 4.1.6 et il suit que et A et B sont inversibles. ■

Remarque
1. Rappelons que dans un monoïde G, un élément g est inversible s'il existe un autre élément h (que l'on note ensuite g^{-1}) tel que $gh = hg = 1$. La condition $gh = 1$ n'implique pas forcément la condition symétrique $hg = 1$. Ce corollaire nous dit que c'est cependant le cas pour les matrices.
2. Même dans le cas $n = 2$, le fait que $AB = I$ implique $BA = I$ est loin d'être immédiat.
3. Ce corollaire illustre le fait que l'on peut obtenir des propriétés fondamentales des matrices grâce à la théorie des applications linéaires.
4. Plus généralement, si on a $u \circ v = \mathrm{Id}$ dans $\mathrm{L}(E)$ alors $u \in \mathrm{GL}(E)$ lorsque E est de dimension finie.
5. Ce dernier énoncé est faux en dimension infinie.

Corollaire 4.1.8 Soient E un espace vectoriel *de dimension finie* et $u \in \mathrm{L}(E)$. Soit E' un sous-espace vectoriel de E stable par u. Soient $u' \in \mathrm{L}(E')$ et $u'' \in \mathrm{L}(E/E')$ les application induites. On a alors

$$u \in \mathrm{GL}(E) \Leftrightarrow u' \in \mathrm{GL}(E') \text{ et } u'' \in \mathrm{GL}(E/E').$$

Démonstration. Puisque les espaces sont de dimension finie, les notions d'injectivité, surjectivité et bijectivité coïncident et l'assertion est alors une conséquence immédiate de la remarque suivant la proposition 2.6.7. ■

Remarque
1. Le couple (E, u) peut-être vu comme un $K[T]$-module, le couple (E', u') comme un sous-module de (E, u) et le couple $(E/E', u'')$ correspond alors vraiment au quotient des modules.
2. Comme conséquence du corollaire, si on se donne une matrice triangulaire par blocs

$$A = \begin{bmatrix} A' & \star \\ 0 & A'' \end{bmatrix}$$

on voit que A est inversible si et seulement si A' et A'' sont inversibles (quoi qu'il y ait en haut à droite).

4.2 Rang

Proposition 4.2.1 Si $(E_s)_{s \in S}$ est une famille d'espaces vectoriels sur K, on a

$$\dim \bigoplus_{s \in S} E_s = \sum_{s \in S} \dim E_s.$$

Démonstration. On se donne pour tout $s \in S$ une base B_s de E_s et on pose $B := \sqcup_{s \in S} B_s$. Il résulte alors formellement des propriétés universelles de la somme directe que $K^{(B)} \simeq \oplus_{s \in S} K^{(B_s)}$ (exercice). ■

Exemple
1. Si $E_1, \ldots, E_n$ sont des espaces vectoriels, alors

$$\dim(E_1 \times \cdots \times E_n) = \dim E_1 + \cdots + \dim E_n.$$

2. C'est faux en dimension infinie : $\dim \prod_{s\in S} E_S \neq \sum_{s\in S} \dim E_s$.
3. Si les E_s sont supplémentaires dans un espace vectoriel E, alors $\dim E = \sum_{s\in S} \dim E_s$.

Corollaire 4.2.2 Si F est un sous-espace vectoriel d'un espace vectoriel E, alors

$$\dim E = \dim F + \operatorname{codim}_E(F)$$

Démonstration. On sait que si G est un supplémentaire pour F, on a un isomorphisme $G \simeq E/F$ si bien que $\dim G = \dim E/F = \operatorname{codim}_E(F)$. On aura donc

$$\dim F + \operatorname{codim}_E(F) = \dim F + \dim G = \dim E. \quad \blacksquare$$

Théoreme 4.2.3 — du rang. Si $u : E \to F$ est une application linéaire, alors

$$\dim E = \dim \ker u + \dim \operatorname{im} u.$$

Démonstration. On dispose de l'isomorphisme de Noether $E/\ker u \simeq \operatorname{im} u$ et on en déduit que $\operatorname{codim}_E(\ker u) = \dim \operatorname{im} u$. ■

Corollaire 4.2.4 — Relation de Grassmann. Si F et G sont deux sous-espaces vectoriels de E, on a

$$\dim F + \dim G = \dim(F+G) + \dim(F\cap G).$$

Démonstration. Résulte du second théorème d'isomorphie de Noether. ■

Remarque 1. Une *suite exacte courte* est une suite d'applications linéaires

$$E' \xrightarrow{\iota} E \xrightarrow{\pi} E''$$

avec ι injective, $\operatorname{im} \iota = \ker \pi$ et π surjective. On a alors

$$\dim E = \dim E' + \dim E''.$$

2. Plus généralement, une *suite exacte longue* est une suite d'applications linéaires $u_i : E_i \to E_{i+1}$ telles que $\operatorname{im} u_i = \ker u_{i+1}$. Si les espaces E_i sont de dimension finie et presque tous nuls, on aura

$$\sum_{i\in\mathbb{N}} (-1)^i \dim E_i = 0.$$

Définition 4.2.5 1. Si $u : E \to F$ est une application linéaire, alors le *rang* de u est

$$\operatorname{rang}(u) := \dim \operatorname{im} u.$$

2. Si E est un espace vectoriel et $X \subset E$, alors le *rang* de X est le rang de l'application habituelle

$$\Phi : K^{(X)} \to E, \quad (a_x)_{x\in X} \mapsto \sum_{x\in X} a_x x.$$

Remarque 1. Le théorème du rang nous dit donc que si $u : E \to F$ est une application linéaire, on a

$$\dim E = \dim \ker u + \operatorname{rang}(u).$$

2. Si X est une partie d'un espace vectoriel E, on a
$$\operatorname{rang}(X) = \dim \operatorname{Vect}(X).$$
3. On définit de même le rang d'une famille $(x_s)_{s\in S}$ de vecteurs d'un espace vectoriel E en considérant l'application
$$K^{(S)} \to E, \quad (a_s)_{s\in S} \mapsto \sum_{s\in S} a_s x_s$$
si bien que
$$\operatorname{rang}((x_s)_{s\in S}) = \dim \operatorname{Vect}((x_s)_{s\in S}).$$
4. On remarquera que si E est un espace vectoriel quelconque, alors $\operatorname{rang}(E) = \dim(E)$ puisque $\operatorname{Vect}(E) = E$. Autrement dit, on pourrait se passer de la notion de dimension qui devient un cas particulier de celle de rang. C'est d'ailleurs ce que l'on fait en théorie des modules sur un anneau.
5. Si $u : E \to F$ est une application linéaire et G est une partie génératrice de E, on a alors $\operatorname{rang}(u) = \operatorname{rang}(X)$ avec $X := u(G)$,
6. Comme d'habitude, on définit le *rang d'une matrice* A comme étant le rang de l'application linéaire $u : K^m \to K^n$ correspondante. Si X désigne l'ensemble des colonnes de A, on aura donc aussi
$$\operatorname{rang}(A) = \operatorname{rang}(X).$$
Pour $A \in \mathrm{M}_n(K)$, on a
$$\operatorname{rang}(A) = n \Leftrightarrow A \in \mathrm{GL}_n(K).$$
7. Le *rang du système linéaire*
$$\mathscr{S} := \begin{cases} a_{1,1}x_1 \cdots + a_{1,m}x_m & = & b_1 \\ & \vdots & \\ a_{n,1}x_1 \cdots + a_{n,m}x_m & = & b_n. \end{cases}$$
est le rang de la matrice $A := [a_{i,j}]$ associée. Si on pose pour tout $i = 1, \ldots, n$,
$$\varphi_i := a_{i,1}p_1 + \cdots + a_{i,m}p_m \in {}^tK^m$$
et $U := \{\varphi_1, \ldots, \varphi_n\}$, on verra aussi que
$$\operatorname{rang}(\mathscr{S}) = \operatorname{rang}(U).$$

Proposition 4.2.6 Soit $u : E \to F$ une application linéaire.
1. On a toujours $\operatorname{rang}(u) \leq \dim F$. Si de plus, u est surjective, alors $\operatorname{rang}(u) = \dim F$ et la réciproque est vraie si F est de dimension *finie*.
2. On a toujours $\operatorname{rang}(u) \leq \dim E$. Si u est injective, alors $\operatorname{rang}(u) = \dim E$ et la réciproque est vraie si E est de dimension *finie*.

Démonstration. 1. Comme $\operatorname{im} u \subset F$, on a $\operatorname{rang}(u) \leq \dim F$. D'autre part, on sait que u est surjective si et seulement si $\operatorname{im} u = F$. De plus, cette dernière condition implique que $\operatorname{rang}(u) = \dim F$; et la réciproque est vraie si ce nombre est fini.
2. Il résulte du théorème du rang que $\operatorname{rang}(u) \leq \dim E$. D'autre part, on sait que u est injective si et seulement si $\ker u = \{0\}$. Toujours d'après le théorème du rang, cette dernière condition implique que $\dim E = \operatorname{rang}(u)$; et la réciproque est vraie si ce nombre est fini.

■

Corollaire 4.2.7 Si X est une partie d'un espace vectoriel E, on a $\mathrm{rang}(X) \leq \mathrm{card}(X)$ et $\mathrm{rang}(X) \leq \dim E$. De plus,

1. Si X est libre, alors $\mathrm{rang}(X) = \mathrm{card}(X)$.
2. Si X est générateur, alors $\mathrm{rang}(X) = \dim E$.

Dans les deux cas, la réciproque est vraie si $\mathrm{rang}(X)$ est fini, et en particulier, si X ou $\dim E$ est *fini*.

Démonstration. ■

Remarque On peut aussi donner une démonstration directe de ce corollaire. Par définition, X est une partie génératrice de $F := \mathrm{Vect}(X)$ et on a $\mathrm{rang}(X) := \dim F$. Comme X est génératrice, on a bien $\dim F \leq \mathrm{card}(X)$ et comme $F \subset E$, on a $\dim F \leq \dim E$.

1. Supposons que X soit libre. Alors c'est une base de F et on a donc $\mathrm{card}(X) = \dim F$. Réciproquement, supposons que $\mathrm{card}(X) = \dim F$ et que ce nombre soit fini. Alors, comme X est générateur de F, c'est nécessairement une base de F et il est donc libre.
2. Supposons maintenant que X engendre E. Nous sommes alors dans le cas $F = E$ et on a donc bien sûr $\dim F = \dim E$. Réciproquement, si $\dim F = \dim E$ et que ce nombre est fini, comme F est un sous-espace vectoriel de E, on a obligatoirement $F = E$.

Proposition 4.2.8 Soient $u : E \to F$ et $v : F \to G$ deux applications linéaires. Alors,

1. si u est surjective, $\mathrm{rang}(v \circ u) = \mathrm{rang}(v)$.
2. si v est injective, $\mathrm{rang}(v \circ u) = \mathrm{rang}(u)$.

Démonstration. En effet, si u est surjective, alors $\mathrm{im}(v \circ u) = \mathrm{im}(v)$ et si v est injective, alors $\mathrm{im}(v \circ u) = v(\mathrm{im}\, u) \simeq \mathrm{im}\, u$ (exercice). ■

Remarque
1. Comme conséquence, on voit que si $A \in \mathrm{M}_{n\times m}(K)$ et $P \in \mathrm{GL}_n(K)$ (resp. $P \in \mathrm{GL}_m(K)$), alors
$$\mathrm{rang}(PA) = \mathrm{rang}(A), \quad (\text{resp.} \quad \mathrm{rang}(AP) = \mathrm{rang}(A)).$$
2. En particulier, une suite d'opérations élémentaires ne change pas le rang d'une matrice. En effet, opérer sur les lignes (resp. colonnes) revient à multiplier à gauche (resp. droite) par une matrice inversible (celle obtenue en faisant les mêmes opérations sur la matrice unité I).

4.3 Changement de base

Dans cette section, tous les espaces sont **de dimension finie**.

Remarque Le contenu de cette section (à part le dernier résultat qui s'appuie sur l'algorithme du pivot de Gauss) s'applique mutatis mutandis aux modules libres de rang fini sur un anneau commutatif.

On rappelle qu'une *base ordonnée* d'un espace vectoriel (de dimension finie) E sur K est une famille $\mathscr{B} := (e_1, \dots, e_n)$ de vecteurs de E telle que l'unique application linéaire $\Phi : K^n \to E, \mathbb{1}_i \mapsto e_i$ soit bijective. L'application réciproque $\Phi^{-1} : E \to K^n$ est celle qui envoie un vecteur x sur ses composantes $(x_1, \dots, x_n)$ dans la base B.

Définition 4.3.1 Soient $u : E \to F$ une application linéaire, $\mathscr{B}$ (resp. $\mathscr{C}$) une base ordonnée de E (resp. F) et $\Phi : K^m \simeq E$ (resp. $\Psi : K^n \simeq F$) l'isomorphisme associé. Alors, la *matrice de u* *dans les base $\mathscr{B}$ et $\mathscr{C}$* est

$$[u]_{\mathscr{C}}^{\mathscr{B}} \left(:= \mathrm{Mat}_{\mathscr{C}}^{\mathscr{B}}(u)\right) := [\Psi^{-1} \circ u \circ \Phi].$$

Remarque 1. Lorsque $E = F$ et $\mathscr{B} = \mathscr{C}$, on écrira $[u]_{\mathscr{B}}$ (ou $\mathrm{Mat}_{\mathscr{B}}(u)$) tout simplement si bien que

$$[u]_{\mathscr{B}} = [\Phi^{-1} \circ u \circ \Phi].$$

et on dira que c'est la *matrice de u dans la base $\mathscr{B}$*.

2. Si on utilise comme d'habitude l'isomorphisme canonique $\mathrm{L}(K,E) \simeq E$ pour voir n'importe quel $x \in E$ comme une application linéaire $i_x : K \to E$, et qu'on munit K de sa base canonique, la *matrice de x dans la base $\mathscr{B}$* est est donc le vecteur colonne

$$[x]_{\mathscr{B}} := [i_x]_{\mathscr{B}}^{\mathrm{can}} = [\Phi^{-1}(x)]$$

3. Si $\mathscr{B} = (e_1, \dots, e_n)$ est une base de E, on aura

$$x = x_1 e_1 + \cdots + x_n e_n \Leftrightarrow [x]_{\mathscr{B}} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Autrement dit, la matrice de x est le vecteur colonne des composantes de x dans la base $\mathscr{B}$.

4. On en déduit que, si on note $\mathscr{B} = (e_1, \dots, e_m)$ et $\mathscr{C} = (f_1, \dots, f_n)$ des bases de E et F respectivement, alors

$$[u]_{\mathscr{C}}^{\mathscr{B}} = [[u(e_1)]_{\mathscr{C}} \cdots [u(e_m]_{\mathscr{C}}].$$

Autrement dit, les colonnes de la matrice de u sont les matrices dans la base $\mathscr{C}$ des images par u des vecteurs de la base $\mathscr{B}$. On a donc

$$[u]_{\mathscr{C}}^{\mathscr{B}} = [a_{i,j}] \Leftrightarrow \forall j = 1, \dots, m, u(e_j) = a_{1,j} f_1 + \cdots + a_{n,j} f_n.$$

Exemple 1. La matrice de la dérivation $K[T] \leq n+1 \to K[T]_{\leq n-1}, P \mapsto P'$ dans les bases canoniques est

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & 2 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & n \end{bmatrix}.$$

2. La matrice de la conjugaison complexe dans la base canonique de $\mathbb{C}$ est $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Proposition 4.3.2 Soient $u : E \to F$ et $v : F \to G$ deux applications linéaires et $\mathscr{B}, \mathscr{C}, \mathscr{D}$ des bases ordonnées de E, F, G respectivement. On a alors

$$[v \circ u]_{\mathscr{D}}^{\mathscr{B}} = [v]_{\mathscr{D}}^{\mathscr{C}} [u]_{\mathscr{C}}^{\mathscr{B}}.$$

Démonstration. Si on désigne par $\Phi : K^m \simeq E$, $\Psi : K^n \simeq F$ et $R : K^p \simeq G$ les isomorphismes associés respectivement aux bases $\mathscr{B}, \mathscr{C}, \mathscr{D}$, on a

$$\begin{aligned} [v]_{\mathscr{D}}^{\mathscr{C}} [u]_{\mathscr{C}}^{\mathscr{B}} &= [R^{-1} \circ v \circ \Psi][\Psi^{-1} \circ u \circ \Phi] \\ &= [R^{-1} \circ v \circ \Psi \circ \Psi^{-1} \circ u \circ \Phi] \\ &= [R^{-1} \circ (v \circ u) \circ \Phi] \\ &= [v \circ u]_{\mathscr{D}}^{\mathscr{B}}. \end{aligned}$$

■

Remarque 1. On voit donc que le choix des bases nous fournit un isomorphisme d'espaces vectoriels
$$\mathrm{L}(E,F) \simeq \mathrm{M}_{n\times m}(K)$$
et que la composition des applications correspond à la multiplication des matrices.
2. À toute une base ordonnée $\mathscr{B}$ d'un espace vectoriel E de dimension n, on peut donc associer, grâce à la proposition, un isomorphisme d'algèbres
$$\mathrm{L}(E) \simeq \mathrm{M}_n(K), \quad u \mapsto [u]_{\mathscr{B}}$$
et donc aussi un isomorphisme de groupes
$$\mathrm{GL}(E) \simeq \mathrm{GL}_n(K), \quad u \mapsto [u]_{\mathscr{B}}.$$
3. Comme cas particulier de la proposition, on voit que si $x \in E$, on aura
$$[u(x)]_{\mathscr{C}} = [u]_{\mathscr{C}}^{\mathscr{B}}[x]_{\mathscr{B}}.$$
Cela signifie que si $\mathscr{B} = (e_1,\dots,e_m)$, $\mathscr{C} = (f_1,\dots,f_n)$ et la matrice de u dans les bases $\mathscr{B}$ et $\mathscr{C}$ est $[a_{i,j}]$, on aura
$$u\left(\sum_{j=1}^{m} x_j e_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}x_j f_i.$$
Autrement dit, si les composantes de x sont $(x_1,\dots,x_m)$, alors celles de $u(x)$ seront
$$(a_{1,1}x_1+\cdots+a_{1,m}x_m,\dots,a_{n,1}x_1+\cdots+a_{n,m}x_m).$$

Définition 4.3.3 Soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases d'un même espace vectoriel E. La *matrice de passage* de $\mathscr{B}$ à $\mathscr{B}'$ est la matrice
$$P := [\mathrm{Id}_E]_{\mathscr{B}}^{\mathscr{B}'}.$$
On dit que $\mathscr{B}'$ est la *nouvelle base* et que $\mathscr{B}$ est l'*ancienne base*.

Remarque 1. Attention : on munit l'espace de départ de la *nouvelle* base $\mathscr{B}'$ et l'espace d'arrivée de l'*ancienne* base $\mathscr{B}$. Autrement dit si $\mathscr{B} = (e_1,\dots,e_n)$ et $\mathscr{B}' = (e'_1,\dots,e'_n)$, on a
$$P = \left[[e'_1]_{\mathscr{B}}\cdots[e'_n]_{\mathscr{B}}\right].$$
On écrit donc les vecteurs de la nouvelle base en colonnes en les exprimant dans l'ancienne base.
2. Lorsque $E = K^n$ est muni de sa base canonique et qu'on considère une autre base $\mathscr{B} = (e_1,\dots,e_n)$, la matrice de passage sera donc naturellement $P = [[e_1]\cdots[e_n]]$.

Proposition 4.3.4 Si $\mathscr{B}$ et $\mathscr{B}'$ sont deux bases d'un même espace vectoriel E, alors la matrice de passage P de $\mathscr{B}$ à $\mathscr{B}'$ est inversible et P^{-1} est la matrice de passage de $\mathscr{B}'$ à $\mathscr{B}$.

Démonstration. Il suffit de remarquer que
$$[\mathrm{Id}_E]_{\mathscr{B}}^{\mathscr{B}'}[\mathrm{Id}_E]_{\mathscr{B}'}^{\mathscr{B}} = [\mathrm{Id}_E\circ\mathrm{Id}_E]_{\mathscr{B}}^{\mathscr{B}} = [\mathrm{Id}_E]_{\mathscr{B}} = I$$
(et inversement). ■

Proposition 4.3.5 Soient $u : E \to F$ une application linéaire, $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E, P la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$, $\mathscr{C}$ et $\mathscr{C}'$ deux bases de F, Q la matrice de passage de $\mathscr{C}$ à $\mathscr{C}'$, A la matrice de u dans les bases $\mathscr{B}$ et $\mathscr{C}$ et enfin A' la matrice de u dans les bases $\mathscr{B}'$ et $\mathscr{C}'$. On a alors

$$A' = Q^{-1}AP.$$

Démonstration. Il suffit de calculer

$$[\mathrm{Id}_F]_{\mathscr{C}'}^{\mathscr{C}}[u]_{\mathscr{C}}^{\mathscr{B}}\mathrm{Id}_E]_{\mathscr{B}}^{\mathscr{B}'} = [\mathrm{Id}_F \circ u \circ \mathrm{Id}_E]_{\mathscr{C}'}^{\mathscr{B}'} = [u]_{\mathscr{C}'}^{\mathscr{B}'}. \quad \blacksquare$$

Remarque
1. S'il existe deux matrices inversibles P, Q telles que $A' = Q^{-1}AP$, on dit que A et A' sont *équivalentes*. On voit donc que les matrices d'une même application linéaires dans différentes bases sont toujours équivalentes (à défaut d'être égales).
2. La réciproque aussi est vraie : si $A = [u]_{\mathscr{C}}^{\mathscr{B}}$ avec $u \in L(E,F)$ et A' est équivalente à A, alors il existe d'autres bases $\mathscr{B}'$ et $\mathscr{C}'$ telles que $A' = [u]_{\mathscr{C}'}^{\mathscr{B}'}$.
3. Comme cas particulier de la proposition, on a le résultat suivant : soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases d'un même espace vectoriel E et $u \in L(E)$. Soit A (resp. A') la matrice de u dans $\mathscr{B}$ (resp. $\mathscr{B}'$). On a alors
$$A' = P^{-1}AP.$$
4. S'il existe une matrice inversible P telles que $A' = P^{-1}AP$, on dit que A et A' sont *semblables*. On voit donc que les matrices d'un même endomorphisme dans deux bases différentes sont toujours semblables.
5. La réciproque aussi est vraie : si $A = [u]_{\mathscr{B}}$ avec $u \in L(E)$ et A' est semblable à A, alors il existe une autre base $\mathscr{B}'$ de E telle que $A' = [u]_{\mathscr{B}'}$.

Proposition 4.3.6 Deux matrices sont équivalentes si et seulement si elles ont même rang.

Démonstration. On a vu dans la remarque suivant la proposition 4.2.8 que le rang ne change pas quand on multiplie à droite ou à gauche par une matrice inversible. Inversement, si on se donne une matrice quelconque A, la méthode du pivot de Gauss nous permet d'opérer sur les lignes *et* sur les colonnes de A pour obtenir la matrice par blocs

$$\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}.$$

Or une opération élémentaire n'est rien d'autre qu'une multiplication par une matrice élémentaire, qui est toujours inversible. Deux matrices de rang r seront donc équivalentes à la même matrice, et donc équivalentes entre elles. $\blacksquare$

4.4 Dual (fin)

Lemme 4.4.1 Soient E un espace vectoriel et $\mathscr{B} := (e_i)_{i\in I}$ une base ordonnée de E. Alors,
1. il existe pour tout $i \in I$ un unique ${}^te_i \in {}^tE$ tel que
$$\forall i, j \in I, \quad {}^te_i(e_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$$
2. La famille ${}^t\mathscr{B} := ({}^te_i)_{i\in I}$ est libre dans ${}^tE$.
3. Si $x \in E$, alors ${}^te_i(x)$ est la i-ème composante de x et on a donc
$$x = \sum_{i\in I} {}^te_i(x)e_i. \tag{4.1}$$

4. Si E est de dimension finie, alors on a pour tout $\varphi \in {}^tE$,

$$\varphi = \sum_{i\in I} \varphi(e_i)\,{}^te_i. \tag{4.2}$$

Démonstration. 1. L'existence comme l'unicité des ${}^te_i$ résultent de la propriété universelle des bases (première assertion de la proposition 3.3.10).

2. Supposons que $\sum_{i\in I} a_i{}^te_i = 0$ dans ${}^tE$. On aura alors pour tout $j \in I$,

$$0 = \left(\sum_{i\in I} a_i{}^te_i\right)(e_j) = \sum_{i\in I} a_i{}^te_i(e_j) = a_j.$$

3. Si $x \in E$, on peut écrire $x = \sum_{i\in I} x_i e_i$ avec $x_i \in K$, et on aura donc pour tout $i \in I$,

$${}^te_i(x) = {}^te_i\left(\sum_{j\in I} x_j e_j\right) = \sum_{j\in I} x_j{}^te_i(e_j) = x_i.$$

On en déduit la formule (4.1).

4. Si $x \in E$, on a

$$\left(\sum_{i\in I} \varphi(e_i){}^te_i\right)(x) = \sum_{i\in I} \varphi(e_i){}^te_i(x) = \sum_{i\in I} {}^te_i(x)\varphi(e_i) = \varphi\left(\sum_{i\in I} {}^te_i(x)e_i\right) = \varphi(x).$$

■

Remarque Si on désigne par $\Phi : K^{(I)} \simeq E$ l'isomorphisme donné par la base $\mathscr{B}$, alors les formes linéaires ${}^te_i$ sont les composantes de l'application $\Phi^{-1} : E \to K^{(I)}$.

Proposition 4.4.2 Si E est un espace vectoriel *de dimension finie* alors ${}^tE$ aussi et on a

$$\dim {}^tE = \dim E.$$

En fait, si $\mathscr{B}$ est une base de E, alors ${}^t\mathscr{B}$ est une base de ${}^tE$. De plus, l'application canonique $E \to {}^{tt}E$ est un isomorphisme.

Démonstration. Si $\mathscr{B}$ est une base de E, alors ${}^t\mathscr{B}$ est libre comme on l'a vu dans le lemme en 2) et engendre ${}^tE$ grâce à l'assertion 4) du même lemme. C'est donc bien une base. Pour montrer la dernière assertion, on utilise d'abord la première partie qui nous dite que $\dim {}^{tt}E = \dim {}^tE = \dim E$. Comme on sait que l'application canonique $E \to {}^{tt}E$ est linéaire et injective par le corollaire 3.5.8, c'est un isomorphisme grâce à la partie 2) de la proposition 4.1.6. ■

Exemple 1. La base duale de la base canonique $(\mathbb{1}_n, \ldots, \mathbb{1}_n)$ de K^n est $(p_1, \ldots, p_n)$.

2. La base duale de la base canonique $(1, i)$ de $\mathbb{C}$ sur $\mathbb{R}$ est $(\Re, \Im)$.

Proposition 4.4.3 Soient $u : E \to F$ une application linéaire entre espaces vectoriels de dimension finies et $\mathscr{B}, \mathscr{C}$ des bases de E et F respectivement. Si A est la matrice de u dans les bases $\mathscr{B}$ et $\mathscr{C}$, alors la matrice ${}^tu$ dans les bases ${}^t\mathscr{C}$ et ${}^t\mathscr{B}$ est ${}^tA$.

Démonstration. On écrit comme d'habitude $\mathscr{B} := (e_1, \ldots, e_m)$ et $\mathscr{C} := (f_1, \ldots, f_n)$. On sait que l'on a toujours $u(e_j) = a_{1,j}f_1 + \cdots + a_{n,j}f_n$ et on veut montrer l'égalité ${}^tu({}^tf_i) = a_{i,1}{}^te_1 + \cdots + a_{i,m}{}^te_m$. En utilisant la formule (4.2), il suffit de remarquer que

$${}^tu({}^tf_i)(e_j) = {}^tf_i(u(e_j)) = {}^tf_i\left(\sum_{k=1}^n a_{k,j}f_k\right) = \sum_{k=1}^n a_{k,j}{}^tf_i(f_k) = a_{i,j}. \quad ■$$

Remarque 1. L'égalité (4.2) nous montre que si $\mathscr{B}$ est une base d'un espace vectoriel de dimension finie E et que $\varphi \in {}^tE$, on a

$$[\varphi]_{^t\mathscr{B}} = {}^t[\varphi]^{\mathscr{B}}_{\text{can}},$$

(formule à rapprocher de $[x]_{\mathscr{B}} = [i_x]^{\text{can}}_{\mathscr{B}}$).

2. Si $\mathscr{B}$ et $\mathscr{B}' := (e'_i)_{i=1}^n$ sont deux bases d'un même espace vectoriel de dimension finie E, la matrice de passage de $\mathscr{B}'$ à $\mathscr{B}$ est

$$P^{-1} = \begin{bmatrix} [{}^te'_1]^{\mathscr{B}}_{\text{can}} \\ \vdots \\ [{}^te'_n]^{\mathscr{B}}_{\text{can}} \end{bmatrix}.$$

3. Dans le cas ou on passe de la base canonique de K^n à une nouvelle base $\mathscr{B} := (e_i)_{i=1}^n$, la formule devient

$$P^{-1} = \begin{bmatrix} [{}^te_1] \\ \vdots \\ [{}^te_n] \end{bmatrix}.$$

et on retrouve la définition de la base duale en effectuant le produit $P^{-1}P = I$.

Corollaire 4.4.4 Soient E un espace vectoriel et F un sous-espace vectoriel *de codimension finie*. On a alors

$$\dim F + \dim {}^\circ F = \dim E.$$

Démonstration. On a vu dans la proposition 2.6.6 que ${}^\circ F \simeq {}^t(E/F)$ et on a donc en particulier $\dim {}^\circ F = \dim {}^t(E/F)$. D'autre part, on suppose que $\dim E/F := \operatorname{codim}_E(F)$ est finie si bien que $\dim {}^t(E/F) = \dim E/F$. Finalement, on a vu dans le corollaire 4.2.2 que $\dim F + \operatorname{codim}_E(F) = \dim E$. ∎

Lemme 4.4.5 Soit E un espace vectoriel de dimension finie. Si $U \subset {}^tE$, l'isomorphisme canonique $E \simeq {}^{tt}E, x \mapsto p_x$ induit un isomorphisme $U^\circ \simeq {}^\circ U$. De plus, on a ${}^\circ(U^\circ) = ({}^\circ U)^\circ$.

Démonstration. Par définition, on a $p_x(\varphi) = \varphi(x)$ si $x \in E$ et $\varphi \in {}^tE$. On voit donc que $x \in U^\circ \Leftrightarrow p_x \in {}^\circ U$. Et on en déduit alors que

$$\begin{aligned} \varphi \in {}^\circ(U^\circ) &\Leftrightarrow \forall x \in U^\circ, \quad \varphi(x) = 0 \\ &\Leftrightarrow \forall x \in U^\circ, \quad p_x(\varphi) = 0 \\ &\Leftrightarrow \forall u \in {}^\circ U \quad u(\varphi) = 0 \\ &\Leftrightarrow \varphi \in ({}^\circ U)^\circ. \end{aligned}$$

∎

Théoreme 4.4.6 Si E est un espace vectoriel de dimension finie, on dispose d'une bijection

$$\begin{array}{c} F \longmapsto {}^\circ F \\ \{\text{sous-espaces vectoriels de } E\} \rightleftarrows \{\text{sous-espaces vectoriels de } {}^tE\} \\ U^\circ \longleftarrow U \end{array}$$

qui renverse l'ordre et échange somme et intersection.

Démonstration. Grâce à la proposition 4.4, il faut juste s'assurer que les deux applications sont réciproques l'une de l'autre. Or, on a vu dans la proposition 3.5.5 que si F est un sous-espace vectoriel de E, alors $(^\circ F)^\circ = F$. En appliquant cela à $U \subset {}^tE$ et en utilisant le lemme, on obtient aussi $U = {}^\circ(U^\circ)$. ■

Nous avons vu dans la proposition 2.5.4 et dans la seconde partie de la proposition que si $u : E \to F$ est une application linéaire, on a

$$\ker {}^t u = {}^\circ \mathrm{im}\, u \quad \text{et} \quad \mathrm{im}\, {}^t u = {}^\circ \ker u.$$

On en déduit alors :

Corollaire 4.4.7 Si $u : E \to F$ est une application linéaire entre espaces vectoriels de dimension finie, on a

$$\ker u = (\mathrm{im}\, {}^t u)^\circ \quad \text{et} \quad \mathrm{im}\, u = (\ker {}^t u)^\circ.$$

Démonstration. ■

Corollaire 4.4.8 Soit $u : E \to F$ une application linéaire entre espaces vectoriels de dimension finie. On a alors

1. u injective $\Leftrightarrow {}^t u$ surjective.
2. u surjective $\Leftrightarrow {}^t u$ injective.
3. u bijective $\Leftrightarrow {}^t u$ bijective.

Démonstration. ■

Corollaire 4.4.9 Si $u : E \to F$ est une application linéaire entre espaces vectoriels de dimension finie, on a

$$\mathrm{rang}\, {}^t u = \mathrm{rang}\, u.$$

Démonstration. ■

Remarque Comme cas particulier, on voit que si A est une matrice quelconque, alors

$$\mathrm{rang}\, {}^t A = \mathrm{rang}\, A$$

Autrement dit, le nombre maximum de lignes indépendantes est égal au nombre maximal de colonnes indépendantes. Voici encore un résultat qui est loin d'être évident, et que nous déduisons du formalisme général.

Corollaire 4.4.10 Soient E un espace vectoriel de dimension finie et U un sous-espace vectoriel de ${}^t E$. On a alors

$$\dim U + \dim U^\circ = \dim E.$$

Démonstration. ■

Exemple Si $\mathscr{S}$ est un système linéaire homogène de rang r à n variables, alors $\mathrm{Sol}(\mathscr{S})$ est un espace vectoriel de dimension $n - r$.

4.5 Exercices

Exercice 4.1
1. Quelle est la dimension de K^n ?
2. Quelle est la dimension de ${}^tK^n$?
3. Quelle est la dimension de $K[T]$?
4. Quelle est la dimension de $K[T]_{\leq n}$?
5. Quelle est la dimension de $K[T]/(P)$ si P est un polynôme de degré n ?
6. Quelle est la dimension de $\mathrm{M}_{n\times m}(K)$?
7. Quelle est la dimension de K^n/K^m ?

Exercice 4.2
1. Quelle est la dimension de $\mathbb{C}$ comme espace vectoriel sur $\mathbb{C}$?
2. Quelle est la dimension de $\mathbb{C}$ comme espace vectoriel sur $\mathbb{R}$?
3. Quelle est la dimension de $\mathbb{C}$ comme espace vectoriel sur $\mathbb{Q}$?

Exercice 4.3
1. Les vecteurs
$$(2,3,5,7),(3,5,7,11),(5,7,11,13),(7,11,13,17),(11,13,17,19)$$
sont ils linéairement indépendants ?
2. Les polynômes X^3-1, X^3-X et X^3-X^2 engendrent-ils $\mathbb{R}[X]_{\leq 3}$?

Exercice 4.4 On désigne par B la base canonique de $K[T]$.
1. Montrer que $L := B\setminus\{T\}$ est libre dans $K[T]$ et que $\mathrm{card}(L) = \dim K[T]$. Est-ce que L est une base de $K[T]$?
2. Montrer que $G := B\cup\{T-1\}$ est génératrice de $K[T]$ et que $\mathrm{card}(G) = \dim K[T]$. Est-ce que G est une base de $K[T]$?

Exercice 4.5
1. Montrer que la dérivation sur $\mathbb{R}[T]$ est linéaire et surjective. Est-elle bijective ?
2. Montrer que l'intégration sur $\mathbb{R}[T]$ (à partir de 0) est linéaire et injective. Est-elle bijective ?

Exercice 4.6
1. Montrer par un calcul que si $A, X \in \mathrm{M}_2(K)$ satisfont $AX = I$, on a aussi $XA = I$. En déduire alors que $A \in \mathrm{GL}_2(K)$ et que $X = A^{-1}$.
2. Désignons par u la dérivation sur $\mathbb{R}[T]$ et par v l'intégration (à partir de 0). Montrer que $u\circ v = \mathrm{Id}$. A-t-on aussi $v\circ u = \mathrm{Id}$?

Exercice 4.7 On se donne $\iota : E' \to E$ injective, $\pi : E \to E''$ surjective et on suppose que $\mathrm{im}\,\iota = \ker\pi$. Montrer que $\dim E = \dim E' + \dim E''$.

Exercice 4.8 Soient E un espace vectoriel de dimension finie et $E_1,\dots,E_k$ des sous-espaces vectoriels. Montrer que
$$E = \oplus_{i=1}^k E_i \Leftrightarrow \begin{cases} \dim E = \sum_{i=1}^k \dim E_i \\ \forall i = 1,\dots,k, \quad E_i \cap \sum_{j\neq i} E_j = 0. \end{cases}$$

Exercice 4.9
1. Montrer que si $u : E \to F$ est linéaire et G engendre E, alors $\mathrm{rang}(u) = \mathrm{rang}(u(G))$.
2. Montrer que si X est une partie d'un espace vectoriel E, alors $\mathrm{rang}(X) = \dim(\mathrm{Vect}(X))$.

Exercice 4.10 Soient $A \in \mathrm{M}_{n\times m}(K)$ et $C_1,\dots,C_m$ les vecteurs colonnes de A. Montrer que
$$\mathrm{rang}(A) = \mathrm{rang}(\{C_1,\dots,C_m\}).$$

Exercice 4.11 Montrer que pour $A \in \mathrm{M}_n(K)$, on a $\mathrm{rang}(A) = n \Leftrightarrow A \in \mathrm{GL}_n(K)$.

Exercice 4.12 Déterminer une base de l'image et du noyau des matrices

$$\begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 4 \\ 7 & 5 & 1 \\ 3 & 4 & 6 \end{bmatrix}, \begin{bmatrix} 1 & 2 & -1 \\ 2 & 3 & -4 \\ -3 & -2 & 12 \end{bmatrix}.$$

Exercice 4.13
1. Quelle est la matrice de la dérivation $K[T]_{\leq n} \to K[T]_{\leq n-1}, P \mapsto P'$ dans les bases canoniques ?
2. Quelle est la matrice de la conjugaison complexe dans la base canonique de $\mathbb{C}$, vu comme espace vectoriel sur $\mathbb{R}$?

Exercice 4.14 Pour $a \in K$, on désigne par $u_a : K[T] \to K[T]$ l'unique morphisme d'algèbres tel que $u_a(T) = T - a$.
1. Montrer que l'on a toujours $u_a \circ u_b = u_{a+b}$ et que $u_0 = \mathrm{Id}_{K[T]}$.
2. En déduire que u_a est un automorphisme de l'algèbre $K[T]$.
3. En déduire un morphisme de groupes $K \to \mathrm{GL}(K[T])$.
4. Montrer que $K[T]_{\leq n}$ est stable par u_a et en déduire que l'application induite $u_{a,n}$ est un automorphisme de l'espace vectoriel $K[T]_{\leq n}$.
5. Montrer que la matrice de $u_{a,n}$ dans la base canonique est inversible et retrouver le résultat précédent.

Exercice 4.15
1. Quelle est la base duale de la base canonique $(\mathbb{1}_n, \ldots, \mathbb{1}_n)$ de K^n ?
2. Quelle est la base duale de la base canonique $(1, i)$ de $\mathbb{C}$ sur $\mathbb{R}$?

Exercice 4.16 Soient $A \in \mathrm{M}_{n\times m}(K)$ et $L_1, \ldots, L_n$ les vecteurs lignes de A. Montrer que

$$\mathrm{rang}(A) = \mathrm{rang}(\{L_1, \ldots, L_n\}).$$

Exercice 4.17 Montrer que des vecteurs $x_1, \ldots, x_n$ de K^n forment une base si et seulement si la matrice dont les colonnes (resp. les lignes) sont les vecteurs $x_1, \ldots, x_n$ est inversible. En déduire le cardinal de $\mathrm{GL}_n(K)$ lorsque K est un corps à q éléments.

Exercice 4.18 Soient E un espace vectoriel de dimension finie et F, G deux sous espaces vectoriels de E tels que $E \simeq F \oplus G$. Montrer que ${}^tE \simeq {}^\circ F \oplus {}^\circ G$.

Exercice 4.19 Montrer que si $\mathscr{S}$ est un système linéaire homogène de rang r à m variables, alors $\mathrm{Sol}(\mathscr{S})$ est un espace vectoriel de dimension $m - r$.

Exercice 4.20 — TP. On considère la matrice

$$Q := \begin{bmatrix} 9 & 0 & -3 \\ 0 & 10 & 0 \\ -3 & 0 & 1 \end{bmatrix} \in \mathbb{Q}^3.$$

1. Montrer que $P := \frac{1}{10}Q$ est une projection.
2. Déterminer le noyau et l'image de P.
3. Vérifiez que $\mathbb{Q}^3 = \ker P \oplus \operatorname{im} P$.

Exercice 4.21 — TP. On considère les sous-espaces vectoriels F et G de $\mathbb{Q}^4$ engendrés respectivement par

$$u_1 := (1,-1,2,1), \quad u_2 := (2,1,1,-1), \quad u_3 := (-1,-5,4,5) \quad \text{et}$$

$$v_1 := (0,1,0,0), \quad v_2 = (4,-5,11,7), \quad v_3 := (-1,1,-3,-2).$$

Montrer que $F \subset G$ et déterminez un supplémentaire H pour F dans G.

Exercice 4.22 — TP. On considère l'application

$$u : \mathbb{Q}^3 \to \mathbb{Q}^3, (x,y,z) \mapsto (x+2y+4z, 7x+5y+z, 3x+4y+6z)$$

et on pose

$$v_1 := (1,2,-3), v_2 := (2,3,-2), v_3 := (-1,-4,12).$$

1. Quelle est la matrice A de u (dans les bases canoniques) ? Déterminer le rang de u, donner une base de $\ker u$ ainsi que de im u. Finalement, donner une équation de im u.
2. Montrer que (v_1, v_2, v_3) est une nouvelle base de $\mathbb{Q}^3$. Quelle est la matrice de passage P. Calculer P^{-1}.
3. Quelle est la matrice de u dans la nouvelle base ?

Exercice 4.23 — TP. Calculer la comatrice de

$$A := \begin{bmatrix} 3 & 2 & -3 \\ 5 & -1 & -2 \\ 1 & 1 & -1 \end{bmatrix} \in \mathrm{M}_3(\mathbb{Q}).$$

En déduire que A est inversible et donner son inverse.

Exercice 4.24 — TP. On considère les vecteurs

$$x_1 := (2,1,0,2,-1,-2,-1,-1), \quad x_2 := (2,2,4,1,-2,-2,-1,-3),$$

$$x_3 := (1,0,-2,0,-3,0,-1,-3), \quad x_4 := (0,1,2,-1,-1,-3,1,0),$$

$$x_5 := (-1,1,1,0,-1,-1,-1,0), \quad x_6 := (4,5,5,2,-8,-8,-3,-7),$$

$$x_7 := (2,2,-1,2,-5,-3,-3,-4), \quad y_1 := (2,2,2,1,-2,-5,0,-1),$$

$$y_2 := (1,3,5,1,-3,-3,-2,-3) \quad \text{et} \quad y_3 := (3,3,4,0,-6,-5,-1,-6) \in \mathbb{Q}^8.$$

1. Vérifier que les vecteurs y_1, y_2, y_3 sont linéairement indépendants.
2. Montrer qu'ils sont tous dans $F = \mathrm{Vect}(\{x_1, \ldots, x_7\})$.
3. Compléter y_1, y_2, y_3 en une base de F (en utilisant les vecteurs $x_1, \ldots, x_7$).

