Chapitre 5

Espaces vectoriels

Sommaire

5.1 Corps

On rappelle qu'un corps est un ensemble muni des quatre opérations usuelles (addition, soustraction, multiplication et division) qui satisfont les règles habituelles d'associativité, de commutativité et de distributivité.

5.1 **Définition (corps).** Un *corps* est un anneau dans lequel tout élément x différent de 0 admet un inverse x^{-1} tel que $x \cdot x^{-1} = x^{-1} \cdot x = 1$. L'opération de division et définie par $x/y := x \cdot y^{-1}$.

Un *corps commutatif* est corps dans lequel la multiplication est commutative. Dans ce cours, on ne considèrera que des corps commutatifs.

5.2 *Exemple.* L'ensemble $\mathbb{Q}$ des nombres rationnels, constitué des fractions de nombres entiers relatifs et muni des opérations usuelles, est un corps commutatif.

5.3 *Exemple.* L'ensemble des nombres décimaux, c'est-à-dire les nombres qui s'écrivent en base 10 avec un nombre fini de chiffres après la virgule, n'est *pas* un corps. Il s'agit bien d'un anneau parce que l'addition et la multiplication y ont les propriétés usuelles d'associativité, commutativité et distributivité, mais tous les éléments non nuls n'ont pas d'inverse. Par exemple, 4 a pour inverse $0,25$ mais 3 n'a pas d'inverse puisque celui-ci s'écrirait $0,3333\ldots$ avec une infinité de chiffres.

5.4 *Exemple.* L'ensemble $\mathbb{R}$ des nombres réels est un corps. Il contient le corps $\mathbb{Q}$ des nombres rationnels. Comme on l'a vu en analyse, sa propriété essentielle est que toute partie non vide et majorée y admet une borne supérieure. En conséquence il est complet, ce qui signifie que toute suite de Cauchy y est convergente, et une conséquence est que tout suite bornée y admet une sous-suite convergente. Ce n'est pas le cas dans $\mathbb{Q}$.

5.5 *Exemple.* L'ensemble $\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$ des nombres complexes est un corps. Rappelons que l'élément i est racine de l'équation $z^2 + 1 = 0$, qui n'a pas de solution dans $\mathbb{R}$, et que le corps des nombres complexes a été imaginé pour disposer d'une telle solution (et même de deux puisque $i^2 = (-i)^2 = -1$). L'addition s'effectue coordonnée par coordonné : si $z = x+iy$ et $z' = x' + iy'$, alors $z + z' = (x + x') + i(y + y')$. La multiplication s'effectue comme s'il s'agissait de nombres réels mais en appliquant la règle $i^2 = -1$, on obtient donc $zz' = (x + iy)(x' + iy') = (xx' - yy') + i(xy' + yx')$. La conjugaison complexe $\bar{z} = x - iy$, qui consiste à changer le signe de la partie imaginaire y, permet d'exprimer facilement l'inverse : $z\bar{z} = (x+iy)(x-iy) = x^2+y^2$ n'est pas nul si z n'est pas nul et par conséquent $z\bar{z}/(x^2 + y^2) = 1$, ainsi l'inverse de $z = x + iy$ est $z^{-1} = x/(x^2 + y^2) - iy/(x^2 + y^2)$.

On voit que $\mathbb{R}$ est un sous-corps de $\mathbb{C}$: si la composante y est nulle, les lois d'addition et de multiplication des nombres complexes sont simplement l'addition et la multiplication des nombres réels. Comme $\mathbb{R}$, le corps des nombres complexes est complet, et comme on l'a vu il possède en plus la propriété d'être *algébriquement clos*, c'est-à-dire que toute équation polynomiale y admet une solution, ce qui n'est pas le cas de $\mathbb{R}$.

5.6 *Exemple.* L'ensemble $\mathbb{Z}$ des entiers relatifs n'est *pas* un corps. En effet, aucun entier non nul n'a d'inverse dans $\mathbb{Z}$, exception faite de 1 et -1 qui sont leur propre inverse.