5. Trace et déterminant

Comme toujours, on fixe un corps de scalaires K.

Remarque Tout ce qui suit reste valable sur un anneau *commutatif* quelconque, quitte à remplacer la notion d'espace vectoriel par celle de module et celle de dimension par celle de rang.

5.1 Application multilinéaire

Définition 5.1.1 Si
$$\Phi : X_1 \times \cdots \times X_n \to Y$$
est une application quelconque et
$$x_1 \in X_1, \ldots, x_{i-1} \in X_{i-1}, x_{i+1} \in X_{i+1}, \ldots, x_n \in X_n,$$
alors, l'application
$$X_i \to Y, \quad x_i \mapsto \Phi(x_1, \ldots, x_n)$$
est dite *partielle*.

Remarque
1. Les applications partielles associées à une application $\Phi : X \times Y \to Z$, sont donc les applications $X \to Z, x \mapsto \Phi(x,y)$ à y fixé et $Y \to Z, y \mapsto \Phi(x,y)$ à x fixé.
2. Plus généralement, on peut définir les applications partielles associées à une application $\Phi : \prod_{s \in S} X_s \mapsto Y$.
3. Nous avons déjà rencontré la notion d'applications partielle juste après la proposition 3.1.5 sur les sommes directes. Ces deux notions coïncident bien dans les cas d'un produit fini.

Définition 5.1.2 Soient $E_1, \ldots, E_n$ et F des espaces vectoriels. Une application
$$\Phi : E_1 \times \cdots \times E_n \to F$$

est *n-linéaire* si les toutes les application partielles $E_i \to F$ sont linéaires.

Remarque 1. Cela signifie donc que l'on a toujours

$$\Phi(x_1,\dots,x_i,\dots,x_n)+\Phi(x_1,\dots,x_i',\dots,x_n)=\Phi(x_1,\dots,x_i+x_i',\dots,x_n)$$

et

$$a\Phi(x_1,\dots,x_i,\dots,x_n)=\Phi(x_1,\dots,ax_i,\dots,x_n).$$

2. Bien sûr, dans le cas ou $n=1$, on retrouve la définition d'une application linéaire.
3. On dit que Φ est *multilinéaire* si on ne veut pas préciser n, *bilinéaire* lorsque $n=2$.
4. On dit *forme multilinéaire* lorsque $F=K$.
5. Si $E_1=\cdots=E_n=E$, on dit que Φ est une forme multilinéaire *sur* E.

Exemple 1. Si E est un espace vectoriel, alors la multiplication externe

$$K\times E\to E \quad (a,x)\mapsto ax$$

est bilinéaire.

2. Si L est une K-algèbre, alors la multiplication

$$L\times L\to L, \quad (u,v)\mapsto uv$$

est une application bilinéaire.

3. Si E, F et G sont trois espaces vectoriels, alors la loi de composition

$$\begin{array}{ccc} \mathrm{L}(F,G)\times\mathrm{L}(E,F) & \longrightarrow & \mathrm{L}(E,G) \\ (v,u) & \longmapsto & v\circ u \end{array}$$

est une application bilinéaire.

4. Si E est un espace vectoriel, alors l'application de dualité

$$E\times {}^tE\to K, \quad (x,\varphi)\mapsto\varphi(x)$$

est une forme bilinéaire.

5. Le *déterminant* (voir plus bas) est une forme multilinéaire.
6. Le *produit scalaire usuel*

$$((x_1,\dots,x_n),(y_1,\dots,y_n))\to x_1y_1+\cdots+x_ny_n$$

est une forme bilinéaire sur K^n. Plus généralement, on peut remplacer le second membre par n'importe quelle expression $\sum a_{i,j}x_iy_j$ (voir plus loin).

7. Le *produit vectoriel*

$$\begin{array}{ccc} K^3\times K^3 & \longrightarrow & K^3 \\ ((x_1,x_2,x_3),(y_1,y_2,y_3)) & \longmapsto & (x_2y_3-x_3y_2,x_3y_1-x_1y_3,x_1y_2-x_2y_1) \end{array}$$

est une application bilinéaire sur K^3.

Proposition 5.1.3 Si $E_1,\dots,E_n$ et F sont des espaces vectoriels, alors les applications multilinéaires $E_1\times\cdots\times E_n\to F$ forment un sous espace vectoriel

$$L(E_1,\dots,E_n,F)\subset\mathscr{F}(E_1\times\cdots\times E_n,F)$$

et les applications $L(E_1,\dots,E_n,F)\to L(E_i,F)$ qui envoient Φ sur une application partielle, sont toutes linéaires.

Démonstration. Par définition d'une somme ou d'un multiple d'une application, on voit déjà que l'application $\mathscr{F}(E_1 \times \cdots \times E_n, F) \to \mathscr{F}(E_i, F)$ qui envoie Φ sur une application partielle est automatiquement linéaire. Et la première assertion résulte alors immédiatement de l'assertion analogue pour les applications linéaires. ■

Proposition 5.1.4 Si E, F et G sont trois espaces vectoriels, il existe des isomorphismes

$$\mathrm{L}(F, \mathrm{L}(E,G)) \simeq \mathrm{L}(E,F,G) \simeq \mathrm{L}(E, L(F,G)), \quad l \leftrightarrow \Phi \leftrightarrow r$$

donnés par

$$\forall x \in E, y \in F, \quad l(y)(x) = \Phi(x,y) = r(x)(y)$$

Démonstration. Par symétrie, il suffit de traiter l'isomorphisme de gauche. On dispose d'une bijection

$$\mathscr{F}(F, \mathscr{F}(E,G)) \simeq \mathscr{F}(E \times F, G), \quad l \leftrightarrow \Phi$$

donnée par la même formule, et qui est linéaire par définition (vérifier). Et on dispose aussi des inclusions $L(F, L(E,G)) \subset (\mathscr{F}(F, \mathscr{F}(E,G))$ d'une part et $L(E,F,G) \subset \mathscr{F}(E \times F, G)$ d'autre part. Il faut montrer que ces deux parties se correspondent. Or, dire que $l \in L(F, L(E,G))$ signifie que l'on a

$$l(y+y')(x) = l(y)(x) + l(y')(x), \quad l(ay)(x) = al(y)(x),$$

$$l(y)(x+x') = l(y)(x) + l(y)(x') \quad \text{et} \quad l(y)(ax) = al(y)(x)$$

chaque fois que $x, x' \in E$, $y, y' \in F$ et $a \in K$. Ceci exprime exactement la bilinéarité de Φ. ■

Proposition 5.1.5 Soit $\Phi : E_1 \times \cdots \times E_n \to F$ une application multilinéaire. Alors,

1. Si, pour tout $i = 1, \ldots, n$, l'application $u_i : E'_i \to E_i$ est linéaire, alors l'application composée

$$\begin{array}{ccc} E'_1 \times \cdots \times E'_n & \longrightarrow & F \\ (x'_1, \ldots, x'_n) & \longmapsto & \Phi(u_1(x'_1), \ldots, u_n(x'_n)) \end{array}$$

   est multilinéaire.
2. Si $u : F \to F'$ est linéaire, alors l'application composée

$$\begin{array}{ccc} E_1 \times \cdots \times E_n & \longrightarrow & F \\ (x_1, \ldots, x_n) & \longmapsto & u(\Phi(x_1, \ldots, x_n)) \end{array}$$

   est multilinéaire.

Démonstration. Résulte encore des résultats analogues pour les applications linéaires (exercice). ■

Exemple Comme $\mathscr{C}^0([0,1], \mathbb{R})$ est une $\mathbb{R}$-algèbre (c'est une sous-algèbre de $\mathbb{R}^{[0,1]}$), la multiplication dans $\mathscr{C}^0([0,1], \mathbb{R})$ est une application bilinéaire. D'autre part, on sait que l'intégration est linéaire. On en déduit (sans calcul) que l'application

$$(f,g) \mapsto \int_0^1 (fg)(t)\mathrm{d}t \tag{5.1}$$

est une forme bilinéaire sur $\mathscr{C}^0([0,1], \mathbb{R})$.

Remarque Avant d'aller plus loin, il est nécessaire de faire quelques rappels sur les permutations.

1. Une *inversion* de $\sigma \in \mathscr{S}_n$ est un couple (i,j) avec $1 \leq i < j \leq n$ mais $\sigma(i) > \sigma(j)$.
2. La *signature* est l'application
$$\mathscr{S}_n \to \{-1,1\}, \quad \sigma \mapsto (-1)^\sigma$$
qui vaut 1 (resp. -1) s'il y a un nombre pair (resp. impair) d'inversions dans σ.
3. La signature est en fait l'unique morphisme de groupes surjectif (pour $n \geq 2$).
4. La *transposition* $\tau := (i\ j)$ est la permutation qui échange i et j. Toute permutation est un produit (c'est à dire, composé) de transpositions. On peut même se limiter aux transpositions de la forme $(i\ i+1)$ avec $1 \leq i < n$ ou bien de la forme $(1\ i)$ avec $1 < i \leq n$ si on veut.
5. Si $\Phi : X \times \cdots \times X \to Y$ est une application quelconque et $\sigma \in \mathscr{S}_n$, on écrira
$$\Phi_\sigma(x_1,\ldots,x_n) := \Phi\left(x_{\sigma(1)},\ldots,x_{\sigma(n)}\right).$$

Définition 5.1.6 Soit $\Phi : E \times \cdots \times E \to F$ une application multilinéaire sur E. Alors, on dit que

1. Φ est *symétrique* si
$$\forall \sigma \in \mathscr{S}_n, \quad \Phi_\sigma = \Phi,$$
2. Φ est *antisymétrique* si
$$\forall \sigma \in \mathscr{S}_n, \quad \Phi_\sigma = (-1)^\sigma \Phi$$
(et il suffit de considérer les transpositions).

Exemple

1. Une application bilinéaire Φ sur E est symétrique (resp. antisymétrique) si et seulement si
$$\forall x,y \in E, \quad \Phi(x,y) = \Phi(y,x) \quad (\text{resp. } = -\Phi(y,x)).$$
2. Le produit scalaire usuel est une forme bilinéaire symétrique.
3. Le déterminant est une forme multilinéaire antisymétrique.
4. Le produit vectoriel est une application bilinéaire antisymétrique.
5. L'application (5.1) est une forme bilinéaire symétrique.

Définition 5.1.7 Une application n-linéaire $\Phi : E \times \cdots \times E \to F$ est *alternée* si elle satisfait
$$(\exists i \neq j, x_i = x_j) \Rightarrow \Phi(x_1,\ldots,x_n) = 0.$$

Proposition 5.1.8 Soit $\Phi : E \times \cdots \times E \to F$ une application n-linéaire. On a alors

1. Φ alternée $\Rightarrow \Phi$ antisymétrique,
2. $(\mathrm{Car}(K) \neq 2)$ Φ alternée $\Leftrightarrow \Phi$ antisymétrique.

Démonstration. Supposons pour commencer que Φ est alternée et donnons nous une transposition $\tau := (i\ j)$ avec $0 \leq i < j \leq n$. Pour $x_1,\ldots,x_n \in E$, on a alors par linéarité,

$$\begin{aligned}
0 &= \Phi(x_1,\ldots,x_{i-1},x_i+x_j,x_{i+1},\ldots,x_{j-1},x_i+x_j,x_{j+1},\ldots,x_n) \\
&= \Phi(x_1,\ldots,x_{j-1},x_i,x_{j+1},\ldots,x_n) + \Phi(x_1,\ldots,x_n) \\
&+ \Phi_\tau(x_1,\ldots,x_n) + \Phi(x_1,\ldots,x_{i-1},x_j,x_{i+1},\ldots\ldots,x_n) \\
&= 0 + \Phi(x_1,\ldots,x_n) + \Phi_\tau(x_1,\ldots,x_n) + 0,
\end{aligned}$$

et donc $\Phi_\tau(x_1,\ldots,x_n) = -\Phi(x_1,\ldots,x_n)$.

Réciproquement, si on suppose que Φ est antisymétrique et que $x_i = x_j$ avec $0 \leq i < j \leq n$, on aura en utilisant la même permutation τ que ci-dessus :

$$\Phi(x_1,\dots,x_n) = \Phi_\tau(x_1,\dots,x_n) = -\Phi(x_1,\dots,x_n)$$

si bien que $2\Phi(x_1,\dots,x_n) = 0$, et si on suppose que $\mathrm{Car}(K) \neq 2$, alors $\Phi(x_1,\dots,x_n) = 0$. ■

Remarque 1. Lorsque $2 = 0$ dans K, on a symétrique $\Leftrightarrow$ antisymétrique, et il suit qu'une application antisymétrique est soit alternée, soit symétrique.
2. Attention, si on travaille avec des modules sur un anneau, la seconde assertion de la proposition n'est plus vraie telle quelle. Il faut par exemple demander que l'on ait un module libre sur un anneau (commutatif) intègre ou que 2 soit inversible.

Proposition 5.1.9 Les applications n-linéaires symétriques (resp. antisymétriques, resp. alternées) sur E à valeurs dans F forment un sous-espace vectoriel $\mathrm{S}_n(E,F)$ (resp. $\mathrm{A}_n(E,F)$, resp. $\bigwedge_n(E,F)$) de $\mathrm{L}_n(E,F) := \mathrm{L}(E,\dots,E,F)$.

Démonstration. On vérifie facilement que si $\sigma \in \mathscr{S}_n$, alors l'application $\Phi \mapsto \Phi_\sigma$ est linéaire. Le cas des applications symétriques et antisymétrique en découle. Pour les applications alternées, c'est encore plus facile. Les détails sont laissés en exercice. ■

Remarque 1. On peut montrer que, dans la proposition 5.1.5, si Φ est une application multilinéaire symétrique (resp. antisymétrique, resp. alternée), il en va de même des applications composées.
2. Comme cas particulier, on voit que si $E' \subset E$ est un sous-espace vectoriel et $\Phi : E \times \cdots \times E \to F$ est une application multilinéaire (resp. multilinéaire symétrique, resp. multilinéaire antisymétrique, resp. multilinéaire alternée) sur E, alors il en va de même de l'application induite $E' \times \cdots \times E' \to F$.

5.2 Produit tensoriel

Définition 5.2.1 Le *produit tensoriel* de deux espaces vectoriels E et F est l'espace quotient $E \otimes F$ de $K^{(E\times F)}$ par le sous-espace vectoriel engendré par tous les éléments de la forme

$$\mathbb{1}_{x+x',y} - \mathbb{1}_{x,y} - \mathbb{1}_{x',y}, \quad \mathbb{1}_{x,y+y'} - \mathbb{1}_{x,y} - \mathbb{1}_{x,y'}, \quad \mathbb{1}_{ax,y} - a\mathbb{1}_{x,y} \quad \text{et} \quad \mathbb{1}_{x,ay} - a\mathbb{1}_{x,y},$$

avec $x, x' \in E$, $y, y' \in F$ et $a \in K$. On dira que $x \otimes y := \overline{\mathbb{1}}_{x,y} \in E \otimes F$ est un *tenseur*.

Remarque 1. On rappelle que $K^{(E\times F)}$ est un espace vectoriel dont une base est donnée par les $\mathbb{1}_{x,y}$ avec $x \in E$ et $y \in F$. Autrement dit, tout élément de $K^{(E\times F)}$ s'écrit de manière unique sous la forme $a_1\mathbb{1}_{x_1,y_1} + \cdots + a_n\mathbb{1}_{x_n,y_n}$ avec $x_1,\dots,x_n \in E$, $y_1,\dots,y_n \in F$ et $a_1,\dots,a_n \in K$.
2. Par définition, on aura
$$\begin{cases} (x+x')\otimes y = x\otimes y + x'\otimes y, \\ x\otimes(y+y') = x\otimes y + x\otimes y', \\ a(x\otimes y) = ax\otimes y = x\otimes ay \end{cases}$$
lorsque $x, x' \in E$, $y, y' \in F$ et $a \in K$.
3. Comme $E \otimes F$ est un quotient de $K^{(E\times F)}$, les tenseurs $x \otimes y := \overline{\mathbb{1}}_{x,y}$ engendrent $E \otimes F$. Cela veut dire que tout élément de $E \otimes F$ s'écrit (de plusieurs manières) sous la forme $a_1x_1 \otimes y_1 + \cdots + a_nx_n \otimes y_n$ avec $x_1,\dots,x_n \in E$, $y_1,\dots,y_n \in F$ et $a_1,\dots,a_n \in K$.
4. On voit en fait que tout élément de $E \otimes F$ s'écrit comme somme de tenseurs (de plusieurs manières).

5. Même si on s'intéresse uniquement aux espaces vectoriels de dimension finie, on voit intervenir l'espace $K^{(E\times F)}$ qui est toujours de dimension infinie si K est infini (à moins que $E = F = \{0\}$).
6. On peut définir plus généralement $E_1 \otimes \cdots \otimes E_n$ comme quotient de $K^{E_1\times\cdots\times E_n}$.

Exemple Considérons $\mathbb{C}$ comme espace vectoriel sur $\mathbb{R}$. On a donc ici $K = \mathbb{R}$ - et on l'indiquera en indice afin d'éviter les confusions - et $E = F = \mathbb{C}$. L'espace vectoriel $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ est donc engendré par les tenseurs $z\otimes w$ avec $z, w \in \mathbb{C}$. Si on écrit $z = a+ib$ et $w = c+id$ avec $a,b,c,d \in \mathbb{R}$, on a

$$z\otimes w = ac(1\otimes 1)+ad(1\otimes i)+bc(i\otimes 1)+bd(i\otimes i).$$

On en déduit que $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ est engendré par $\{1\otimes 1, 1\otimes i, i\otimes 1, i\otimes i\}$ (on verra plus loin que c'est une base). Remarquons cependant qu'il existe des éléments dans le produit tensoriel $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ qui ne sont *pas* des tenseurs : $1\otimes i+i\otimes 1$ par exemple.

On dispose alors de la propriété universelle du produit tensoriel :

Proposition 5.2.2 Si E et F sont deux espace vectoriels, alors l'application

$$E\times F \to E\otimes F, \quad (x,y)\mapsto x\otimes y$$

est bilinéaire. De plus, si $\Phi : E\times F \to G$ est une application bilinéaire, alors il existe une unique application linéaire $\overline{\widetilde{\Phi}} : E\otimes F \to G$ telle que

$$\forall x\in E, y\in F, \quad \Phi(x,y) = \overline{\widetilde{\Phi}}(x\otimes y):$$

Démonstration. La première assertion résulte immédiatement de la définition (voir remarque 2 ci-dessus). Pour la seconde, on utilise successivement les propriétés universelles de $K^{(E\times F)}$ (voir corollaire 3.1.6) et du quotient (théorème 2.6.4) :

$$\begin{tikzcd}
E\times F \arrow[r, "\Phi"] \arrow[d] & G \\
K^{(E\times F)} \arrow[ur, dashed, "\widetilde{\Phi}"] \arrow[d] & \\
E\otimes F. \arrow[uur, dashed, "\overline{\widetilde{\Phi}}"'] &
\end{tikzcd} \quad \blacksquare$$

Remarque 1. On obtient en fait un isomorphisme $\mathrm{L}(E,F,G)\simeq \mathrm{L}(E\otimes F, G)$.
2. En combinant avec le second isomorphisme de la proposition 5.1.4, on obtient ce qu'on appelle l'isomorphisme (d'*adjonction*)

$$\mathrm{L}(E,\mathrm{L}(F,G))\simeq \mathrm{L}(E\otimes F,G).$$

3. Par un argument direct, ou en utilisant les propriétés universelles, on peut vérifier que, si E, F et G sont des espaces vectoriels, on a
   (a) $(E\otimes F)\otimes G \simeq E\otimes(F\otimes G)$ (associativité)
   (b) $E\otimes K\simeq K\otimes E\simeq E$ (élément neutre)
   (c) $E\otimes F\simeq F\otimes E$ (commutativité)
   (d) $(E\oplus F)\otimes G\simeq (E\otimes G)\oplus(F\otimes G)$ (distributivité)

4. La proposition se généralise à un nombre fini d'espaces vectoriels et on en déduit formellement
$$E_1 \otimes \cdots \otimes E_n \simeq (E_1 \otimes \cdots \otimes E_{n-1}) \otimes E_n.$$
C'est d'ailleurs souvent cette dernière expression qui est utilisée pour définir par récurrence le produit tensoriel d'un nombre fini d'espaces vectoriels.

Corollaire 5.2.3 Si $u : E \to E'$ et $v : F \to F'$ sont deux applications linéaires, il existe une unique application linéaire $u \otimes v : E \otimes F \to E' \otimes F'$ telle que
$$\forall x \in E, y \in F, \quad (u \otimes v)(x \otimes y) = u(x) \otimes v(y).$$

Démonstration. Par composition, l'application $E \times F \to E' \otimes F', (x,y) \mapsto u(x) \otimes v(y)$ est bilinéaire. On utilise ensuite la propriété universelle du produit tensoriel. ■

Proposition 5.2.4 Si E et F sont deux espaces vectoriels de base $(e_i)_{i \in I}$ et $(f_j)_{j \in J}$ respectivement, alors $(e_i \otimes f_j)_{i \in I, j \in J}$ est une base de $E \otimes F$.

Démonstration. Il s'agit de montrer que l'application canonique
$$K^{(I \times J)} \to E \otimes F, \quad (a_{i,j})_{i \in I, j \in J} \mapsto \sum a_{i,j} e_i \otimes f_j$$
est bijective. Pour ce faire, on va exhiber un inverse. On commence avec l'application évidente
$$K^I \times K^J \to K^{I \times J}, \quad ((a_i)_{i \in I}, (b_j)_{i \in J}) \mapsto (a_i b_j)_{i \in I, j \in J}.$$
Celle ci est clairement bilinéaire (vérifier) et induit une application (toujours bilinéaire) $K^{(I)} \times K^{(J)} \to K^{(I \times J)}$ car, si les a_i et les b_j sont presque tous nuls, il en va de même de leurs produits $a_i b_j$. En composant avec les isomorphismes $E \simeq K^{(I)}$ et $F \simeq K^{(J)}$ associés à nos bases, on en déduit une application bilinéaire $E \times F \to K^{(I \times J)}$ et donc finalement une application linéaire
$$E \otimes F \to K^{(I \times J)}, \quad \sum_{i \in I, j \in J} a_i e_i \otimes b_j f_j \mapsto (a_i b_j)_{i \in I, j \in J}.$$
On vérifie aisément que c'est bien un inverse par un argument direct ou, si on préfère, en utilisant les propriétés universelles (exercice). ■

Corollaire 5.2.5 Si E et F sont deux espaces vectoriels, on a $\dim(E \otimes F) = \dim E \times \dim F$.

Démonstration. ■

Remarque 1. On peut rappeler que $\dim(E \oplus F) = \dim E + \dim F$.

2. Ces résultats (pour la somme directe comme pour le produit) sont toujours valides pour des modules libres sur un anneau commutatif (bien qu'on dise alors *rang* au lieu de *dimension*).

Exemple On a $\dim(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}) = 4$ et
$$\{1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i\}$$
est bien une base. Et on a aussi $\dim(\mathbb{C} \oplus \mathbb{C}) = 4$ avec base
$$((1,1),(1,i),(i,1),(i,i))$$
(mais cette similitude est une coïncidence due au fait que $2 \times 2 = 2 + 2$).

5.3 Trace

Proposition 5.3.1 Soient E et F deux espaces vectoriels.

1. Si $\varphi \in {}^tE$ et $y \in F$, alors l'application
$$u : E \to F, \quad x \mapsto \varphi(x)y$$
est linéaire.
2. L'application
$$F \times {}^tE \to \mathrm{L}(E,F), \quad (y,\varphi) \mapsto (u : x \mapsto \varphi(x)y)$$
est bilinéaire
3. Si E est de *dimension finie*, l'application induite est un isomorphisme
$$F \otimes {}^tE \simeq \mathrm{L}(E,F).$$

Démonstration. 1. Exercice.

2. Exercice.
3. On exhibe un un inverse à notre application lorsque E possède une base finie $(e_1,\dots,e_n)$ en considérant
$$\mathrm{L}(E,F) \to F \otimes {}^tE, \quad u \mapsto u(e_1) \otimes {}^te_1 + \cdots + u(e_n) \otimes {}^te_n.$$
Il faut s'assurer que c'est bien un inverse (exercice encore). ∎

Exemple 1. On dispose d'une suite d'isomorphismes
$$\mathrm{M}_{n\times 1}(K) \otimes \mathrm{M}_{1\times m}(K) \simeq K^n \otimes {}^tK^m \simeq \mathrm{L}(K^m,K^n) \simeq \mathrm{M}_{n\times m}(K), \quad \mathbb{1}_{i,1} \otimes \mathbb{1}_{1,j} \leftrightarrow \mathbb{1}_{i,j}$$

2. On a ${}^t\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathrm{L}_{\mathbb{R}}(\mathbb{C})$.

Remarque 1. Si E et F sont des espaces vectoriels de dimension finie munis respectivement de bases $(e_1,\dots,e_m)$ et $(f_1,\dots,f_n)$, on obtient une base $(e_{i,j})$ de $\mathrm{L}(E,F)$ en posant
$$e_{i,j}(x) = x_j f_i \quad \text{si} \quad x = x_1e_1 + \cdots + x_me_m \in E.$$
Et on a les correspondances suivantes
$$F \otimes {}^tE \simeq \mathrm{L}(E,F) \simeq \mathrm{M}_{n\times m}(K), \quad f_i \otimes {}^te_j \leftrightarrow e_{i,j} \leftrightarrow \mathbb{1}_{i,j}.$$

2. La composition des applications corresponds à la « contraction » sur les produits :
$$\begin{tikzcd}
\mathrm{L}(F,G) \times \mathrm{L}(E,F) \arrow[r, "(v,u)\mapsto v\circ u"] & \mathrm{L}(E,G) \\
G \times {}^tF \times F \times {}^tE \arrow[u] \arrow[r, "(z,\psi,y,\varphi)\mapsto\psi(y)(z,\varphi)"'] & G \otimes {}^tE. \arrow[u]
\end{tikzcd}$$

Définition 5.3.2 Si E est un espace vectoriel de dimension finie, l'unique forme linéaire tr :

$\mathrm{L}(E) \to K$ rendant commutatif le diagramme

$$\begin{tikzcd}
E \times {}^tE \arrow[r, "(x,\varphi)\mapsto\varphi(x)"] \arrow[d] & K \\
E \otimes {}^tE \arrow[ur] \arrow[d, "\simeq"'] & \\
\mathrm{L}(E). \arrow[uur, dashed, "\mathrm{tr}"'] &
\end{tikzcd}$$

est la *trace*.

Remarque Cette définition nous donne deux propriétés classiques de la trace d'un endomorphisme :

1. La trace de u ne dépend pas du choix de la base de E,
2. La trace est linéaire en u,

mais il faut tout de même s'assurer que l'on retrouve bien la définition classique.

Proposition 5.3.3 Soit E un espace vectoriel de dimension finie. Si $A := [a_{i,j}]$ est la matrice de $u \in L(E)$ dans une base $\mathscr{B} := (e_1, \dots, e_n)$, alors $\mathrm{tr}(u) = a_{1,1} + \cdots + a_{n,n}$.

Démonstration. On dispose d'une suite d'isomorphismes

$$E \otimes {}^tE \simeq L(E) \simeq M_n(K), \quad e_i \otimes {}^te_j \leftrightarrow e_{i,j} \leftrightarrow \mathbb{1}_{i,j}.$$

Et par définition, on a

$$\mathrm{tr}(e_{i,j}) = {}^te_j(e_i) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$$

On conclut par linéarité puisque $u = \sum a_{i,j} e_{i,j}$. ■

Remarque

1. On définit la *trace* de la matrice $A \in M_n(K)$ comme étant la trace de l'endomorphisme $u \in \mathrm{L}(K^n)$ correspondant. La proposition nous dit donc bien que si $A = [a_{i,j}]$, on a $\mathrm{tr}(A) := a_{1,1} + \cdots + a_{n,n}$. Comme notre définition ne dépend pas de la base, on voit que si A et A' sont semblables, alors $\mathrm{tr}(A) = \mathrm{tr}(A')$.
2. Attention, on a $\mathrm{tr}(\mathrm{Id}_E) = \dim E \neq 1$ si E n'est pas une droite. Notons aussi que, bien que l'on ait toujours $\mathrm{tr}(u+v) = \mathrm{tr}(u) + \mathrm{tr}(v)$ et $\mathrm{tr}(au) = a\mathrm{tr}(u)$, on a en général $\mathrm{tr}(u \circ v) \neq \mathrm{tr}(u)\mathrm{tr}(v)$.

Proposition 5.3.4 Soit E un espace vectoriel de dimension finie. Si $u, v \in L(E)$, on a

$$\mathrm{tr}(u \circ v) = \mathrm{tr}(v \circ u).$$

Démonstration. On dispose d'un diagramme commutatif

$$\begin{tikzcd}
\mathrm{L}(E) \times \mathrm{L}(E) \arrow[r, "(v,u)\mapsto v\circ u"] & L(E) \\
E \times {}^tE \times E \times {}^tE \arrow[u] \arrow[r, "(y,\psi,x,\varphi)\mapsto\psi(x)(y,\varphi)"'] & {}^tE \otimes E \arrow[u]
\end{tikzcd}$$

qui nous donne $\mathrm{tr}(v \circ u) = \varphi(y)\psi(x)$ quand u et v proviennent de (x, φ) et (y, ψ) respectivement. Le cas général s'obtient par linéarité. ■

Remarque 1. De manière équivalente, la proposition nous dit que si $A, B \in \mathrm{M}_n(K)$, alors $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. Ça se démontre aussi directement : si $A := [a_{i,j}]$, $B := [b_{i,j}]$ et $AB := [c_{i,j}]$, on a

$$\forall i,k = 1,\dots,n, \quad c_{i,k} = \sum_{j=1}^{n} a_{i,j} b_{j,k}$$

si bien que

$$\mathrm{tr}(AB) = \sum_{i=1}^{n} c_{i,i} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,j} b_{j,i}$$

qui est une formule symétrique en A et B.

2. Afin de définir la trace d'un endomorphisme, on aurait aussi pu définir d'abord la trace d'une matrice, puis montrer la commutativité, et l'utiliser pour montrer que deux matrices semblables ont la même trace :

$$\mathrm{tr}(P^{-1}AP) = \mathrm{tr}(PP^{-1}A) = \mathrm{tr}(IA) = \mathrm{tr}(A).$$

Proposition 5.3.5 Soient E un espace vectoriel de dimension finie, $u \in L(E)$, E' un sous-espace vectoriel de E stable par u et $u' \in L(E'), u'' \in L(E/E')$ les applications induites. On a alors

$$\mathrm{tr}(u) = \mathrm{tr}(u') + \mathrm{tr}(u'').$$

Démonstration. Exercice. ∎

5.4 Puissance extérieure

On utilise ici librement l'extension du produit tensoriel à un nombre fini de facteurs (au lieu de seulement deux).

Définition 5.4.1 Si E est un espace vectoriel, alors la k-ème *puissance tensorielle* de E est

$$\otimes^k E := \underbrace{E \otimes \cdots \otimes E}_{k \text{ fois}}.$$

Remarque 1. Tout élément de $\otimes^k E$ est donc somme de *tenseurs* $x_1 \otimes \cdots \otimes x_k$ avec $x_1, \dots, x_k \in E$, ceux-ci étant soumis à des relations de linéarité (que l'on peut expliciter).

2. On dispose d'une application multilinéaire *universelle*

$$E \times \cdots \times E \to \otimes^k E, \quad (x_1, \dots, x_k) \mapsto x_1 \otimes \cdots \otimes x_k.$$

3. Comme conséquence de la proposition 5.2.4 (base d'un produit tensoriel), on voit que si $\mathscr{B} := (e_i)_{i \in I}$ est une base de E, alors la famille des $e_{f(1)} \otimes \cdots \otimes e_{f(k)}$ avec $f : k \to I$, est une base de $\otimes^k E$. On préfère travailler ici avec des applications $k := \{1, \dots, k\} \to I$ plutôt qu'avec des k-uples d'éléments de I pour des raisons qui devraient être claires plus tard.

4. Si on a, pour tout $i = 1, \dots, k$, $x_i = \sum_{j \in I} a_{i,j} e_j$, on peut même écrire explicitement

$$\begin{aligned} x_1 \otimes \cdots \otimes x_k &= \sum_{j \in I} a_{1,j} e_j \otimes \cdots \otimes \sum_{j \in I} a_{k,j} e_j \\ &= \sum_{f : k \to I} a_{1,f(1)} \dots a_{k,f(k)}\, e_{f(1)} \otimes \cdots \otimes e_{f(k)}. \end{aligned}$$

Définition 5.4.2 Soit E un espace vectoriel. La k-ème *puissance extérieure* de E est le quotient $\bigwedge^k E$ de $\otimes^k E$ par le sous-espace vectoriel engendré par tous les tenseurs $x_1 \otimes \cdots \otimes x_k$ pour lesquels il existe $i \neq j$ avec $x_i = x_j$.

On posera

$$x_1 \wedge \cdots \wedge x_k := \overline{x_1 \otimes \cdots \otimes x_k} \in \bigwedge^k E.$$

Remarque 1. Par définition, tout élément de $\bigwedge^k E$ est somme d'éléments de la forme $x_1 \wedge \cdots \wedge x_k$ avec $x_1, \ldots, x_k \in E$, et on dispose de relations de linéarité comme pour les puissances tensorielles. De plus, on a $x_1 \wedge \cdots \wedge x_k = 0$ lorsqu'il existe $i \neq j$ avec $x_i = x_j$.

2. On définit aussi la k-ème *puissance symétrique* de E en prenant le quotient $\mathrm{S}^k E$ par le sous-espace vectoriel engendré par tous les $x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(k)} - (-1)^\sigma x_1 \otimes \cdots \otimes x_k$ avec $\sigma \in \mathscr{S}_k$ (et on peut se limiter aux transpositions). On note alors tout simplement

$$x_1 \ldots x_k := \overline{x_1 \otimes \cdots \otimes x_k} \in \mathrm{S}^k E$$

On dispose de nouveau d'une propriété universelle :

Proposition 5.4.3 Si E est un espace vectoriel, alors l'application

$$E \times \cdots \times E \to \bigwedge^k E, \quad (x_1, \ldots, x_k) \mapsto x_1 \wedge \cdots \wedge x_k$$

est multilinéaire alternée et si $\Phi : E \times \cdots \times E \to F$ est une application k-linéaire alternée, alors il existe une unique application linéaire $\bigwedge^k E \to F$ rendant commutatif le diagramme

$$\begin{tikzcd}
E \times \cdots \times E \arrow[r, "\Phi"] \arrow[d] & F \\
\bigwedge^k E. \arrow[ur, dashed] &
\end{tikzcd}$$

Démonstration. On utilise la propriété universelle de la puissance tensorielle ainsi que celle du quotient (exercice). ∎

Remarque 1. On voit de même que les puissances symétriques sont universelles pour les applications multilinéaires symétriques.

2. On a en fait un isomorphisme

$$\bigwedge^k \mathrm{L}(E,F) \simeq \mathrm{L}(\bigwedge^k E, F)$$

(et un résultat analogue pour les puissances symétriques).

3. Puisqu'une application multilinéaire alternée est toujours antisymétrique, on voit que si $\sigma \in \mathscr{S}_k$, on aura toujours

$$x_{\sigma(1)} \wedge \cdots \wedge x_{\sigma(k)} = (-1)^\sigma x_1 \wedge \cdots \wedge x_k.$$

4. On peut montrer que, si E est de dimension finie, on a un isomorphisme

$$\begin{array}{ccc}
\bigwedge^k E & \xrightarrow{\simeq} & \bigwedge^k({}^tE, K) \\
x_1 \wedge \cdots \wedge x_k & \longmapsto & (\varphi_1, \ldots, \varphi_k) \mapsto \varphi_1(x_1) \cdots \varphi_k(x_k)
\end{array}$$

qui permet d'utiliser un espace d'applications multilinéaires alternées à la place de celui des puissances extérieures.

5. Comme conséquence de la propriété universelle, on voit que toute application linéaire $u : E \to F$ fournit une application linéaire
$$\bigwedge^k u : \bigwedge^k E \to \bigwedge^k F, \quad x_1 \wedge \cdots \wedge x_k \mapsto u(x_1) \wedge \cdots \wedge u(x_k).$$
Bien sûr, si on se donne une autre application linéaire $v : F \to G$, on aura
$$\bigwedge^k (v \circ u) = \bigwedge^k v \circ \bigwedge^k u.$$

Lemme 5.4.4 Soit E un espace vectoriel. Si $x_1, \ldots, x_k \in E$ sont liés, alors $x_1 \wedge \cdots \wedge x_k = 0$.

Démonstration. Par hypothèse, il existe $i \in \{1, \ldots, k\}$ tels que $x_i = \sum_{j \neq i} a_j x_j$ et on aura donc
$$\begin{aligned} x_1 \wedge \cdots \wedge x_k &= x_1 \wedge \cdots \wedge x_{i-1} \wedge \sum_{j \neq i} a_j x_j \wedge x_{i+1} \wedge \cdots \wedge x_k \\ &= \sum_{j \neq i} a_j x_1 \wedge \cdots \wedge x_{i-1} \wedge x_j \wedge x_{i+1} \wedge \cdots \wedge x_k \\ &= 0. \end{aligned}$$
■

Remarque Afin de démontrer le prochain lemme, rappelons que l'on dispose du *groupe alterné* $\mathscr{A}_n$ qui est le sous-groupe de $\mathscr{S}_n$ formé des permutations *paires* (c'est le noyau de la signature). De plus, si τ est une transposition, on a une union disjointe
$$\mathscr{S}_n = \mathscr{A}_n \cup \mathscr{A}_n \tau$$
(autrement dit, $\mathscr{A}_n \tau$ est exactement l'ensemble des permutations *impaires*).

Lemme 5.4.5 Si $(e_1, \ldots, e_n)$ est une base d'un espace vectoriel E, alors le noyau de l'application canonique $\pi : \otimes^n E \to \wedge^n E$ a pour base
- les $e_{f(1)} \otimes \cdots \otimes e_{f(n)}$ avec $f \notin \mathscr{S}_n$ et
- les $e_{\sigma(1)} \otimes \cdots \otimes e_{\sigma(n)} - (-1)^\sigma e_1 \otimes \cdots \otimes e_n$ avec $\sigma \in \mathscr{S}_n \setminus \{\mathrm{Id}\}$.

Démonstration. Pour $f : n \to n$, on pose $e_f := e_{f(1)} \otimes \cdots \otimes e_{f(n)}$. Puisque l'application canonique $E \times \cdots \times E \to \bigwedge^n E$ est alternée on a toujours $e_f \in \ker \pi$ si f n'est pas injective. De plus, comme une application alternée est antisymétrique, on a aussi $e_\sigma - (-1)^\sigma e_{\mathrm{Id}} \in \ker \pi$ si $\sigma \in \mathscr{S}_n$. On voit aussi aisément que les e_f avec f non injective et les $e_\sigma - (-1)^\sigma e_{\mathrm{Id}}$ avec $\sigma \neq 1$ sont linéairement indépendants (exercice).

Donnons nous maintenant $x_1 \otimes \cdots \otimes x_n \in \otimes^n E$ et supposons qu'il existe $i < j$ tel que $x_i = x_j$. On écrit pour tout $u = 1, \ldots, n$, $x_u = \sum_{v=1}^n a_{u,v} e_v$ si bien que
$$x_1 \otimes \cdots \otimes x_n = \sum_{f \notin \mathscr{S}_n} a_{1,f(1)} \ldots a_{n,f(n)}\, e_f + \sum_{\sigma \in \mathscr{S}_n} a_{1,\sigma(1)} \ldots a_{n,\sigma(n)}\, e_\sigma.$$
On remarque maintenant que, si τ désigne la transposition qui échange i et j, on a
$$\prod_{u=1}^n a_{u,\sigma(u)} = \prod_{u=1}^n a_{u,\sigma(\tau(u))}.$$
En effet, si $u \neq i, j$, on a $a_{u,\sigma(u)} = a_{u,\sigma(\tau(u))}$ et d'autre part $a_{i,\sigma(i)} = a_{j,\sigma(\tau(j))}$ (et symétriquement) puisque $x_i = x_j$.

Puisque l'on dispose d'une union disjointe $\mathscr{S}_n = \mathscr{A}_n \cup \mathscr{A}_n\tau$, on voit donc que

$$\sum_{\sigma\in\mathscr{S}_n} a_{1,\sigma(1)}\cdots a_{n,\sigma(n)}\, e_\sigma$$

$$= \sum_{\sigma\in\mathscr{A}_n} a_{1,\sigma(1)}\cdots a_{n,\sigma(n)}(e_\sigma + e_{\sigma\tau})$$

et il suffit pour conclure de noter que

$$e_\sigma + e_{\sigma\tau} = (e_\sigma - (-1)^\sigma e_{\mathrm{Id}}) + (e_{\sigma\tau} - (-1)^{\sigma\tau} e_{\mathrm{Id}}). \quad \blacksquare$$

Remarque Plus généralement, on montre exactement de la même façon que le noyau de l'application canonique $\pi : \otimes^k E \to \wedge^k E$ a pour base les $e_{f(1)} \otimes \cdots \otimes e_{f(k)}$ avec f *non* injective et les $e_{f(\sigma(1))} \otimes \cdots \otimes e_{f(\sigma(k))} - (-1)^\sigma e_{f(1)} \otimes \cdots \otimes e_{f(k)}$ avec f strictement croissante et $\sigma \in \mathscr{S}_k \setminus \{\mathrm{Id}\}$.

Théoreme 5.4.6 Si E est un espace vectoriel de dimension finie, alors $\bigwedge^{\dim E} E$ est une droite. Plus précisément, si $(e_1,\ldots,e_n)$ est une base de E, alors $e_1 \wedge \cdots \wedge e_n$ est une base de $\bigwedge^n E$.

Démonstration. Il suffit de remarquer que, grâce au lemme, $e_1 \otimes \cdots \otimes e_n$ est une base d'un supplémentaire du noyau de $\pi : \otimes^n E \to \bigwedge^n E$. $\blacksquare$

Remarque

1. On voit donc qu'on associe à la base $\mathscr{B}$ un isomorphisme

$$K \simeq \bigwedge^n E, \quad a \mapsto a\, e_1 \wedge \cdots \wedge e_n.$$

2. Plus généralement, on aura

$$\dim \bigwedge^k E = \binom{n}{k} :$$

   si $(e_1,\ldots,e_n)$ est une base de E, alors les $e_{f(1)} \wedge \cdots \wedge e_{f(k)}$ avec $f : k \to n$ strictement croissante, forment une base de $\bigwedge^k E$.
3. On peut aussi montrer que les $e_1^{k_1}\ldots e_n^{k_n}$ avec $k_1,\ldots,k_n \in \mathbb{N}$ et $k_1 + \cdots + k_n = k$ forment une base de $\mathrm{S}^k(E)$ (penser aux polynômes en n variables de degré total k).