5.7 *Exemple.* L'ensemble $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p est un corps si p est un nombre premier. De façon générale, on sait que si n est un entier alors l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence modulo n forme un anneau : si a et b sont des entiers vérifiant $0 \leq a \leq n - 1$ et $0 \leq b \leq n - 1$, leurs classes de congruence

$$[a] = \{a + kn \mid k \in \mathbb{Z}\} \qquad\qquad [b] = \{b + kn \mid k \in \mathbb{Z}\}$$

s'additionnent et se multiplient :

$$[a] + [b] = \{a + b + kn \mid k \in \mathbb{Z}\} \qquad\qquad [a] \cdot [b] = \{ab + kn \mid k \in \mathbb{Z}\}.$$

Le zéro pour l'addition des classes modulo n est donc $[0] = \{kn \mid k \in \mathbb{Z}\} = n\mathbb{Z}$, la classe formée des multiples entiers de n. On vérifie que l'unité pour la multiplication est $[1] = \{1 + kn \mid k \in \mathbb{Z}\}$. Lorsque p est premier, si $[a] \neq 0$, alors a est premier avec p. D'après le théorème de Bézout, il existe donc $u, v \in \mathbb{Z}$ tels que $up + va = 1$, ainsi $[v] \cdot [a] = [1]$. On a donc démontré que tout élément non nul de $\mathbb{Z}$ possède un inverse modulo p. Ainsi $\mathbb{Z}/p\mathbb{Z}$ est bien un corps lorsque p est premier.

5.8 **Exercice.** Les équations $3x = 1$ et $2x = 1$ ont-elles des solutions dans $\mathbb{Z}/4\mathbb{Z}$? Mêmes questions dans $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

5.2 Espaces vectoriels

Les espaces vectoriels sont les objets d'étude fondamentaux de l'algèbre linéaire. Ils généralisent la notion géométrique de *vecteur* en retenant les propriétés essentielles que les vecteurs peuvent être additionnés entre eux et aussi multipliés par des un nombre réel quelconque. On peut en fait généraliser encore un peu et remplacer les nombres réels par n'importe quel autre corps et les propriétés fondamentales resteront les mêmes. Ceci dit, dans ce cours on s'intéressera principalement aux espaces vectoriels *réels*, c'est-à-dire sur le corps $\mathbb{R}$.

5.9 **Définition (espace vectoriel).** Un *espace vectoriel* E sur un corps $\mathbb{K}$ est un *groupe commutatif* (c'est-à-dire un ensemble non vide E muni d'une addition qui est associative et commutative, admet un élément neutre noté 0, et pour laquelle chaque élément $v \in E$ admet un opposé $-v$ tel que $v + (-v) = 0$) sur lequel *opère* le corps $\mathbb{K}$, c'est-à-dire que l'on peut multiplier tout *vecteur* $v \in E$ par un *scalaire* $\lambda \in \mathbb{K}$ et que le résultat de l'opération, noté λv, est un élément de E. On demande que les règles suivantes de compatibilité entre l'addition et la multiplication par un scalaire soient vérifiées :

associativité	$\lambda(\mu v) = (\lambda\mu)v$	pour tous $\lambda, \mu \in \mathbb{K}$ et $v \in E$
neutralité	$1v = v$	pour tout $v \in \mathbb{K}$
distributivité à gauche	$(\lambda + \mu)v = \lambda v + \mu v$	pour tous $\lambda, \mu \in \mathbb{K}$ et $v \in E$
distributivité à droite	$\lambda(v + w) = \lambda v + \lambda w$	pour tous $\lambda \in \mathbb{K}$ et $v, w \in E$

5.10 *Exemple.* Soit $E = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$. C'est un espace vectoriel sur $\mathbb{R}$ si on définit l'addition et la multiplication par un scalaire coordonnée par coordonnée :

$$(x, y) + (x', y') := (x + x', y + y') \qquad \lambda(x, y) := (\lambda x, \lambda y).$$

Cet exemple assez simple est très important pour deux raisons. La première est qu'il permet de visualiser la structure d'espace vectoriel : on imagine un plan muni des coordonnées cartésiennes habituelles. L'addition est celle des vecteurs et la multiplication par un scalaire consiste à appliquer une homothétie sur un vecteur. Pour un vecteur (x, y) fixé, l'ensemble $\{\lambda(x, y) \mid \lambda \in \mathbb{R}\}$ est représenté par la droite du plan passant par l'origine $(0, 0)$ et le vecteur (x, y) (à supposer qu'il soit distinct de l'origine).

La seconde raison est que l'on peut facilement généraliser cet exemple dans deux directions. D'une part on peut remplacer le corps $\mathbb{R}$ par un corps $\mathbb{K}$ quelconque et la construction fonctionne aussi bien, on obtient alors que $\mathbb{K} \times \mathbb{K}$ est un espace vectoriel sur $\mathbb{K}$. D'autre part peut considérer un nombre n quelconque de copies de $\mathbb{K}$: on pose

$$\mathbb{K}^n := \{(x_1, x_2, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{K}\},$$

on effectue l'addition coordonnée par coordonnée et on définit la multiplication par un scalaire par

$$\lambda(x_1, x_2, \ldots, x_n) := (\lambda x_1, \lambda x_2, \ldots, \lambda x_n).$$

On verra plus loin que tout espace vectoriel *de dimension finie* sur $\mathbb{K}$ est essentiellement de cette forme.

5.11 *Exemple.* Le corps $\mathbb{C}$ des nombres complexes est un espace vectoriel sur le corps $\mathbb{R}$. En effet, le sous-ensemble des nombres complexes $\{x + iy \mid x \in \mathbb{R}, y = 0\}$ s'identifie à $\mathbb{R}$, ainsi une opération $(\lambda, z) \mapsto \lambda z$ de $\mathbb{R} \times \mathbb{C}$ dans $\mathbb{C}$ vérifiant toutes les propriétés de compatibilité est automatiquement définie : on considère $\lambda \in \mathbb{R}$ comme nombre complexe $\lambda + i0$ et si $z = x + iy$, $\lambda z = (\lambda + i0)(x + iy) = \lambda x + i\lambda y$. La même construction fonctionne pour tout corps $\mathbb{L}$ qui contient un sous-corps $\mathbb{K}$: l'addition est celle de $\mathbb{L}$ et l'opération $(\lambda, z) \mapsto \lambda z$ de $\mathbb{K} \times \mathbb{L}$ dans $\mathbb{L}$ consiste simplement a considérer $\lambda \in \mathbb{K} \subset \mathbb{L}$ et à effectuer la multiplication λz des deux éléments de $\mathbb{L}$.

5.12 **Lemme.** *Dans tout espace vectoriel, pour tout vecteur v on a $0v = 0$ et $(-1)v = -v$, c'est-à-dire que multiplier un vecteur v quelconque par le scalaire 0 donne le vecteur nul et que le multiplier par le scalaire -1 donne l'opposé de v.*

Démonstration. Soit v un vecteur quelconque. Dans le corps $\mathbb{K}$ on a toujours $0 = 0 + 0$ donc par distributivité on a $0v = 0v + 0v$. Le vecteur $0v$ a un opposé $-0v$, on a donc $0 = 0v + (-0v) = (0v + 0v) + (-0v) = 0v + (0v + (-0v)) = 0v + 0 = 0v$. De plus on a toujours $1 + (-1) = 0$ donc $v + (-1)v = (1 + (-1))v = 0v = 0$, donc $(-v)$ est l'opposé de v. □

Ce lemme montre que le neutre et l'opposé dans $\mathbb{K}$, par leur action, donnent le neutre et l'opposé dans E. Cela peut sembler évident mais il convient quand même de l'établir puisque rien dans les propriétés que l'on demande dans la définition 5.9 n'impose que ce soit vrai.