Proposition 5.4.7 Soient E un espace vectoriel de dimension finie et $u : E \to F$ une application linéaire. Si $\bigwedge^{\dim E} u \neq 0$, alors u est injective.

Démonstration. On se donne une base $\mathscr{B} := (e_1,\ldots,e_n)$ de E. Dire que u n'est pas injective signifie que $u(e_1),\ldots,u(e_n)$ sont liés si bien que, par le lemme 5.4.4, on aura

$$\bigwedge^n u(e_1 \wedge \cdots \wedge e_n) = u(e_1) \wedge \cdots \wedge u(e_n) = 0. \quad \blacksquare$$

Proposition 5.4.8 Soient E un espace vectoriel de dimension n et E' un sous-espace vectoriel de dimension n' de E. On dispose alors d'un isomorphisme

$$\begin{array}{ccc} \bigwedge^{n'} E' \otimes \bigwedge^{n-n'} E/E' & \xrightarrow{\simeq} & \bigwedge^n E \\ (x_1 \wedge \cdots \wedge x_{n'}) \otimes (\bar{x}_{n'+1} \wedge \cdots \wedge \bar{x}_n) & \longmapsto & x_1 \wedge \cdots \wedge x_n. \end{array}$$

Démonstration. Il faut s'assurer que cette application est bien définie (la linéarité étant immédiate). Or si $x_k \in E'$ pour $k > n'$, alors $x_1, \ldots, x_{n'}, x_k$ sont tous dans E', et donc liés car $\dim E' = n'$, et on a alors nécessairement $x_1 \wedge \cdots \wedge x_n = 0$. Cela implique que l'image d'un élément ne dépend que de $\bar{x}_k$ et pas de x_k en général. Il faut aussi s'assurer que cette application est bien un isomorphisme. Or, on peut toujours compléter une base $(e_1, \ldots, e_{n'})$ de E' en une base $(e_1, \ldots, e_n)$ de E et on voit alors que notre application envoie la base $(e_1 \wedge \cdots \wedge e_{n'}) \otimes (\bar{e}_{n'+1} \wedge \cdots \wedge \bar{e}_n)$ de $\bigwedge^{n'} E' \otimes \bigwedge^{n-n'} E/E'$ sur la base $e_1 \wedge \cdots \wedge e_n$ de $\bigwedge^n E$. ■

Proposition 5.4.9 Si E est un espace vectoriel de dimension n, on dispose d'un isomorphisme

$$\begin{array}{ccc} \bigwedge^n {}^tE & \xrightarrow{\simeq} & {}^t\bigwedge^n E \\ (\varphi_1 \wedge \cdots \wedge \varphi_n) & \longmapsto & (x_1 \wedge \cdots \wedge x_n \mapsto \varphi_1(x_1) \ldots \varphi_n(x_n)). \end{array}$$

Démonstration. L'existence de l'application résulte des propriétés universelles et si on choisit une base $(e_1, \ldots, e_n)$ de E, alors la base ${}^te_1 \wedge \cdots \wedge {}^te_n$ est envoyée sur la base ${}^t(e_1 \wedge \cdots \wedge e_n)$. ■

5.5 Déterminant

Dans cette section, on suppose que tous les espaces vectoriels sont de dimension finie.

Définition 5.5.1 Soient E un espace de vectoriel de dimension n et $\mathscr{B}$ une base de E. Alors, le *déterminant* associé à la base $\mathscr{B}$ est l'application composée

$$\det_{\mathscr{B}} : E \times \cdots \times E \to \bigwedge^n E \simeq K,$$

où la première flèche est l'application canonique et la seconde est l'inverse de l'isomorphisme associé à la base $\mathscr{B}$.

Remarque Par définition, si $\mathscr{B} := (e_1, \ldots, e_n)$ et $x_1, \ldots, x_n \in E$, alors $\det_{\mathscr{B}}(x_1, \ldots, x_n)$ est l'unique élément de K tel que

$$x_1 \wedge \cdots \wedge x_n = \det_{\mathscr{B}}(x_1, \ldots, x_n)\, e_1 \wedge \cdots \wedge e_n.$$

Proposition 5.5.2 Si E est un espace vectoriel de dimension n et $\mathscr{B}$ une base de E, alors $\det_{\mathscr{B}}$ est une une forme n-linéaire alternée. De plus, si $\mathscr{B} := (e_1, \ldots, e_n)$ et pour tout $i = 1, \ldots, n$, $x_i = a_{i,1}e_1 + \cdots + a_{i,n}e_n$, on a

$$\det_{\mathscr{B}}(x_1, \ldots, x_n) := \sum_{\sigma \in \mathscr{S}_n} (-1)^\sigma a_{1,\sigma(1)} \ldots a_{n,\sigma(n)}.$$

Démonstration. Pour obtenir la première assertion, il suffit de rappeler que le déterminant est la composée d'une application multilinéaire alternée et d'une application linéaire. Pour démontrer la seconde, on rappelle d'abord que, par multilinéarité, on a

$$x_1 \wedge \cdots \wedge x_n = \sum_{f : n \to n} a_{1,f(1)} \ldots a_{n,f(n)}\, e_{f(1)} \wedge \cdots \wedge e_{f(n)}.$$

Comme l'application est alternée, si $f \notin \mathscr{S}_n$, on a nécessairement $e_{f(1)} \wedge \cdots \wedge e_{f(n)} = 0$. Et comme une application alternée est antisymétrique, si $\sigma \in \mathscr{S}_n$, alors $e_{\sigma(1)} \wedge \cdots \wedge e_{\sigma(n)} = (-1)^\sigma e_1 \wedge \cdots \wedge e_n$. ■

Remarque On en déduit immédiatement l'effet des opérations élémentaires sur les déterminants :
1. Multiplier un vecteur par un scalaire revient à multiplier le déterminant par ce même scalaire,
2. Échanger deux vecteurs revient à changer le signe du déterminant,
3. Ajouter à un vecteur un multiple d'un autre vecteur ne change pas le déterminant.

Définition 5.5.3 Soient E un espace vectoriel de dimension n et $u \in L(E)$. Alors, le *déterminant* de u est la composante $\det(u)$ de $\bigwedge^n u$ dans la base canonique de $L(\bigwedge^n E)$.

Remarque 1. Par définition, $\det(u)$ est l'unique élément de K tel que si $x_1, \dots, x_n \in E$, alors

$$u(x_1) \wedge \cdots \wedge u(x_n) = \det(u) x_1 \wedge \cdots \wedge x_n.$$

2. Comme ce fut le cas pour sa trace, nous voyons donc que le déterminant d'un endomorphisme ne dépend pas du choix de la base (contrairement au déterminant d'une famille de vecteurs).
3. Si $\mathscr{B}$ est une base de E, on aura

$$\det(u) = \det_{\mathscr{B}}(u(\mathscr{B})).$$

4. Si $A = [a_{i,j}]$ est la matrice de u dans la base $\mathscr{B}$, on aura

$$\det(u) := \sum_{\sigma \in \mathscr{S}_n} (-1)^{\sigma} a_{1,\sigma(1)} \dots a_{n,\sigma(n)}.$$

5. On définit le *déterminant* d'une matrice $A \in \mathrm{M}_n(K)$ comme étant le déterminant de l'application linéaire $u \in L(K^n)$ qui lui est associée. C'est aussi le déterminant des vecteurs colonnes de A.
6. Puisque le déterminant ne dépend pas de la base, voit que si A et A' sont des matrices semblables, alors $\det(A) = \det(A')$.

Proposition 5.5.4 Soit E un espace vectoriel (de dimension finie). Alors,
1. si $u, v \in L(E)$, on a $\det(u \circ v) = \det(u)\det(v)$,
2. Si $u \in \mathrm{L}(E)$, alors $u \in \mathrm{GL}(E)$ si et seulement si $\det u \neq 0$, et alors

$$\det(u^{-1}) = \frac{1}{\det(u)}.$$

Démonstration. 1. Résulte immédiatement du fait que $\bigwedge^n(u \circ v) = \bigwedge^n u \circ \bigwedge^n v$.
2. Si u est inversible, on a $\det(u)\det(u^{-1}) = \det(u \circ u^{-1}) = \det(\mathrm{Id}_E) = 1$. Cela montre que $\det(u) \neq 0$ et on obtient bien la formule annoncée. Réciproquement, il résulte du lemme 5.4.7 que si $\det u \neq 0$, alors u est injective et c'est donc nécessairement un automorphisme. ∎

Remarque 1. On dispose donc d'un morphisme multiplicatif $\det : \mathrm{L}(E) \to K$, qui induit un morphisme de groupes $\mathrm{GL}(E) \to K^{\times}$, dont le noyau est le sous-groupe

$$\mathrm{SL}(E) = \{u \in \mathrm{L}(E) \ / \ \det(u) = 1\}.$$

2. Si on travaille sur un anneau, il faut remplacer la condition $\det(u) \neq 0$ par la condition $\det(u)$ inversible. Et de même ci-dessous pour les matrices.

Corollaire 5.5.5 1. Si $A, B \in \mathrm{M}_n(K)$, alors $\det(AB) = \det(A)\det(B)$.
2. Si $A \in \mathrm{M}_n(K)$, on a $A \in \mathrm{GL}_n(K) \Leftrightarrow \det(A) \neq 0$, et alors $\det(A^{-1}) = \det(A)^{-1}$.

Démonstration. ■

Remarque 1. Comme pour la trace, on aurait pu procéder à l'envers : définir d'abord le déterminant d'une matrice, montrer la formule $\det(AB) = \det(A)\det(B)$ par un calcul, en déduire que deux matrices semblables ont le même déterminant, puis utiliser cela pour définir le déterminant d'une application linéaire, etc.
2. Notons que l'on a encore ici un morphisme multiplicatif $\det : \mathrm{M}_n(K) \to K$ qui induit un morphisme de groupes $\mathrm{GL}_n(K) \to K^\times$ dont le noyau est le sous-groupe

$$\mathrm{SL}_n(K) = \{A \in \mathrm{M}_n(K)) \ / \ \det(A) = 1\}.$$

Corollaire 5.5.6 Soit E un espace vectoriel de dimension n muni d'une base $\mathscr{B}$. Alors, $x_1, \ldots, x_n \in E$ forment une base de E si et seulement si $\det_{\mathscr{B}}(x_1, \ldots, x_n) \neq 0$.

Démonstration. ■

Proposition 5.5.7 Soient E un espace vectoriel (de dimension finie), $u \in L(E)$, E' un sous-espace vectoriel de E stable par u et $u' \in L(E'), u'' \in L(E/E')$ les applications induites. On a alors

$$\det(u) = \det(u') \ \det(u'').$$

Démonstration. Résulte facilement de la proposition 5.4.8. Les détails sont laissés en exercice. ■

Remarque 1. On en déduit le calcul d'un déterminant triangulaire par blocs : si

$$A := \begin{bmatrix} A' & \star \\ 0 & A'' \end{bmatrix},$$

alors $\det(A) = \det(A')\det(A'')$.
2. On peut aussi montrer directement cette égalité à partir de la formule du déterminant. En effet, on a $a_{i,j} = 0$ pour $i > n'$ et $j \leq n'$. On en déduit que $a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} = 0$ sauf si $\sigma(\{1, \ldots, n'\}) \subset \{1, \ldots, n'\}$ et $\sigma(\{n'+1, \ldots, n\}) \subset \{n'+1, \ldots, n\}$. On désigne alors par σ' la restriction de σ à $\{1, \ldots, n'\}$ et on pose $\sigma''(i) = \sigma(n'+i) - i$ pour $i = 1, \ldots, n''$. On voit donc que

$$\begin{aligned}
\det(A) &= \sum_{\sigma' \in \mathscr{S}_{n'}, \sigma'' \in \mathscr{S}_{n''}} (-1)^{\sigma'}(-1)^{\sigma''} a_{1,\sigma'(1)} \cdots a_{n',\sigma'(n')} a_{n'+1,n'+\sigma''(1)} \cdots a_{n'+n'',n'+\sigma''(n'')} \\
&= \sum_{\sigma' \in \mathscr{S}_{n'}} (-1)^{\sigma'} a_{1,\sigma'(1)} \cdots a_{n',\sigma'(n')} \sum_{\sigma'' \in \mathscr{S}_{n''}} (-1)^{\sigma''} a_{n'+1,n'+\sigma''(1)} \cdots a_{n'+n'',n'+\sigma''(n'')} \\
&= \det(A') \ \det(A'').
\end{aligned}$$

3. Comme conséquence, on voit que le déterminant d'une matrice triangulaire est égal au produit des éléments diagonaux :

$$\det\left(\begin{bmatrix} a_1 & \star & \cdots & \star \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \cdots & 0 & a_n \end{bmatrix}\right) = a_1 \cdots a_n.$$

Proposition 5.5.8 Si E est un espace vectoriel (de dimension finie) et $u \in L(E)$, on a

$$\det({}^t u) = \det(u).$$

Démonstration. Grâce à la proposition 5.4.9, l'assertion se ramène facilement au cas $\dim E = 1$ qui se vérifie à la main. Les détails sont de nouveau laissés en exercice. ■

Remarque 1. Comme cas particulier, on voit que si A est une matrice carrée, alors

$$\det({}^t A) = \det(A).$$

2. On peut bien sûr montrer directement ce résultat en remarquant que la bijection $\sigma \leftrightarrow \sigma^{-1}$ de $\mathscr{S}_n$ sur lui même fournit une égalité

$$\det(A) = \sum_{\sigma \in \mathscr{S}_n} (-1)^{\sigma^{-1}} a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)} = \sum_{\sigma \in \mathscr{S}_n} (-1)^{\sigma} a_{\sigma(1),1} \cdots a_{\sigma(n),n}.$$

Définition 5.5.9 Si $A \in \mathrm{M}_n(K)$, on dit que

$$a'_{i,j} := \det(A + \mathbb{1}_{i,j}) - \det(A)$$

est un *cofacteur* de A et que la matrice $A' := [a'_{i,j}]$ est la *comatrice* de A.

Remarque 1. Si on note $C_1, \dots, C_n$ (resp. $\mathbb{1}_1, \dots, \mathbb{1}_n$) les colonnes de A (resp. de I), on aura

$$\begin{aligned} a'_{i,j} &= C_1 \wedge \cdots \wedge C_{i-1} \wedge C_i + \mathbb{1}_j \wedge C_{i+1} \wedge \cdots C_n - C_1 \wedge \cdots \wedge C_n \\ &= C_1 \wedge \cdots \wedge C_{i-1} \wedge \mathbb{1}_j \wedge C_{i+1} \wedge \cdots \wedge C_n. \end{aligned}$$

2. En pratique, le cofacteur s'obtient en effaçant la i-ème ligne et la j-ème colonne et en multipliant par $(-1)^{i+j}$.

Proposition 5.5.10 — Formules de Laplace. Si A est une matrice carrée et A' sa comatrice, on a

$$A\,{}^t\!A' = {}^t\!A' A = \det(A) I.$$

Démonstration. Exercice. ■

Remarque 1. Si on pose $A := [a_{i,j}]$ et $A' := [a'_{i,j}]$, alors les formules de Laplace disent que

$$\forall i \in \{1, \dots, n\}, \quad a_{i,1}a'_{i,1} + \cdots + a_{i,n}a'_{i,n} = a_{1,i}a'_{1,i} + \cdots + a_{n,i}a'_{n,i} = \det(A)$$

et

$$\forall i \neq j \in \{1, \dots, n\}, \quad a_{i,1}a'_{j,1} + \cdots + a_{i,n}a'_{j,n} = a_{1,i}a'_{1,j} + \cdots + a_{n,i}a'_{n,j} = 0.$$

2. En particulier, les formules de Laplace permettent de développer un déterminant le long d'une ligne ou d'une colonne.
3. Si $A \in \mathrm{GL}_n(K)$ et A' désigne sa comatrice, alors

$$A^{-1} = \frac{1}{\det(A)} {}^t\!A'.$$

5.6 Exercices

Exercice 5.1
1. Montrer que si E est un espace vectoriel, alors l'application canonique $E \times {}^tE \to K$ est une forme bilinéaire.
2. Montrer que le produit scalaire usuel est une forme bilinéaire symétrique sur K^n.
3. Montrer que le produit vectoriel est une application bilinéaire alternée sur K^3.
4. Montrer que le produit est bilinéaire sur une algèbre, et qu'il est symétrique si et seulement si l'algèbre est commutative.
5. Montrer que la composition des applications linéaires est bilinéaire.
6. Montrer que l'application $(f,g) \mapsto \int_0^1 f(t)g(t)\mathrm{d}t$ est une forme bilinéaire symétrique sur $\mathscr{C}([0,1],\mathbb{R})$.

Exercice 5.2 Montrer que si E est un espace vectoriel sur K avec $\mathrm{Car}(K) \neq 2$, on a un isomorphisme

$$\mathrm{L}_2(E,F) \simeq \mathrm{S}_2(E,F) \oplus \mathrm{A}_2(E,F)$$

(on pourra considérer la symétrie s définie par $s(\Phi)(x,y) = \Phi(y,x)$).

Exercice 5.3
1. Montrer que si $\Phi : E \times \cdots \times E \to F$ est une application multilinéaire symétrique et $u : E' \to E$ est une application linéaire, alors l'application multilinéaire composée $\Phi \circ (u \times \cdots \times u)$ est aussi symétrique.
2. En déduire que si E' est un sous-espace de E, alors la restriction de Φ à $E' \times \cdots \times E'$ est aussi symétrique.
3. Montrer que si $u : F \to F'$ est une application linéaire alors l'application multilinéaire composée $u \circ \Phi$ est aussi symétrique.
4. Mêmes questions avec « antisymétrique » ou « alternée » au lieu de « symétrique ».

Exercice 5.4
1. Établir des isomorphismes

$$K \otimes_K E \simeq E, \quad F \otimes_K E \simeq E \otimes_K F \quad \text{et} \quad (E \otimes_K F) \otimes_K G \simeq E \otimes_K (F \otimes_K G)$$

lorsque E, F et G sont des espaces vectoriels sur K.
2. Montrer que si $E = \oplus_{s\in S} E_s$, alors $\oplus_{s\in S}(E_s \otimes_K F) \simeq E \otimes_K F$.
3. Montrer que si E' est un sous-espace vectoriel de E, alors $E' \otimes_K F$ est un sous-espace vectoriel de $E \otimes_K F$ et que $(E \otimes_K F)/(E' \otimes_K F) \simeq E/E' \otimes_K F$.
4. Établir un isomorphisme ${}^tE \otimes_K {}^tF \simeq {}^t(E \otimes_K F)$ quand E et F sont de dimension finie.

Exercice 5.5 On rappelle qu'une *extension* L du corps K est une K-algèbre qui est un corps.
1. Montrer que si E est un K-espace vectoriel, il existe une unique structure de L-espace vectoriel sur $L \otimes_K E$ telle que $\alpha(\beta \otimes x) = \alpha\beta \otimes x$ si $\alpha, \beta \in L$ et $x \in E$.
2. Montrer que si $(e_i)_{i\in I}$ est une base de E sur K, alors $(1 \otimes e_i)_{i\in I}$ est une base de $L \otimes_K E$ sur L.
3. En déduire que $\dim_L(L \otimes_K E) = \dim_K E$.

Exercice 5.6 Montrer que si les familles $(u_i)_{i\in I}$ et $(v_j)_{j\in J}$ sont libres dans E et F respectivement, alors $(u_i \otimes v_j)_{i\in I, j\in J}$ est une famille libre de $E \otimes_K F$. En déduire que si $u \otimes v = 0$, alors $u = 0$ ou $v = 0$.

Exercice 5.7
1. Montrer qu'il existe un unique isomorphisme de $\mathbb{R}$-espaces vectoriels $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}, z_1 \otimes z_2 \mapsto (z_1 z_2, z_1 \bar{z}_2)$ (on pourra choisir une base de chaque coté et expliciter la matrice).
2. À quoi correspond la conjugaison complexe sous l'isomorphisme naturel ${}^t\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq$

$\mathrm{End}_{\mathbb{R}}(\mathbb{C})$.

Exercice 5.8 Soit E un espace vectoriel de dimension finie n. Que valent $\mathrm{Tr}(\mathrm{Id}_E)$? Quelle est la trace d'une projection sur un sous-espace F de dimension m ? d'une symétrie par rapport à F ? d'une transvection ? Mêmes questions à propos du déterminant.

Exercice 5.9 Quelle est la trace d'une rotation d'angle θ dans $\mathbb{R}^2$? d'une rotation d'angle θ et d'axe Δ dans $\mathbb{R}^3$? Mêmes questions à propos du déterminant.

Exercice 5.10 On considère $z \in \mathbb{C}$ comme un endomorphisme du $\mathbb{R}$-espace vectoriel $\mathbb{C}$ (via la multiplication par z). Que valent $\mathrm{tr}(z)$ et $\det(z)$?

Exercice 5.11 Montrer par un exemple qu'on a pas toujours $\mathrm{tr}(u \circ v) = \mathrm{tr}(u)\mathrm{tr}(v)$ ni $\det(u+v) = \det u + \det v$.

Exercice 5.12 Montrer qu'en posant $\varphi_A(B) = \mathrm{tr}(AB)$, on obtient un isomorphisme

$$\mathrm{M}_n(K) \simeq {}^t\mathrm{M}_n(K), \quad A \mapsto \varphi_A.$$

Exercice 5.13 Démontrer les formules de Laplace (proposition 5.5.10).

Exercice 5.14 Calculer pour tout $n \geq 2$

$$\Delta_n := \begin{vmatrix} 0 & \cdots & \cdots & 0 & a_n \\ x & \ddots & & \vdots & a_{n-1} \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & x & a_1 \end{vmatrix} \quad \text{puis} \quad \Gamma_n := \begin{vmatrix} x & 0 & \cdots & 0 & a_n \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & x & a_1 \\ a_n & \cdots & \cdots & a_1 & x \end{vmatrix}.$$

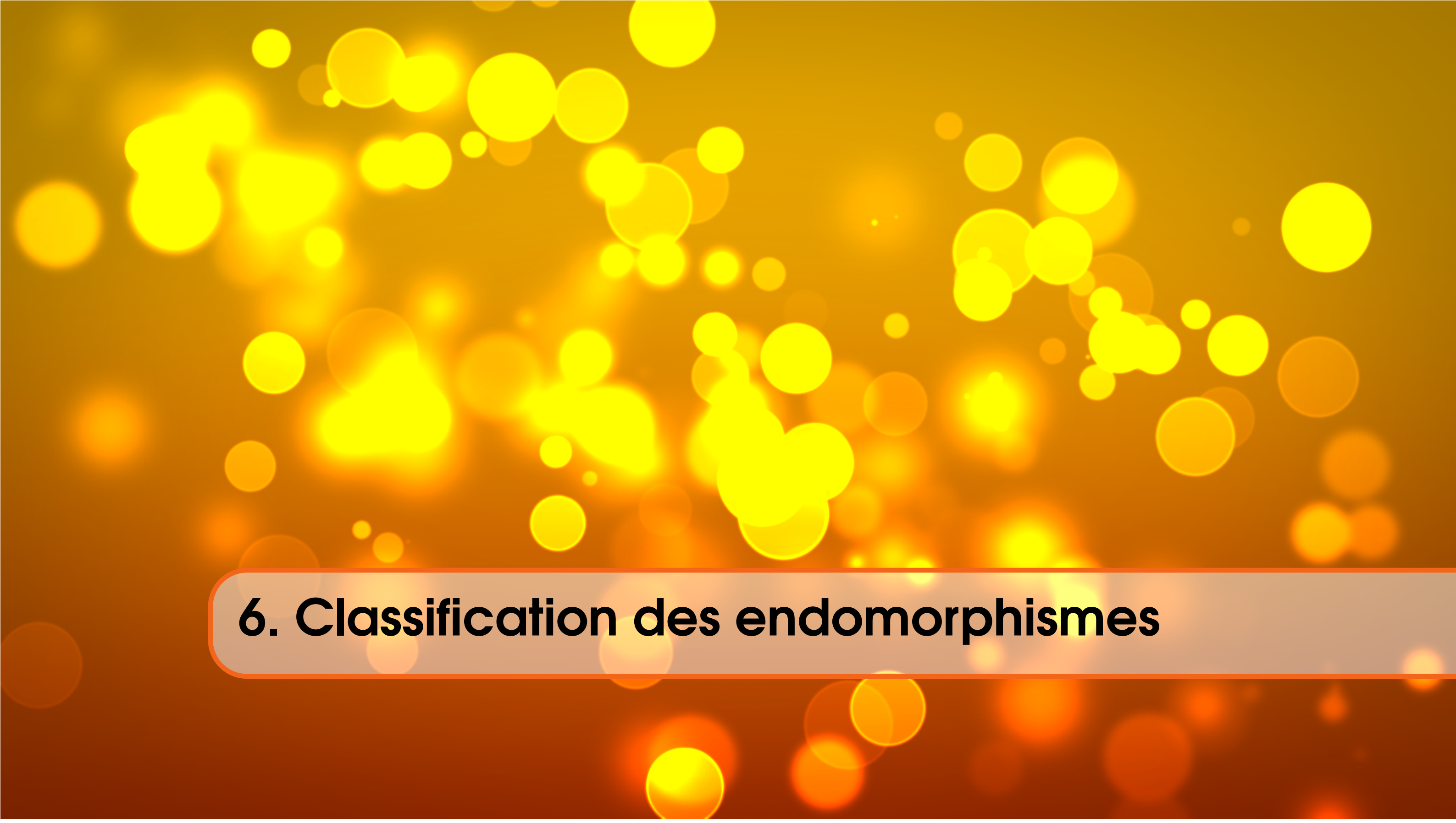
Exercice 5.15 On veut calculer

$$\Delta := \begin{vmatrix} \lambda_1 & b & \cdots & b \\ a & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ a & \cdots & a & \lambda_n \end{vmatrix}$$

avec $a \neq b$. Montrer que

$$\Delta(X) := \begin{vmatrix} \lambda_1 + X & b+X & \cdots & b+X \\ a+X & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b+X \\ a+X & \cdots & a+X & \lambda_n + X \end{vmatrix}$$

est un polynôme de degré (au plus) 1. Calculer $\Delta(-a)$ et $\Delta(-b)$. En déduire Δ.



6. Classification des endomorphismes

On fixe un corps de scalaires K.

6.1 Polynôme annulateur

Définition 6.1.1 Soient L une algèbre et $u \in L$. On dit que $P \in K[T]$ est un *polynôme annulateur* de u si $P(u) = 0$.

Exemple $T^2 + 1$ est un polynôme annulateur de $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in \mathrm{M}_2(K)$:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Remarque

1. Si on se donne $u \in L$, on peut considérer le morphisme d'algèbres
$$\Phi : K[T] \to L, \quad P \mapsto P(u). \tag{6.1}$$
On voit donc que P est un polynôme annulateur de u si et seulement si $P \in \ker \Phi$.
2. Le noyau d'un morphisme d'anneaux est un idéal. Il suit que les polynômes annulateurs de u forment un idéal.

Lemme 6.1.2 Si L est une algèbre *de dimension finie* et $u \in L$, alors il existe un polynôme annulateur non nul pour u.

Démonstration. En appliquant le théorème du rang au morphisme (6.1), on voit que

$$\dim K[T] = \dim \ker \Phi + \dim \operatorname{im} \Phi.$$

Comme $K[T]$ est de dimension infinie mais que $\dim \operatorname{im} \Phi \leq \dim L$ est finie, on voit que $\ker \Phi$ est de dimension infinie, et en particulier, $\ker \Phi \neq \{0\}$. ■

Remarque Si E est un espace vectoriel de dimension n, alors $L(E)$ est une algèbre de dimension n^2 et le lemme s'applique. Il en va bien sûr aussi de même pour $M_n(K)$.

Proposition 6.1.3 Si L est une K-algèbre et $u \in L$, il existe un unique polynôme unitaire μ_u tel que les polynômes annulateurs de u soient les multiples de μ_u. Si L est de dimension finie, alors μ_u est le polynôme unitaire annulateur non nul de plus bas degré.

Démonstration. En effet, tout idéal non nul de $K[T]$ est de la forme (M) pour un unique M unitaire. Et M est le polynôme unitaire non nul de plus bas degré dans l'idéal si ce dernier n'est pas nul. ■

Définition 6.1.4 On dit alors que μ_u est le *polynôme minimal* de u.

Exemple T^2+1 est le polynôme minimal de $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in \mathrm{M}_2(K)$.

Définition 6.1.5 Si E est un espace vectoriel de dimension finie et $u \in L(E)$, alors le *polynôme caractéristique* de u est

$$\chi_u := \det(T\mathrm{Id}_E - u) \in K[T].$$

Remarque

1. Plus précisément, il faut remarquer que $K[T] \otimes E$ est naturellement un $K[T]$-module et poser $\chi_u := \det_{K[T]}(T\mathrm{Id}_{K[T]} \otimes \mathrm{Id}_E - \mathrm{Id}_{K[T]} \otimes u)$.
2. Si K est infini, on peut procéder autrement : poser pour chaque $a \in K$, $\chi_u(a) := \det(a\mathrm{Id}_E - u) \in K$ et montrer que l'application ainsi obtenue est polynomiale.
3. On peut aussi choisir une base $\mathscr{B}$ de E et poser brutalement
$$\chi_u := \sum_{\sigma \in \mathscr{S}_n} (-1)^\sigma \prod_{\sigma(i) \neq i} (-a_{i,\sigma(i)}) \prod_{\sigma(i)=i} (T - a_{i,\sigma(i)})$$
si $[u]_{\mathscr{B}} = [a_{i,j}]_{i,j=1}^n$. Il faut alors s'assurer que la définition est indépendante de la base.
4. Bien sûr, comme d'habitude, le *polynôme caractéristique* d'une matrice carrée A est par définition le polynôme caractéristique de l'endomorphisme u de K^n associé à A.
5. Attention, on rencontre aussi parfois la définition $\chi_u := \det(u - T\mathrm{Id}_E)$ qui diffère de la notre par un signe en dimension impaire.
6. En développant, on voit que l'on a (avec notre définition)
$$\chi_u = T^n - \mathrm{tr}(u)T^{n-1} + \cdots + (-1)^n \det(u).$$

Théoreme 6.1.6 — de Cayley-Hamilton. Soient E un espace vectoriel de dimension finie et $u \in L(E)$. Alors, le polynôme caractéristique de u est un polynôme annulateur de u.

Démonstration. On choisit une base afin de se ramener à l'énoncé analogue avec des matrices. Soient donc A une matrice carrée d'ordre n et $\chi(T)$ son polynôme caractéristique. Si on désigne par $B(T)$ la transposée de la comatrice de $TI - A$, on a

$$B(T)(TI - A) = \chi(T)I. \tag{6.2}$$

Il suffit alors de substituer A à T. ■

Remarque

1. Remarquons que l'égalité (6.2) a lieu dans l'anneau de matrices $M_n(K[T])$, que l'on identifie avec l'anneau des polynômes $M_n(K)[T]$. On utilise ensuite la propriété universelle de l'anneau des polynômes (qui est aussi valide sur l'anneau non commutatif $M_n(K)$).

2. Alternativement, si on pose $B(T) = \sum B_i T^i$ et $\chi(T) = \sum a_i T^i$, et qu'on développe le premier terme de l'égalité (6.2), on obtient pour chaque indice i, $B_{i-1} - B_i A = a_i I$. Ensuite, si on multiplie par A^i, qu'on additionne et qu'on factorise, on obtient $B(A)(A-A) = \chi(A)$.

Proposition 6.1.7 Soient E un espace vectoriel de dimension finie, $u \in L(E)$ et $E' \subset E$ un sous-espace vectoriel stable par u. On désigne par $u' \in L(E')$ et $u'' \in L(E/E')$ les applications induites. Alors,
1. $\chi_u = \chi_{u'} \chi_{u''}$, et en particulier $\chi_{u'}, \chi_{u''} \mid \chi_u$,
2. $\mu_{u'}, \mu_{u''} \mid \mu_u$.

Démonstration. 1. Résulte immédiatement de la proposition 5.5.7.
2. Il suffit de remarquer que μ_u est un polynôme annulateur de u' et de u''.

■

Remarque 1. En terme de matrices, on voit que si

$$A := \begin{bmatrix} A' & \star \\ 0 & A'' \end{bmatrix},$$

alors $\chi_A = \chi_{A'} \chi_{A''}$ et $\mu_{A'}, \mu_{A''} \mid \mu_A$.
2. Comme cas particulier de la proposition, on voit aussi que si $u_1 \in L(E_1)$ et $u_2 \in L(E_2)$, alors $\chi_{u_1 \times u_2} = \chi_{u_1} \chi_{u_2}$, et $\mu_{u_1}, \mu_{u_2} \mid \mu_u$. En termes de matrices, ça correspond au cas ou le bloc supérieur droit aussi est nul.
3. Attention cependant, on a $\mu_u \neq \mu_{u'} \mu_{u''}$ en général. Prenons par exemple

$$A := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

avec $A' = A'' = 1$. On a donc $\mu_A = \mu_{A'} = \mu_{A''} = T - 1$ mais $(T-1)^2 \neq T - 1$.

Lemme 6.1.8 — des noyaux. Soient $P_1, \ldots, P_r \in K[T]$ premiers entre eux deux à deux et $P := P_1 \ldots P_r$. Si E est un espace vectoriel de dimension finie et $u \in L(E)$, alors

$$\ker P(u) \simeq \ker P_1(u) \oplus \cdots \oplus \ker P_r(u).$$

De plus, les projections associées sont polynomiales en u.

Démonstration. Par récurrence, on peut se ramener au cas $r = 2$ (exercice). Posons alors $E_0 := \ker P(u), E_1 := \ker P_1(u), E_2 := \ker P_2(u)$. Puisque $P = P_1 P_2$, on voit que $E_1, E_2 \subset E_0$ et on désignera par i_1 et i_2 les applications d'inclusion. Le théorème de Bézout affirme qu'il existe $Q_1, Q_2 \in K[T]$ tels que

$$Q_2 P_1 + Q_1 P_2 = 1.$$

Puisque $P_1 Q_1 P_2 = Q_1 P$, on voit que $(Q_1 P_2)(u)$ induit une application (linéaire) $p_1 : E_0 \to E_1$. Et on obtient symétriquement une application $p_2 : E_0 \to E_2$. On vérifie aisément (exercice) que

$$p_1 \circ i_1 = \mathrm{Id}, \quad p_2 \circ i_2 = \mathrm{Id}, \quad p_1 \circ i_2 = 0, \quad p_2 \circ i_1 = 0 \quad \text{et} \quad i_1 \circ p_1 + i_2 \circ p_2 = \mathrm{Id},$$

et il suit que nous disposons bien d'une somme directe. ■

Remarque 1. Dans le cas ou P est un polynôme annulateur de E (par exemple le polynôme minimal ou le polynôme caractéristique), on obtient

$$E \simeq \ker P_1(u) \oplus \cdots \oplus \ker P_r(u).$$

2. Comme $K[T]$ est *factoriel*, si P est un polynôme quelconque, on peut toujours écrire $P = P_1^{m_1}\cdots P_r^{m_r}$ avec $P_1,\ldots,P_r$ irréductibles, et on aura donc
$$\ker P(u) \simeq \ker P_1(u)^{m_1} \oplus \cdots \oplus \ker P_r(u)^{m_r}.$$
3. Si P et Q sont deux polynômes quelconques, alors $\ker P(u)$ est toujours stable par $Q(u)$ puisque $K[T]$ est commutatif. En particulier, on voit que dans le lemme, aussi bien $\ker P(u)$ que tous les $\ker P_i(u)$ sont stables par u.
4. Cette dernière remarque peut être reformulée en disant que le lemme des noyaux donne une décomposition en somme directe de $K[T]$-modules (et pas seulement d'espaces vectoriels).

Exemple Si p est une projection (resp. s est une symétrie), on peut considérer le polynôme $T-T^2 = T(1-T)$ (resp. $1-T^2 = (1-T)(1+T)$) et on retrouve la décomposition en somme directe
$$E = \ker p \oplus \ker(\mathrm{Id}-p) \quad (\text{resp.} \quad E = \ker(\mathrm{Id}-s)\oplus\ker(\mathrm{Id}+s)).$$

6.2 Diagonalisation

Définition 6.2.1
1. Une matrice carrée $A := [a_{i,j}]$ est *diagonale* si $a_{i,j} = 0$ pour $i \neq j$.
2. Un endomorphisme u d'un espace vectoriel E de dimension finie est *diagonalisable* dans une base $\mathscr{B}$ de E si $[u]_{\mathscr{B}}$ est diagonale.

Remarque On dira qu'une matrice carrée A est *diagonalisable* si l'endomorphisme u de K^n correspondant est diagonalisable. Cela signifie que A est semblable à une matrice diagonale D. En d'autres termes, il existe P inversible et D diagonale telles que $A = PDP^{-1}$.

Exemple La matrice $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ n'est pas diagonalisable sur $\mathbb{R}$ (mais elle l'est sur $\mathbb{C}$).

Définition 6.2.2 Soit u un endomorphisme d'un espace vectoriel de dimension finie E.
1. Si $u(x) = ax$ avec $x \in E \setminus \{0\}$ et $a \in K$, on dit que a est une *valeur propre* pour u et que x est un *vecteur propre* pour a.
2. Si $a \in K$, on pose
$$E_a := \ker(a\mathrm{Id}_E - u),$$
et on dit que E_a est un *sous-espace propre* si $E_a \neq \{0\}$.

Remarque
1. Par définition, on a $x \in E_a \Leftrightarrow u(x) = ax$.
2. E_a est un sous-espace vectoriel de E qui est stable par u : si $x \in E_a$ alors $u(x) \in E_a$.
3. Comme E_a est stable par u, on peut considérer l'endomorphisme induit u_a et on a $u_a - a\mathrm{Id}_{E_a} = 0$ si bien que $T-a$ est un polynôme annulateur de u_a.

Exemple
1. Si $\mathscr{B}$ est une base formée de vecteurs *propres* $e_1,\ldots,e_n$ de u, on peut écrire pour tout $i = 1,\ldots,n$, $u(e_i) = a_ie_i$ et la matrice de u dans la base $\mathscr{B}$ est diagonale :
$$A = \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_n \end{bmatrix}.$$

Réciproquement, si on se donne une telle matrice diagonale A, et $(x_1,\dots,x_n)\in K^n$, on aura

$$\begin{aligned} A[x]=a[x] &\Leftrightarrow \forall i=1,\dots,n, \quad a_ix_i=ax_i \\ &\Leftrightarrow \forall i=1,\dots,n, \quad a_i=a \quad \text{ou} \quad x_i=0 \end{aligned}$$

On voit donc que les valeurs propres de A sont $a_1,\dots,a_n$ et que pour tout $i=1,\dots,n$, le vecteur $\mathbb{1}_i$ est un vecteur propre pour a_i.

2. Si A est une matrice diagonale, on peut réorganiser la diagonale (quitte à permuter les vecteurs de la base canonique) pour écrire

$$A=\begin{bmatrix} a_1I_{m_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_rI_{m_r} \end{bmatrix}$$

avec $a_1,\dots,a_r$ *distincts*. Les sous espaces propres sont alors

$$E_1:=\mathrm{Vect}(\mathbb{1}_1,\dots,\mathbb{1}_{m_1}),\dots,E_r:=\mathrm{Vect}(\mathbb{1}_{n-m_r+1},\dots,\mathbb{1}_n).$$

En particulier, on a

$$E\simeq E_1\oplus\cdots\oplus E_r \quad \text{et} \quad \chi_A=(T-a_1)^{m_1}\cdots(T-a_r)^{m_r},$$

si bien que $\dim E_i=\mathrm{mult}_{\chi_A}(a_i)$.

Proposition 6.2.3 Soit u un endomorphisme d'un espace vectoriel de dimension finie E. Pour $a\in K$, les conditions suivantes sont équivalentes :

1. a est une valeur propre pour u,
2. $E_a\neq\{0\}$,
3. $\chi_u(a)=0$,
4. $\mu_u(a)=0$.

Dans ce cas, si $x\in E$, les condition suivantes sont équivalentes :

1. x est un vecteur propre pour a,
2. $x\in E_a\setminus\{0\}$.

Démonstration. Dire que x est un vecteur propre pour a signifie que $x\neq 0$ et que $u(x)=ax$. Et cette dernière condition signifie que $x\in E_a$. On voit donc que les deux première assertions sont équivalentes et on obtient aussi la dernière propriété.

D'autre part, on sait que $\chi_u(a)$ est non nul si et seulement si $a\mathrm{Id}_E-u$ est bijectif, c'est à dire injectif, ce qui signifie que son noyau est nul. La troisième assertion est donc aussi équivalente aux deux premières. Et elles sont toutes impliquées par la dernière puisque $\mu_u\mid\chi_u$.

Enfin, comme $T-a$ est un polynôme annulateur de u_a sur E_a, on voit que si $E_a\neq 0$, alors $T-a=\mu_{u_a}\mid\mu_u$, et on a donc donc $\mu_u(a)=0$. Cela montre que les premières assertions impliquent aussi la dernière. ■

Remarque La proposition nous dit que le polynôme minimal et le polynôme caractéristique ont les mêmes racines et que ces racines sont exactement les valeurs propres de u.

Théoreme 6.2.4 Soient E un espace vectoriel de dimension finie et $u \in \mathrm{L}(E)$. Alors, les conditions suivantes sont équivalentes

1. u est diagonalisable,
2. E est somme directe des sous-espaces propres pour u,
3. μ_u est scindé à racines simples,
4. χ_u est scindé et, si a est une valeur propre pour u, alors

$$\dim E_a = \mathrm{mult}_{\chi_u}(a).$$

Démonstration. Soient $a_1, \ldots, a_r$ les valeurs propres (distinctes) de u et $E_1, \ldots, E_r$ les sous-espaces propres associés. Si on applique le lemme des noyaux à

$$P := (T - a_1) \cdots (T - a_r) \in K[T],$$

on voit que

$$\ker P(u) \simeq E_1 \oplus \cdots \oplus E_r.$$

et on en déduit que E est somme directe de ses sous-espaces propres si et seulement $\ker P(u) = E$, ce qui signifie que P est un polynôme annulateur de u. On a alors obligatoirement $\mu_u = P$ grâce à la proposition 6.2.3 et il suit que les conditions du milieu sont équivalentes.

Si u est diagonalisable dans une base $\mathscr{B}$, on sait alors que la dernière condition est satisfaite. On sait aussi, dans ce cas, que E est somme directe de sous-espaces propres. Réciproquement, si cette hypothèse est satisfaite, il existe une base formée de vecteurs propres et u est diagonalisable dans cette base.

Enfin, supposons que la dernière assertion soit satisfaite si bien que

$$\chi_u = (T - a_1)^{m_1} \cdots (T - a_r)^{m_r}$$

avec $m_i = \dim E_i$. On a alors

$$\dim E_i + \cdots + \dim E_r = \deg \chi_u = \dim E$$

et il suit que $E_1 \oplus \cdots \oplus E_r = E$. ■

Proposition 6.2.5 Soit E un espace vectoriel de dimension finie. Si $u \in \mathrm{L}(E)$ est diagonalisable et E' est un sous-espace stable par u, alors les endomorphismes induits $u' \in \mathrm{L}(E')$ et $u'' \in \mathrm{L}(E/E')$ sont aussi diagonalisables.

Démonstration. En effet, on sait que $\mu_{u'} \mid \mu_u$ et que $\mu_{u''} \mid \mu_u$. ■

Remarque

1. La réciproque est fausse comme le montre la matrice $A := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ qui n'est pas diagonalisable.
2. Par contre, si on se donne $u_1 \in \mathrm{L}(E_1)$ et $u_2 \in \mathrm{L}(E_2)$, alors $u_1 \times u_2$ est diagonalisable si et seulement si u_1 et u_2 le sont.

Proposition 6.2.6 Soit E un espace vectoriel de dimension finie. Si $u, v \in \mathrm{L}(E)$ *commutent* et sont tous deux diagonalisables, alors il existe une base $\mathscr{B}$ de E dans laquelle les matrices de u et v sont toutes *deux* diagonales.

Démonstration. On remarque d'abord que, si a est une valeur propre pour u, alors $E_a := \ker(a\mathrm{Id}(E) - u)$ est stable par v car u et v commutent. De plus, la restriction v_a de v à E_a est diagonalisable grâce à la proposition. On choisit alors une base $\mathscr{B}_a$ de E_a dans laquelle la matrice de v est diagonale et on pose $\mathscr{B} = \cup \mathscr{B}_a$. Comme c'est une base formée de vecteurs propres pour u, sa matrice aussi sera diagonale dans $\mathscr{B}$. ■

6.3 Endomorphisme nilpotent

Définition 6.3.1 Un élément u d'un anneau L est *nilpotent* s'il existe $m \in \mathbb{N}$ tel que $u^m = 0$. On dit que u est *unipotent* si $u - 1$ est nilpotent.

Exemple Dans $M_2(K)$, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ est nilpotent et $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ est unipotent.

Proposition 6.3.2 Soient E un espace vectoriel de dimension n et $u \in L(E)$. Alors, les propriétés suivantes sont équivalentes

1. u est nilpotent,
2. Il existe $m \in \mathbb{N}$ tel que T^m soit un polynôme annulateur de u,
3. Il existe $m \in \mathbb{N}$ tel que $\mu_u = T^m$,
4. $\chi_u = T^n$.

Démonstration. Si $u^m = 0$, on a

$$(T\mathrm{Id}_E - u) \circ \left(T^{m-1}\mathrm{Id}_E + T^{m-2}u + \cdots + u^{m-1}\right) = T^m \mathrm{Id}_E - u^m = T^m \mathrm{Id}_E.$$

En considérant les déterminants, on voit donc que $\chi_u := \det(T\mathrm{Id}_E - u)$ divise $T^{mn} = \det(T^m \mathrm{Id}_E)$. Et comme $\deg \chi_u = n$, on a nécessairement $\chi_u = T^n$. Le reste, très facile, est laissé en exercice. ■

Corollaire 6.3.3 Soient E un espace vectoriel de dimension finie, $u \in L(E)$ et E' un sous-espace stable par u. Alors, u est nilpotent si et seulement si les endomorphismes induits $u' \in L(E')$ et $u'' \in L(E/E')$ le sont.

Démonstration. En effet, on a $\chi_u = \chi_{u'}\chi_{u''}$. ■

Exemple La matrice

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

est nilpotente.

Théoreme 6.3.4 Soient E un espace vectoriel de dimension finie et $u \in L(E)$ nilpotent. Alors, il existe une base $(e_1, \ldots, e_n)$ de E telle que

$$\forall i = 1, \ldots, n, \quad u(e_i) = \left| \begin{array}{l} e_{i-1} \text{ ou} \\ 0. \end{array} \right.$$

Démonstration. Si $u = 0$, n'importe quelle base fait l'affaire. Sinon, il existe $m > 0$ et $x \in E$ tel que $u^m = 0$ et $u^{m-1}(x) \neq 0$: il suffit de prendre le plus petit m tel que $u^m = 0$. On pose alors

$$\forall i = 1, \ldots, m, \quad e_i := u^{m-i}(x).$$

Par construction, le sous-espace $F := \mathrm{Vect}(e_1, \ldots, e_m)$ est stable par u. En fait, on a $u(e_1) = 0$ et $u(e_i) = e_{i-1}$ pour $i > 1$. Montrons que $(e_1, \ldots, e_m)$ est une base de F. Supposons le contraire et qu'on puisse écrire $a_1e_1 + \cdots + a_re_r = 0$ avec r minimal. Comme $u^{r-1}(e_i) = 0$ pour $i < r$ et que $u^{r-1}(e_r) = e_1$, on aura

$$0 = u^{r-1}(0) = u^{r-1}(a_1e_1 + \cdots a_re_r) = a_re_1$$

Puisque $e_1 := u^{m-1}(x) \neq 0$, on voit que $a_r = 0$. Contradiction.

On considère maintenant l'espace dual ${}^tE$ et l'application duale ${}^tu$. On a bien sûr $({}^tu)^m = {}^tu^m = 0$. Comme E est de dimension finie, on sait grâce au théorème 4.4.6 que $({}^tE)^\circ = \{0\}$. Puisque $e_1 \neq 0$, on en déduit qu'il existe $\varphi \in {}^tE$ tel que $\varphi(e_1) \neq 0$. Et il suit que

$$ {}^tu^{m-1}(\varphi)(x) = \varphi(u^{m-1}(x)) = \varphi(e_1) \neq 0 $$

si bien que ${}^tu^{m-1}(\varphi) \neq 0$. On voit donc comme ci-dessus, que si on pose

$$ \forall i = 1, \dots, m, \quad \varphi_i := {}^tu^{m-i}(\varphi), $$

alors $U := \mathrm{Vect}(\varphi_1, \dots, \varphi_m)$ est un sous-espace vectoriel de dimension m qui est stable par ${}^tu$. Il suit formellement que U° est stable par u (exercice).

On a

$$ \dim F + \dim U^\circ = \dim U + \dim U^\circ = \dim E $$

et

$$ F \cap U^\circ = ({}^tF)^\circ = \{0\}, $$

puisque les restrictions de $\varphi_1, \dots, \varphi_m$ à F sont linéairement indépendantes et forment donc une base de ${}^tF$. On a donc une décomposition en somme directe $E \simeq F \oplus U^\circ$ stable par u. Comme nous avons prouvé le théorème pour F ci-dessus, on peut conclure par récurrence sur la dimension de E. ■

Remarque 1. Le théorème nous dit que si on pose, pour tout $r \in \mathbb{N}$,

$$ N_r := \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{bmatrix} \in \mathrm{M}_r(K), $$

alors toute matrice nilpotente est semblable à une matrice diagonale par blocs

$$ \begin{bmatrix} N_{r_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & N_{r_m} \end{bmatrix}. $$

2. On a toujours $u^r(\sum a_i e_i) = \sum_{u^r(e_i) \neq 0} a_i e_{i-r}$ et il suit que $\ker u^r$ est engendré par les e_i qui sont dans $\ker u^r$.
3. Les blocs de taille r sont en bijection avec les e_i tels que $u^r(e_i) = 0$ mais $u^{r-1}(e_i) \neq 0$. Cela signifie que $e_i \in \ker u^r \setminus \ker u^{r-1}$. Le nombre de blocs de taille m est donc exactement $\dim \ker u^r - \dim \ker u^{r-1}$ qui ne dépend que de u et pas de la base $\mathscr{B}$.

6.4 Trigonalisation

Théoreme 6.4.1 — de Jordan. Soient E un espace vectoriel de dimension finie et $u \in \mathrm{L}(E)$ à polynôme caractéristique *scindé*. Alors, il existe une base $(e_1, \dots, e_n)$ de E telle que

$$ \forall i = 1, \dots, n, \quad u(e_i) = \left| \begin{array}{l} a_i e_i + e_{i-1} \text{ ou} \\ a_i e_i \end{array} \right. $$

avec $a_1,\dots,a_n \in K$. De plus, si $u(e_i) = a_i e_i + e_{i-1}$, alors $a_{i-1} = a_i$.

Démonstration. Supposons d'abord qu'il existe $a \in K$ tel que $u - a\mathrm{Id}_E$ soit nilpotent sur E. Grâce au théorème 6.3.4, il existe donc une base $(e_1,\dots,e_n)$ de E telle que

$$\forall i = 1,\dots,n, \quad u(e_i) - ae_i = \left| \begin{array}{l} e_{i-1} \text{ ou} \\ 0, \end{array} \right.$$

et on a fini.

En général, on écrit

$$\chi_u = (T-a_1)^{m_1}\cdots(T-a_r)^{m_r},$$

et le lemme des noyaux nous fournit une décomposition en somme directe

$$E \simeq E_1 \oplus \cdots \oplus E_r \quad \text{avec} \quad E_i = \ker(u - a_i\mathrm{Id}_E)^{m_i}.$$

Chaque E_i est stable par u et $u - a_i\mathrm{Id}_E$ est nilpotent sur E_r. On est donc ramené au cas précédent. ■

Remarque 1. Le théorème de Jordan nous dit donc que si on pose, pour tout $a \in K$ et $r \in \mathbb{N}$,

$$J_{a,r} := aI_r + N_r = \begin{bmatrix} a & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & a \end{bmatrix} \in \mathrm{M}_r(K)$$

(on appelle ça un *bloc de Jordan*), alors toute matrice dont le polynôme caractéristique est scindé est semblable à une matrice diagonale par blocs

$$\begin{bmatrix} J_{a_1,r_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J_{a_m,r_m} \end{bmatrix}$$

(on appelle ça une *matrice de Jordan*).

2. Les sous-espaces $E_i = \ker(u - a_i\mathrm{Id}_E)^{m_i}$ qui apparaissent dans la décomposition de E ne sont *pas* les sous-espaces propres mais les *sous-espaces caractéristiques*.
3. On obtient ainsi une décomposition, dite de Dunford, $u = d + n$ avec d diagonalisable, n nilpotent et $nd = dn$. Nous aurons besoin plus tard du fait que d et n sont polynomiales en u : cela résulte du fait que, dans le lemme des noyaux, les projections sont polynomiales en u.

Proposition 6.4.2 — de Dunford (additive). Soient E un espace vectoriel de dimension finie et $u \in \mathrm{L}(E)$ à polynôme caractéristique *scindé*. On peut alors écrire de manière unique $u = d + n$ avec d diagonalisable, n nilpotent et $nd = dn$.

Démonstration. Nous connaissons déjà l'existence d'une telle décomposition et nous pouvons même supposer que d et n sont polynomiale en u. On voit aussi aisément que la décomposition est unique dans le cas $u = 0$ car on a alors $n = -d$ et qu'une matrice diagonale nilpotente est nécessairement nulle. Revenons au cas général et supposons qu'il existe une autre telle décomposition $u = d' + n'$. Comme d' commute avec lui même et avec n', il commute avec u, et donc aussi avec d qui est un polynôme en u. Il existe alors une base dans laquelle les matrices de d et d' sont toutes les deux diagonales. Il suit que la matrice de $d - d'$ est diagonale. Mais on sait aussi que $n' - n$ est nilpotent (si $n^r = 0$ et $n'^{r'} = 0$, alors $(n-n')^{rr'} = 0$). On est donc ramenés au cas $u = 0$. ■

Corollaire 6.4.3 — de Dunford multiplicative. Soient E un espace vectoriel de dimension finie et $u \in \mathrm{GL}(E)$ à polynôme caractéristique *scindé*. On peut alors écrire de manière unique $u = di = id$ avec d diagonalisable et i unipotent.

Démonstration. L'unicité est immédiate car on aura $u = d + n$ avec d diagonalisable, $n := d - di$ nilpotent et $nd = dn$. Réciproquement, si on part de la décomposition de Dunford additive $u = d + n$, on remarque d'abord que, comme $\det u = \det d$, on a d inversible et on peut écrire $u = di = id$ avec $i = \mathrm{Id}_E + d^{-1}n$. ∎

Remarque Lorsque $K = \mathbb{C}$, tout polynôme est scindé et tous les résultats précédents s'appliquent donc sans restriction.

6.5 Exercices

Exercice 6.1 Soient E un espace vectoriel de dimension n et $u \in \mathrm{L}(E)$.

1. Montrer que si $m \in \mathbb{N}$, il existe $R \in K[T]_{<n}$ tel que $u^m = R(u)$.
2. Montrer que si $u \in \mathrm{GL}(E)$, il existe $P \in K[T]_{<n}$ tel que $u^{-1} = P(u)$.

Exercice 6.2 Soient E un espace vectoriel de dimension finie et $u \in \mathrm{L}(E)$. Montrer que $u \in \mathrm{GL}(E)$ si et seulement 0 n'est pas une valeur propre pour u. En déduire que $u \in \mathrm{GL}(E)$ si et seulement si $\chi(0) \neq 0$ si et seulement si $\mu(0) \neq 0$.

Exercice 6.3 Montrer que si E un espace vectoriel de dimension finie et $u \in \mathrm{L}(E)$, alors

$$\chi_u = T^n - \mathrm{tr}(u)T^{n-1} + \cdots + (-1)^n \det(u).$$

En déduire une formule pour χ_A lorsque $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Exercice 6.4 Montrer que $T^2 + 1$ est un polynôme annulateur de $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Est-ce le polynôme caractéristique, le polynôme minimal ? La matrice est-elle diagonalisable sur $\mathbb{R}$? sur $\mathbb{C}$?

Exercice 6.5 Soit E un espace vectoriel de dimension finie.

1. Montrer qu'un endomorphisme p de E est une projection si et seulement si p est diagonalisable et ses valeurs propres sont dans $\{0,1\}$.
2. ($\mathrm{Car}(K) \neq 2$) Montrer qu'un endomorphisme s de E est une symétrie si et seulement si s est diagonalisable et ses valeurs propres sont dans $\{-1,1\}$.
3. Montrer que $A := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ est une symétrie sur $\mathbb{F}_2$ qui n'est pas diagonalisable.

Exercice 6.6 Soient E un espace vectoriel de dimension n sur K, $u \in \mathrm{L}(E)$, μ son polynôme minimal et χ son polynôme caractéristique.

1. Montrer que si $x \in E$, il existe un unique $\mu_x \in K[T]$ unitaire tel que $P(u)(x) = 0 \Leftrightarrow \mu_x \mid P$.
2. En déduire un isomorphisme $K[T]/(\mu_x) \simeq E_x := \mathrm{Vect}(u^k(x), k \in \mathbb{N})$, puis que $\dim E_x = \deg \mu_x$.
3. En déduire aussi que $\mu_x \mid \mu \mid \chi$, puis que $E = E_x$ si et seulement si $\mu_x = \mu = \chi$. On dit alors que x est un *vecteur cyclique* pour u.
4. Montrer que si $E \simeq E_1 \oplus \cdots \oplus E_r$, avec les E_i stables par u, et si $x = x_1 + \cdots + x_r$ est la décomposition correspondante de $x \in E$, alors $\mu_{x_i} \mid \mu_x$ pour tout $i = 1, \ldots, r$.
5. Montrer, grâce au lemme des noyaux, qu'il existe $x \in E$ tel que $\mu_x = \mu$ (on pourra traiter d'abord le cas $\mu = P^m$ avec P irréductible).
6. En déduire que $\chi = \mu$ si et seulement si il existe un vecteur cyclique.

Exercice 6.7

1. Déterminer la forme de Jordan J de $A := \begin{bmatrix} 4 & -1 \\ 4 & 0 \end{bmatrix}$.
2. Calculer J^n pour tout $n \in \mathbb{N}$.
3. Déterminer une matrice de passage P pour A et calculer son inverse.
4. Rappeler la formule pour A^n et effectuer le calcul.
5. Déterminer le reste dans la division euclidienne de T^n par le polynôme caractéristique de A, puis substituer A afin de retrouver le résultat précédent par une autre méthode.

Exercice 6.8 Résoudre la suite de Fibonacci $x_{n+2} = x_n + x_{n+1}$ en termes de x_0 et x_1.

Exercice 6.9 Déterminer les décompositions de Dunford des matrices

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ -1 & 1 & 2 \end{bmatrix}.$$

Exercice 6.10 (on pourra s'appuyer sur l'exercice 6.15). On pose

$$A := \begin{bmatrix} 3 & 2 & 4 \\ -1 & 3 & -1 \\ -2 & -1 & -3 \end{bmatrix}.$$

1. Résoudre l'équation différentielle $Y' = AY$.
2. Résoudre la suite récurrente $X_{n+1} = AX_n$.
3. Mêmes questions avec les matrices

$$\begin{bmatrix} 8 & -1 & -5 \\ -2 & 3 & 1 \\ 4 & -1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ 1 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 0 & 0 \\ -2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & -1 & 2 \end{bmatrix}.$$

Exercice 6.11 — TP. Diagonaliser si possible les matrices suivantes

$$\begin{bmatrix} 1 & -2 & -2 \\ -\frac{1}{2} & 2 & 0 \\ \frac{1}{2} & 1 & 3 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ -1 & 0 & -2 \\ 1 & 1 & 3 \end{bmatrix},$$

$$\text{et} \quad \begin{bmatrix} 1 & -1 & -4 \\ 3 & 5 & 4 \\ -1 & -1 & 2 \end{bmatrix}.$$

Exercice 6.12 — TP. Soient

$$A := \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad B := \begin{bmatrix} 1 & 0 & -10 \\ 1 & 1 & -5 \\ 0 & 1 & -1 \end{bmatrix},$$

$$C := \begin{bmatrix} 2 & 0 & 4 \\ 3 & -4 & 12 \\ 1 & -2 & 5 \end{bmatrix}, \quad D := \begin{bmatrix} -4 & 0 & -2 \\ 0 & 1 & 0 \\ 5 & 1 & 3 \end{bmatrix}.$$

Calculer les polynômes caractéristiques, les valeurs propres et les vecteurs propres des matrices A, B, C et D. Si possible, les diagonaliser. En déduire celles qui sont inversibles. Exprimez leur inverse en vous aidant du polynôme caractéristique.

Exercice 6.13 — TP. À quelle condition la matrice

$$A := \begin{bmatrix} a & 0 & 0 & 0 & b \\ 0 & a & 0 & b & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & b & 0 & a & 0 \\ b & 0 & 0 & 0 & a \end{bmatrix} \in \mathrm{M}_5(\mathbb{Q})$$

est elle diagonalisable ? Déterminer les sous-espaces propres et leur dimension.

Exercice 6.14 — TP. Déterminer la forme de Jordan J ainsi qu'une matrice de passage P pour

$$A := \begin{bmatrix} -3 & 2 & 3 \\ -6 & 4 & 4 \\ -2 & 1 & 3 \end{bmatrix}.$$

Exercice 6.15 — TP. Déterminer la forme de Jordan J ainsi qu'une matrice de passage P pour les matrices

$$\begin{bmatrix} 3 & 2 & 4 \\ -1 & 3 & -1 \\ -2 & -1 & -3 \end{bmatrix}, \quad \begin{bmatrix} 8 & -1 & -5 \\ -2 & 3 & 1 \\ 4 & -1 & -1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ 1 & 0 & 2 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 2 & 1 & 0 & 0 \\ -2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & -1 & 2 \end{bmatrix}.$$

Exercice 6.16 — TP. On considère les matrices suivantes dans $\mathrm{M}_8(\mathbb{Q})$:

$$A := \begin{bmatrix} -2 & 0 & 1 & -2 & -1 & 3 & 1 & 2 \\ -9 & 7 & -5 & -5 & -4 & 6 & 4 & -1 \\ 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ -9 & 7 & -3 & -5 & -4 & 6 & 4 & -1 \\ -4 & 1 & -3 & 0 & 0 & 3 & 3 & -3 \\ -13 & 14 & -6 & -9 & -8 & 7 & 8 & -5 \\ 5 & -11 & 6 & 5 & 5 & 1 & -2 & 4 \\ -1 & 1 & 0 & -1 & -1 & 1 & 1 & 1 \end{bmatrix}, \quad B := \begin{bmatrix} -1 & -5 & 2 & 5 & -2 & 3 & 0 & 5 \\ -1 & -3 & 1 & 4 & 1 & 0 & 0 & 1 \\ -4 & 6 & -4 & -3 & 7 & 10 & -3 & -6 \\ -2 & 3 & -2 & 0 & 4 & 5 & -2 & -3 \\ -4 & 2 & -2 & 1 & 5 & 11 & -3 & -2 \\ 0 & -1 & 1 & 1 & -1 & 1 & 0 & 1 \\ -2 & 3 & 0 & 0 & 2 & 10 & -2 & -3 \\ 1 & -9 & 4 & 7 & -4 & -6 & 2 & 7 \end{bmatrix},$$

$$C := \begin{bmatrix} -1 & 0 & -2 & 2 & 0 & 0 & 0 & 0 \\ -3 & 0 & -3 & 2 & 1 & 1 & 0 & 0 \\ 6 & 0 & 8 & -6 & -3 & 0 & 3 & -3 \\ 6 & 0 & 7 & -5 & -3 & 0 & 3 & -3 \\ -7 & -1 & -7 & 6 & 4 & 1 & -2 & 2 \\ -5 & -1 & -4 & 4 & 2 & 2 & -1 & 1 \\ -3 & -1 & -2 & 2 & 2 & 1 & 0 & 1 \\ 4 & 0 & 5 & -4 & -3 & 0 & 3 & -2 \end{bmatrix}, \quad D := \begin{bmatrix} 4 & -1 & 1 & -2 & -2 & 1 & 0 & -1 \\ 6 & -1 & 1 & -5 & -3 & 2 & 0 & 0 \\ 10 & -5 & -1 & -8 & -5 & 3 & 2 & 5 \\ 3 & -1 & 1 & -1 & -2 & 1 & 0 & -1 \\ 16 & -8 & -2 & -12 & -7 & 4 & 4 & 6 \\ 14 & -6 & -1 & -11 & -7 & 5 & 2 & 4 \\ 9 & -4 & -2 & -7 & -4 & 2 & 3 & 4 \\ 10 & -5 & 0 & -8 & -5 & 3 & 2 & 4 \end{bmatrix}$$

$$\text{et } E := \begin{bmatrix} 1 & 1 & -1 & 1 & 1 & 0 & -1 & -1 \\ 0 & 1 & 0 & 0 & 3 & 1 & -3 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & -1 & 0 \\ 0 & 1 & -1 & 2 & 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & 1 & 2 & 1 & -2 & -1 \\ 1 & 1 & -1 & 0 & 2 & 1 & -3 & 0 \\ 0 & 1 & -1 & 1 & 3 & 1 & -3 & -1 \\ 1 & 1 & -1 & 0 & 0 & 0 & -1 & 1 \end{bmatrix}.$$

1. Déterminer le polynôme caractéristique et le polynôme minimal de A. Les factoriser. Établir la liste de leurs racines, en précisant lesquelles sont dans $\mathbb{Q}$ ou dans $\mathbb{C}$, et comparer les multiplicités. Mêmes questions avec B, C, D et E.
2. Déterminer les sous-espaces propres de A. Comparer pour chacun, leur dimension avec la multiplicité de la valeur propre correspondante dans le polynôme caractéristique ainsi que dans le polynôme minimal. Mêmes questions avec B, C, D et E.
3. Calculer les noyaux des matrices $(E-I)^k$ lorsque k augmente. Observer l'évolution de leur dimension et comparer avec les multiplicités de la valeur propre 1 ainsi qu'avec la dimension du sous-espace propre associé.
4. Parmi ces cinq matrices, lesquelles sont diagonalisables sur $\mathbb{Q}$? sur $\mathbb{C}$?

Troisième partie

7. Forme quadratique

7.1 Forme bilinéaire sur un espace vectoriel

Définition 7.1.1 Une *forme bilinéaire* sur un espace vectoriel E est une application

$$\Phi : E \times E \to K$$

telle que

1. $\forall x, y, z \in E, \quad \Phi(x+y,z) = \Phi(x,z) + \Phi(y,z) \quad \text{et} \quad \Phi(x,y+z) = \Phi(x,y) + \Phi(x,z)$
2. $\forall x, y \in E, \forall a \in K, \quad \Phi(ax,y) = \Phi(x,ay) = a\Phi(x,y)$

Remarque
1. Bien sûr, il s'agit d'une spécialisation de la définition 5.1.2 d'une application multilinéaire.
2. Comme nous l'avons montré dans la proposition 5.1.4, nous avons alors à notre disposition un isomorphisme
$$\mathrm{L}_2(E,K) \simeq \mathrm{L}(E, {}^tE), \quad \Phi \leftrightarrow l$$
entre l'espace des formes bilinéaires sur E celui des applications linéaires de E vers son dual, et qui est donné par
$$\Phi(x,y) = l(y)(x).$$
On écrira l_Φ pour indiquer que l dépend de Φ et on notera aussi parfois $\Phi_y : E \to K$ la forme linéaire partielle donnée par $\Phi_y(x) = \Phi(x,y)$.
3. On peut aussi échanger les facteurs et considérer l'application $r : E \to {}^tE$ donnée par $r(x)(y) : \Phi(x,y)$ et les formes linéaires partielles ${}_x\Phi : E \to K$ données par ${}_x\Phi(y) = \Phi(x,y)$.
4. On appliquera systématiquement à la forme bilinéaire Φ les notions habituellement utilisées pour l'application linéaire l_Φ. Par exemple, le *noyau* de Φ (aussi appelé *radical*) sera
$$\ker \Phi := \ker l_\Phi = \{y \in E \ / \ \forall x \in E, \Phi(x,y) = 0\}.$$
Et le *rang* de Φ sera $\mathrm{rang}(\Phi) := \mathrm{rang}(l_\Phi)$ si bien que le théorème du rang s'applique à Φ.

5. Si E est de dimension finie, on définit de même la *matrice* de la forme bilinéaire Φ dans une base $\mathscr{B} := (e_1, \ldots, e_n)$:
$$[\Phi]_{\mathscr{B}} := [l_\Phi]^{\mathscr{B}}_{{}^t\mathscr{B}} = [\Phi(e_i, e_j)]$$
On pourra aussi écrire $\mathrm{Mat}_{\mathrm{B}}(\Phi)$. On voit donc que, par définition, le noyau (resp. le rang) de la forme bilinéaire Φ est le noyau (resp. le rang) de la matrice $[\Phi]_{\mathscr{B}}$.

Exemple 1. La forme bilinéaire *canonique* sur K^n est définie par
$$((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \mapsto x_1y_1 + \cdots + x_ny_n.$$
Sa matrice dans la base canonique est la matrice unité I, son noyau est nul et son rang est n.
2. Si $\mathscr{B}$ est une base ordonnée d'un plan H, alors l'application $\det_{\mathscr{B}}$ est une forme bilinéaire sur H. Sa matrice dans la base $\mathscr{B}$ est $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, son noyau est nul et elle est de rang 2.
3. L'application $\Phi((a,b),(c,d)) = ac - bc - ad + bd$ définit une forme bilinéaire sur K^2. Sa matrice dans la base canonique est $\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$. C'est une forme bilinéaire de rang 1 dont le noyau est la diagonale Δ.
4. L'application $(z_1, z_2) \mapsto \Re(z_1z_2)$ définit une forme bilinéaire sur $\mathbb{C}$ (vu comme espace vectoriel sur $\mathbb{R}$) dont la matrice dans la base canonique est $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Elle est de rang 2 (et son noyau est nul).
5. L'application
$$(f,g) \mapsto \int_0^1 (fg)(t)\mathrm{d}t$$
est une forme bilinéaire sur $\mathscr{C}^0([0,1], \mathbb{R})$ dont le noyau est nul (et le rang infini).
6. Si E est un espace vectoriel de dimension finie, l'application $(u,v) \mapsto \mathrm{tr}(u \circ v)$ définit une forme bilinéaire sur $L(E)$. Rang ? Noyau ? Matrice ? Ça devient compliqué.

Remarque Si $J := [c_{i,j}] \in M_n(K)$, alors la forme bilinéaire associée sur K^n est donnée par
$$\Phi((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \sum_{i,j=1}^{n} c_{i,j}x_iy_j.$$

Proposition 7.1.2 Soient Φ une forme bilinéaire sur un espace vectoriel E, $u, v : F \to E$ deux applications linéaires et $\Psi := \Phi \circ (u \times v)$ la forme bilinéaire composée sur F. On aura alors
$$l_\Psi = {}^tu \circ l_\Phi \circ v.$$

Démonstration. On dispose donc du diagramme commutatif de gauche et on doit montrer que celui de droite est commutatif :

$$\begin{tikzcd} E \times E \arrow[r, "\Phi"] & K \\ F \times F \arrow[u, "u \mid v"] \arrow[ur, "\Psi"] & \end{tikzcd}, \qquad \begin{tikzcd} E \arrow[r, "l_\Phi"] & {}^tE \arrow[d, "{}^tu"] \\ F \arrow[u, "v"] \arrow[r, "l_\Psi"] & {}^tF \end{tikzcd}$$

Il suffit en fait de calculer. On a
$$({}^tu \circ l_\Phi \circ v)(y) = {}^tu(l_\Phi(v(y)) = l_\Phi(v(y)) \circ u$$
et donc
$$({}^tu \circ l_\Phi \circ v)(y)(x) = l_\Phi(v(y))(u(x)) = \Phi(u(x), v(y)) = \Psi(x,y). \qquad \blacksquare$$

Corollaire 7.1.3 Dans la situation de la proposition, supposons que E et F soient de dimension finie et munis de bases $\mathscr{B}$ et $\mathscr{C}$ respectivement. Désignons les matrices de Φ, u et v dans ces bases par J, A et B respectivement. Alors, la matrice de Ψ sera ${}^tAJB$.

Démonstration. ∎

Remarque Comme cas particulier, on peut considérer le cas ou u et v désignent tous les deux l'inclusion d'un sous-espace vectoriel E'. On obtient alors la restriction $\Phi_{|E'}$ de Φ à E'. Si $\mathscr{B}'$ est une base de E' et qu'on la prolonge en une base $\mathscr{B}$ de E et si J, J' désignent les bases de Φ et $\Phi_{|E'}$, aura

$$J = \begin{bmatrix} J' & \star \\ \star & \star \end{bmatrix}$$

Corollaire 7.1.4 Soient Φ une forme bilinéaire sur un espace vectoriel E de dimension finie et $x, y \in E$. Si J, X et Y désignent les matrices de Φ, x et y respectivement dans une base $\mathscr{B}$ de E, on a

$$\Phi(x,y) = {}^tXJY.$$

Démonstration. Il suffit de composer Φ avec les inclusions $i_x, i_y : K \hookrightarrow E$. ∎

Corollaire 7.1.5 Soient Φ une forme bilinéaire sur un espace de dimension finie E et J sa matrice dans une base $\mathscr{B}$. Alors, Φ est symétrique (resp. antisymétrique) si et seulement si J l'est.

Démonstration. Il suffit de remarquer que ${}^tYJX = {}^t({}^tYJX) = {}^tX{}^tJY$. ∎

Remarque Si $\dim E = n$, on dispose donc d'isomorphismes

$$\mathrm{S}_2(E,K) \simeq \mathrm{SM}_n(K) \quad \text{et} \quad \mathrm{A}_2(E,K) \simeq \mathrm{AM}_n(K).$$

Corollaire 7.1.6 Soient Φ une forme bilinéaire sur un espace de dimension finie E, J sa matrice dans une base $\mathscr{B}$, J' sa matrice dans une base $\mathscr{B}'$ et P la matrice de passage. On a alors

$$J' = {}^tPJP.$$

Démonstration. Il suffit de considérer l'identité sur $E \times E$ en utilisant $\mathscr{B}'$ à gauche et $\mathscr{B}$ à droite. ∎

Remarque S'il existe une matrice inversible P telle que $J' = {}^tPJP$, on dit que J et J' sont *congruentes*. Attention, ne pas confondre avec *semblables* $A' = P^{-1}AP$.

7.2 Forme bilinéaire symétrique non dégénérée

Définition 7.2.1 Une forme bilinéaire Φ est *non dégénérée* (ou *définie*) si $\ker\Phi = 0$.

Remarque

1. Cela signifie que donc l'on a une application *injective* $l_\Phi : E \hookrightarrow {}^tE$. Fixer Φ revient donc à voir E comme *contenu* dans ${}^tE$. En dimension infinie, cette inclusion sera toujours stricte (on aura pas égalité).
2. Lorsque E est de dimension finie, on peut utiliser le théorème du rang et la condition de la définition est donc équivalente à $\mathrm{rang}(\Phi) = \dim E$. Cela revient aussi à dire que la matrice J de Φ est inversible ou encore que $\det(J) \neq 0$.

3. C'est redondant avec ce qui précède, mais il est important de remarquer que se donner une forme bilinéaire non dégénérée sur un espace vectoriel E de dimension finie est équivalent à se donner un isomorphisme entre E et ${}^tE$. Fixer Φ revient donc à *identifier* E et son dual.

Exemple 1. La forme bilinéaire *canonique* sur K^n est non dégénérée et fournit l'identification habituelle entre K^n et son dual :

$$(a_1,\dots,a_n) \leftrightarrow \varphi \Leftrightarrow \varphi(x_1,\dots,x_n) = a_1x_1+\dots+a_nx_n.$$

2. La forme bilinéaire $(z_1,z_2) \mapsto \Re(z_1z_2)$ est non dégénérée et permet d'identifier $\mathbb{C}$ avec son dual via $1 \leftrightarrow \Re$ et $i \leftrightarrow -\Im$.
3. L'application
$$(f,g) \mapsto \int_0^1 (fg)(t)\mathrm{d}t$$
est non dégénérée.

Proposition 7.2.2 Soit Φ une forme bilinéaire *non dégénérée* sur un espace vectoriel E *de dimension finie*. Si $u \in L(E)$, il existe un unique opérateur linéaire u^* sur E tel que

$$\forall x,y \in E, \quad \Phi(u(x),y) = \Phi(x,u^*(y)).$$

En fait, on a
$$u^* = l_\Phi^{-1} \circ {}^tu \circ l_\Phi.$$

Démonstration. La condition s'écrit encore

$$\forall x,y \in E, \quad l_\Phi(y)(u(x)) = l_\Phi(u^*(y))(x)$$

c'est à dire
$$\forall y \in E, \quad l_\Phi(y)\circ u = (l_\Phi \circ u^*)(y)$$
et donc finalement ${}^tu \circ l_\Phi = l_\Phi \circ u^*$, c'est à dire $u^* = l_\Phi^{-1} \circ {}^tu \circ l_\Phi$. D'où l'existence et l'unicité. ■

Définition 7.2.3 Si Φ est une forme bilinéaire non dégénérée sur un espace vectoriel E de dimension finie, alors u^* est l'*opérateur transposé* de $u \in L(E)$ relativement à Φ.

Corollaire 7.2.4 Soient Φ une forme bilinéaire non dégénérée sur un espace vectoriel E de dimension finie et $u \in L(E)$. Si on désigne par J et A les matrices de Φ et u respectivement dans une base $\mathscr{B}$, alors la matrice de u^* est $A^* := J^{-1}\,{}^tAJ$.

Démonstration. ■

Remarque 1. On définit la *matrice transposée* de $A \in \mathrm{M}_n(K)$ relativement à $J \in \mathrm{GL}_n(K)$ comme étant $A^* := J^{-1}\,{}^tAJ$. Dans le cas $J = I$, on retrouve bien la définition usuelle.
2. Dans le cas ou $K = \mathbb{R}$, on dit plutôt que u^* est l'*adjoint* de u. Attention cependant que ceci prend un autre sens lorsque $K = \mathbb{C}$.

Proposition 7.2.5 Si Φ est une forme bilinéaire *symétrique* sur E, elle induit une forme bilinéaire symétrique non dégénérée

$$\begin{array}{ccc} E/\ker\Phi \times E/\ker\Phi & \xrightarrow{\overline{\Phi}} & K \\ (\overline{x},\overline{y}) & \longmapsto & \Phi(x,y) \end{array}$$

Démonstration. On a toujours une telle forme bilinéaire (exercice) et elle est bien sûr symétrique lorsque Φ l'est. Il reste à montrer qu'elle est non dégénérée. Mais on a

$$\overline{x} \in \ker\overline{\Phi} \Leftrightarrow \forall y \in E, \Phi(x,y) = 0 \Leftrightarrow x \in \ker\Phi \leftrightarrow \overline{x} = 0. \quad \blacksquare$$

Remarque 1. Supposons que E soit de dimension finie. Soient $\mathscr{C}$ une base de $\ker\Phi$, $\mathscr{B}$ une base de E qui prolonge $\mathscr{C}$ et $\overline{\mathscr{B}}$ la base induite sur $E/\ker\Phi$. Alors, si on désigne par J (resp. $\overline{J}$) la matrice de Φ (resp $\overline{\Phi}$) dans la base $\mathscr{B}$ (resp. $\overline{\mathscr{B}}$), on a

$$J = \begin{bmatrix} 0 & 0 \\ 0 & \overline{J} \end{bmatrix}$$

et $\overline{J}$ est une matrice symétrique inversible.

2. Dans la proposition, le fait que Φ soit symétrique est essentiel pour que $\overline{\Phi}$ soit non dégénérée (prendre $J = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ comme contre exemple).

Remarque Si $\Phi : E \times F \to K$ est une forme bilinéaire, on dit que $A \subset E$ et $B \subset F$ sont *orthogonaux* par rapport à Φ, et on écrit $A \perp B$, si $\Phi(x,y) = 0$ pour tout $x \in A$ et $y \in B$. On pose aussi

$$B^\perp := \{x \in E \ / \ \forall y \in B, \Phi(x,y) = 0\} \quad \text{et} \quad {}^\perp A := \{y \in F \ / \ \forall x \in A, \Phi(x,y) = 0\}.$$

Dans le cas de la forme canonique $E \times {}^tE \to K$, on retrouve notre ancienne définition avec des notation un peu différentes. Nous allons considérer ci-dessous le cas particulier d'une forme bilinéaire symétrique sur E.

Définition 7.2.6 Soit Φ une forme bilinéaire *symétrique* sur E. On dit que $A \subset E$ est *orthogonale* à $B \subset E$ relativement à Φ, et on écrit $A \perp B$, si

$$\forall x \in A, \forall y \in B, \quad \Phi(x,y) = 0.$$

Remarque 1. Comme on suppose que Φ est symétrique, on voit que $A \perp B \Leftrightarrow B \perp A$.

2. Lorsque $B = \{y\}$ (resp. $A = \{x\}$), on dit que x est *orthogonal* à B (resp. A est *orthogonal* à y).
3. On pose $A^\perp := \{x \in E, \forall y \in A, \Phi(x,y) = 0\}$ et on écrit $x^\perp$ lorsque $A = \{x\}$.
4. On a $A \perp B \Leftrightarrow A \subset B^\perp \Leftrightarrow B \subset A^\perp$.
5. $A^\perp$ est un sous-espace vectoriel de E et $A \subset A^{\perp\perp}$. De plus, si $A \subset B$, alors $B^\perp \subset A^\perp$.
6. Remarquons aussi que $\ker\Phi = E^\perp$.

Théoreme 7.2.7 Si Φ est une forme bilinéaire symétrique non dégénérée sur un espace vectoriel E de dimension finie, alors l'application $F \mapsto F^\perp$, sur l'ensemble des sous-espaces vectoriels de E, est une symétrie qui renverse l'inclusion et échange somme et intersection. De plus, on a toujours

$$\dim F + \dim F^\perp = \dim E.$$

Démonstration. On dispose d'un isomorphisme $l_\Phi : E \simeq {}^tE$ et si U est l'image d'un sous-espace vectoriel F, alors $F^\perp = U^\circ$. Notre assertion résulte donc immédiatement du théorème 4.4.6 et du corollaire 4.4.4. $\blacksquare$

Remarque Cette assertion signifie que l'on a toujours

$$F^{\perp\perp} = F, \quad (F_1 \cap F_2)^{\perp} = F_1^{\perp} + F_2^{\perp}, \quad (F_1 + F_2)^{\perp} = F_1^{\perp} \cap F_2^{\perp} \quad \text{et} \quad F_1 \subset F_2 \Leftrightarrow F_2^{\perp} \subset F_1^{\perp}.$$

Corollaire 7.2.8 Soient Φ est une forme bilinéaire symétrique non dégénérée sur un espace vectoriel E de dimension finie et F un sous-espace vectoriel de E. Alors, les conditions suivantes sont équivalentes

1. $\Phi_{|F}$ est non dégénérée,
2. $F \cap F^{\perp} = \{0\}$,
3. $E = F \oplus F^{\perp}$.

Démonstration. En effet, par définition, le noyau de $\Phi_{|F}$ est $F \cap F^{\perp}$ et le reste suit (exercice). ■

Exemple Si on prend $\Phi((x_1,x_2),(y_1,y_2) = x_1y_2 + x_2y_1$ sur $E = K^2$ et qu'on considère $F := Ox$, on voit que $F^{\perp} = F$. Il suit que $\Phi_{|F}$ est dégénérée (et donc nulle).

7.3 Forme quadratique

On suppose que $\mathrm{Car}(K) \neq 2$.

Définition 7.3.1 Une application $Q : E \to K$, ou E est un espace vectoriel, est une *forme quadratique* s'il existe une forme bilinéaire symétrique Φ sur E, appelée alors *polaire* de Q, telle que

$$\forall x \in E, \quad Q(x) = \Phi(x,x).$$

Exemple

1. Sur K^2, on peut considérer :
   (a) $Q(x_1,x_2) = x_1^2 + x_2^2$ de polaire $\Phi((x_1,x_2),(y_1,y_2)) = x_1y_1 + x_2y_2$.
   (b) $Q(x_1,x_2) = x_1^2 - x_2^2$ de polaire $\Phi((x_1,x_2),(y_1,y_2)) = x_1y_1 - x_2y_2$.
   (c) $Q(x_1,x_2) = (x_1 - x_2)^2$ de polaire $\Phi((x_1,x_2),(y_1,y_2)) = x_1y_1 - x_1y_2 - x_2y_1 + x_2y_2$.
2. En géométrie plane, la forme quadratique usuelle est donnée par
$$Q(\overrightarrow{AB}) = AB^2.$$
   On pourra illustrer toute la théorie avec cet exemple.
3. Si $\mathbb{C}$ est vu comme un espace vectoriel sur $\mathbb{R}$, on peut considérer la forme quadratique $Q(z) = |z|^2$. Via l'affixe d'un point, on retrouve la forme quadratique usuelle sur le plan.

Proposition 7.3.2 Si Q est une forme quadratique, alors sa polaire Φ est unique. De plus, on a

1. $\forall x,y \in E, \quad Q(x+y) = Q(x) + 2\Phi(x,y) + Q(y)$,
2. $\forall a \in K, \forall x \in E, \quad Q(ax) = a^2Q(x)$.

Démonstration. L'unicité de la polaire résulte de la première formule : en effet, on aura alors pour tout $x,y \in E$,

$$\Phi(x,y) = \frac{1}{2}(Q(x+y) - Q(x) - Q(y)).$$

1. On a
$$\begin{aligned} Q(x+y) &= \Phi(x+y,x+y) \\ &= \Phi(x,x) + \Phi(x,y) + \Phi(y,x) + \Phi(y,y) \\ &= Q(x) + 2\Phi(x,y) + Q(y). \end{aligned}$$

2. On a
$$Q(ax) = \Phi(ax, ax) = a^2\Phi(x,x) = a^2 Q(x). \quad \blacksquare$$

Remarque 1. On dispose donc une bijection $\Phi \leftrightarrow Q$ entre les formes bilinéaires symétriques et les formes quadratiques sur E. En particulier, les formes quadratiques forment un espace vectoriel isomorphe à $\mathrm{S}_2(E,K)$, et donc aussi à $\mathrm{SM}_n(K)$ si $\dim E = n$ (et si on choisit une base).

2. On appliquera à Q le vocabulaire déjà introduit pour Φ. On parlera ainsi du noyau $\ker Q$ de Q, de son rang $\mathrm{rang}(Q)$ ou de sa matrice $[Q]_{\mathscr{B}}$ dans une base $\mathscr{B}$. On dira aussi que Q est non dégénérée si c'est le cas pour Φ et on parlera aussi d'orthogonalité par rapport à Q.
3. Si $J := [c_{i,j}] \in \mathrm{SM}_n(K)$, alors la forme quadratique associée est donnée par
$$Q(x_1,\dots,x_n) = \sum_{i=1}^{n} c_{i,i}x_i^2 + 2\sum_{i<j} c_{i,j}x_ix_j.$$
4. La première identité dans la proposition est la *formule du binôme* et la seconde exprime la *quadraticité* $Q(ax) = a^2Q(x)$ (à comparer avec la linéarité d'une application : $u(x+y) = u(x)+u(y)$ et $u(ax) = au(x)$).
5. Géométriquement, la première égalité correspond au théorème de Pythagore généralisé :
$$AC^2 = AB^2 - 2(AB)(BC)\cos(ABC) + BC^2$$
Et la seconde nous dit simplement que si $\overrightarrow{AC} = \lambda\overrightarrow{AB}$, alors $AC = |\lambda|AB$.

Proposition 7.3.3 Si Q une forme quadratique sur E, on a
1. $\forall x,y \in E, \quad Q(x+y)+Q(x-y) = 2Q(x)+2Q(y)$,
2. $\forall x,y \in E, \quad x \perp y \Leftrightarrow Q(x+y) = Q(x)+Q(y)$.

Démonstration. On désigne par Φ la polaire de Q.
1. On utilise la formule du binôme, que l'on rappelle ici :
$$Q(x+y) = Q(x)+2\Phi(x,y)+Q(y),$$
ainsi que sa variante en remplaçant y par $-y$:
$$Q(x-y) = Q(x)+2\Phi(x,-y)+Q(-y) = Q(x)-2\Phi(x,y)+Q(y),$$
et il suffit d'additionner.
2. Cela résulte encore de la formule du binôme :
$$x \perp y \Leftrightarrow \Phi(x,y) = 0 \Leftrightarrow Q(x+y) = Q(x)+Q(y). \quad \blacksquare$$

Remarque 1. La première propriété est la *règle du parallélogramme* qui dit classiquement que la somme des carrés des diagonales d'un parallélogramme $(ABDC)$ est égale à la somme des carrés des cotés (faire un dessin) :
$$AD^2 + BC^2 = AB^2 + CD^2 + AC^2 + BD^2.$$
2. La règle du parallélogramme peut s'écrire sous la forme
$$Q\left(\frac{x+y}{2}\right) = \frac{1}{2}Q(x) + \frac{1}{2}Q(y) - \frac{1}{4}Q(x-y)$$

et on retrouve alors la *règle de la médiane* qui dit classiquement que le carré de la médiane est égal à la demi-somme des carrés des cotés à laquelle on retranche le quart du carré de du coté opposé (faire un dessin) :

$$AI^2 = \frac{1}{2}AB^2 + \frac{1}{2}AC^2 - \frac{1}{4}BC^2.$$

3. La seconde propriété est le *théorème de Pythagore* qui dit classiquement qu'un triangle est rectangle en un sommet si et seulement si le carré du coté opposé (alors appelé *hypoténuse*) est la somme des carrés des deux autres cotés (faire un dessin aussi) :

$$(AB) \perp (BC) \Leftrightarrow AC^2 = AB^2 + BC^2.$$

Définition 7.3.4 Soit Q une forme quadratique sur E. Un vecteur $x \in E$ est *isotrope* pour Q si $Q(x) = 0$. Plus généralement, un ensemble A de vecteurs de E est *isotrope* pour Q si $Q_{|A} = 0$.

Remarque 1. Dire qu'une partie est isotrope signifie donc tout simplement qu'elle est composée de vecteurs isotropes.

2. Attention, ne pas confondre avec le noyau ! On a

$$y \in \ker Q \Leftrightarrow \forall x \in E, Q(x+y) = Q(x) + Q(y).$$

3. Si $x \in \ker Q$, alors x est isotrope. Mais la réciproque est complètement fausse. Par exemple, si $Q(x,y) = 2xy$ sur K^2, alors le vecteur $(1,0)$ est isotrope bien que Q soit *non* dégénérée.

Définition 7.3.5 Soit Q une forme quadratique sur E. On dit que $u \in \mathrm{GL}(E)$ est *orthogonal* relativement à Q si

$$\forall x \in E, \quad Q(u(x)) = Q(x).$$

Le *groupe orthogonal* de Q est l'ensemble $\mathrm{O}(Q)$ de tous les opérateurs orthogonaux relativement à Q.

Remarque 1. On dit aussi que u est *orthogonal* relativement à une forme bilinéaire symétrique Φ si et seulement si

$$\forall x,y \in E, \quad \Phi(u(x),u(y)) = \Phi(x,y).$$

2. Un opérateur est orthogonal relativement à une forme quadratique Q si et seulement si il est orthogonal relativement à sa polaire Φ (utiliser la formule du binôme). En particulier, on voit que si u est orthogonal, alors

$$x \perp y \Rightarrow u(x) \perp u(y),$$

ce qui justifie la terminologie.

3. Si $J \in \mathrm{SM}_n(K)$, on dira que qu'une matrice $A \in \mathrm{M}_n(K)$ est *orthogonale* par rapport à J si ${}^tAJA = J$ et que

$$\mathrm{O}(J) := \{A \in \mathrm{GL}_n(K) \ / \ {}^tAJA = J\}$$

est le *groupe orthogonal* de J.

4. Si E est de dimension finie et si Q (resp. u) a pour matrice J (resp. Q) dans une base $\mathscr{B}$, on voit que u est orthogonal relativement à Q si et seulement si A est orthogonale relativement à J : en effet, nous avons vu qu'en général, si Φ est une forme bilinéaire sur E et $u : F \to E$ deux applications linéaires, on a toujours

$$[\Phi \circ (u \times v)] = {}^t[u]\ [\Phi]\ [v].$$

5. Il est clair que $\mathrm{O}(Q)$ (resp. $\mathrm{O}(J)$) est un bien un sous-groupe de $\mathrm{GL}(E)$ (resp. $\mathrm{GL}_n(K)$).

Proposition 7.3.6 Si Q est une forme quadratique non dégénérée sur un espace vectoriel E de dimension finie et $u \in \mathrm{GL}(E)$, alors

$$u \in \mathrm{O}(Q) \Leftrightarrow u^{-1} = u^*.$$

Démonstration. Soient $x, y \in E$. Si u est orthogonal, on a

$$\Phi(u(x), y) = \Phi(u(x), u(u^{-1}(y)) = \Phi(x, u^{-1}(y))$$

et on voit donc que $u^{-1} = u^*$. Et réciproquement, si on suppose que $u^{-1} = u^*$, alors

$$\Phi(u(x), u(y)) = \Phi(x, u^*(u(y)) = \Phi(x, y). \quad \blacksquare$$

Remarque 1. En terme de matrices, le résultat immédiat : si J et A sont des matrices inversibles, alors la condition ${}^tAJA = J$ (matrice orthogonale) est équivalente à $J^{-1}{}^tAJ = A^{-1}$ (transposé=inverse).

2. Lorsque Q est non dégénérée, si u est orthogonal, alors $\det u = \pm 1$.
3. On désigne par $\mathrm{O}(p, q)$ le groupe orthogonal de

$$J = \begin{bmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

4. On note plus simplement $\mathrm{O}(n)$ le groupe orthogonal de $I \in \mathrm{M}_n(K)$ si bien que

$$\mathrm{O}(n) = \{A \in \mathrm{GL}_n(K) \;/\; A^{-1} = {}^tA\} \quad (= \{A \in \mathrm{M}_n(K) \;/\; {}^tAA = I\}.$$

5. En général, on écrira $\mathrm{SO}(Q) := \mathrm{O}(Q) \cap \mathrm{SL}(E)$ et $\mathrm{SO}(n) := \mathrm{O}(n) \cap \mathrm{SL}_n(K)$.

Exemple Le groupe orthogonal du plan est l'ensemble des rotations et des réflexions

$$\mathrm{O}(2) = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \;/\; a^2 + b^2 = 1 \right\} \bigcup \left\{ \begin{bmatrix} a & b \\ b & -a \end{bmatrix} \;/\; a^2 + b^2 = 1 \right\}.$$

On voit donc que $\mathrm{SO}(2)$ est le groupe des rotations.

7.4 Décomposition d'une forme quadratique

On suppose toujours que $\mathrm{Car}(K) \neq 2$.

Définition 7.4.1 Soit Q une forme quadratique sur un espace vectoriel E. Une partie X de E est *orthogonale* relativement à Q si

$$\forall x \neq y \in X, \quad x \perp y.$$

Elle est *orthonormée* si, de plus

$$\forall x \in X, \quad Q(x) = 1.$$

Proposition 7.4.2 Une partie orthonormée est libre.

Démonstration. Si $\sum a_x x = 0$ avec $a_x \in K$ presque tous nuls, alors pour tout $y \in X$, on aura

$$0 = \Phi(0, y) = \Phi\left(\sum a_x x, y\right) = \sum a_x \Phi(x, y) = a_y. \quad \blacksquare$$

Remarque 1. On peut aussi considérer la notion de *famille orthogonale* $(x_i)_{i\in I}$ avec la condition

$$\forall i \neq j \in I, \quad x_i \perp x_j,$$

et de *famille orthonormée* avec la condition supplémentaire

$$\forall i \in I, \quad Q(x_i) = 1.$$

2. Une partie orthogonale n'est pas automatiquement libre : prendre $Q(x,y) = 2xy$ sur K^2 et $x_1 = (1,0)$ et $x_2 = (2,0)$.
3. En dimension finie, une base $\mathscr{B}$ est orthogonale (resp. orthonormée) pour Q si et seulement si la matrice J de Q dans $\mathscr{B}$ est diagonale (resp. si $J = I$).
4. Lorsque $E = K^n$, dire que J est diagonale (resp. que $J = I$) signifie que $Q(x_1,\dots,x_n) = \sum c_i x_i^2$ (resp. $= \sum x_i^2$).
5. S'il existe une base orthonormée finie pour Q, on a un isomorphisme de groupes $O(Q) \simeq O(n)$.

Proposition 7.4.3 Si Q est une forme quadratique sur un espace vectoriel de dimension finie E, il existe une base orthogonale pour Q.

Démonstration. On peut supposer que $Q \neq 0$ et choisir $e_n \in E$ tel que $Q(e_n) \neq 0$. On pose alors $\varphi := l_Q(e_n) \in {}^tE$. Comme $\varphi(e_n) = Q(e_n) \neq 0$, on voit que $H := \ker\varphi$ est un hyperplan, et par récurrence, il existe une base orthogonale $(e_1,\dots,e_{n-1})$ pour $Q_{|H}$. Par construction, $(e_1,\dots,e_n)$ est une base orthogonale pour Q. ∎

Remarque 1. Cela signifie que toute matrice symétrique est congruente à une matrice diagonale, ce qui contraste avec le cas des matrices semblables.
2. Si la matrice de Q dans l'ancienne base $\mathscr{B}$ est J et que sa matrice dans la nouvelle base $\mathscr{B}'$ est D, on aura donc

$$D = {}^tPJP \quad \text{et} \quad J = {}^tP^{-1}DP^{-1},$$

où P désigne matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$.

Corollaire 7.4.4 Si Q est une forme quadratique sur un espace vectoriel de dimension finie E, il existe $\varphi_1,\dots,\varphi_n \in {}^tE$ tels que

$$\forall x \in E, \quad Q(x) = c_1\varphi_1(x)^2 + \cdots + c_n\varphi_n(x)^2$$

Démonstration. Il suffit de choisir une base orthogonale $(e_1,\dots,e_n)$ et de poser $\varphi_i := {}^te_i$. ∎

Remarque 1. On devrait dire qu'on a décomposé Q en *combinaison linéaire de carrés*, mais on dit plutôt en *somme de carrés*.
2. Si on part de $J \in \mathrm{SM}_n(K)$, on obtient une matrice diagonale D et une matrice de passage P. On aura alors

$$D = \begin{bmatrix} c_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c_n \end{bmatrix} \quad \text{et} \quad P^{-1} = \begin{bmatrix} [\varphi_1] \\ \vdots \\ [\varphi_n] \end{bmatrix}$$

(attention : il faudra inverser cette dernière matrice pour trouver P).

3. Voici un algorithme dû à Gauss pour décomposer une forme quadratique en somme de carrés. On part de
$$Q(x_1,\dots,x_n)=\sum_{i=1}^{n}c_ix_i^2+2\sum_{i<j}c_{i,j}x_ix_j,$$
et on fait une récurrence sur n. S'il existe $k\in\{1,\dots,n\}$ tel que $c_k\neq 0$, on écrit
$$Q(x)=c_k\left(x_k+\sum_{j\neq k}\frac{c_{k,j}}{c_k}x_j\right)^2+Q'(x_1,\dots,x_{k-1},x_{k+1},\dots,x_n),$$
Sinon, on a
$$Q(x_1,\dots,x_n)=2\sum_{i<j}c_{i,j}x_ix_j,$$
Si $Q\neq 0$, il existe $k<l\in\{1,\dots,n\}$ tels que $c_{k,l}\neq 0$, on écrit
$$Q(x)=2c_{k,l}\left(x_k+\sum_{j\neq k,l}\frac{c_{l,j}}{c_{k,l}}x_j\right)\left(x_l+\sum_{j\neq k,l}\frac{c_{k,j}}{c_{k,l}}x_j\right)+Q'(x_1,\dots,x_{k-1},x_{k+1},\dots,x_{l-1},x_{l+1},\dots,x_n),$$
On est ainsi ramenés au cas $n=2$, c'est à dire $Q(x,y)=2cxy$ et on a alors
$$2cxy=2c\left(\frac{x+y}{2}\right)^2-2c\left(\frac{x-y}{2}\right)^2.$$

Exemple Voici comment on peut décomposer $xy+xz+yz$ en somme de carrés :
$$\begin{aligned}xy+xz+yz&=(x+z)(y+z)-z^2\\&=\left(\frac{x+z+y+z}{2}\right)^2-\left(\frac{x+z-y-z}{2}\right)^2-z^2\\&=\left(\frac{x+y}{2}+z\right)^2-\left(\frac{x-y}{2}\right)^2-z^2.\end{aligned}$$
$$J=\begin{bmatrix}0&\frac12&\frac12\\\frac12&0&\frac12\\\frac12&\frac12&0\end{bmatrix},\quad D=\begin{bmatrix}1&0&0\\0&-1&0\\0&0&-1\end{bmatrix}\quad\text{et}\quad P^{-1}=\begin{bmatrix}\frac12&\frac12&1\\\frac12&-\frac12&0\\0&0&1\end{bmatrix}.$$
Il suffit allors d'inverser P^{-1} pour trouver
$$P=\begin{bmatrix}1&1&-1\\1&-1&-1\\0&0&1\end{bmatrix}$$
et en déduire la nouvelle base $((1,1,0),(1,-1,0),(-1,-1,1))$.

7.5 Formes quadratiques complexes et réelles

Proposition 7.5.1 Si Q est une forme quadratique complexe (resp. réelle) sur un espace vectoriel de dimension finie, alors il existe une base dans laquelle la matrice J de Q vaut
$$J=\begin{bmatrix}I_r&0\\0&0\end{bmatrix}\quad\left(\text{resp.}\quad J=\begin{bmatrix}I_p&0&0\\0&-I_q&0\\0&0&0\end{bmatrix}\right).$$

Démonstration. Après avoir choisi une base orthogonale $(e_1,\dots,e_n)$, on peut supposer que $E=\mathbb{C}^n$ (resp. $E=\mathbb{R}^n$) et que
$$Q(x)=a_1x_1^2+\cdots+a_nx_n^2.$$
Il suffit alors de faire un changement de base $x_i\mapsto b_ix_i$ avec $b_i^2=a_i$ (resp. $b_i^2=|a_i|$), puis de réordonner les vecteurs. Les détails sont laissés en exercice. ■

Remarque 1. Cette proposition est en fait valide pour n'importe quel corps *algébriquement clos* (resp. *réel clos*).
2. La proposition implique que, lorsque $K=\mathbb{C}$ (resp $K=\mathbb{R}$), on a un isomorphisme de groupes
$$\mathrm{O}(Q)\simeq \mathrm{O}(r)\quad (\text{resp.}\simeq \mathrm{O}(p,q))$$
avec $\operatorname{rang}(Q)=r$ (resp. $=p+q$).
3. On voit aussi que, lorsque $K=\mathbb{C}$ et Q est non dégénérée, il existe une base *orthonormée*.

Théoreme 7.5.2 — d'inertie de Sylvester. Si Q est une forme quadratique réelle sur un espace vectoriel de dimension finie, il existe p,q *uniques* telle que la matrice J de Q dans une base $(e_1,\dots,e_n)$ soit
$$J=\begin{bmatrix} I_p & 0 & 0\\ 0 & -I_q & 0\\ 0 & 0 & 0\end{bmatrix}.$$

Démonstration. Grâce au corollaire 7.5.1, il suffit de montrer l'unicité. Supposons donc que la matrice J' de Q dans une base $(e'_1,\dots,e'_n)$ soit
$$J'=\begin{bmatrix} I_{p'} & 0 & 0\\ 0 & -I_{q'} & 0\\ 0 & 0 & 0\end{bmatrix}.$$
Nous allons montrer que $(e_1,\dots,e_p,e_{p'+1},\dots,e_{p'+q'})$ est libre. En effet, si
$$a_1e_1+\cdots+a_pe_p+b_1e'_{p'+1}+\cdots+b_{q'}e'_{p'+q'}=0,$$
et si on pose $x:=a_1e_1+\cdots+a_pe_p$, on aura aussi $x=-b_1e'_{p'+1}-\cdots-b_{q'}e'_{p'+q'}$. On en déduit d'une part, que
$$Q(x)=a_1^2Q(e_1)+\cdots+a_p^2Q(e_p)=a_1^2+\cdots+a_{p^2}\geq 0$$
et d'autre part que
$$Q(x)=(-1)^2b_1^2Q(e'_{p'+1})+\cdots+(-1)^2b_{q'}^2Q(e'_{p'+q'})=-b_1^2-\cdots-b_{q'}^2\leq 0.$$
Cela implique que $Q(x)=0$ et donc que $a_1=\cdots=a_p=b_1=\cdots=b_{q'}=0$ et nous voyons que la famille est bien libre. Il suit que $p+q'\leq r:=\operatorname{rang}(Q)=p+q$ et donc $q'\leq q$. Symétriquement, on aura $q\leq q'$ si bien que $q=q'$. Et on conclut avec $p'+q'=\operatorname{rang}(Q)=p+q$. ■

Définition 7.5.3 On dit alors que $\operatorname{sign}(Q):=(p,q)$ est la *signature* de Q.

Corollaire 7.5.4 Deux formes quadratiques complexes (resp. réelles) sur un espace vectoriel de dimension finie sont congruentes si et seulement si elles ont même rang (resp. même signature).

Démonstration. ■

Exemple La signature de $xy+xz+yz$ est $(1,2)$.

Définition 7.5.5 Une forme quadratique (réelle) Q sur E est *positive* (resp. *négative*) si

$$\forall x \in E, \quad Q(x) \geq 0 \quad (\text{resp. } \leq 0).$$

Remarque

1. On étendra ce vocabulaire aux formes bilinéaires symétriques ainsi qu'aux matrices symétriques.
2. On rappelle que l'on dit parfois *défini* au lieu de *non dégénéré*, cela signifie donc que le rang est maximum.
3. Pour démontrer les énoncés qui suivent, il suffit d'écrire

$$Q(x) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2.$$

Proposition 7.5.6 Soit Q une forme quadratique sur un espace vectoriel réel de dimension n. On a alors

1. Q est positive $\Leftrightarrow \operatorname{sign}(Q) = (p,0)$,
2. Q est négative $\Leftrightarrow \operatorname{sign}(Q) = (0,q)$,
3. Q est définie positive $\Leftrightarrow \operatorname{sign}(Q) = (n,0)$,
4. Q est définie négative $\Leftrightarrow \operatorname{sign}(Q) = (0,n)$.

Démonstration. ■

Proposition 7.5.7 Une forme quadratique réelle Q sur un espace vectoriel de dimension finie E est définie positive (resp. définie négative) si et seulement si

$$\forall x \in E \setminus \{0\}, \quad Q(x) > 0 \quad (\text{resp. } < 0).$$

Démonstration. ■

7.6 Exercices

Exercice 7.1 Vérifiez que les formules suivantes définissent des formes bilinéaires. Déterminer à chaque fois le noyau et le rang - ainsi que la matrice le cas échéant.

1. $((x_1,\dots,x_n),(y_1,\dots,y_n)) \mapsto x_1y_1+\cdots+x_ny_n$ sur K^n.
2. $\det_{\mathscr{B}}$ lorsque $\mathscr{B}$ est une base ordonnée d'un plan H.
3. $\Phi((a,b),(c,d)) = a^2-2bc+d^2$ sur K^2.
4. $(f,g) \mapsto \int_0^1 (fg)(t)\mathrm{d}t$ sur $\mathscr{C}^0([0,1],\mathbb{R})$.
5. $(z_1,z_2) \mapsto \Re(z_1z_2)$ sur $\mathbb{C}$ (vu comme espace vectoriel sur $\mathbb{R}$)

Exercice 7.2 Montrer que $(u,v) \mapsto \mathrm{tr}(u\circ v)$ est une forme bilinéaire symétrique non dégénérée sur $L(E)$ lorsque E est un espace vectoriel de dimension finie.

Exercice 7.3 Soit Φ la forme bilinéaire symétrique donnée par

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 5 \end{bmatrix}.$$

1. Expliciter Φ ainsi que la forme quadratique Q associée.
2. Déterminer son rang et son noyau. Est-ce une forme non dégénérée ?
3. Quel est l'orthogonal de H : $\mathrm{Vect}((1,0,0),(1,0,1))$? A-t-on $\dim H+\dim H^{\perp}=3$?
4. Mêmes questions lorsque $H=\mathrm{Vect}((0,1,0),(1,0,1))$. Expliquer pourquoi ceci peut arriver.

Exercice 7.4 Quelle est la matrice de la forme quadratique y^2-2xz (dans la base canonique) ? Et dans la base $((1,1,0),(0,1,1),(1,1,1))$?

Exercice 7.5

1. Montrer que $\Phi(P,Q) := P(1)Q(-1)+P(-1)Q(1)$ définit une forme bilinéaire symétrique sur $E := K[T]_{\leq 2}$ dont on déterminera la matrice dans la base canonique $\mathscr{B}$. Quelle est la forme quadratique associée ?
2. Montrer que $\mathscr{B}' := (1-T^2,T,T^2)$ est une base de E et déterminer la matrice de Φ dans la base $\mathscr{B}'$.
3. Déterminer le rang et le noyau de Φ. Est-ce une forme bilinéaire symétrique non dégénérée ?

Exercice 7.6

1. Montrer que $\Phi(P,Q) := \int_0^1 P(t)Q(t)\mathrm{d}t$ définit une forme bilinéaire symétrique sur $E := \mathbb{R}[T]_{\leq 2}$ dont on déterminera la matrice dans la base canonique B. Écrire la forme quadratique correspondante ?
2. Rang ? Noyau ? Est-elle non-dégénérée ?
3. Mêmes questions avec $\Phi(P,Q) := P(0)Q(0)+P(1)Q(1)$.

Exercice 7.7 Soit E un espace vectoriel de dimension finie muni d'une forme quadratique Q de noyau N.

1. Soient F un sous-espace vectoriel de E et $G := F+N$. Montrer que $N \subset F^{\perp}$ et que $(G/N)^{\perp} = F^{\perp}/N$. En déduire que $F^{\perp\perp}=G$.
2. Vérifiez ces résultats dans le cas ou Q est $x^2-z^2+2xy+2yz$ et $F=\mathrm{Vect}(1,1,1)$.

Exercice 7.8 On considère la forme quadratique Q donnée par $x_1x_2-x_3x_4$ ainsi qu'un hyperplan H d'équation $a_1x_1+a_2x_2+a_3x_3+a_4x_4=0$.

1. Quelle est la matrice de Q (dans la base canonique) ?

2. Quel est son rang ? Est-elle non dégénérée ? Quelle est la dimension de l'orthogonal de H ?
3. Expliciter la condition $u \perp H$ lorsque $u = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. En déduire une base de $H^\perp$.
4. En déduire une condition nécessaire et suffisante sur les a_i pour que la restriction de Q à H soit non dégénérée.

Exercice 7.9 1. Déterminer le groupe orthogonal $\mathrm{O}(2)$ en résolvant ${}^tAA = I$ avec $A := \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. On examinera plus particulièrement le cas $K = \mathbb{R}$.

2. Mêmes question avec $\mathrm{O}(1,1)$ en résolvant ${}^tAJA = J$ lorsque $J := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Exercice 7.10 Appliquer l'algorithme de Gauss aux formes quadratiques suivantes
1. $2x^2 + y^2 - z^2 + 3xy - 4xz$.
2. $2x^2 - 2y^2 - 6z^2 + 3xy - 4xz + 7yz$.
3. $xy + yz + zt + tx$.
4. $xy - xt + yz - yt + ys + zt - zs + 2st$.

Exercice 7.11 Décomposer en carrés la forme quadratique $xy + yz + xz$. Quelle est sa signature ? Quel est son rang ? Écrire une base orthogonale pour cette forme quadratique. On désigne par D l'axe des x. Déterminer $D^\perp$. Est-ce que D et $D^\perp$ sont supplémentaires ?

Exercice 7.12 On considère la forme quadratique $x^2 + 3y^2 - 8z^2 - 4xy + 2xz - 10yz$. Déterminer son noyau. Montrer que l'ensemble des vecteurs isotropes est la réunion de deux plans dont on donnera des équations. Donner aussi la signature de cette forme quadratique. Enfin, quel est l'orthogonal de $(1, 1, 1)$?

Exercice 7.13 Montrer que pour une forme quadratique Q sur un plan vectoriel H, les conditions suivantes sont équivalentes :
1. Q est non dégénérée et il existe un vecteur isotrope non nul.
2. Il existe une base de H dans laquelle la matrice de Q est $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
3. Il existe une base de H dans laquelle la matrice de Q est $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Exercice 7.14 Déterminer la signature des formes quadratiques de l'exercice 7.6.

Exercice 7.15 On pose

$$A := \begin{bmatrix} 5 & 4 & 3 \\ 4 & 5 & 3 \\ 3 & 3 & 2 \end{bmatrix} \quad \text{et} \quad B := \begin{bmatrix} 9 & 0 & -6 \\ 0 & 1 & 0 \\ -6 & 0 & 4 \end{bmatrix}.$$

Montrer (sans la calculer !) l'existence de $P \in \mathrm{GL}(\mathbb{R}^3)$ telle que $B = {}^tPAP$.

8. Espace vectoriel normé

8.1 Topologie

On rappelle ici le vocabulaire de base en topologie en renvoyant l'étudiant curieux vers des ouvrages plus savants, comme par exemple, celui de Gilles Christol, Anne Cot et Charles-Michel Marle ([CCM97]).

Définition 8.1.1 Un *espace topologique* est un ensemble X muni d'un ensemble non vide de parties $U \subset X$, qui seront dites *ouvertes*, qui est stable par union quelconque et intersection finie. Le complémentaire F d'une partie ouverte U est dite *fermée*.

Remarque

1. On demande donc que si $(U_i)_{i\in I}$ est une famille d'ouverts de X, alors $\cup_{i\in I} U_i$ est ouvert et que si $(U_1,\dots,U_n)$ est une famille finie d'ouverts, alors $U_1 \cap \cdots \cap U_n$ soit aussi ouvert.
2. De manière équivalente, on pourrait demander que les fermés soient stables par intersection quelconque et par union finie.
3. Comme cas particulier, on voit que $\emptyset$, qui est l'union vide, de même que X, qui est l'intersection vide sont tous les deux ouvert et fermé.
4. Attention, il y a en général des parties de X qui ne sont ni ouverte, ni fermée.

Définition 8.1.2

1. Une application $f : X \to Y$ entre deux espaces topologiques est *continue* si l'image inverse d'un ouvert est toujours ouvert. C'est un *homéomorphisme* si f est bijective *et* f^{-1} est continue.
2. Un *sous-espace* d'un espace topologique X est un espace topologique Y qui est contenu dans X et tel que l'inclusion soit continue.

Remarque

1. Pour qu'une application soit continue, on demande donc que si $V \subset Y$ est un ouvert quelconque, alors $f^{-1}(V) \subset X$ soit aussi ouvert.
2. De manière équivalente, on pourrait demander la propriété analogue pour les fermés.
3. Attention : une application continue et bijective n'est pas nécessairement un homéomorphisme.

4. Par contre, la composée de deux applications continue est toujours continue.
5. Sur une partie Y d'un espace topologique X, il existe une topologie universelle (dite *induite*) : une application $Z \to Y$ sera continue si et seulement si la composée $Z \to Y \hookrightarrow X$ est continue. En fait, les ouverts de Y sont les $U \cap Y$ avec U ouvert dans X.
6. Sur un produit $\prod_{s\in S} X_s$ d'espaces topologiques, il existe aussi une topologie universelle (dite *produit*) : une application $Y \mapsto \prod_{s\in S} X_s$ sera continue si et seulement si ses composantes sont continues.

Définition 8.1.3 Une *distance* sur un ensemble X est une application $d : X \times X \to \mathbb{R}_{\geq 0}$ telle que

1. $\forall x, y \in X, \quad d(x,y) = 0 \Leftrightarrow x = y,$
2. $\forall x, y \in X, \quad d(x,y) = d(y,x),$
3. $\forall x, y, z \in X, \quad d(x,z) \leq d(x,y) + d(y,z).$

Un ensemble muni d'une distance est un *espace métrique*. La *boule ouverte* (resp. fermée) de centre $x \in X$ et de rayon $r \in \mathbb{R}_{\geq 0}$ est alors

$$\mathrm{B}(x, r^-) = \{y \in x, \quad d(x,y) < r\} \quad \text{resp.} \quad \mathrm{B}(x, r^+) = \{y \in x, \quad d(x,y) \leq r\}$$

Enfin, une partie U de X est *ouverte* si

$$\forall x \in X, \exists r > 0, \quad \mathrm{B}(x, r^-) \subset U.$$

Remarque 1. Les ouverts d'un espace métrique X définissent une topologie sur X et les boules ouvertes (resp. fermées) sont bien des parties ouvertes (resp. fermées).
2. Attention : des distances distinctes peuvent donner naissance à la même topologie. Il y a aussi des espaces topologiques qui ne sont aucunement des espaces métriques.
3. Attention : en général, dans un espace métrique, il y a d'autres ouverts que les boules ouvertes.
4. On dit qu'une partie $Y \subset X$ d'un espace métrique est *bornée* si Y est contenu dans une boule. Plus généralement, on dit qu'une application $Y \to X$ est *bornée* si $f(Y)$ est bornée.

Définition 8.1.4 Une application $f : X \to Y$ entre deux espaces métriques est *continue en* $x \in X$ si

$$\forall \varepsilon > 0, \exists \eta \geq 0, \forall y \in X, \quad d(x,y) \leq \eta \Rightarrow d(f(x), f(y)) \leq \varepsilon.$$

Elle est *uniformément continue* si

$$\forall x, y \in X, \forall \varepsilon > 0, \exists \eta \geq 0, \quad d(x,y) \leq \eta \Rightarrow d(f(x), f(y)) \leq \varepsilon.$$

Elle est *lipschitzienne* s'il existe $k \in \mathbb{R}$ tel que

$$\forall x, y \in X, \quad d(f(x), f(y)) \leq k d(x,y).$$

Remarque 1. On a la suite d'implications : lipschitzienne $\Rightarrow$ uniformément continue $\Rightarrow$ continue $\Leftrightarrow$ continue en tout $x \in X$.
2. Si f est continue en x, on dit aussi que la *limite* de f en x est $f(x)$ ou encore que $f(y)$ *tend vers* $f(x)$ quand y *tend vers* x.
3. On dit parfois *contractante* (resp. *strictement contractante*) pour une application lipschitzienne de rapport 1 (resp. strictement inférieur à 1).
4. On dit aussi *isométrie* si

$$\forall x, y \in X, \quad d(f(x), f(y)) = d(x,y).$$

5. Si Y est une partie d'un espace métrique X, la restriction à Y de la distance est encore une distance et la topologie de Y est la topologie induite.
6. La distance produit sur un produit fini $X_1 \times \cdots \times X_n$ d'espaces métriques est définie par

$$d((x_1,\ldots,x_n),(y_1,\ldots y_n)) = \max_{i=1}^{n} d(x_i,y_i).$$

La topologie correspondante est la topologie produit.

Définition 8.1.5 Soit X un espace métrique. Une suite $(x_n)_{n\in\mathbb{N}} \in X^{\mathbb{N}}$ *converge* vers $x \in X$ si

$$\forall \varepsilon > 0, \exists M \in \mathbb{R}, \forall n \geq M, \quad d(x_n,x) \leq \varepsilon.$$

Une suite $(x_n)_{n\in\mathbb{N}} \in X^{\mathbb{N}}$ est *de Cauchy* si

$$\forall \varepsilon > 0, \exists M \in \mathbb{R}, \forall n,m \geq M, \quad d(x_n,x_m) \leq \varepsilon.$$

L'espace X est *complet* si toute suite de Cauchy est convergente.

Remarque 1. Une application est continue (en x) si et seulement si l'image d'une suite convergente (vers x) est une suite convergente (vers $f(x)$).
2. Une partie Y d'un espace métrique X est fermée si et seulement si toute suite dans Y qui converge dans X, converge en fait dans Y.
3. En conséquence, si Y est complet, alors il est fermé dans X. Réciproquement, si X est complet et si Y est fermé dans X, alors Y est complet.

8.2 Valeur absolue

Définition 8.2.1 Une *valeur absolue* sur un corps K est une application $|\ | : K \to \mathbb{R}_{\geq 0}$ telle que
1. $\forall a \in K, \quad |a| = 0 \Leftrightarrow a = 0,$
2. $\forall a,b \in K, \quad |ab| = |a||b|$
3. $\forall a,b \in K, \quad |a+b| \leq |a|+|b|.$

Elle est *archimédienne* si

$$\forall M \in \mathbb{R}, \exists n \in \mathbb{N}, \quad |n| \geq M,$$

ultramétrique si

$$\forall a,b \in K, \quad |a+b| \leq \max\{|a|,|b|\},$$

et *triviale* si

$$\forall a \in K \setminus \{0\}, \quad |a| = 1.$$

Exemple 1. $|a| := \max\{a,-a\}$ définit une valeur absolue archimédienne sur $\mathbb{R}$ ou $\mathbb{Q}$.
2. $|a+ib| := \sqrt{a^2+b^2}$ définit une valeur absolue archimédienne sur $\mathbb{C}$.
3. $|a| = \frac{1}{2^v}$ si $a = 2^v \frac{p}{q}$ avec p,q impairs, définit une valeur absolue ultramétrique sur $\mathbb{Q}$.
4. $|R(T)| = e^{-v}$ si $R(T) = T^v \frac{P(T)}{Q(T)}$ avec $P(0) \neq 0$ et $Q(0) \neq 0$, définit une valeur absolue ultramétrique sur le corps $k(T)$ si k est un corps quelconque.

Remarque 1. La valeur absolue est un morphisme de monoïdes qui induit un morphisme de groupes $K^\times \to \mathbb{R}_{>0}$. En particulier, on a toujours $|1_K| = 1_{\mathbb{R}}$, $|a^n| = |a|^n$ pour $n \in \mathbb{Z}$ si $a \neq 0$.
2. Par récurrence, on voit qu'on a toujours $|n| \leq n$ si $n \in \mathbb{N}$ mais on a même $|n| \leq 1$ si la valeur absolue est ultramétrique.
3. Une valeur absolue est non triviale si et seulement si $\exists c \in K, \quad 0 < |c| < 1$.

Proposition 8.2.2 Une valeur absolue est ultramétrique si et seulement si elle n'est pas archimédienne.

Démonstration. Nous avons déjà remarqué que les entiers naturels sont bornés par 1 lorsque la valeur absolue est ultramétrique. Inversement, supposons que les entiers naturels soient bornés. Si $n \in \mathbb{N}$ satisfait $|n| > 1$, on a alors $|n^k| = |n|^k \to +\infty$. Contradiction. On voit donc que les entiers naturels sont en fait bornés par 1. Maintenant, si $a, b \in K$, on a pour tout $n \in \mathbb{N}$,

$$(a+b)^n = \sum_{k=1}^{n} \binom{n}{k} a^k b^{n-k}$$

et donc

$$|a+b|^n \leq \sum_{k=1}^{n} \left|\binom{n}{k}\right| |a|^k |b|^{n-k} \leq (n+1)\max\{|a|,|b|\}^n.$$

si bien que $|a+b| \leq (n+1)^{\frac{1}{n}} \max\{|a|,|b|\}$. Or $(n+1)^{\frac{1}{n}} \to 1$ quand $n \to +\infty$. ■

Théoreme 8.2.3 — d'Ostrowski. Soit K un corps valué.
1. Si $|\ |$ est archimédienne, il existe $\alpha > 0$ tel que $\forall n \in \mathbb{N}, |n| = n^\alpha$.
2. Si $|\ |$ est ultramétrique, il existe au plus un p premier tel que $|p| < 1$, et alors $|n| = 1$ lorsque p ne divise pas n.

Démonstration. Hors programme. ■

8.3 Norme

On fixe un corps K muni d'une valeur absolue non triviale (penser à $\mathbb{R}$ ou $\mathbb{C}$).

Définition 8.3.1 Une *norme* sur un espace vectoriel E est une application $\|\ \| : E \to \mathbb{R}_{\geq 0}$ telle que
1. $\forall V \in E, \quad \|V\| = 0 \Leftrightarrow V = 0$,
2. $\forall \lambda \in \mathbb{R}, \forall V \in E, \quad \|\lambda V\| = |\lambda| \|V\|$
3. $\forall V, W \in E, \quad \|V+W\| \leq \|V\| + \|W\|$.

Exemple 1. K muni de sa valeur absolue est un espace vectoriel normé.
2. Si $E_1, \ldots, E_n$ sont des espaces vectoriels normés, on munit $E_1 \times \cdots \times E_n$ de

$$\|(x_1, \ldots, x_n)\|_\infty := \max_{i=1}^{n} \|x_i\|.$$

En particulier, K^n devient un espace vectoriel normé.
3. On munit l'espace $\ell_\infty(K)$ des suites *bornées* de

$$\|(x_i)_{i\in\mathbb{N}}\|_\infty := \sup_{i\in\mathbb{N}} |x_i|.$$

4. Plus généralement, si on se donne une famille d'espace vectoriels normés $(E_s)_{s\in S}$, alors les familles bornées de $\prod_{s\in S} E_s$ forment un espace vectoriel $\prod_{s\in S}^{b} E_s$ normé pour la norme sup.
5. De même, les fonctions bornées $f : X \to E$ définies sur un ensemble X et à valeurs dans un espace vectoriel normé, forment un espace vectoriel normé $\mathscr{F}^b(X,E)$ pour la norme sup.
6. On peut munir K^n de $\|\ \|_\infty$ mais aussi de

$$\|(x_1, \ldots, x_n)\|_p := \left(\sum_{i=1}^{n} |x_i|^p\right)^{\frac{1}{p}}$$

pour $p \geq 1$.

7. On peut munir $\mathscr{C}([0,1],\mathbb{R})$ de
$$\|f\|_p := \left(\int_0^1 f(t)^p \mathrm{d}t\right)^{\frac{1}{p}} \quad \text{pour } p \geq 1 \quad \text{ou} \quad \|f\|_\infty := \sup_{0\leq t\leq 1} |f(t)|.$$

Remarque 1. Si F est un sous-espace vectoriel d'un espace vectoriel normé, alors $\| \ \|_{|F}$ est une norme sur F.
2. Si E est un espace vectoriel normé, alors $d(x,y) := \|y-x\|$ définit une distance sur E.

Proposition 8.3.2 Si E est un espace vectoriel normé, les lois
$$\begin{array}{rcl} E\times E & \longrightarrow & E \\ (x,y) & \longmapsto & x+y \end{array} \qquad \text{et} \qquad \begin{array}{rcl} K\times E & \longrightarrow & E \\ (a,x) & \longmapsto & ax \end{array}$$
sont continues.

Démonstration. L'addition est en fait lipschitzienne :
$$\begin{aligned} d(x_1+y_1,x_2+y_2) &= \|x_2+y_2-x_1-y_1\| \\ &\leq \|x_2-x_1\|+\|y_2-y_1\| \\ &= d(x_1,x_2)+d(y_1,y_2) \\ &\leq 2d((x_1,x_2),(y_1,y_2)). \end{aligned}$$
On montre de même que la multiplication est continue en (x,a) donné en utilisant
$$\|by-ax\| \leq |b-a|\|x\|+|b-a|\|y-x\|+|a|\|y-x\|.$$
Les détails sont laissés en exercice. ∎

Remarque En fait, K est un corps topologique (addition, multiplication et inverse continus – vérifier) et E est un espace vectoriel topologique (addition et multiplication continus).

Proposition 8.3.3 Si F est un sous-espace vectoriel *fermé* d'un espace vectoriel normé E, alors la formule
$$\|x+F\| := d(x,F) := \inf_{y\in F} d(x,y)$$
définit une norme sur E/F.

Démonstration. On a bien sûr toujours $d(x,F)=0$ si $x\in F$. On montre aussi facilement que, si $x_1,x_2\in E$, alors $d(x_1+x_2,F)\leq d(x_1,F)+d(x_2,F)$. On en déduit que si $x_2-x_1\in F$, alors $d(x_1,F)=d(x_2,F)$. Ensuite, si $a\in K$ et $x\in E$, on montre que $d(ax,F)=|a|d(x,F)$. Enfin, puisque F est fermé, on peut montrer que si $d(x,F)=0$, on aura bien $x\in F$. Détails en exercice. ∎

Remarque La topologie sur E/F est la topologie *quotient* : Une application $E/F\to X$ est continue si et seulement si la composée $E \twoheadrightarrow E/F\to X$ est continue.

Proposition 8.3.4 Soit $u: E\to F$ une application linéaire entre deux espaces vectoriels normés. Alors, les conditions suivantes sont équivalentes :
1. u est continue en 0,
2. $\exists M\in\mathbb{R}, \forall x\in E, \quad \|u(x)\|\leq M\|x\|$,
3. u est lipschitzienne,
4. u est uniformément continue,

5. u est continue.

Démonstration. On fait une démonstration cyclique, et seule la première implication nécessite vraiment une preuve. En prenant $\varepsilon = 1$ dans la définition de la continuité en 0, on voit qu'il existe $\eta > 0$ tel que $\|x\| \leq \eta \Rightarrow \|u(x)\| \leq 1$. Si $K = \mathbb{R}$ ou $\mathbb{C}$, il suffit de poser $M = \frac{1}{\eta}$ (le cas général est discuté plus bas). ■

Remarque 1. Pour démontrer la proposition dans le cas général, on fait intervenir un $c \in K$ avec $0 < |c| < 1$ et on procède par l'absurde. On suppose qu'il existe une suite y_n telle que $\|u(y_n)\| \geq \frac{1}{|c|^n}\|y_n\|$. Pour chaque entier n, il existe $m_n \in \mathbb{Z}$ tel que $1 \leq |c|^{m_n}\|u(y_n)\| < |c|$ et on pose $x_n = c^{m_n}y_n$. On a alors $x_n \to 0$ mais $u(x_n) \geq 1$ pour tout n.

2. On dispose d'un résultat analogue pour les applications multilinéaires. En particulier, une application multilinéaire $\Phi : E_1 \times \cdots \times E_n \to F$ sera continue si et seulement

$$\exists M \in \mathbb{R}, \forall x_1 \in E_1, \ldots, x_n \in E_n, \quad \|\Phi(x_1, \ldots, x_n)\| \leq M \max_{i=1}^{n} \|x_i\|.$$

3. On voit aussi aisément qu'une application linéaire $u : E \to F$ est une isométrie si et seulement si

$$\forall x \in E, \quad \|u(x)\| = \|x\|.$$

Exemple Toute application linéaire $u : K^m \to K^n$ est continue (si on munit les espaces de la norme max) : si $A := [a_{i,j}]$ désigne la matrice de u, on a

$$\|u(x)\| \leq M\|x\| \quad \text{avec } M = \sum_{i,j} |a_{i,j}|.$$

Proposition 8.3.5 Si E et F sont deux espaces vectoriels normés, alors l'ensemble $\mathscr{L}(E,F) \subset \mathrm{L}(E,F)$ des applications linéaires continues est un sous-espace vectoriel et la formule

$$\|u\| := \sup_{x \neq 0} \frac{\|u(x)\|}{\|x\|}$$

définit une norme. On écrira $\mathscr{L}(E)$ si $E = F$ (avec la même norme).

Démonstration. La première assertion résulte de la proposition 8.3.2. La seconde se vérifie aisément. Les détails sont laissés en exercice. ■

Remarque 1. Si $u \in \mathscr{L}(E,F)$, alors

$$\forall x \in E, \quad \|u(x)\| \leq \|u\|\|x\|.$$

2. On peut aussi montrer (et c'est immédiat si $K = \mathbb{R}$ ou $\mathbb{C}$) que

$$\|u\| := \sup_{\|x\| \leq 1} \|u(x)\|.$$

3. On montre aussi facilement que si $u : E \to F$ et $v : F \to G$ sont deux applications linéaires continues entre espaces vectoriels normés, alors $v \circ u$ aussi que $\|v \circ u\| \leq \|v\|\|u\|$.

Proposition 8.3.6 Soient $\varphi : E \to K$ une forme linéaire non nulle et $H = \ker\varphi$. Alors, φ est continue si et seulement si H est fermé.

Démonstration. Comme $\{0\} \subset K$ est fermé, on voit immédiatement que, si φ est continue, alors $H := \varphi^{-1}(\{0\})$ est nécessairement fermé. Pour montrer l'implication réciproque, on peut considérer le diagramme commutatif

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, "\pi"] & K , \\ E/H \arrow[ur, "\overline{\varphi}", "\simeq"'] & \end{tikzcd}$$

Puisque H est fermé, E/H est un espace vectoriel normé et π est continue (contractante). Il suffit donc de montrer que $\overline{\varphi}$ est continue. Autrement dit, on peut supposer que φ est un isomorphisme, c'est à dire que E est une droite. On choisit une base e de E et on pose $M := \frac{\|\varphi(e)\|}{\|e\|}$. Si $x = ae \in E$, on aura

$$\|\varphi(x)\| = |a|\|\varphi(e)\| = |a|M\|e\| = M\|x\|. \quad \blacksquare$$

8.4 Espace de Banach

On suppose maintenant que K est un corps valué **complet** (pour une valeur absolue non triviale).

Exemple

1. Le corps $\mathbb{Q}$, muni de la valeur absolue habituelle ou de la valeur absolue p-adique, n'est pas complet.
2. Les corps $\mathbb{R}$ et $\mathbb{C}$ sont complets.
3. Si k est un corps quelconque, alors le corps $k(T)$, muni de la valeur absolue T-adique, n'est pas complet.
4. Le corps
$$k((T)) = \left\{ \sum_{n>>-\infty} a_n T^n, \quad a_n \in k \right\},$$
où k est un corps quelconque, muni de $\|\sum_{n\geq\nu} a_n T^n\| = e^{-\nu}$ si $a_\nu \neq 0$, est complet.
5. Le corps
$$\mathbb{Q}_p = \left\{ \sum_{n>>-\infty} a_n p^n, \quad a_n \in \{0,\ldots,p-1\} \right\},$$
muni de $\|\sum_{n\geq\nu} a_n p^n\| = \frac{1}{p^\nu}$ si $a_\nu \neq 0$, est complet.

Définition 8.4.1 Un *espace de Banach* est un espace vectoriel normé complet.

Exemple

1. Le corps K est un espace de Banach. Plus généralement, K^n est un espace de Banach.
2. Un produit fini d'espaces de Banach est un espace de Banach.
3. Si $(E_s)_{s\in S}$ est une famille d'espace de Banach, alors $\prod^{\mathrm{b}}_{s\in S} E_s$ est un espace de Banach. En particulier, si E est un espace de Banach et X un ensemble, alors $\mathscr{F}^{\mathrm{b}}(X,E)$ est un espace de Banach.

Définition 8.4.2 Soit $(x_n)_{n\in\mathbb{N}}$ une suite dans un espace vectoriel normé E. Si la suite $\sum_{n\leq N} x_n$ est convergente, on dit que la série $\sum x_n$ est *convergente* et on désigne par $\sum_0^\infty x_n$ la limite. On dit que la série est *absolument convergente* si la série $\sum \|x_n\|$ est convergente dans $\mathbb{R}$.

Proposition 8.4.3 Si une série $\sum x_n$ est absolument convergente dans un espace de Banach E, alors elle est convergente.

Démonstration. On a toujours $\left\|\sum_{N_1}^{N_2} u_n\right\| \leq \sum_{N_1}^{N_2} \|u_n\|$. Il suit que si la suite $\sum_{n\leq N} \|x_n\|$ est de Cauchy, il en va de même de la suite $\sum_{n\leq N} x_n$. ■

Définition 8.4.4 Un *isomorphisme* d'espaces vectoriels normés $u : E \simeq F$ est une application linéaire qui est un homéomorphisme. Deux normes sur un même espace vectoriel sont *équivalentes* si l'identité est un isomorphisme (d'espaces vectoriels normés).

Remarque 1. On voit aisément qu'une application linéaire $u : E \to F$ est un isomorphisme d'espaces vectoriels normés si et seulement si

$$\exists m, M \in \mathbb{R}_{>0}, \forall x \in E, \quad m\|x\| \leq \|u(x)\| \leq M\|x\|.$$

2. On en déduit que deux normes $\|\ \|$ et $\|\ \|'$ sur un espace vectoriel E sont équivalentes si et seulement si

$$\exists m, M \in \mathbb{R}_{>0}, \forall x \in E, \quad m\|x\| \leq \|x\|' \leq M\|x\|.$$

Lemme 8.4.5 Si $(e_1, \ldots, e_n)$ est une base d'un espace vectoriel normé E, alors l'application associée

$$\Phi : K^n \to E, \quad (a_1, \ldots, a_n) \mapsto a_1e_1 + \cdots a_ne_n,$$

est un isomorphisme d'espaces vectoriels normés. En particulier, E est complet.

Démonstration. Rappelons que l'on munit K^n par défaut de la norme max (ce qui n'aura a posteriori aucune importance). On sait que Φ est linéaire et bijective et on voit aisément qu'elle est continue :

$$\|\Phi(a_1, \ldots, a_n)\| \leq M \max_{i=1}^{n} |a_i|,$$

avec $M = \sum_{i=1}^{n} \|e_i\|$. Pour montrer que Φ^{-1} est continue, il suffit de s'assurer que ses composantes ${}^te_i : E \to K$ le sont. Or $H_i := \ker {}^te_i$ est un sous-espace vectoriel de dimension $n-1$. Par récurrence, il est complet et donc fermé dans E. Et on conclut avec le lemme (8.3.6). ■

Théoreme 8.4.6 1. Tout espace vectoriel normé de dimension finie est complet.
2. Toute application linéaire entre espaces vectoriels de dimension finie est continue.

Démonstration. Grâce au lemme, il suffit de considérer des espaces vectoriels de la forme K^n munis de la norme max. ■

Corollaire 8.4.7 Sur un espace vectoriel de dimension finie, toutes les normes sont équivalentes.

Démonstration. ■

Corollaire 8.4.8 Dans un espace vectoriel de dimension finie, tout sous-espace vectoriel est fermé.

Démonstration. ■

8.5 Algèbre de Banach

Soit K un corps valué (pour une valeur absolue non triviale)

Définition 8.5.1 Une *algèbre normée* sur K est une algèbre L munie d'une norme qui satisfait

1. $\forall u,v\in L,\quad \|uv\|\leq\|u\|\|v\|$
2. $\|1_L\|\leq 1$.

Remarque 1. On peut montrer qu'on a en fait $\|1_L\|=1$.
2. La multiplication $L\times L\to L$ est alors une application bilinéaire continue.

Exemple 1. Si E est un espace vectoriel normé, alors $\mathscr{L}(E)$ est une algèbre normée pour la norme
$$\|u\|=\sup_{x\neq 0}\frac{\|u(x)\|}{\|x\|}$$
qui sera dite *subordonnée* à la norme de E.
2. Si E est un espace vectoriel de *dimension finie*, alors $L(E)$ est une algèbre normée pour toute norme subordonnée à une norme sur E.
3. Si X est un ensemble quelconque, alors $\mathscr{F}^b(X,K)$ est une K-algèbre normée (pour la norme sup).
4. $\mathscr{C}([0,1],\mathbb{R})$ est une $\mathbb{R}$-algèbre de Banach pour les normes p avec $p\in[1,\infty]$.
5. Via l'isomorphisme $\mathrm{M}_n(K)\simeq L(K^n)$, on peut munir $\mathrm{M}_n(K)$ d'une norme d'algèbre subordonnée à une norme donnée sur K^n.
6. La norme max sur $\mathrm{M}_n(K)$ est une norme d'algèbre si la valeur absolue est ultramétrique mais *pas* si elle est archimédienne (et $n\geq 2$).

Lemme 8.5.2 Soit L une algèbre *de Banach*. Si $h\in L$ et $\|h\|\leq 1$, alors $1-h\in L^\times$ et $(1-h)^{-1}=\sum_{n=0}^\infty h^n$. De plus, on a
$$\|1-(1-h)^{-1}\|\leq\frac{\|h\|}{1-\|h\|}.$$

Démonstration. La série $\sum h^n$ est absolument convergente et donc convergente. De plus, on a
$$(1-h)\sum_{n=0}^N h^n=1-h^{N+1}\to 1$$
quand $N\to\infty$. Puisque la multiplication est continue, la première assertion est démontrée. De plus, on a
$$1-(1-h)^{-1}=-\sum_{n=1}^\infty h^n=-h\sum_{n=0}^\infty h^n,$$
si bien que
$$\|1-(1-h)^{-1}\|\leq\|h\|\sum_{n=0}^\infty\|h\|^n=\frac{\|h\|}{1-\|h\|}.\quad\blacksquare$$

Proposition 8.5.3 Si L est une algèbre *de Banach*, alors $L^\times\subset L$ est ouvert et l'application $u\mapsto u^{-1}$ est continue sur $L^\times$.

Démonstration. Si $u\in L^\times$, la multiplication par u est continue sur L et son inverse aussi (c'est la multiplication par u^{-1}). C'est donc un homéomorphisme et il suit que
$$V_u:=\{u(1-h),\quad h\in L\text{ et }\|h\|<1\}=u\mathbb{B}^-(1,1)$$

est ouvert dans L. De plus, il résulte du lemme que $V_u \subset L^\times$. Il suit que $L^\times = \cup_{u \in L^\times} V_u$ est aussi ouvert. Toujours grâce au lemme, l'application $u \mapsto u^{-1}$ est continue en $1 \in L^\times$. Pour conclure, il suffit de remarquer que $(u+h)^{-1} = u^{-1}(1+hu^{-1})^{-1} \to u^{-1}$ quand $h \to 0$. ■

Remarque
1. Comme conséquence, on voit que si K est complet, alors $\mathrm{GL}_n(K)$ est ouvert dans $\mathrm{M}_n(K)$ et que l'application $A \mapsto A^{-1}$ est continue.
2. On peut démontrer directement ce dernier résultat en rappelant d'abord que
$$\mathrm{GL}_n(K) = \{A \in \mathrm{M}_n(K), \quad \det(A) \neq 0\}$$
et que det est une application continue car polynomiale. Pour la deuxième partie, on utilise la formule
$$A^{-1} = \frac{1}{\det(A)} {}^t A'$$
ou A' est la comatrice de A dont les coefficients sont aussi polynomiaux.

8.6 Exponentielle

On suppose ici que K est un corps valué **complet archimédien** (et même, pour simplifier, que $K = \mathbb{R}$ ou $\mathbb{C}$).

Lemme 8.6.1 Si L est une algèbre normée et $u \in L$, alors la série $\sum \frac{u^n}{n!}$ est absolument convergente.

Démonstration. Exercice. ■

Remarque
1. C'est manifestement faux sur un corps ultramétrique où l'on a toujours $\|\frac{1}{n!}\| \geq 1$ (si bien que l'exponentielle aura un rayon de convergence inférieur à 1).
2. Il suit du lemme que, lorsque L est complet, la série converge.
3. Cela s'appliquera en particulier lorsque L est de dimension finie, par exemple si $L = L(E)$ avec E un espace vectoriel de dimension finie, ou si $L = \mathrm{M}_n(K)$.

Définition 8.6.2 Si L est une algèbre de Banach et $u \in L$, alors l'*exponentielle* de u est
$$\exp(u) := \sum_{n=0}^{\infty} \frac{u^n}{n!}.$$

Exemple On a
$$\exp\left(\begin{bmatrix} 0 & t \\ -t & 0 \end{bmatrix}\right) = \begin{bmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{bmatrix}.$$

Proposition 8.6.3 Soient L une algèbre de Banach et $u, v \in L$. On a alors
$$uv = vu \Rightarrow \exp(u+v) = \exp(u)\exp(v).$$

Démonstration. On peut utiliser la formule du binôme car u et v commutent et on a donc

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{(u+v)^n}{n!} &= \sum_{n=0}^{\infty}\frac{1}{n!}\sum_{k+l=n}\binom{n}{k}u^k v^l \\ &= \sum_{n=0}^{\infty}\sum_{k+l=n}\frac{u^k}{k!}\frac{v^l}{l!} \\ &= \left(\sum_{k=0}^{\infty}\frac{u^k}{k!}\right)\left(\sum_{l=0}^{\infty}\frac{u^l}{l!}\right)\end{aligned}$$

(puisque les séries sont absolument convergentes). ■

Remarque L'hypothèse est nécessaire comme le montre par exemple le cas de

$$A := \begin{bmatrix} 0 & \pi \\ 0 & 0 \end{bmatrix}, \quad B := \begin{bmatrix} 0 & 0 \\ -\pi & 0 \end{bmatrix} \in \mathbb{M}_2(\mathbb{R}).$$

où $\exp(A+B) \neq \exp(A)\exp(B)$.

Corollaire 8.6.4 Soit L une algèbre de Banach. Si $u \in L$, alors $\exp(u) \in L^\times$.

Démonstration. Faire $v = -u$ dans la proposition. ■

Lemme 8.6.5 Soit L une algèbre de Banach. Si $u, h \in L$, on a

$$\|\exp(u+h) - \exp(u)\| \leq \|h\| \exp(\|u\|)\exp(\|h\|).$$

Démonstration. En développant, on voit aisément que

$$\|(u+h)^n - u^n\| \leq (\|u\| + \|h\|)^n - \|u\|^n.$$

On en déduit que

$$\left\|\sum_{n=0}^{\infty}\frac{(u+h)^n}{n!} - \sum_{n=0}^{\infty}\frac{u^n}{n!}\right\| \leq \sum_{n=0}^{\infty}\frac{(\|u\|+\|h\|)^n}{n!} - \sum_{n=0}^{\infty}\frac{\|u\|^n}{n!}$$

et on est donc ramené au cas ou $L = \mathbb{R}$ (qui est bien sûr laissé en exercice). ■

Proposition 8.6.6 Si L est une algèbre de Banach, alors l'application $\exp : L \to L^\times$ est continue.

Démonstration. Il suffit de faire tendre h vers 0 dans le lemme. ■

Proposition 8.6.7 Soit E un espace vectoriel de dimension finie. Si $u \in \mathrm{L}(E)$, alors

$$\exp({}^t u) = {}^t\exp(u)$$

Démonstration. Exercice. ■

Remarque Soient E un espace vectoriel de dimension finie et $u \in L(E)$. Soient $\mathscr{B}$ une base de E et A la matrice de u dans E. Alors, la matrice de $\exp(u)$ sera $\exp(A)$: en effet, la bijection $M_n(K) \simeq L(E)$ induite par $\mathscr{B}$ est un isomorphisme d'algèbre normées.

Proposition 8.6.8 On dispose d'une application continue

$$\mathrm{M}_n(K) \to \mathrm{GL}_n(K), \quad A \mapsto \exp(A) := \sum_{n=0}^{\infty} \frac{1}{n!} A^n$$

satisfaisant

1. Si $A, B \in \mathrm{M}_n(K)$, alors $\exp(A+B) = \exp(A)\exp(B)$ lorsque $AB = BA$.
2. Si $A \in \mathrm{M}_n(K)$, alors $\exp({}^t A) = {}^t \exp(A)$.
3. Si $A \in \mathrm{M}_n(K)$ et $P \in \mathrm{GL}_n(K)$, alors $\exp(P^{-1}AP) = P^{-1}\exp(A)P$.

Démonstration. Résulte immédiatement de la discussion précédente. ■

Proposition 8.6.9 Soit E un espace vectoriel de dimension finie. Si $u \in \mathrm{L}(E)$ et $E' \subset E$ est un sous-espace stable par u, alors E' est stable par $\exp(u)$. De plus, si $u' \in \mathrm{L}(E'), u'' \in \mathrm{L}(E/E')$ désignent les applications induites par u, alors $\exp(u)$ induit $\exp(u')$ et $\exp(u'')$ sur E' et E'' respectivement.

Démonstration. Il suffit d'écrire les formules (détails en exercice). ■

Remarque En termes de matrices, on voit donc que l'on a

$$\exp\left(\begin{bmatrix} A' & \star \\ 0 & A'' \end{bmatrix}\right) = \begin{bmatrix} \exp(A') & \star \\ 0 & \exp(A'') \end{bmatrix}$$

(attention, ce ne sont pas les mêmes étoiles). Par récurrence, on en déduit de qui se passe pour une matrice triangulaire :

$$A = \begin{bmatrix} a_1 & \star & \cdots & \star \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \cdots & 0 & a_n \end{bmatrix} \quad \Rightarrow \quad \exp(A) = \begin{bmatrix} e^{a_1} & \star & \cdots & \star \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \cdots & 0 & e^{a_n} \end{bmatrix}.$$

Proposition 8.6.10 Si E est un espace vectoriel de dimension finie et $u \in L(E)$, alors

$$\det(\exp(u)) = \exp(\mathrm{tr}(u)).$$

Démonstration. On se ramène à l'énoncé analogue pour une matrice. On peut supposer en fait que $K = \mathbb{C}$, et donc que la matrice est triangulaire, auquel cas c'est immédiat. ■

Proposition 8.6.11 Soient E', E'' deux sous-espaces vectoriels de dimension finie et $E = E' \times E''$. Si $u' \in \mathrm{L}(E'), u'' \in \mathrm{L}(E'')$ et $u = u' \times u''$, alors $\exp(u) = \exp(u') \times \exp(u'')$.

Démonstration. Il suffit encore d'écrire les formules (détails en exercice). ■

Remarque 1. On aura donc toujours

$$\exp\left(\begin{bmatrix} A' & 0 \\ 0 & A'' \end{bmatrix}\right) = \begin{bmatrix} \exp(A') & 0 \\ 0 & \exp(A'') \end{bmatrix}.$$

2. Pour une matrice diagonale
$$A=\begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_n \end{bmatrix} \quad \Rightarrow \quad \exp(A)=\begin{bmatrix} e^{a_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & e^{a_n} \end{bmatrix}.$$
3. En général, le calcul de l'exponentielle peut toujours se ramener à des blocs de Jordan et on a
$$\exp(aI+N)=e^a\exp(N)$$
avec
$$\exp(N)=I+N+\frac{1}{2}N^2+\cdots+\frac{1}{n!}N^n$$
si N est nilpotent.

8.7 Fonction vectorielle

On désigne par K un corps valué pour une valeur absolue non triviale.

Remarque Soient X,Y deux espaces métriques et $x_0 \in X$. On dit que $f : X\setminus\{x_0\} \to Y$ a pour *limite* $\ell \in Y$ en x_0 si f se prolonge de manière unique en une application $\widetilde{f}$ qui est continue en x_0 et que $\ell = \widetilde{f}(x_0)$. On écrit alors
$$\ell = \lim_{x\to x_0} f(x).$$
Notons que $\widetilde{f}$ est unique si et seulement si x n'est pas *isolé* dans X (*isolé* signifie qu'il existe une boule ouverte qui ne contient que x).

Définition 8.7.1 Soient E un espace vectoriel normé et $I \subset K$. Une application $\theta : I \to E$ est *dérivable* en $t_0 \in I$ (non isolé) si
$$\theta'(t_0) := \lim_{t\to t_0} \frac{\theta(t)-\theta(t_0)}{t-t_0}$$
existe dans E. On dit alors que $\theta'(t_0)$ est le *vecteur dérivé* de θ en t_0.

Remarque 1. Alternativement, cela signifie que
$$\theta(t)=\theta(t_0)+\theta'(t_0)(t-t_0)+\varepsilon(t)(t-t_0)$$
avec $\varepsilon(t)\to 0$ quand $t\to t_0$.
2. Si θ est dérivable en tout $t_0 \in I$, alors l'application $\theta' : I \to E$ est la *dérivée* de θ. On dit que θ est *de classe* $\mathscr{C}^k$ si θ est k fois dérivable et que $\theta^{(k)}$ est continue (pour $k \in \mathbb{N}\cup\{\infty\}$). Tous les résultats qui suivent ont des variantes dans ce contexte que nous n'expliciterons pas.
3. Une application $I \to E_1 \times E_2$ est dérivable en t_0 si et seulement si ses composantes le sont. En particulier, une application $I \to K^n$ est dérivable si et seulement si toutes ses composantes le sont.
4. Les fonctions dérivables en $t_0 \in I$ forment un sous espace vectoriel de $\mathscr{F}(I,E)$ et l'application $\theta \mapsto \theta'(t_0)$ est linéaire.
5. Si $u : E \to F$ est linéaire continue et θ est dérivable en t_0, alors $u\circ\theta : I \to F$ est aussi dérivable en t_0 et $(u\circ\theta')(t_0) = u\circ\theta'(t_0)$.

Proposition 8.7.2 Soient L une algèbre normée et $I \subset K$. Si $\theta_1, \theta_2 : I \to L$ sont dérivables en $t_0 \in I$, alors $\theta_1\theta_2$ aussi et on a

$$(\theta_1\theta_2)'(t_0) = \theta_1'(t_0)\theta_2(t_0) + \theta_1(t_0)\theta_2'(t_0).$$

Démonstration. C'est classique. On écrit

$$\theta_1(t) = \theta_1(t_0) + \theta_1'(t_0)(t - t_0) + \varepsilon_1(t)(t - t_0)$$

avec $\varepsilon_1(t) \to 0$ quand $t \to t_0$. Et on fait de même pour θ_2. Puis on effectue le produit :

$$(\theta_1\theta_2)(t) = (\theta_1\theta_2)(t_0) + (\theta_1'(t_0)\theta_2(t_0) + \theta_1(t_0)\theta_2'(t_0))(t - t_0)$$
$$+(\theta_1(t_0)\varepsilon_2(t) + \varepsilon_1(t)\theta_2(t_0))(t - t_0) + \star(t - t_0)^2. \quad \blacksquare$$

Proposition 8.7.3 (K complet archimédien) Si L est une algèbre de Banach et $u \in L$, alors l'application

$$K \to L, \quad t \mapsto \exp(tu)$$

est $\mathscr{C}^\infty$ et a pour dérivée $t \mapsto u \exp tu$.

Démonstration. Il suffit bien sûr de montrer la dernière assertion. En développant de chaque coté, on a la majoration

$$\|\exp(tu) - 1 - tu\| \leq \exp(|t|\|u\|) - 1 - |t|\|u\|.$$

et on en déduit que

$$\|\frac{\exp(tu) - 1}{t} - u\| \leq \frac{\exp(|t|\|u\|) - 1}{|t|} - \|u\|.$$

Il suit donc immédiatement du cas $L = \mathbb{R}$ que l'application $t \mapsto \exp(tu)$ est dérivable en 0 et que sa dérivée vaut u. Pour le cas général, il suffit de rappeler que

$$\exp(tu) = \exp(t_0u)\exp((t - t_0)u). \quad \blacksquare$$

Corollaire 8.7.4 (K complet archimédien) Soient E un espace vectoriel de dimension finie, $u \in L(E)$ et $\theta_0 \in E$. Si

$$\theta : K \to E, \quad t \mapsto \exp(tu)(\theta_0),$$

alors on a

$$\theta' = u \circ \theta \quad \text{et} \quad \theta(0) = \theta_0. \tag{8.1}$$

Démonstration. Il suffit de composer avec l'application $L(E) \to E$ d'évaluation en θ_0. $\blacksquare$

Remarque
1. On exprime encore ce résultat en disant que l'*équation différentielle* (8.1) a pour solution θ définie sur K tout entier.
2. On peut demander la condition moins restrictive $\theta(t_0) = \theta_0$ et il faut alors poser $\theta(t) = \exp((t - t_0)u)(\theta_0)$.
3. En termes de matrices, ce résultat nous dit que le système différentiel

   $$X' = AX \quad \text{et} \quad X(0) = X_0$$

   a pour solution $X = \exp(tA)X_0$.

Exemple On veut résoudre l'équation différentielle

$$x'' = -x \quad \text{avec} \quad x(0) = x'(0) = 1,$$

ou, ce qui revient au même, le système différentiel

$$\begin{cases} x' = y \\ y' = -x \end{cases} \quad \text{avec} \quad \begin{cases} x(0) = 1 \\ y(0) = 1 \end{cases}.$$

On le réécrit sous la forme $X' = AX$ et $X(0) = X_0$ avec

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad X = \begin{bmatrix} x \\ y \end{bmatrix}, \quad X' = \begin{bmatrix} x' \\ y' \end{bmatrix} \quad \text{et} \quad X_0 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

On calcule

$$\exp(tA) = \begin{bmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{bmatrix},$$

et on a donc

$$X = \exp(tA)X_0 = \begin{bmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} \cos t + \sin t \\ \cos t - \sin t \end{bmatrix}$$

si bien que $x = \cos t + \sin t$ et $y = \cos t - \sin t$.

8.8 Exercices

Exercice 8.1 1. Montrer que $|a| := \max(a, -a)$ définit une valeur absolue archimédienne sur $\mathbb{Q}$ ou $\mathbb{R}$.
2. Montrer que $|a+ib| := \sqrt{a^2+b^2}$ définit une valeur absolue absolue archimédienne sur $\mathbb{C}$.
3. Montrer que $|r| := \frac{1}{2^v}$ si $r = 2^v \times \frac{\text{impair}}{\text{impair}}$ définit une valeur absolue ultramétrique sur $\mathbb{Q}$ (on pose aussi $|0| = 0$).
4. Montrer que $|R| := e^{-v}$ si $R(T) = \dfrac{T^v P(T)}{Q(T)}$ avec $P(0) \neq 0$ et $Q(0) \neq 0$, définit une valeur absolue ultramétrique sur $\mathbb{Q}(T)$ (on pose aussi $|0| = 0$).

Exercice 8.2 Montrer que si K est un corps valué, alors l'application $a \mapsto a^{-1}$ est continue sur $K^\times$.

Exercice 8.3 1. Montrer que si $E_1, \dots, E_n$ sont des espaces vectoriels normés, alors $\|(x_1, \dots, x_n)\|_\infty := \max_{i=1}^n \|x_i\|$ définit une norme sur $E_1 \times \cdots \times E_n$.
2. Montrer que $\|(x_i)_{i\in\mathbb{N}}\|_\infty := \sup_{i\in\mathbb{N}} \|x_i\|$ définit une norme sur l'espace $l_\infty(K)$ des suites bornées.
3. Montrer que $\|f\|_\infty := \sup_{[0,1]} |f(t)|$ définit une norme sur $\mathscr{C}([0,1], \mathbb{R})$.
4. Montrer que si E est est un espace vectoriel normé et X un ensemble, alors

$$F := \{f : X \to E, \exists M \in \mathbb{R}, \forall x \in S, \|f(x)\| \leq M\}$$

est un sous-espace vectoriel et que $\|f\|_\infty := \sup_{x\in S} \|f(x)\|$ définit une norme sur F.

Exercice 8.4 1. On se donne $p, q \in \mathbb{R}_{>0}$ avec $\frac{1}{p} + \frac{1}{q} = 1$.
(a) Montrer que $AB \leq \frac{1}{p}A^p + \frac{1}{q}B^q$ dans $\mathbb{R}_{\geq 0}$. On utilisera le fait que le logarithme est une fonction concave et croissante.
(b) Montrer l'*inégalité de Hölder*

$$\sum_{i=1}^n u_i v_i \leq (\sum_{i=1}^n u_i^p)^{\frac{1}{p}} (\sum_{i=1}^n v_i^q)^{\frac{1}{q}}$$

dans $\mathbb{R}_{\geq 0}$. On appliquera l'inégalité précédente avec $A := u_i/\alpha$ où $\alpha := (\sum_{i=1}^n u_i^p)^{\frac{1}{p}}$ et $B = v_i/\beta$ où $\beta := (\sum_{i=1}^n v_i^q)^{\frac{1}{q}}$.
2. On se donne $p \in \mathbb{R}_{>0}$.
(a) Montrer l'*inégalité de Minkowski* :

$$\left(\sum_{i=1}^n |a_i + b_i|^p\right)^{\frac{1}{p}} \leq (\sum_{i=1}^n |a_i|^p)^{\frac{1}{p}} + (\sum_{i=1}^n |b_i|^p)^{\frac{1}{p}}.$$

On fera d'abord la majoration

$$\sum_{i=1}^n |a_i + b_i|^p \leq \sum_{i=1}^n |a_i||a_i + b_i|^{p-1} + \sum_{i=1}^n |b_i||a_i + b_i|^{p-1}$$

et on appliquera l'inégalité de Hölder aux deux termes.
(b) Montrer enfin que $\|(a_1, \dots, a_n)\|_p := (\sum_{i=1}^n |a_i|^p)^{\frac{1}{p}}$ définit une norme sur K^n.
3. Procéder de même avec $\|f\|_p := \left(\int_0^1 |f(t)|^p \mathrm{d}t\right)^{\frac{1}{p}}$ pour $f \in \mathscr{C}([0,1], \mathbb{R})$.

Exercice 8.5 1. Montrer que $\mathbb{R}$ et $\mathbb{C}$ sont des corps archimédiens complets, mais pas $\mathbb{Q}$.
2. Montrer que $|\sum_{i=v}^{\infty} a_i T^i| := \frac{1}{e^v}$ si $a_v \neq 0$ fait de $\mathbb{Q}((T))$ un corps valué complet.
3. Montrer que $l_\infty(K)$ est un espace de Banach pour $\|-\|_\infty$ quand K est complet.
4. Montrer que $\mathscr{C}([0,1],\mathbb{R})$ est complet pour pour $\|-\|_\infty$ mais pas pour pour $\|-\|_1$.

Exercice 8.6 Dire dans chaque cas s'il s'agit d'une norme d'algèbre sur $\mathrm{M}_n(K)$:
1. $\|A\| := \max_{i,j} |a_{ij}|$ (on traitera séparément le cas archimédien et le cas ultramétrique).
2. $\|A\| := \max_j \sum_i |a_{ij}|$ (on pourra munir K^n de $\|-\|_1$).
3. $\|A\| := \max_i \sum_j |a_{ij}|$ (on pourra munir K^n de $\|-\|_\infty$).
4. Calculer dans chacun des cas la norme de $A := \begin{bmatrix} 2 & 1 & 1 \\ 2 & 3 & 2 \\ 1 & 1 & 2 \end{bmatrix}$.

Exercice 8.7 On fixe une norme sur $\mathbb{C}^n$ (par exemple $\|-\|_\infty$). Soient $A \in \mathrm{GL}_n(\mathbb{C})$ et $B \in \mathbb{C}^n \setminus 0$. On pose $c(A) = \|A\| \cdot \|A^{-1}\|$ (*conditionnement*). Montrer que si $AX = B$, alors
1. si $A(X+\delta(X)) = B + \delta(B)$, on a $\frac{\|\delta(X)\|}{\|X\|} \leq c(A)\frac{\|\delta(B)\|}{\|B\|}$.
2. si $(A+\delta(A))(X+\delta(X)) = B$, on a $\frac{\|\delta(X)\|}{\|X+\delta(X)\|} \leq c(A)\frac{\|\delta(A)\|}{\|A\|}$.
3. Application numérique avec $A = \begin{bmatrix} 1 & 2 \\ 1{,}001 & 2 \end{bmatrix}$, $B = \begin{bmatrix} 3 \\ 3{,}001 \end{bmatrix}$, $X + \delta(X) = \begin{bmatrix} 3 \\ 0 \end{bmatrix}$.
Calculer $B + \delta(B)$. En déduire $\delta(B)$ puis $\|\delta(B)\|/\|B\|$. Résoudre $AX = B$ puis calculer $\|\delta(X)\|/\|X\|$. Calculer enfin $c(A)$ et vérifier la première égalité.

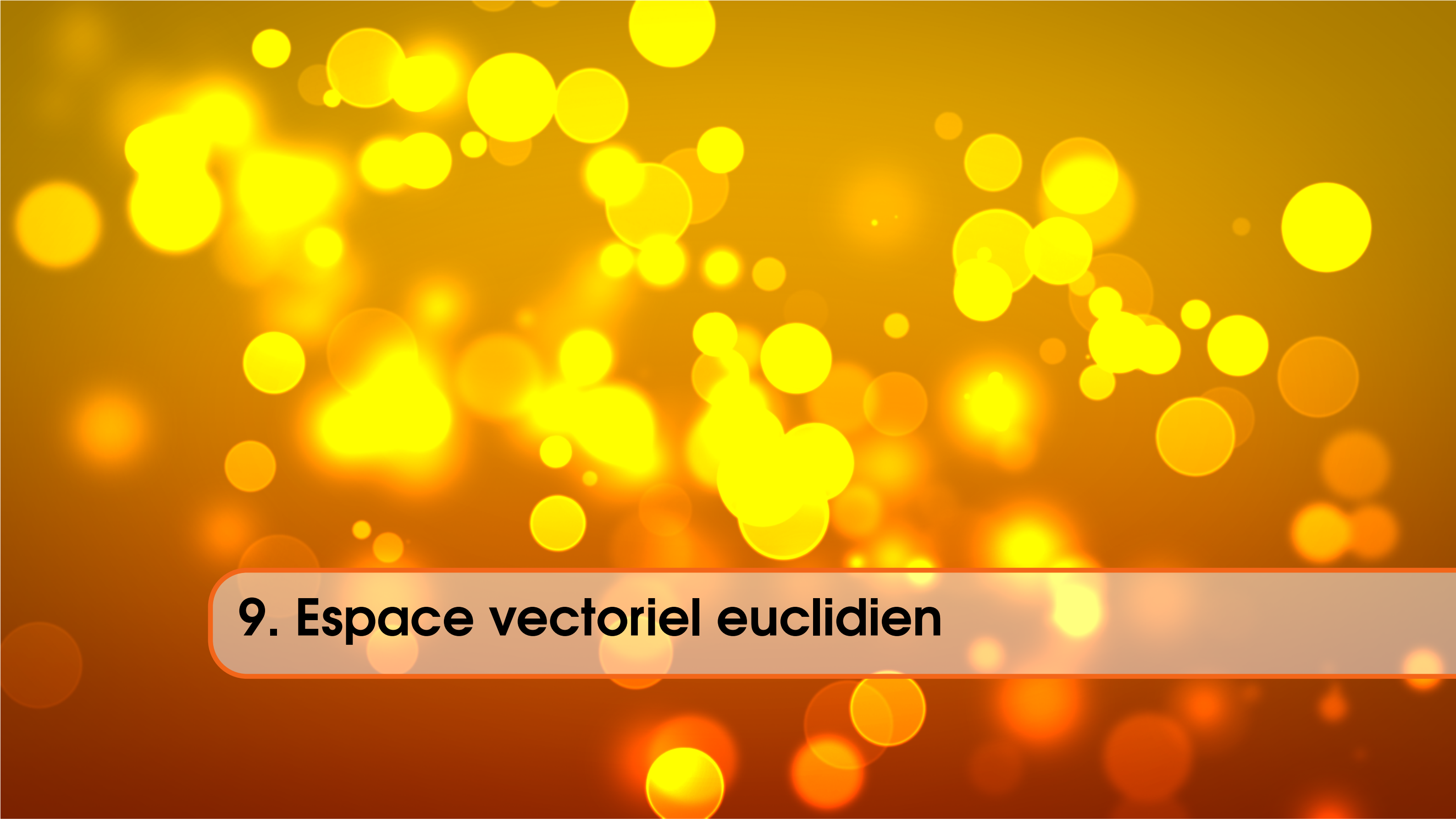
Exercice 8.8 On pose $A := \begin{bmatrix} 0 & \pi \\ 0 & 0 \end{bmatrix}$, $B := \begin{bmatrix} 0 & 0 \\ -\pi & 0 \end{bmatrix}$ et $C := A + B$.
1. Calculer les matrices $\exp(A)$ et $\exp(B)$ puis faire leur produit.
2. Diagonaliser C sur $\mathbb{C}$. En déduire $\exp(C)$.
3. A-t-on $\exp(C) = \exp(A)\exp(B)$? Que peux-t-on en déduire sur A et B ?

Exercice 8.9 On pose $A := \begin{bmatrix} 0 & t \\ -t & 0 \end{bmatrix}$. Calculer $\exp(A)$ en montrant par récurrence sur $k \in \mathbb{N}$ que

$$A^{2k} = \begin{bmatrix} (-1)^k t^{2k} & 0 \\ 0 & (-1)^k t^{2k} \end{bmatrix} \quad \text{et} \quad A^{2k+1} = \begin{bmatrix} 0 & (-1)^k t^{2k+1} \\ (-1)^{k+1} t^{2k+1} & 0 \end{bmatrix}.$$

Exercice 8.10 Calculer $\exp\left(\begin{bmatrix} 21 & 17 & 6 \\ -5 & -1 & -6 \\ 4 & 4 & 16 \end{bmatrix}\right)$.

Exercice 8.11 On pose $M := \begin{bmatrix} 2 & -1 & 1 \\ 0 & 3 & -1 \\ 2 & 1 & 3 \end{bmatrix}$.
1. Calculer $\exp(tM)$.
2. En déduire les solutions du système différentiel $\begin{cases} x' = 2x - y + z \\ y' = 3y - z \\ z' = 2x + y + 3z \end{cases}$.



9. Espace vectoriel euclidien

9.1 Produit scalaire

Définition 9.1.1 Soit E un espace vectoriel sur $\mathbb{R}$. Un *produit scalaire* sur E est une forme bilinéaire symétrique définie positive

$$E \times E \to \mathbb{R}, \quad (x,y) \mapsto \langle x,y \rangle.$$

Remarque

1. Cela signifie donc que
   (a) $\forall x,y \in E, \quad \langle x,y \rangle = \langle y,x \rangle$,
   (b) $\forall x,x',y \in E, \quad \langle x+x',y \rangle = \langle x,y \rangle + \langle x',y \rangle$,
   (c) $\forall x,y \in E, \forall a \in K, \quad \langle ax,y \rangle = a\langle x,y \rangle$,
   (d) $\forall x \in E \setminus \{0\}, \quad \langle x,x \rangle > 0$.
2. Notons que si $F \subset E$ est un sous-espace vectoriel, alors la restriction $\langle\ ,\ \rangle_{|F}$ du produit scalaire de E est encore un produit scalaire sur F.

Exemple

1. Tout sous-espace vectoriel $E \subset \mathbb{R}^n$ avec
$$\langle (x_1,\ldots,x_n),(y_1,\ldots,y_n) \rangle = x_1y_1 + \cdots + x_ny_n.$$
2. Tout sous-espace vectoriel $E \subset \mathscr{C}([0,1],\mathbb{R})$ avec
$$\langle f,g \rangle = \int_0^1 f(t)g(t)\mathrm{d}t.$$

Proposition 9.1.2 — Cauchy-Schwarz. Si $\langle\ ,\ \rangle$ est un produit scalaire sur un espace vectoriel E, alors l'application

$$E \to \mathbb{R}_{\geq 0}, \quad x \mapsto \|x\| := \sqrt{\langle x,x \rangle}$$

est une norme sur E et on a

$$\forall x,y \in E, \quad |\langle x,y \rangle| \leq \|x\|\|y\|,$$

avec égalité si et seulement si x et y sont liés.

Démonstration. C'est bien une norme :

1. si $x \in E \setminus \{0\}$, alors $\|x\|^2 = \langle x, x\rangle > 0$ et en particulier $\|x\| \neq 0$,
2. si $x \in E$ et $a \in \mathbb{R}$, on a $\|ax\|^2 = \langle ax, ax\rangle = a^2\|x\|^2$ et donc $\|ax\| = |a|\|x\|$,
3. si $x, y \in E$, en utilisant l'inégalité de Cauchy-Schwarz que nous allons démontrer ensuite, on voit que
$$\|x+y\|^2 = \|x\|^2 + 2\langle x, y\rangle + \|y\|^2 \leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2.$$
et on a donc bien $\|x+y\| \leq \|x\| + \|y\|$.

Dans le reste de la démonstration, nous fixons $x, y \in E$. Si $x = 0$, alors x et y sont liés et on a $|\langle x, y\rangle| = 0 = \|x\|\|y\|$. Sinon, on considère le polynôme du second degré :

$$P := T^2\|x\|^2 + 2T\langle x, y\rangle + \|y\|^2 \in \mathbb{R}[T].$$

Si $a \in \mathbb{R}$, on a

$$\|ax+y\|^2 = \langle ax+y, ax+y\rangle = a^2\|x\|^2 + 2a\langle x, y\rangle + \|y\|^2 = P(a),$$

si bien que $P(a) \geq 0$. Ceci étant vrai pout tout $a \in \mathbb{R}$, le discriminant de P est nécessairement négatif :

$$4\langle x, y\rangle^2 - 4\|x\|^2\|y\|^2 \leq 0.$$

En d'autre termes, on a $\langle x, y\rangle^2 \leq \|x\|^2\|y\|^2$ et on sait que deux nombres positifs sont dans le même ordre que leurs carrés. L'inégalité de Cauchy-Schwarz est donc bien satisfaite. De plus, on a égalité si et seulement si le discriminant est nul (ou positif, ce qui est équivalent ici), ce qui signifie que P a une racine $a \in \mathbb{R}$. C'est équivalent à dire que $\|ax+y\|^2 = 0$, soit encore $ax+y = 0$, ce qui signifie que x et y sont liés puisque $x \neq 0$. ■

Définition 9.1.3 Soient E un espace vectoriel muni d'un produit scalaire et $x, y \in E$. L'*angle (non orienté)* entre x et y est

$$\widehat{(x,y)} := \arccos\left(\frac{\langle x, y\rangle}{\|x\|\|y\|}\right).$$

Remarque

1. Cette définition a un sens grâce à l'inégalité de Cauchy-Schwarz qui nous dit que
$$-1 \leq \frac{\langle x, y\rangle}{\|x\|\|y\|} \leq 1.$$
2. On peut réécrire la définition sous la forme
$$\langle x, y\rangle = \|x\|\|y\|\cos\widehat{(x,y)}.$$
3. Le cas d'égalité dans la proposition nous dit que x et y sont liés si et seulement si l'angle est *nul* : $\widehat{(x,y)} = 0$ ou *plat* : $\widehat{(x,y)} = \pi$. Et on voit aussi que x et y sont orthogonaux si et seulement si l'angle est *droit* : $\widehat{(x,y)} = \pi/2$. On n'en sera pas surpris.

9.2 Espace euclidien

Définition 9.2.1 Un *espace vectoriel euclidien* est un espace vectoriel réel *de dimension finie* E muni d'un produit scalaire $\langle\ ,\ \rangle$. La norme associée est dite *euclidienne*.

Exemple Tout sous-espace vectoriel $E \subset \mathbb{R}^n$ avec le produit scalaire usuel

$$\langle (x_1,\ldots,x_n),(y_1,\ldots,y_n)\rangle = x_1y_1+\cdots+x_ny_n.$$

Remarque

1. La forme quadratique associée au produit scalaire est donc $x \mapsto \|x\|^2$. On voit en particulier qu'un $u \in L(E)$ est une isométrie pour la distance associée à $\|\ \|$ si et seulement si c'est un opérateur orthogonal relativement à la forme quadratique. Ces deux termes sont donc interchangeables.
2. On a une bijection entre produits scalaires et normes euclidiennes sur E donnée par
$$\|x\| = \sqrt{\langle x,x\rangle} \quad \text{et} \quad \langle x,y\rangle = \frac{1}{2}(\|x+y\|^2-\|x\|^2-\|y\|^2).$$
3. On peut montrer qu'une norme est euclidienne si et seulement si elle satisfait la *règle du parallélogramme*
$$\|x+y\|^2+\|x-y\|^2 = 2\left(\|x\|^2+\|y\|^2\right),$$
(ou de manière équivalente, la *règle de la médiane*).
4. Si on ne fait plus l'hypothèse que E est de dimension finie, il faudrait dire *préeuclidien* et réserver le mot *euclidien* au cas complet.

Théorème 9.2.2 Soit E un espace vectoriel euclidien. Alors, l'application $F \mapsto F^\perp$ induit une bijection de l'ensemble des sous-espaces vectoriels de E sur lui même, qui est est symétrique ($F^{\perp\perp} = F$), qui renverse l'inclusion ($F \subset G \Rightarrow G^\perp \subset F^\perp$) et échange intersection et produit ($(F+G)^\perp = F^\perp \cap G^\perp$ et $(F\cap G)^\perp = F^\perp + G^\perp$). De plus, on a toujours $E \simeq F \oplus F^\perp$.

Démonstration. À part la dernière, toutes les assertions ont déjà été vues dans le théorème 9.4.7. Et la dernière assertion résulte du corollaire de ce même théorème : en effet, la restriction du produit scalaire à F est toujours un produit scalaire qui est donc non dégénéré. ■

Définition 9.2.3 Soient E un espace vectoriel euclidien et $F \subset E$ un sous-espace vectoriel. Alors, la *projection orthogonale* sur F est la première projection associée à la décomposition $E \simeq F \oplus F^\perp$.

Lemme 9.2.4 Si F est un sous-espace vectoriel d'un espace vectoriel euclidien E, alors la projection orthogonale sur F est l'unique application telle que

$$\forall x \in E, \quad \begin{cases} p(x) \in F \\ \forall y \in F, \quad \langle p(x),y\rangle = \langle x,y\rangle. \end{cases}$$

Démonstration. Si $x \in E$, on peut écrire de manière unique $x = p(x)+(x-p(x))$ avec $p(x) \in F$ et $x-p(x) \in F^\perp$. Et la seconde condition, s'écrit aussi

$$\forall y \in F, \quad \langle x-p(x),y\rangle = 0,$$

que l'on peut réécrire comme dans l'énoncé. ■

Proposition 9.2.5 Si F est un sous-espace vectoriel d'un espace vectoriel euclidien E et $(y_1,\ldots,y_r)$ une base *orthogonale* de F, alors la projection orthogonale sur F est donnée par

$$\forall x \in E, \quad p(x) = \frac{\langle x,y_1\rangle}{\|y_1\|^2}y_1 + \cdots + \frac{\langle x,y_r\rangle}{\|y_r\|^2}y_r.$$

Démonstration. Comme $p(x) \in F$, on peut écrire $p(x) = a_1y_1 + \cdots + a_ry_r$ et on aura donc pour tout $i = 1,\ldots,r$,

$$\langle x,y_i\rangle = a_1\langle y_1,y_i\rangle + \cdots + a_r\langle y_r,y_i\rangle = a_i\|y_i\|^2. \quad \blacksquare$$

Exemple Si on muni $\mathbb{R}^2$ de sa structure euclidienne canonique, alors la projection orthogonale sur la diagonale est donnée par

$$p(x,y) = \frac{\langle (x,y),(1,1)\rangle}{\|(1,1)\|^2}(1,1) = (\frac{x+y}{2},\frac{x+y}{2})$$

(faire un dessin).

Remarque 1. Dans le cas d'une base orthonormée, on aura

$$p(x) = \langle x,y_1\rangle y_1 + \cdots + \langle x,y_r\rangle y_r.$$

2. Dans le cas ou $F = E$, c'est à dire où $(y_1,\ldots,y_n)$ est une base orthogonale de E, on voit que

$$x = \frac{\langle x,y_1\rangle}{\|y_1\|^2}y_1 + \cdots + \frac{\langle x,y_r\rangle}{\|y_n\|^2}y_n.$$

3. En général, on peut aussi calculer

$$\|p(x)\|^2 = \frac{\langle x,y_1\rangle^2}{\|y_1\|^2} + \cdots + \frac{\langle x,y_r\rangle^2}{\|y_r\|^2}.$$

Proposition 9.2.6 Soit E un espace vectoriel euclidien. Alors,

1. E possède une base orthonormée $\mathscr{B}$,
2. Si $u \in L(E)$, les conditions suivantes sont équivalentes :
   (a) u est orthogonal (c'est à dire une isométrie),
   (b) si $\mathscr{B}$ est une base orthonormée de E, alors $u(\mathscr{B})$ est aussi une base orthonormée,
   (c) Il existe une base orthonormée $\mathscr{B}$ de E telle que $u(\mathscr{B})$ soit aussi une base orthonormée.

Démonstration. Si E est de dimension n, la signature du produit scalaire est $(n,0)$ et il suit qu'il existe une base dans laquelle la matrice est I. Par définition, c'est une base orthonormée. Si u est orthogonal, alors u commute avec le produit scalaire. On voit donc que si $\langle e_i,e_j\rangle = \delta_{i,j}$, on aura aussi $\langle u(e_i),u(e_j)\rangle = \delta_{i,j}$. Réciproquement, supposons que $\mathscr{B} := (e_1,\ldots,e_n)$ et $u(\mathscr{B}) := (u(e_1),\ldots,u(e_n))$ soient des bases orthonormées et soit $x = \sum a_ie_i \in E$. On aura alors $u(x) = \sum a_iu(e_i)$ si bien que

$$\|x\|^2 = \sum a_i^2 = \|(u(x)\|^2. \quad \blacksquare$$

Corollaire 9.2.7 Soit $A \in \mathrm{M}_n(\mathbb{R})$. Alors, $A \in \mathrm{O}(n)$ si et seulement si ses colonnes forment une base orthonormée pour la structure euclidienne usuelle.

Démonstration. $\blacksquare$

Théoreme 9.2.8 — Gram-Schmidt. Soit E un espace vectoriel euclidien. Si $x_1,\dots,x_r$ sont linéairement indépendants dans E, alors il existe $y_1,\dots,y_r \in E$ uniques tels que, pour tout $i=1,\dots,r$, $(y_1,\dots,y_i)$ est une base orthonormée de $F_i := \mathrm{Vect}(x_1,\dots,x_i)$ et $\langle x_i,y_i\rangle > 0$.

Démonstration. On peut bien sûr supposer que $E=F_r$. En procédant par récurrence sur r, on voit qu'il existe $y_1,\dots,y_{r-1}$ uniques tels que, pour $i<r$, $(y_1,\dots,y_i)$ soit une base orthonormée de F_i et que $\langle x_i,y_i\rangle > 0$. Et il existe alors un unique $y_r \in F_{r-1}^{\perp}$, qui est une droite, tel que $\|y_r\|=1$ et $\langle x_r,y_r\rangle > 0$. ■

Remarque 1. En pratique, on utilise la formule de la projection, et on construit donc par récurrence
$$y'_i = x_i - p_{i-1}(x_i) = x_i - \frac{\langle x_i,y'_1\rangle}{\|y'_1\|^2}y'_1 - \cdots - \frac{\langle x_i,y'_{i-1}\rangle}{\|y'_{i-1}\|^2}y'_{i-1}.$$
pour obtenir une base orthogonale et on pose ensuite $y_i = \dfrac{y'_i}{\|y'_i\|}$.

2. Alternativement, on peut construire les y_i au fur et à mesure et utiliser la formule d'apparence plus simple
$$y'_i = x_i - \langle x_i,y_1\rangle y_1 - \cdots - \langle x_i,y_{i-1}\rangle y_{i-1}.$$
Attention cependant que cette méthode introduit des racines carrées pendant les calculs alors que la méthode précédente repousse leur apparition à la fin.

3. On peut voir au passage que
$$\begin{aligned}\|y'_i\|^2 &= \|x_i\|^2 - \frac{\langle x_i,y'_1\rangle^2}{\|y'_1\|^2} - \cdots - \frac{\langle x_i,y'_{i-1}\rangle^2}{\|y'_{i-1}\|^2}\\ &= \|x_i\|^2 - \langle x_i,y_1\rangle^2 - \cdots - \langle x_i,y_{i-1}\rangle^2.\end{aligned}$$

Exemple 1. On cherche une base orthogonale du plan d'équation $x+y+z=0$ dans $\mathbb{R}^3$ (muni de sa structure euclidienne usuelle). On voit aisément que $u_1 := (1,-1,0)$ et $u_2 := (1,0,-1)$ forment une base du plan et on pose alors
$$v'_1 := u_1 = (1,-1,0)$$
et
$$v'_2 := u_2 - \frac{\langle u_2,v'_1\rangle}{\|v'_1\|^2}v'_1 = (1,0,-1) - \frac{1}{2}(1,-1,0) = \left(\frac{1}{2},\frac{1}{2},-1\right).$$
On en déduit que
$$v_1 := \frac{v'_1}{\|v'_1\|} = \frac{1}{\sqrt{2}}(1,-1,0) = \left(\frac{\sqrt{2}}{2},-\frac{\sqrt{2}}{2},0\right)$$
et
$$v_2 := \frac{v'_2}{\|v'_2\|} = \frac{1}{\sqrt{\frac{3}{2}}}\left(\frac{1}{2},\frac{1}{2},-1\right) = \left(\frac{\sqrt{6}}{6},\frac{\sqrt{6}}{6},-\frac{\sqrt{6}}{3}\right).$$

2. On munit $\mathbb{R}[X]_{\leq 2}$ de
$$\langle P,Q\rangle = \int_{-1}^{1} P(t)Q(t)\mathrm{d}t$$

et on applique le procédé d'orthogonalisation de Gram-Schmidt à la base canonique. On part donc de $P_0 = 1, P_1 = X, P_2 = X^2$ pour construire Q_0, Q_1, Q_2. On commence par poser $Q'_0 := P_0 = 1$ puis on calcule

$$\|Q'_0\|^2 = \int_{-1}^{1} \mathrm{d}t = [t]_{-1}^{1} = 2$$

si bien que

$$Q_0 := \frac{Q'_0}{\|Q'_0\|} = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}.$$

On pose ensuite

$$Q'_1 := P_1 - \langle P_1, Q_0\rangle Q_0.$$

et on calcule

$$\langle P_1, Q_0\rangle = \int_{-1}^{1} \frac{\sqrt{2}}{2} t \,\mathrm{d}t = 0$$

(fonction impaire) si bien que $Q'_1 := P_1 = X$. On calcule alors

$$\|Q'_1\|^2 = \|P_1\|^2 - \langle P_1, Q_0\rangle^2 = \int_{-1}^{1} t^2 \mathrm{d}t = \left[\frac{t^3}{3}\right]_{-1}^{1} = \frac{2}{3}$$

si bien que

$$Q_1 := \frac{Q'_1}{\|Q'_1\|} = \frac{X}{\sqrt{\frac{2}{3}}} = \frac{\sqrt{6}}{2} X.$$

Enfin, on pose

$$Q'_2 := P_2 - \langle P_2, Q_0\rangle Q_0 - \langle P_2, Q_1\rangle Q_1.$$

On calcule alors

$$\langle P_2, Q_0\rangle = \int_{-1}^{1} \frac{\sqrt{2}}{2} t^2 \mathrm{d}t = \frac{\sqrt{2}}{2}\left[\frac{t^3}{3}\right]_{-1}^{1} = \frac{\sqrt{2}}{3}$$

ainsi que

$$\langle P_2, Q_1\rangle = \int_{-1}^{1} \frac{\sqrt{6}}{2} t^3 \mathrm{d}t = 0.$$

On a donc

$$Q'_2 := X^2 - \frac{\sqrt{2}}{3}\frac{\sqrt{2}}{2} = X^2 - \frac{1}{3}$$

et on veut connaître

$$\|Q'_2\|^2 = \|P_2\|^2 - \langle P_2, Q_0\rangle^2 - \langle P_2, Q_1\rangle^2.$$

On calcule

$$\|P_2\|^2 = \int_{-1}^{1} t^4 \mathrm{d}t = \left[\frac{t^5}{5}\right]_{-1}^{1} = \frac{2}{5}$$

si bien que

$$\|Q'_2\|^2 = \frac{2}{5} - \left(\frac{\sqrt{2}}{3}\right)^2 = \frac{8}{45}$$

et finalement

$$Q_2 := \frac{Q'_2}{\|Q'_2\|} = \frac{X^2 - \frac{1}{3}}{\sqrt{\frac{8}{45}}} = 3\frac{\sqrt{10}}{4} X^2 - \frac{\sqrt{10}}{4}.$$

9.3 Réduction des matrices symétriques

On fixe un espace vectoriel euclidien E.

Remarque Il est peut-être utile de rappeler que nous avons défini le *transposé* (aussi appelé l'*adjoint*) u^* d'un opérateur u par la formule

$$\forall x, y \in E, \quad \langle u(x), y \rangle = \langle x, u^*(y) \rangle.$$

Rappelons aussi que u est dit *orthogonal* si $u^* \circ u = \mathrm{Id}_E$. Cela signifie que u est bijectif et que $u^* = u^{-1}$, et s'exprime aussi par la condition

$$\forall x, y \in E, \quad \langle u(x), u(y) \rangle = \langle x, y \rangle.$$

Définition 9.3.1 Un opérateur linéaire u sur E est *symétrique* (ou *autoadjoint*) si $u^* = u$ et *antisymétrique* si $u^* = -u$.

Remarque 1. Cela signifie que

$$\forall x, y \in E, \quad \langle u(x), y \rangle = \pm \langle x, u(y) \rangle.$$

2. Si on fixe une base orthonormée $\mathscr{B}$ de E et qu'on désigne par A la matrice de u dans la base $\mathscr{B}$, on voit alors que u est (anti-) symétrique si et seulement si A est (anti-) symétrique.

Proposition 9.3.2 Il existe un isomorphisme d'espaces vectoriels

$$\mathrm{L}_2(E, \mathbb{R}) \simeq \mathrm{L}(E), \quad \Phi \leftrightarrow u$$

donné par

$$\forall x, y \in E, \quad \Phi(x, y) = \langle x, u(y) \rangle.$$

De plus, Φ est une forme symétrique si et seulement si u est un opérateur symétrique.

Démonstration. La seconde assertion résulte immédiatement des définitions. Pour la première, on remarque d'abord que si $u \in \mathrm{L}(E)$, alors la formule définit bien une forme bilinéaire sur E. On vérifie ensuite aisément que l'application $u \mapsto \Phi$ est linéaire. Comme les deux espaces ont même dimension, il suffit pour conclure de montrer que le noyau est nul. Or si on suppose que pour tout $x, y \in E$, $\langle x, u(y) \rangle = 0$, alors on a nécessairement pour tout $y \in E$, $u(y) = 0$ car un produit scalaire est non dégénéré. Et il suit que $u = 0$. ∎

Remarque Si $A := [a_{i,j}]$ est la matrice de u dans une base orthonormée $\mathscr{B} := (e_1, \ldots, e_n)$, on aura pour tout $i, j = 1, \ldots, n$,

$$\Phi(e_i, e_j) = \langle e_i, u(e_j) \rangle = \langle e_i, a_{1,j} e_1 + \cdots + a_{n,j} e_n \rangle = a_{i,j}$$

si bien que la matrice de Φ dans $\mathscr{B}$ est aussi égale à A.

Proposition 9.3.3 Soit u un opérateur symétrique sur E. Si F est un sous-espace vectoriel de E stable par u, alors $F^\perp$ aussi.

Démonstration. Soit $x \in F^\perp$. Si $y \in F$, on aura aussi $u(y) \in F$ si bien que

$$\langle u(x), y \rangle = \langle x, u(y) \rangle = 0. \quad ∎$$

Lemme 9.3.4 Si V est un espace vectoriel non nul de dimension finie sur $\mathbb{R}$ et $u \in \mathrm{L}(V)$, alors il existe une droite ou un plan dans V qui est stable par u.

Démonstration. Puisque V n'est pas nul, il existe une valeur propre complexe λ pour u dans $\mathbb{C}$. On écrit donc $\lambda = a + ib$ avec $a, b \in \mathbb{R}$. Si $z := x + iy$ est un vecteur propre de u pour λ, on aura

$$u(x) + iu(y) = u(x + iy) = u(z) = \lambda z = (a + ib)(x + iy) = (ax - by) + i(ay + bx).$$

si bien que

$$u(x) = ax - by \quad \text{et} \quad u(y) = ay + bx.$$

et $\mathrm{Vect}(x, y)$ répond à la question. ■

Remarque Pour être tout à fait rigoureux, il faudrait travailler dans $\mathbb{C} \otimes_{\mathbb{R}} V$, ou alors, avec des matrices et utiliser le fait que $\mathrm{M}_n(\mathbb{R})$ est contenu dans $\mathrm{M}_n(\mathbb{C})$.

Théoreme 9.3.5 — spectral. Si u est un opérateur symétrique sur E, alors il est diagonalisable dans une base orthonormée.

Démonstration. On procède par récurrence sur $n = \dim E$. Lorsque $n = 1$, il n'y a rien à faire. Supposons maintenant que $n = 2$. Si

$$A := \begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

est la matrice de u dans une base quelconque, on aura

$$\chi_u := T^2 - (a + c)T + (ac - b^2).$$

Et on voit que le discriminant est positif :

$$\Delta = (a + c)^2 - 4(ac - b^2) = (a - c)^2 + 4b^2 \geq 0.$$

Il suit que u possède une valeur propre $a_1 \in \mathbb{R}$. Soient e_1 un vecteur propre de norme 1 pour a_1 et $F := \mathrm{Vect}(e_1)$. Soit e_2 un vecteur de norme 1 dans $F^\perp$ (qui est une droite). On utilise alors la proposition 9.3.3 qui nous dit que comme F est stable par u, il en va de même pour $F^\perp$ si bien que $u(e_2) = a_2 e_2$ avec $a_2 \in \mathbb{R}$. On obtient ainsi une base orthonormée dans laquelle la matrice de u est diagonale.

Dans le cas général, on sait grâce au lemme qu'il existe un sous-espace vectoriel F de dimension 1 ou 2 dans E qui est stable par u. De nouveau, grâce au lemme 9.3.3, on sait que $F^\perp$ est stable par u. On conclut alors aisément (exercice). ■

Corollaire 9.3.6 Si A est une matrice réelle symétrique, elle est diagonalisable dans une base orthonormée : il existe une matrice orthogonale P et une matrice diagonale D telles que $A = PDP^{-1}$.

Démonstration. ■

Exemple Diagonaliser

$$A := \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

dans une base orthonormée :

— Première méthode : on écrit la forme quadratique associée comme (somme de) carré(s) :

$$Q := x^2+y^2+z^2+2xy+2yz+2xz = (x+y+z)^2.$$

On réalise alors qu'on peut réécrire cette somme comme combinaison linéaire de carrés de formes linéaires qui forment une base orthonormée :

$$Q = 3(\frac{\sqrt{3}}{3}x+\frac{\sqrt{3}}{3}y+\frac{\sqrt{3}}{3}z)^2+0(\frac{\sqrt{2}}{2}x-\frac{\sqrt{2}}{2}y)^2+0(\frac{\sqrt{6}}{6}x+\frac{\sqrt{6}}{6}y-\frac{\sqrt{6}}{3}z)^2$$

Pour obtenir ça, on regarde d'abord la forme linéaire $x+y+z$ qui a pour composantes $(1,1,1)$ et on la normalise pour trouver $\frac{\sqrt{3}}{3}x+\frac{\sqrt{3}}{3}y+\frac{\sqrt{3}}{3}z$. Ensuite, on regarde le plan orthogonal au vecteur $(1,1,1)$ qui a pour équation $x+y+z=0$ (on travaille dans ${}^t\mathbb{R}^3$ ici) dont on cherche une base orthonormée (calcul) et on obtient ainsi $\frac{\sqrt{2}}{2}x-\frac{\sqrt{2}}{2}y$ et $\frac{\sqrt{6}}{6}x+\frac{\sqrt{6}}{6}y-\frac{\sqrt{6}}{3}z$. Il suffit ensuite de poser

$$D := \begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad P^{-1} := \begin{bmatrix} \frac{\sqrt{3}}{3} & \frac{\sqrt{3}}{3} & \frac{\sqrt{3}}{3} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & 0 \\ \frac{\sqrt{6}}{6} & \frac{\sqrt{6}}{6} & -\frac{\sqrt{3}}{6} \end{bmatrix} \quad \text{et} \quad P = {}^tP^{-1} = \begin{bmatrix} \frac{\sqrt{3}}{3} & \frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{6} \\ \frac{\sqrt{3}}{3} & -\frac{\sqrt{2}}{2} & \frac{\sqrt{6}}{6} \\ \frac{\sqrt{3}}{3} & 0 & -\frac{\sqrt{3}}{6} \end{bmatrix}.$$

— Seconde méthode : on trouve aisément le polynôme caractéristique $\chi = T^2(T-3)$ de A. En effet, comme la matrice est de rang 1, on sait que 0 est valeur propre de multiplicité 2. D'autre part, la trace, qui est égale à la somme des valeurs propres, vaut 3. On obtient ainsi la matrice D. On cherche alors le sous-espace propre associé à la valeur propre 3 en résolvant le système

$$\begin{cases} x+y+z=3x \\ x+y+z=3y \\ x+y+z=3z \end{cases},$$

ce qui nous donne $x=y=z$. On peut prendre $(1,1,1)$ comme vecteur propre qu'on normalise pour trouver la première colonne de P. On cherche ensuite le sous-espace propre associé à la valeur propre 0, c'est le noyau de A qui a pour équation $x+y+z=0$. On cherche alors une base orthonormée pour obtenir les deux dernières colonnes de P. Finalement, on sait que $P^{-1} = {}^tP$. On remarquera que les calculs sont presque identiques à ceux de la première méthode.

9.4 Forme hermitienne

On travaille sur $\mathbb{C}$ et on désigne par $\bar{a}$ le conjugué d'un nombre complexe $a \in \mathbb{C}$. On étendra cette notation aux éléments de $\mathbb{C}^n$ ou de $M_{n\times m}(\mathbb{C})$.

Définition 9.4.1 Une application $u : E \to F$ entre deux espaces vectoriels complexes est dite *semi-linéaire* si

1. $\forall x,y \in E, \quad u(x+y) = u(x)+u(y)$,
2. $\forall x \in E, \forall a \in \mathbb{C}, \quad u(ax) = \bar{a}u(x)$.

Remarque Si on on fait opérer $\mathbb{C}$ sur F par $(a,y) \mapsto \bar{a}y$, alors u devient une application linéaire usuelle et on peut utiliser toute la théorie de l'algèbre linéaire. En dimension finie, si A est la matrice de u (dans des bases fixées $\mathscr{B}$ et $\mathscr{C}$), X le vecteur colonne associé à un vecteur u et Y celui associé à $u(x)$, on aura $Y = A\overline{X}$. On remarquera qu'une application semi-linéaire est toujours $\mathbb{R}$-linéaire.

Définition 9.4.2 Une *application sesquilinéaire* est une application

$$\Phi : E \times F \to G,$$

où E, F et G sont des espaces vectoriels complexes, telle que

1. (a) $\forall x, y \in E, \forall z \in F, \quad \Phi(x+y, z) = \Phi(x, z) + \Phi(y, z)$
   (b) $\forall x \in E, \forall y, z \in F, \quad \Phi(x, y+z) = \Phi(x, y) + \Phi(x, z)$,
2. $\forall x \in E, \forall y \in F, \forall a \in \mathbb{C}, \quad \Phi(ax, y) = a\Phi(x, y) \quad$ et $\quad \Phi(x, ay) = \overline{a}\Phi(x, y)$.

Remarque Une application sesquilinéaire est donc linéaire par rapport à la première variable et *semi-linéaire* par rapport à la seconde. Alternativement, si on fait opérer $\mathbb{C}$ sur le premier facteur par $(a, x) \mapsto \overline{a}x$, une application sesquilinéaire est tout simplement une application bilinéaire et la théorie générale s'applique. On remarquera qu'une application sesquilinéaire est toujours $\mathbb{R}$-bilinéaire.

À partir d'ici, on développe pour les formes sesquilinéaires sur un espace vectoriel complexe E, l'analogue de la théorie des formes bilinéaires sur un espace vectoriel réel E. La plupart des démonstrations étant quasiment identiques sont laissées en exercice.

Remarque
1. Les formes sesquilinéaires sur E forment un espace vectoriel $\mathrm{L}_{3/2}(E, \mathbb{C})$ isomorphe à l'espace $L_{1/2}(E, {}^tE)$ des applications *semi-linéaires* de E vers ${}^tE$ via $\Phi(x, y) = l_\Phi(y)(x)$.
2. On considérera le *noyau* (ou *radical*) d'une forme sesquilinéaire Φ :
$$\ker\Phi := \ker l_\Phi = \{y \in E \ / \ \forall x \in E, \Phi(x, y) = 0\},$$
ainsi que son *rang* : $\mathrm{rang}(\Phi) := \mathrm{rang}(l_\Phi)$. On dira que Φ est *non dégénérée* (ou *définie*) si $\ker\Phi = \{0\}$.
3. Si E est de dimension finie, on définit de même la *matrice* de la forme bilinéaire Φ dans une base $\mathscr{B} := (e_1, \ldots, e_n)$:
$$[\Phi]_{\mathscr{B}} := [l_\Phi]^{\mathscr{B}}_{{}^t\mathscr{B}} = [\Phi(e_i, e_j)].$$

Exemple La forme sesquilinéaire *canonique* sur $\mathbb{C}^n$ est définie par

$$((x_1, \ldots, x_n), (y_1, \ldots, y_n)) \mapsto x_1\overline{y}_1 + \cdots + x_n\overline{y}_n.$$

Plus généralement, la forme sesquilinéaire associée à $J := [c_{i,j}] \in M_n(\mathbb{C})$ est donnée par

$$\Phi((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \sum_{i,j=1}^{n} c_{i,j} x_i \overline{y}_j.$$

Proposition 9.4.3 Si Φ est une forme sesquilinéaire sur un espace vectoriel complexe E et $u, v : F \to E$ deux applications linéaires, alors l'application composée $\Psi := \Phi \circ (u \times v)$ est sesquilinéaire et on a

$$l_\Psi = {}^tu \circ l_\Phi \circ v.$$

Démonstration. Exercice. ∎

Remarque
1. Supposons que E et F soient de dimension finie et munis de bases $\mathscr{B}$ et $\mathscr{C}$ respectivement. Désignons les matrices de Φ, u et v dans ces bases par J, A et B respectivement. Alors, il résulte de la proposition que la matrice de Ψ sera ${}^tAJ\overline{B}$.

2. Comme cas particulier ($F = \mathbb{C}$ avec sa base canonique), on voit que si $x, y \in E$ et X et Y désignent leur matrices dans la base $\mathscr{B}$, alors on a
$$\Phi(x,y) = {}^tXJ\overline{Y}.$$
3. Autre cas particulier ($u = v = \mathrm{Id}_E$ et $\mathscr{C} = \mathscr{B}'$) : on voit que si J' est la matrice de Φ dans une autre base $\mathscr{B}'$ et si P la matrice de passage, on aura
$$J' = {}^tPJ\overline{P}.$$

Proposition 9.4.4 Soit Φ une forme sesquilinéaire *non dégénérée* sur un espace vectoriel complexe E *de dimension finie*. Si $u \in L(E)$, il existe un unique opérateur linéaire u^* sur E tel que
$$\forall x, y \in E, \quad \Phi(u(x), y) = \Phi(x, u^*(y)).$$

Démonstration. Exercice. ■

Définition 9.4.5 On dits que u^* est l'*opérateur adjoint* à $u \in L(E)$ relativement à Φ.

Remarque Si on désigne par J et A les matrices de Φ et u respectivement dans une base $\mathscr{B}$, alors la matrice de u^* est la *matrice adjointe* relativement à $J \in \mathrm{GL}_n(\mathbb{C})$ de A :
$$A^* := \overline{J}^{-1}\,{}^t\overline{AJ}.$$
Bien sûr, lorsque $J = I$, on trouve $A^* = {}^t\overline{A}$.

Définition 9.4.6 Une forme sesquilinéaire est dite *hermitienne* si
$$\forall x, y \in E, \quad \Phi(y,x) = \overline{\Phi(x,y)}.$$
On dit alors qu'une partie $A \subset E$ est *orthogonale* à une partie $B \subset E$ relativement à Φ, et on écrit $A \perp B$, si
$$\forall x \in A, \forall y \in B, \quad \Phi(x,y) = 0.$$

Remarque
1. On voit donc qu'une application $\Phi : E \times E \to \mathbb{C}$ est une forme sesquilinéaire hermitienne si et seulement si
   (a) $\forall x, y, z \in F, \quad \Phi(x+y, z) = \Phi(x,z) + \Phi(y,z)$,
   (b) $\forall x, y \in E, \forall a \in \mathbb{C}, \quad \Phi(ax, y) = a\Phi(x,y)$,
   (c) $\forall x, y \in E, \quad \Phi(y,x) = \overline{\Phi(x,y)}$.
2. Sur un espace vectoriel de dimension finie, une forme sesquilinéaire est hermitienne lorsque sa matrice J est *hermitienne* :
$${}^tJ = \overline{J}.$$
   Cela signifie que $c_{i,i} \in \mathbb{R}$ pour tout $i = 1, \dots, n$ et que $\overline{c_{i,j}} = c_{j,i}$ pour $i \neq j$.

Théoreme 9.4.7 Si Φ est une forme sesquilinéaire hermitienne non dégénérée sur un espace vectoriel E de dimension finie, alors l'application $F \mapsto F^\perp$, sur l'ensemble des sous-espaces vectoriels de E, est une symétrie qui renverse l'inclusion et échange somme et intersection. De plus, on a toujours
$$\dim F + \dim F^\perp = \dim E,$$
et les conditions suivantes sont équivalentes
1. $\Phi_{|F}$ est non dégénérée,

2. $F \cap F^{\perp} = \{0\}$,
3. $E \simeq F \oplus F^{\perp}$.

Démonstration. Exercice. ■

Définition 9.4.8 Une application $Q : E \to \mathbb{R}$, ou E est un espace vectoriel complexe, est une *forme quadratique hermitienne* s'il existe une forme sesquilinéaire hermitienne Φ sur E, appelée alors *polaire* de Q, telle que
$$\forall x \in E, \quad Q(x) = \Phi(x,x).$$

Exemple La forme sesquilinéaire canonique est hermitienne et la forme quadratique hermitienne associée est
$$Q(x_1,\ldots,x_n) = \sum_{i=1}^{n} |x_i|^2.$$
Plus généralement, si $J := [c_{i,j}]$ est une matrice hermitienne, la forme quadratique associée est donnée par
$$Q(x_1,\ldots,x_n) = \sum_{i=1}^{n} c_{i,i}|x_i|^2 + 2\sum_{i<j} \Re(c_{i,j}x_i\bar{x}_j).$$

Remarque 1. La polaire Φ d'une forme quadratique hermitienne Q est uniquement déterminée par Q (utiliser la formule du binôme ci-dessous et l'identité $\Im(a) = -\Re(ia)$).
2. On dispose de la *formule du binôme*
$$\forall x,y \in E, \quad Q(x+y) = Q(x) + 2\Re(\Phi(x,y)) + Q(y).$$
3. La *quadraticité* nous dit que
$$\forall a \in \mathbb{C}, \forall x \in E, \quad Q(ax) = |a|^2 Q(x).$$
4. On peut remarquer que Q est aussi une forme $\mathbb{R}$-quadratique de polaire $(x,y) \mapsto \Re(\Phi(x,y))$.

Définition 9.4.9 Soit Q une forme quadratique hermitienne sur un espace vectoriel complexe E. On dit que $u \in \mathrm{GL}(E)$ est *unitaire* relativement à Q si
$$\forall x \in E, \quad Q(u(x)) = Q(x).$$
Le *groupe unitaire* de Q est l'ensemble $\mathrm{U}(Q)$ de tous les opérateurs unitaires relativement à Q.

Remarque 1. C'est équivalent à dire que u est *unitaire* relativement à la forme sesquilinéaire hermitienne Φ :
$$\forall x,y \in E, \quad \Phi(u(x),u(y)) = \Phi(x,y).$$
2. En dimension finie, c'est aussi équivalent à dire que la matrice A de u est *unitaire* relativement à la matrice J de Φ :
$${}^t A J \overline{A} = J.$$
On désignera par $\mathrm{U}(J)$ le groupe des matrices unitaires relativement à J.
3. Dans le cas de la forme quadratique hermitienne canonique (c'est à dire $J = I$), on écrit
$$U(n) = \{A \in \mathrm{M}_n(C) \,/\, {}^t A\overline{A} = I\}.$$
Plus généralement, on note $\mathrm{U}(p,q)$ le groupe unitaire de
$$J = \begin{bmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

4. Si E est de dimension finie et Φ est non-dégénérée, on voit aisément que u est unitaire si et seulement si u est inversible et $u^{-1} = u^*$ (en termes de matrices, c'est immédiat).

Définition 9.4.10 Soit Q une forme quadratique hermitienne sur un espace vectoriel complexe de dimension finie E. Une partie X de E est *orthogonale* relativement à Q si

$$\forall x \neq y \in X, \quad x \perp y.$$

Elle est *orthonormée* si, de plus

$$\forall x \in X, \quad Q(x) = 1.$$

Remarque 1. Une partie orthonormée est toujours libre.

2. Une base $\mathscr{B}$ est orthogonale (resp. orthonormée) pour Q si et seulement si la matrice J de Q dans $\mathscr{B}$ est diagonale (resp. si $J = I$).
3. Lorsque $E = \mathbb{C}^n$, dire que J est diagonale (resp. que $J = I$) signifie que $Q(x_1, \ldots, x_n) = \sum c_i |x_i|^2$ (resp. $= \sum |x_i|^2$).

Proposition 9.4.11 Si Q est une forme quadratique hermitienne sur un espace vectoriel complexe de dimension finie E, alors il existe une base orthogonale pour Q.

Démonstration. Exercice. ■

Remarque 1. Cela signifie donc qu'il existe $\varphi_1, \ldots, \varphi_n \in {}^tE$ (formant une base) tels que

$$\forall x \in E, \quad Q(x) = c_1|\varphi_1(x)|^2 + \cdots + c_n|\varphi_n(x)|^2.$$

2. Si la matrice de Q dans l'ancienne base $\mathscr{B}$ est J, que sa matrice dans la base orthogonale $\mathscr{C}$ est D et que P désigne matrice de passage de $\mathscr{B}$ à $\mathscr{C}$, on aura donc

$$D = {}^tPJ\overline{P} \quad \text{et} \quad J = {}^tP^{-1}D\overline{P}^{-1}$$

avec

$$D = \begin{bmatrix} c_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c_n \end{bmatrix} \quad \text{et} \quad P^{-1} = \begin{bmatrix} [\varphi_1] \\ \vdots \\ [\varphi_n] \end{bmatrix}.$$

3. On dispose toujours d'un algorithme dû à Gauss pour décomposer Q en somme de carrés.

Théoreme 9.4.12 — d'inertie de Sylvester. Si Q est une forme quadratique hermitienne sur un espace vectoriel complexe de dimension finie E, il existe p, q *uniques* telle que la matrice J de Q dans une base $(e_1, \ldots, e_n)$ soit

$$J = \begin{bmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Démonstration. Exercice ■

Définition 9.4.13 On dit alors que $\mathrm{sign}(Q) := (p,q)$ est la *signature* de Q.

Définition 9.4.14 Une forme quadratique hermitienne Q sur un espace vectoriel complexe E est *positive* (resp. *négative*) si

$$\forall x \in E, \quad Q(x) \geq 0 \quad (\text{resp. } \leq 0).$$

Remarque Cela signifie que sa signature est $(p,0)$ (resp. $(0,q)$). En particulier, on voit qu'elle est définie positive (resp. définie négative) si et seulement si sa signature est $(n,0)$ (resp. $(0,n)$) où n désigne la dimension de E, ce qui correspond au cas $J = I$ (resp. $J = -I$) dans une base bien choisie.

9.5 Espace préhilbertien

Définition 9.5.1 Soit E un espace vectoriel complexe. Un *produit scalaire hermitien* sur E est une forme sesquilinéaire hermitienne définie positive

$$E \times E \to \mathbb{C}, \quad (x,y) \mapsto \langle x,y \rangle.$$

Remarque Cela signifie donc que
1. $\forall x,y \in E, \quad \langle y,x \rangle = \overline{\langle x,y \rangle}$,
2. $\forall x,x',y \in E, \quad \langle x+x',y \rangle = \langle x,y \rangle + \langle x',y \rangle$,
3. $\forall x,y \in E, \forall a \in \mathbb{C}, \quad \langle ax,y \rangle = a\langle x,y \rangle$,
4. $\forall x \in E \setminus \{0\}, \quad \langle x,x \rangle > 0$.

Proposition 9.5.2 — Cauchy-Schwarz. Si $\langle\ ,\ \rangle$ est un produit scalaire hermitien sur un espace vectoriel complexe E, alors l'application

$$E \to \mathbb{R}_{\geq 0}, \quad x \mapsto \|x\| := \sqrt{\langle x,x \rangle}$$

est une norme sur E et on a

$$\forall x,y \in E, \quad |\langle x,y \rangle| \leq \|x\|\|y\|,$$

avec égalité si et seulement si x et y sont liés.

Démonstration. Exercice ∎

Définition 9.5.3 Un *espace vectoriel préhilbertien* est un espace vectoriel complexe E muni d'un produit scalaire hermitien $\langle\ ,\ \rangle$. On dit *hilbertien* si E est complet (par exemple, de dimension finie).

Proposition 9.5.4 Si E est un espace vectoriel hilbertien de dimension finie et $F \subset E$ un sous-espace vectoriel, alors F et $F^\perp$ sont supplémentaires.

Démonstration. Exercice. ∎

Définition 9.5.5 Soient E un espace vectoriel hilbertien de dimension finie et $F \subset E$ un sous-espace vectoriel. Alors, la *projection orthogonale* sur F est la première projection associée à la décomposition $E \simeq F \oplus F^\perp$.

Proposition 9.5.6 Soit E un espace vectoriel hilbertien de dimension finie. Alors,

1. E possède une base orthonormée $\mathscr{B}$,
2. si $u \in L(E)$, les conditions suivantes sont équivalentes :
   (a) u est unitaire,
   (b) l'image par u d'une (resp. de toute) base orthonormée est une base orthonormée.

Démonstration. Exercice. ■

Remarque On dispose toujours de l'algorithme de Gram-Schmidt : si $x_1, \dots, x_r$ sont linéairement indépendants dans un espace vectoriel préhilbertien E, alors il existe $y_1, \dots, y_r \in E$ uniques tels que, pour tout $i = 1, \dots, r$, $(y_1, \dots, y_i)$ soit une base orthonormée de $F_i := \mathrm{Vect}(x_1, \dots, x_i)$ et $\langle x_i, y_i \rangle > 0$.

Définition 9.5.7 Soit E un espace vectoriel hilbertien de dimension finie et $u \in L(E)$. Alors,

1. u est *hermitien* (ou *autoadjoint*) si $u^* = u$.
2. u est *antihermitien* si $u^* = -u$.
3. u est *normal* si $u \circ u^* = u^* \circ u$.

Remarque

1. Si on fixe une base orthonormée $\mathscr{B}$ de E et qu'on désigne par A la matrice de u dans la base $\mathscr{B}$, on a
   (a) u hermitien $\Leftrightarrow {}^tA = \overline{A}$ (matrice hermitienne),
   (b) u antihermitien $\Leftrightarrow {}^tA = -\overline{A}$ (matrice antihermitienne),
   (c) u normal $\Leftrightarrow {}^tA\overline{A} = \overline{A}{}^tA$.
2. Un opérateur unitaire, hermitien ou antihermitien sont des exemples d'opérateurs normaux.
3. Il existe un isomorphisme d'espaces vectoriels
   $$\mathrm{L}_{3/2}(E, \mathbb{C}) \simeq \mathrm{L}(E), \quad \Phi \leftrightarrow u$$
   donné par
   $$\forall x, y \in E, \quad \Phi(x, y) = \langle x, u(y) \rangle.$$
   De plus, Φ est une forme hermitienne si et seulement si u est un opérateur hermitien.
4. On voit aisément qu'un sous-espace vectoriel F d'un espace hilbertien de dimension finie E est stable par un opérateur u si et seulement si $F^\perp$ est stable par u^*.

Théoreme 9.5.8 — spectral. Si u est un opérateur normal sur un espace hilbertien de dimension finie E, alors u est diagonalisable dans une base orthonormée.

Démonstration. On peut supposer que $E \neq \{0\}$ et qu'il existe donc une valeur propre $a \in \mathbb{C}$ pour u. Soit F le sous-espace propre associé. Si $F = E$, alors u est la multiplication par a, et n'importe quelle base orthonormée fait l'affaire. Bien sûr, le sous-espace F est stable par u, mais aussi par u^* puisque ce dernier commute avec u. Il suit que $F^\perp$ est aussi stable par u et on peut conclure par récurrence puisque $E \simeq F \oplus F^\perp$ avec $\dim F < \dim E$ et $\dim F^\perp < \dim E$. ■

Remarque Dans le cas ou u est unitaire (resp. hermitien, resp. antihermitien), les valeurs propres sont de norme 1 (resp. réelles, resp. imaginaires pures).

9.6 Exercices

Exercice 9.1 On se place dans un espace euclidien E et on illustrera chaque résultat par un dessin dans le plan. Soient $x, y \in E$.

1. Montrer le théorème de Pythagore : $x \perp y \Leftrightarrow \|x-y\|^2 = \|x\|^2 + \|y\|^2$.
2. Montrer la règle du parallélogramme : $\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2$.
3. En déduire l'identité de la médiane : $\|\frac{x+y}{2}\|^2 = \frac{\|x\|^2}{2} + \frac{\|y\|^2}{2} - \frac{\|x-y\|^2}{4}$.

Exercice 9.2 On se place dans un espace euclidien E et on illustrera chaque résultat par un dessin dans le plan. Soient $x, y \in E \setminus \{0\}$.

1. Montrer que x et y sont orthogonaux si et seulement $\widehat{(x,y)} = \pi/2$.
2. Montrer que x et y sont linéairement dépendants si et seulement si $\widehat{(x,y)} = 0$ ou $\widehat{(x,y)} = \pi$.
3. Montrer le théorème de Pythagore généralisé :

$$\|x-y\|^2 = \|x\|^2 + \|y\|^2 - 2\|x\|\|y\| \cos \widehat{(x,y)}.$$

Exercice 9.3 Montrer que, dans un espace euclidien, deux vecteurs x et y sont colinéaires si et seulement si $\|x+y\| = |\|x\| \pm \|y\||$. L'implication est-elle toujours vraie pour une norme quelconque ? Et pour un espace vectoriel sur $\mathbb{C}$? Et la réciproque ?

Exercice 9.4 Soient $x_1, \ldots, x_n$ tous distincts de norme 1 dans un espace vectoriel euclidien E et $a_1, \ldots, a_n \in \mathbb{R}_{\geq 0}$ tels que $\sum_{i=1}^n a_i = 1$ et $\|\sum_{i=1}^n a_i x_i\| = 1$. Montrer que tous les a_i sont nuls sauf un (qui vaut 1).

Exercice 9.5 Montrer que tout vecteur de norme 1 dans $\mathbb{R}^3$ se met sous la forme

$$u = (\cos\varphi, \sin\varphi\cos\psi, \sin\varphi\sin\psi)$$

et compléter en une base orthonormée.

Exercice 9.6 Montrer que la projection orthogonale sur la diagonale de $\mathbb{R}^2$ est donnée par

$$\forall x, y \in E, \quad p(x,y) = \left(\frac{x+y}{2}, \frac{x+y}{2}\right).$$

Exercice 9.7 Soient H un hyperplan d'un espace vectoriel euclidien E et v un vecteur *normal* (c'est à dire orthogonal) à H. Soient p la projection orthogonale sur H et s la *réflexion* (c'est à dire symétrie orthogonale) par rapport à H. Montrer que pour tout $x \in E$, on a

$$p(x) = x - \frac{\langle x, v\rangle}{\|v\|^2} v \quad \text{et} \quad s(x) = x - 2\frac{\langle x, v\rangle}{\|v\|^2} v.$$

Exercice 9.8 Quelle est l'image de $v := (-1,2,6)$ par la projection orthogonale sur le plan $H := \mathrm{Vect}((-1,1,0),(1,1,0))$? et avec $H := \mathrm{Vect}((3,-1,2),(1,-1,-2))$?

Exercice 9.9 Déterminer une base (orthogonale puis) orthonormée de

$$H := \mathrm{Vect}((3,1,-1,3),(-5,1,5,-7),(1,1,-2,8)).$$

Exercice 9.10 Déterminer la matrice de la projection orthogonale sur le plan d'équations $y+z+t=0$ et $x+z=0$.

Exercice 9.11 On va montrer que si E est un espace euclidien et $u \in \mathrm{L}(E)$, alors $\|u^* \circ u\| = \|u\|^2$. On pose $v = u^* \circ u$.

1. Montrer que si $x \in E$, alors $\|u(x)\|^2 \leq \|v(x)\|\|x\|$. En déduire que $\|u\|^2 \leq \|v\|$.
2. Montrer que si $x \in E$, alors $\|v(x)\|^2 \leq \|u(v(x)\|\|u(x)\|$. En déduire que $\|v\| \leq \|u\|^2$.

Exercice 9.12 Si E est un espace vectoriel euclidien, on définit le *rayon spectral* de $u \in \mathrm{L}(E)$ comme étant $\rho(u) := \max|\lambda|$ lorsque λ parcourt les valeurs propres de u.

1. Montrer que si u est un opérateur autoadjoint, alors $\|u\| = \rho(u)$.
2. En déduire qu'en général, on a $\|u\| := \sqrt{\rho(u^* \circ u)}$.

Exercice 9.13 Déterminer une matrice orthogonale P telle que $P^{-1}AP$ soit diagonale dans les cas suivants :

$$1) \quad A := \begin{bmatrix} 2 & \sqrt{6} \\ \sqrt{6} & 1 \end{bmatrix} \quad 2) \quad A := \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Exercice 9.14 Montrer que si S est une matrice réelle symétrique définie positive, alors il existe T tel que $S = T^2$.

Exercice 9.15 On considère, pour $a \in \mathbb{R}$, la forme quadratique

$$Q_a(x,y,z) := a(x^2+y^2+z^2) - 2(xy+xz+yz).$$

1. Écrire la matrice M_a de Q_a et calculer son déterminant.
2. Quel est le rang de M_a (on discutera selon les valeurs de a).
3. Déterminer une matrice diagonale D telle que $M_0 = PDP^{-1}$ avec $P \in \mathrm{O}(3)$.
4. En déduire qu'il existe une matrice diagonale D_a que l'on calculera telle que $M_a = PD_aP^{-1}$.
5. Peut-on trouver une même base qui est orthogonale pour tous les Q_a ?
6. Montrer que Q_a est définie positive si et seulement si $a > 2$.

Exercice 9.16

1. Diagonaliser dans une base orthonormée

$$A := \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad B := \begin{bmatrix} 0 & 3 \\ 3 & -8 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 6 & 2 \\ 2 & 3 \end{bmatrix}.$$

2. De même avec

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 2 & 2 & 0 \\ 2 & 0 & 2 \\ 0 & 2 & 2 \end{bmatrix}.$$

Exercice 9.17 On rappelle que l'application $\Phi : (A,B) \mapsto \mathrm{tr}(AB)$ est une forme bilinéaire symétrique sur $\mathrm{M}_n(\mathbb{R})$. Montrer que la restriction au sous-espace $\mathrm{SM}_n(\mathbb{R})$ des matrices symétriques est définie positive. Montrer que l'orthogonal de $\mathrm{SM}_n(\mathbb{R})$ est le sous-espace $\mathrm{AM}_n(\mathbb{R})$ des matrices antisymétriques (on pourra s'aider de la formule $\mathrm{tr}(AE_{ji}) = a_{ij}$).

Exercice 9.18 Montrer que l'application $(A,B) \mapsto \langle A,B\rangle := \mathrm{tr}({}^tAB)$ est un produit scalaire sur $\mathrm{M}_n(\mathbb{R})$ et que la base canonique est une base orthonormée (on pourra s'aider de la formule $\mathrm{tr}({}^tAE_{ij}) = a_{ij}$). Quel est l'adjoint de l'endomorphisme $M \mapsto AM$ pour A fixé.

IV Compléments

Solutions des exercices
Initiation à Sagemath
Références

Solutions des exercices

Remarque Certains exercices font usage d'un logiciel de calcul formel. Le code proposé peut être rentré en ligne sur

`https://cloud.sagemath.com`

après avoir créé un identifiant.

Corrigé de l'exercice 1.11 : Supposons que dans un groupe G, on ait $gh = gh'$. Puisque l'on a toujours $g^{-1}(gh) = (g^{-1}g)h = 1h = h$, on voit qu'il suffit de multiplier par g^{-1} à gauche pour obtenir $h = h'$. On montre de même que si $gh = g'h$, alors $g = g'$.

Bien sûr, le monoïde $\{0, 1\}$, muni de la multiplication, n'est pas intègre car $0 \times 0 = 0 = 0 \times 1$ bien que $0 \neq 1$.

Soient A un anneau et $a, b, c \neq 0$ dans A. Si on suppose que $ab = ac$, on voit immédiatement que $a(b - c) = 0$. Si A est intègre, cela implique que $b - c = 0$ et donc que $b = c$. De même, si $ac = bc$, on aura $a = b$.

Corrigé de l'exercice 1.17 :

1.
2. Remarquons pour commencer que $\{0\} = (0)$. Maintenant, si I est un idéal non nul de $K[T]$, il existe un polynôme $M \in I \setminus \{0\}$ de plus petit degré d. Quitte à le multiplier par une constante, on peut supposer qu'il est unitaire. Si $P \in I$, on peut écrire $AP = MQ + R$ avec $\deg R < \deg M$. On a alors $R = P - MQ \in I$ et comme $\deg R < \deg M$, on doit avoir $R = 0$ si bien que $P = MQ \in (M)$. Cela montre l'existence de M et aussi que $\deg P = \deg Q + \deg M \geq \deg M$ avec égalité si et seulement si Q est constant, c'est à dire si $P = aM$ avec $a \in K$. Si $(M) = (P)$, on peut écrire $M = SP$ si bien que $\deg M \geq \deg P$, et donc obligatoirement $\deg M = \deg P$ et $P = aM$. Si on suppose de plus P unitaire, on a $a = 0$ et il suit que $P = M$. Cela montre l'unicité.

Corrigé de l'exercice 1.22 :

On montre que $M^2 - (a + d)M + (ad - bc)I = 0$ en tapant :

```
a=var('a')
b=var('b')
c=var('c')
d=var('d')
M=matrix(2,2,[a,b,c,d])
I=matrix(2,2,[1,0,0,1])
N=M^2-(a+d)*M+(a*d-b*c)*I
N.expand()
```

On en déduit que

$$((a+d)I-M)M = M((a+d)I-M) = (ad-bc)I.$$

On voit donc que si $ad-bc$ est inversible, alors M aussi et on obtient son inverse en calculant :

```
(1/(a*d-b*c))*((a+d)*I-M)
```

Corrigé de l'exercice 1.24 :
On peut définir trois fonctions qui effectuent les opérations élémentaires (on pourrait aussi utiliser les fonctions intégrées) puis une dernière qui effectue la réduction de Gauss en affichant toutes les étapes (et pas plus) :

```
def Ech (A,i,j):
 n=A.ncols()
 for k in range(n):
 A[i,k],A[j,k]=A[j,k],A[i,k]
 return(A)
def Dil (A,i,m):
 n=A.ncols()
 for j in range (n):
 A[i,j]=m*A[i,j]
 return(A)
def Tra (A,i,j,m):
 n=A.ncols()
 for k in range(n):
 A[i,k]=A[i,k]+m*A[j,k]
 return(A)

def Gau(A):
 U=copy(A)
 m=U.nrows()
 n=U.ncols()
 k=0
 l=0
 while (k < m and l < n):
 i=k
 while U[i,l]==0:
 if i==m-1:
 if l==n-1:
 return
```

```
l=l+1
i=k
else:
i=i+1
if i!=k:
Ech(U,k,i)
print U
if U[k,l] != 1:
Dil(U,k,1/U[k,l])
print U
for i in [k+1..m-1]:
if U[i,l]!=0:
Tra(U,i,k,-U[i,l])
print U
k=k+1
l=l+1
```

Il suffit ensuite d'appliquer cette dernière fonction aux différentes matrices en rentrant par exemple :

```
M=matrix(QQ,3,3,[3,2,-3,5,-1,-2,1,1,-1])
M
Gau(M)
```

Corrigé de l'exercice 2.5 : On rappelle qu'un anneau est un corps si et seulement si il possède exactement deux idéaux. Comme un idéal est, par définition, un sous-module d'un anneau et qu'un sous-espace vectoriel est, par définition, un sous-module d'un espace vectoriel, cela montre que K possède exactement deux sous-espaces vectoriels. Nous savons aussi qu'une application linéaire induit une bijection entre sous-espaces contenant le noyau est sous-espaces contenus dans l'image. Comme conséquence, un isomorphisme induit une bijection entre tous les sous-espaces de chaque coté.

On peut aussi démontrer directement que K a exactement deux sous-espaces. Tout d'abord, comme $1 \neq 0$, K a au moins deux sous espaces, $\{0\}$ et K lui même. Dans l'autre sens, si I est un sous-espace de K, alors soit $I = \{0\}$, ou alors il existe $c \in I$ avec $c \neq 0$. Dans ce cas, si $a \in K$, on aura $a = \frac{a}{c}c \in I$ et donc $K = I$.

Réciproquement, supposons que E possède exactement deux sous-espaces vectoriels. Alors, $E \neq \{0\}$ et il existe donc $x \in E$ avec $x \neq 0$. On considère alors l'application $u : K \to E, a \mapsto ax$. On vérifie immédiatement que celle-ci est linéaire : $ax + bx = (a+b)x$ et $c(ax) = (ca)x$. Comme $x \neq 0$, on voit que $ax = 0 \Leftrightarrow a = 0$ et le noyau est donc réduit à 0. Enfin, l'image de notre application linéaire u est un sous-espace vectoriel de E qui contient $x = 1.x$. Ce ne peut donc pas être $\{0\}$ et c'est alors nécessairement E (car E n'a que deux sous-espaces vectoriels).

Corrigé de l'exercice 2.12 : On considère pour $i = 0, \ldots, d-1$, l'application $f_i : (T^d)^\circ \to K, \varphi \mapsto \varphi(T^i)$. C'est une forme linéaire car composée d'inclusions de sous-espaces puis d'une évaluation qui sont toutes des applications linéaires. L'application $f : (T^d)^\circ \to K^d$ dont les composantes sont les f_i pour $i = 0, \ldots, d-1$, est donc linéaire.

Par division euclidienne, tout $P \in K[T]$ s'écrit de manière unique $P = T^d Q + \sum_{i=0}^{d-1} a_i T^i$. Si $\varphi \in (T^d)^\circ$, on aura $\varphi(T^d Q) = 0$ et donc $\varphi(P) = \varphi(T^d Q) + \sum_{i=0}^{d-1} a_i \varphi(T^i) = \sum_{i=0}^{d-1} a_i \varphi(T^i)$. Si en fait, $\varphi \in \ker f$, on aura pour tout $i = 0, \ldots, d-1, \varphi(T^i) = 0$ et donc $\varphi(P) = 0$. Cela montre que f est injective.

Inversement, si on se donne $(c_0,\dots,c_{d-1}) \in K^d$ et $P = \sum_{i=0}^n a_iT^i \in K[T]$, on peut poser $\varphi(P) = \sum_{i=0}^{d-1} a_ic_i$. Supposons pour l'instant que l'on sache que φ est linéaire. Comme clairement, $\varphi(P) = 0$ pour $P \in (T^d)$, on aura $\varphi \in (T^d)^\circ$. Et comme, pour tout $i = 0,\dots,d-1$, on a $f_i(\varphi) = \varphi(T^i) = c_i$, on aura $f(\varphi) = (c_0,\dots,c_{d-1})$. D'où la surjectivité. Il ne reste donc qu'à montrer que φ est linéaire. On se donne $\lambda,\mu \in K$ et $P = \sum a_iT^i, Q = \sum b_iT^i \in K[T]$ si bien que $\lambda P + \mu Q = \sum(\lambda a_i + \mu b_i)T^i$. On calcule alors $\varphi(\lambda P + \mu Q) = \sum(\lambda a_i + \mu b_i)c_i = \lambda(\sum a_ic_i) + \mu \sum b_i)c_i = \lambda\varphi(P) + \mu\varphi(Q)$.

Corrigé de l'exercice 3.4 :

1. Si $q = \mathrm{Id}_E - p$, on a $q \circ q = (\mathrm{Id}_E - p) \circ (\mathrm{Id}_E - p) = \mathrm{Id}_E - 2p + p \circ p$. Donc, si p est une projection, on a $q \circ q = \mathrm{Id}_E - 2p + p = \mathrm{Id}_E - p = q$. Et on voit donc que q est aussi une projection. Comme on a $q = \mathrm{Id}_E - p$ si et seulement $p = \mathrm{Id}_E - q$, la réciproque est aussi vraie.
   Si p et q sont des projections complémentaires comme ci-dessus, on a $\mathrm{Id}_E = p + q$ et donc l'identité $x = p(x) + q(x)$ sur E. On en déduit immédiatement que $E = \mathrm{im}\, p + \mathrm{im}\, q$ mais aussi que $\ker q \cap \ker p = 0$ car si $p(x) = q(x) = 0$, alors $x = 0$. On voit aussi que $\ker p \subset \mathrm{im}\, q$ car si $p(x) = 0$, alors $x = q(x)$. Pour montrer l'inclusion réciproque, on utilise enfin le fait que p est une projection si bien que $p \circ q = p \circ (\mathrm{Id}_E - p) = p - p \circ p = 0$. Cela signifie que si $x \in E$, alors $p(q(x)) = 0$ et donc qu'on a bien $\mathrm{im}\, q \subset \ker p$. Bien sûr, par symétrie, on a aussi $\mathrm{im}\, p = \ker q$. On obtient donc les décompositions en somme directe annoncées.
2.

Corrigé de l'exercice 3.15 :

1.
2. On suppose d'abord que, dans S, les polynômes sont tous de degré distinct et on se donne $P_1,\dots,P_n \in S$ distincts tels que $a_1P_1 + \cdots + a_nP_n = 0$ avec $a_1,\dots,a_n$ tous non nuls. On peut supposer que $\deg P_1 < \cdots < \deg P_n$. Mais on voit alors que $\deg P_{n-1} = \deg(a_1P_1 + \cdots + a_{n-1}P_{n-1}) = \deg(-a_nP_n) = \deg P_n$. Contradiction.
   Supposons maintenant qu'il existe dans S un polynôme de chaque degré. Il suffit alors de montrer par récurrence sur n que $T^n \in \mathrm{Vect}(S)$ ou de manière équivalente que $K[T]_{\leq n} = \mathrm{Vect}(T^0,\dots,T^n) \subset \mathrm{Vect}(S)$. Supposons que c'est le cas (il faut aussi traiter le cas $n = 0$). Il existe un polynôme $P \in S$ de degré $n+1$. Si son coefficient dominant est a, on a $Q := T^{n+1} - \frac{1}{a}P \in K[T]_{\leq n}$. Il suit que $T^{n+1} = \frac{1}{a}P + Q \in \mathrm{Vect}(S)$.
3.
4.

Corrigé de l'exercice 4.2 :

1. C'est 1 (la dimension de K^n sur K est toujours n et ici c'est le cas $K = \mathbb{C}$ et $n = 1$).
2. C'est 2 car tout complexe s'écrit de manière unique $x1 + yi$ avec x,y réels.
3. C'est ∞ car $\{\pi^i\}_{i\in\mathbb{N}}$, par exemple, est une famille libre infinie de $\mathbb{C}$: sinon, on pourrait écrire une somme finie $\sum a_i\pi^i = 0$ et π ne serait pas transcendant. Plus précisément, la dimension de $\mathbb{C}$ sur $\mathbb{Q}$ est la puissance du continu car si E est un espace vectoriel de dimension infinie sur $\mathbb{Q}$, alors $\dim E = |E|$.

Corrigé de l'exercice 5.4 : Les énoncés de cet exercice sont toujours valables pour des modules sur un anneau quelconque. Dans ce cas, on doit utiliser la propriété universelle du produit tensoriel pour construire des applications linéaires dans les deux sens et montrer qu'elles sont inverses l'une de l'autre. Pour des espaces vectoriels sur un corps K, c'est bien plus simple : il suffit d'utiliser la propriété universelle des bases (toute bijection entre deux bases se prolonge alors de manière unique en un isomorphisme). Par contre cette méthode laisse sous-entendre que l'isomorphisme dépend du choix de la base alors qu'il est naturel.

1. On sait que K a pour base 1. Donc si E a pour base $(e_i)_{i\in I}$, on en déduit que $K \otimes E$ a pour base $(1 \otimes e_i)_{i\in I}$. La bijection $1 \otimes e_i \leftrightarrow e_i$ se prolonge de manière unique en un isomorphisme

$K \otimes E \simeq E$. Voyons maintenant la démonstration qui n'utilise pas les bases. On considère l'unique application bilinéaire $K \times E \to E, (a,x) \mapsto ax$. Elle induit une application linéaire $u : a \otimes x \mapsto ax$ (propriété universelle du produit tensoriel). On dispose aussi dans l'autre sens de l'application linéaire $v : x \mapsto 1 \otimes x$. On voit immédiatement que $u \circ v = \mathrm{Id}$. Dans l'autre sens, il suffit de remarquer que $(v \circ u)(a \otimes x) = 1 \otimes ax = a \otimes x$ et d'utiliser de nouveau la propriété universelle du produit tensoriel (ou le fait que tout élément du produit tensoriel est somme de tenseurs).
Les deux autres isomorphismes s'obtiennent exactement de la même façon.

2.
3.
4. Si on se donne $\varphi \in {}^tE$ et $\psi \in {}^tF$, on peut considérer la composée du produit $\varphi \times \psi : E \times F \to K \times K$ et de la multiplication $K \times K \to K$. C'est une application bilinéaire qui induit donc une application linéaire

$$u(\varphi,\psi) : E \otimes F \to K, \quad x \otimes y \mapsto \varphi(x)\psi(y)$$

On obtient ainsi une application

$$u : {}^tE \times {}^tF \to {}^t(E \otimes F)$$

et on veut s'assurer qu'elle est bilinéaire. Par symétrie, on ne le fait que d'un coté : si on se donne $\varphi_1, \varphi_2 \in {}^tE$, $\psi \in {}^tF$ et $a_1, a_2 \in K$, on aura bien pour $x \in E$ et $y \in F$,

$$(a_1\varphi_1 + a_2\varphi_2)(x)\psi(y) = a_1\varphi_1(x)\psi(y) + a_2\varphi_2(x)\psi(y).$$

Pour prouver que u est un isomorphisme, on choisit des bases $(e_1,\ldots,e_n)$ et $(f_1,\ldots,f_m)$ de E et F respectivement, et on montre que pour tout $i = 1,\ldots,n$ et $j = 1,\ldots,m$, on a $u({}^te_i \otimes {}^tf_j) = {}^t(e_i \otimes f_j)$. Pour cela, on prend $k \in \{1,\ldots,n\}$ et $l \in \{1,\ldots,m\}$ et on calcule

$$u({}^te_i \otimes {}^tf_j)(e_k \otimes e_l) = {}^te_i(e_k){}^tf_j(e_l) = \begin{cases} 1 & \text{si } (i,j) = (k,l) \\ 0 & \text{sinon.} \end{cases}$$

Remarquons que ce dernier argument suffit pour définir un tel isomorphisme, mais une fois encore, on ne saura pas qu'il est naturel, c'est à dire, indépendant du choix des bases.

Corrigé de l'exercice 6.15 :
Il suffit de taper pour chaque matrice M,

```
M.jordan_form(transformation=true)
```

1. Avec

```
M = matrix(QQ,3,3,[3,2,4,-1,3,-1,-2,-1,-3])
```

on obtient

$$J = \left(\begin{array}{r|rr} -1 & 0 & 0 \\ \hline 0 & 2 & 1 \\ 0 & 0 & 2 \end{array}\right) \quad \text{et} \quad P = \begin{pmatrix} 1 & -1 & 1 \\ 0 & -\frac{1}{2} & 0 \\ -1 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

2. Avec

```
M = matrix(QQ,3,3,[8,-1,-5,-2,3,1,4,-1,-1])
```

on obtient

$$J = \left(\begin{array}{r|rr} 2 & 0 & 0 \\ \hline 0 & 4 & 1 \\ 0 & 0 & 4 \end{array}\right) \quad \text{et} \quad P = \begin{pmatrix} 1 & \frac{3}{2} & 1 \\ 1 & -\frac{3}{2} & 0 \\ 1 & \frac{3}{2} & \frac{1}{2} \end{pmatrix}.$$

3. Avec

```
M = matrix(QQbar,4,4,[0,0,0,-1,1,0,0,0,0,1,0,-2,0,0,1,0])
```

on obtient

$$J=\left(\begin{array}{cc|cc} -i & 1 & 0 & 0\\ 0 & -i & 0 & 0\\ \hline 0 & 0 & i & 1\\ 0 & 0 & 0 & i\end{array}\right) \quad \text{et} \quad P=\begin{pmatrix} -i & 1 & i & 1\\ 1 & 0 & 1 & 0\\ -i & 3 & i & 3\\ 1 & 2i & 1 & -2i\end{pmatrix}.$$

4. Avec

```
M = matrix(QQ,3,3,[1,-1,-1,-1,1,-1,1,0,2])
```

on obtient

$$J=\left(\begin{array}{c|cc} 2 & 0 & 0\\ \hline 0 & 1 & 1\\ 0 & 0 & 1\end{array}\right) \quad \text{et} \quad P=\begin{pmatrix} 0 & -1 & 1\\ 1 & -1 & 1\\ -1 & 1 & 0\end{pmatrix}.$$

5. Avec

```
M = matrix(QQbar,4,4,[2,1,0,0,-2,0,0,0,1,0,0,2,0,1,-1,2])
```

on obtient

$$J=\left(\begin{array}{cc|cc} 1-i & 1 & 0 & 0\\ 0 & 1-i & 0 & 0\\ \hline 0 & 0 & 1+i & 1\\ 0 & 0 & 0 & 1+i\end{array}\right) \quad \text{et} \quad P=\begin{pmatrix} 0 & 1 & 0 & 1\\ 0 & -1-i & 0 & -1+i\\ \frac{3-3i}{2} & 0 & \frac{3+3i}{2} & 0\\ -\frac{3i}{2} & \frac{1-3i}{4} & \frac{3i}{2} & \frac{1+3i}{4}\end{pmatrix}.$$

Corrigé de l'exercice 8.5 :

1.
2. On se donne une suite de Cauchy f_n et on écrit pour tout $n\in\mathbb{N}$, $f_n=\sum_i a_{n,i}T^i$. Soit $i\in\mathbb{Z}$. Comme la suite est de Cauchy, il existe $n(i)\in\mathbb{N}$ tel que si $n\geq n(i)$, on ait $d(f_{n(i)},f_n)\leq\frac{1}{2^i}$. On a par définition $d(f_{n(i)},f_n)=\|f_{n(i)}-f_n\|$ et $f_{n(i)}-f_n=\sum_j(a_{n(i),j}-a_{n,j})T^j$. La condition s'écrit donc $a_{n(i),j}-a_{n,j}=0$ pour $j\leq i$. En particulier, voit que $a_{n(i),i}=a_{n,i}$ tant que $n\geq n(i)$. On pose alors $f=\sum_i a_{n(i),i}T^i$. On se donne $\varepsilon>0$ et on choisit $k\in\mathbb{N}$ tel que $\varepsilon\geq\frac{1}{2^k}$. Alors, si $n\geq\max_{i\leq k}n(i)$, on a $a_{n(i),i}=a_{n,i}$ tant que $i\leq k$. Comme on a $f-f_n=\sum_i(a_{n(i),i}-a_{n,i})T^i$, on voit que $d(f,f_n)=\|f-f_n\|\leq\frac{1}{2^k}\leq\varepsilon$.
3.
4.

Corrigé de l'exercice 8.6 :

1. Dans le cas archimédien, il suffit de prendre $a_{ij}=1$ pour tout $i,j\in\{1\ldots n\}$. Comme on a $A^2=nA$, on voit que $\|A^2\|=n^\alpha>1=\|A\|$ avec $\alpha>0$ si $n\geq 2$.
Par contre, dans le cas ultramétrique, on aura toujours
$$\max_{i,j}|\sum_k a_{ik}b_{kj}|\leq\max_{i,j}\max_k|a_{ik}b_{kj}|\leq\max_{i,j}|a_{ij}|.\max_{i,j}|b_{ij}|.$$
2. On a
$$\|AX\|_1=\left\|\left(\sum_{j=1}^n a_{ij}x_j\right)_{i=1}^n\right\|_1=\sum_{i=1}^n\left|\sum_{j=1}^n a_{ij}x_j\right|\leq\sum_{i=1}^n\sum_{j=1}^n|a_{ij}||x_j|=\sum_{j=1}^n\sum_{i=1}^n|a_{ij}||x_j|$$

$$\leq \sum_{j=1}^{n} \max_{k=1}^{n} \sum_{i=1}^{n} |a_{ik}||x_j| = \max_{k=1}^{n} \sum_{i=1}^{n} |a_{ik}| \sum_{j=1}^{n} |x_j| = \left(\max_{j=1}^{n} \sum_{i=1}^{n} |a_{ij}| \right) \|X\|_1,$$

D'autre part, si on note E_j le j-ème vecteur de la base canonique, alors

$$\max_{j=1}^{n} \|AE_j\|_1 = \max_{j=1}^{n} \left\|(a_{ij})_{i=1}^{n}\right\|_1 = \max_{j=1}^{n} \sum_{i=1}^{n} |a_{ij}| = \left(\max_{j=1}^{n} \sum_{i=1}^{n} |a_{ij}| \right) \|E_j\|_1.$$

Cela montre que notre formule définit la norme subordonnée à $\| - \|_1$ qui est automatiquement une norme d'algèbre.

3. On a

$$\|AX\|_\infty = \left\| \left(\sum_{j=1}^{n} a_{ij} x_j \right)_{i=\infty}^{n} \right\|_\infty = \max_{i=1}^{n} \left| \sum_{j=1}^{n} a_{ij} x_j \right| \leq \max_{i=1}^{n} \sum_{j=1}^{n} |a_{ij}||x_j|$$

$$\leq \max_{i=1}^{n} \sum_{j=1}^{n} |a_{ij}| \max_{k=1}^{n} |x_k| = \left(\max_{i=1}^{n} \sum_{j=1}^{n} |a_{ij}| \right) \|X\|_\infty.$$

D'autre part, il existe k tels que $\max_{i=1}^{n} \sum_{j=1}^{n} |a_{ij}| = \sum_{j=1}^{n} |a_{kj}|$. On pose alors $E = \sum_{j=1}^{n} \varepsilon_j E_j$ ou ε_j est le signe de a_{kj}, et on a

$$\|AE\|_\infty = \left\| \left(\sum_{j=1}^{n} a_{ij} \varepsilon_j \right)_{i=\infty}^{n} \right\|_1 = \max_{i=1}^{n} \left| \sum_{j=1}^{n} a_{ij} \varepsilon_j \right|$$

$$= \sum_{j=1}^{n} |a_{kj}| = \max_{i=1}^{n} \sum_{j=1}^{n} |a_{ij}| = \left(\max_{i=1}^{n} \sum_{j=1}^{n} |a_{ij}| \right) \|X\|_\infty.$$

Cela montre que notre formule définit la norme subordonnée à $\| - \|_\infty$.

Corrigé de l'exercice 8.10 : On va faire ça en détail. On appelle A la matrice et on calcule son polynôme caractéristique (on retranche la seconde colonne à la première puis on ajoute la première ligne à la seconde) :

$$\chi_A(T) = \begin{vmatrix} T-21 & -17 & -6 \\ 5 & T+1 & 6 \\ -4 & -4 & T-16 \end{vmatrix} = \begin{vmatrix} T-4 & -17 & -6 \\ 4-T & T+1 & 6 \\ 0 & -4 & T-16 \end{vmatrix}$$

$$= \begin{vmatrix} T-4 & -17 & -6 \\ 0 & T-16 & 0 \\ 0 & -4 & T-16 \end{vmatrix} = (T-4)(T-16)^2.$$

On a donc une valeur propre simple qui est 4 et une valeur propre double qui est 16. On cherche ensuite les sous-espaces propres. On résout $AX = 4X$ ou encore $(A-4I)X = 0$, c'est à dire

$$\begin{cases} 17x + 17y + 6z = 0 \\ -5x - 5y - 6z = 0 \\ 4x + 4y + 12z = 0 \end{cases},$$

qui est clairement équivalent à $x + y = 0$ et $z = 0$. On peut donc choisir le vecteur propre $(1, -1, 0)$. Pour la valeur propre 16, on procède de la même manière et on obtient

$$\begin{cases} 5x + 17y + 6z = 0 \\ -5x - 17y - 6z = 0 \\ 4x + 4y = 0 \end{cases}$$

qui est équivalent à $x+y=0$ et $z=2x$. On peut donc choisir le vecteur propre $(1,-1,2)$ mais on préférera $(2,-2,4)$ pour simplifier un peu les calculs qui suivent. En effet, la matrice n'est pas diagonalisable et il faut donc résoudre $AX = 16X + E$ ou E est le vecteur précédent (écrit en colonne). On doit donc résoudre

$$\left\{\begin{array}{l} 5x+17y+6z=2 \\ -5x-17y-6z=-2 \\ 4x+4y=4 \end{array}\right.$$

On peut prendre $x=1$ par exemple, ce qui donne $y=0$ et $z=-\frac{1}{2}$. Notre dernier vecteur de base sera donc $(1,0,-\frac{1}{2})$. En d'autres termes, on a $A = PJP^{-1}$ avec

$$J = \begin{bmatrix} 4 & 0 & 0 \\ 0 & 16 & 1 \\ 0 & 0 & 16 \end{bmatrix} \quad \text{et} \quad P = \begin{bmatrix} 1 & 2 & 1 \\ -1 & -2 & 0 \\ 0 & 4 & -\frac{1}{2} \end{bmatrix}$$

Pour obtenir P^{-1}, on peut calculer d'abord la comatrice de P :

$$\begin{bmatrix} 1 & -\frac{1}{2} & -4 \\ 5 & -\frac{1}{2} & -4 \\ 2 & -1 & 0 \end{bmatrix},$$

puis le déterminant de P :

$$\begin{vmatrix} 1 & 2 & 1 \\ -1 & -2 & 0 \\ 0 & 4 & -\frac{1}{2} \end{vmatrix} = 1-4-1 = -4.$$

On obtiendra donc l'inverse de P en transposant la comatrice et divisant par -4 (et on vérifie bien que $PP^{-1} = I$) :

$$P^{-1} = \begin{bmatrix} -\frac{1}{4} & -\frac{5}{4} & -\frac{1}{2} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{4} \\ 1 & 1 & 0 \end{bmatrix}$$

Pour calculer $\exp(A)$, on va avoir besoin de $\exp(J)$ que l'on peut calculer bloc par bloc. On rappelle qu'on a toujours

$$\exp\left(\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}\right) = e^{\lambda} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

En effet, on peut écrire notre matrice sous la forme $\lambda I + N$ avec $N^2 = 0$, et on aura donc

$$\exp(\lambda I + N) = \exp(\lambda I)\exp(N) = e^{\lambda}(I+N).$$

On en déduit que

$$\exp(J) = \begin{bmatrix} e^4 & 0 & 0 \\ 0 & e^{16} & e^{16} \\ 0 & 0 & e^{16} \end{bmatrix}$$

et on utilise la formule $\exp(A) = P\exp(J)P^{-1}$ pour calculer

$$\exp\left(\begin{bmatrix} 21 & 17 & 6 \\ -5 & -1 & -6 \\ 4 & 4 & 16 \end{bmatrix}\right) = \begin{bmatrix} 1 & 2 & 1 \\ -1 & -2 & 0 \\ 0 & 4 & -\frac{1}{2} \end{bmatrix} \begin{bmatrix} e^4 & 0 & 0 \\ 0 & e^{16} & e^{16} \\ 0 & 0 & e^{16} \end{bmatrix} \begin{bmatrix} -\frac{1}{4} & -\frac{5}{4} & -\frac{1}{2} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{4} \\ 1 & 1 & 0 \end{bmatrix}$$

$$= \frac{1}{4}\begin{bmatrix} e^4 & 2e^{16} & 3e^{16} \\ -e^4 & -2e^{16} & -2e^{16} \\ 0 & 4e^{16} & \frac{7}{2}e^{16} \end{bmatrix}\begin{bmatrix} -1 & -5 & -2 \\ \frac{1}{2} & \frac{1}{2} & 1 \\ 4 & 4 & 0 \end{bmatrix}$$

$$= \frac{1}{4}\begin{bmatrix} 13e^{16}-e^4 & 13e^{16}-5e^4 & 2e^{16}-2e^4 \\ -9e^{16}+e^4 & -9e^{16}+5e^4 & -2e^{16}+2e^4 \\ 16e^{16} & 16e^{16} & 4e^{16} \end{bmatrix}.$$

Corrigé de l'exercice 9.5 : Tout vecteur de norme 1 se met clairement sous la forme

$$u = (\cos\varphi, \sin\varphi\cos\psi, \sin\varphi\sin\psi)$$

et il suffit de poser ensuite

$$v = (-\sin\varphi, \cos\varphi\cos\psi, \cos\varphi\sin\psi) \quad \text{et} \quad w = (0, -\sin\psi, \cos\psi).$$

Corrigé de l'exercice 9.16 :

1. On écrit aisément la forme quadratique associée à $A := \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ comme (somme de) carré(s) :
$$x^2 + 2xy + y^2 = (x+y)^2.$$
Pour poursuivre, il faut réécrire cette somme comme combinaison linéaire de carrés d'une base orthonormée de l'espace des formes linéaires :
$$x^2 + 2xy + y^2 = 2(\frac{\sqrt{2}}{2}x + \frac{\sqrt{2}}{2}y)^2 + 0(\frac{\sqrt{2}}{2}x - \frac{\sqrt{2}}{2}y)^2$$
Il suffit ensuite de poser
$$D := \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}, \quad P^{-1} := \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{bmatrix} \quad \text{et} \quad P = {}^tP^{-1} = \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{bmatrix}.$$
Pour s'assurer du résultat, on peut calculer
$$\begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{bmatrix}\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{bmatrix} = \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{bmatrix}\begin{bmatrix} \sqrt{2} & \sqrt{2} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

2.

Initiation à Sage

Exercice 1 — TP.
1. Assigner à a la valeur 2.
2. Afficher la valeur de a.
3. Tester si $a = 2$.

Exercice 2 — TP.
1. Afficher le résultat de $5+2$.
2. Afficher le résultat de 5×2.
3. Afficher le résultat de 5^2.
4. Afficher le résultat de $5/2$.
5. Afficher le quotient dans la division de 5 par 2.
6. Afficher le reste dans la division de 5 par 2.

Exercice 3 — TP.
1. Tester si 1001 est un nombre premier.
2. Quels sont ses diviseurs ?
3. Quel est le pgcd de 1001 et 1155 ?
4. Quel est leur ppcm ?

Exercice 4 — TP.
1. Afficher les 10 premiers entiers naturels non nuls.
2. Afficher les nombres de Mersenne $2^n - 1$ qui sont premier lorsque $1 \leq n \leq 20$.

Exercice 5 — TP.
1. Définir une fonction « estpair » qui teste si un nombre est pair.
2. tester si 2 et 3 sont pairs ou pas.

Exercice 6 — TP.
1. Nommer L la liste des diviseurs de 1001.
2. Afficher L.
3. Afficher le premier terme de L.
4. Afficher le dernier terme de L.
5. Afficher la liste de tous les autres termes.

Exercice 7 — TP.
1. Définir le vecteur *ligne* $v := (1, 1, -4)$.

2. Définir la matrice

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

3. Multipliez les d'un coté puis de l'autre.
4. Quel est le noyau de A ?

Corrigé de l'exercice 1 :

```
a = 2
a
a == 2
```

Corrigé de l'exercice 2 :

```
5 + 2
5 * 2
5^2
5/2
5//2
5 % 2
```

Corrigé de l'exercice 3 :

```
1001.is_prime()
1001.divisors()
1001.gcd(1155)
1001.lcm(1155)
```

Corrigé de l'exercice 4 :

```
for i in [1..10] :
        print i
for n in [1..20] :
    a = 2^n-1
    if a.is_prime() :
        print a
```

Corrigé de l'exercice 5 :

```
def estpair(n) :
    return n%2==0
estpair(2) ; estpair(3)
```

Corrigé de l'exercice 6 :

```
L = 1001.divisors()
L
L[0]
L[-1]
L[1:-1]
```

Corrigé de l'exercice 7 :

```
v=vector([1,1,-4])
A = matrix([[1, 2, 3], [3, 2, 1], [1, 1, 1]])
v*A ; A*v
A.right_kernel()
```

Bibliographie

[CCM97] Gilles CHRISTOL, Anne COT et Charles-Michel MARLE. *Topologie*. Sous la direction d'ELLIPSES. 1997 (cf. page 137).

[Gob01] Rémi GOBLOT. *Algèbre Commutative*. 2e édition. Sciences Sup. Dunod, 2001 (cf. page 22).

[Gui13] Daniel GUIN. *Algèbre : Tome 2, Anneaux, modules et algèbre multilinéaire*. Enseignement sup. EDP Sciences, 2013 (cf. page 24).

[Kri07] Jean-Louis KRIVINE. *Théorie des ensembles*. 2e édition. Nouvelle bibliothéque mathématique Numéro 5. Paris : Cassini, 2007 (cf. page 13).

[Ulm12] Felix ULMER. *Théorie des groupes*. Références sciences. Ellipses, 2012 (cf. page 18).