5.13 *Exemple.* Soient a, b et c trois nombres réels, posons

$$E := \left\{(x, y, z) \in \mathbb{R}^3 \;\middle|\; ax + by + cz = 0\right\}.$$

L'ensemble E est un espace vectoriel sur $\mathbb{R}$ car c'est un sous-ensemble de l'espace vectoriel $\mathbb{R}^3$ et lorsque l'on applique l'addition de $\mathbb{R}^3$ à deux éléments de V on retrouve un élément de V : si (x, y, z) et (x', y', z') sont tels que $ax + by + cz = 0$ et $ax' + by' + cz' = 0$, alors on a $a(x+x')+b(y+y')+c(z+z') = 0$. De même, pour tout $\lambda \in \mathbb{R}$, on a $a\lambda x+b\lambda y+c\lambda z = 0$.

Cet exemple est important pour plusieurs raisons. On peut tout d'abord l'interpréter géométriquement : on identifie $\mathbb{R}^3$ à l'espace euclidien dans lequel nous vivons (en première approximation !) et l'équation définit alors le plan orthogonal au vecteur (a, b, c) (que l'on suppose différent de zéro sans quoi l'équation disparaît et $E = \mathbb{R}^3$) passant par l'origine. D'un point de vue plus algébrique, on a donc vérifié que les solutions de l'équation (linéaire homogène) $ax + by + cz = 0$ forment un espace vectoriel : en additionnant deux solutions on en retrouve une nouvelle, en multipliant une solution par un scalaire on en obtient une nouvelle. Ce sont ces deux propriétés qui rendent les espaces vectoriels si importants en mathématiques. Finalement, l'exemple est un cas particulier de sous-espace vectoriel qui fait l'objet de la définition suivante.

5.14 **Définition (sous-espace vectoriel).** Soit V un sous-ensemble non vide d'un espace vectoriel E sur un corps $\mathbb{K}$. Si chaque fois que l'on additionne dans E deux vecteurs v et w de V, on obtient encore un point de V, et si pour tout $\lambda \in \mathbb{K}$ et tout $v \in V$, le vecteur $\lambda v \in E$ est élément de V (en d'autre termes le sous-ensemble V est stable par les lois de E) alors V est lui-même un espace vectoriel, pour les mêmes lois que E. On dit que V est un *sous-espace vectoriel* de E.

5.15 *Exemple.* Dans $\mathbb{R}^2$, l'ensemble des vecteurs (x, y) tels que $y = 2x$ est un sous-espace vectoriel. Géométriquement, c'est la droite de pente 2 qui passe par l'origine. Plus généralement, toute droite passant par l'origine est un sous-espace vectoriel de $\mathbb{R}^2$.

5.16 *Exemple.* Dans $\mathbb{R}^2$, une droite ne passant pas par l'origine, par exemple la droite D d'équation $y = x + 1$, n'est pas un sous-espace vectoriel. En effet, elle n'est pas stable par multiplication par un scalaire : le point $(0, 1)$ est élément de D mais si on le multiplie par 2 on obtient $(0, 2)$ qui n'est pas élément de D puisqu'il ne satisfait pas l'équation.

5.17 On peut noter que la définition 5.14 entraîne qu'un sous-espace vectoriel V contient toujours le vecteur nul 0. En effet, il suffit de prendre n'importe quel élément de V (il en existe puisqu'on demande que V ne soit pas vide) et de le multiplier par le scalaire 0 pour obtenir le vecteur 0.

5.18 **Exercice.** Soit $\mathcal{D}^2$ l'ensemble des fonctions $f : \mathbb{R} \to \mathbb{R}$ qui sont deux fois dérivables. On définit point par point l'addition et la multiplication par un scalaire :

$$(f+g)(x) = f(x) + g(x) \qquad\qquad (\lambda f)(x) = \lambda f(x).$$

Vérifier que $\mathcal{D}^2$ est un espace vectoriel sur $\mathbb{R}$. Soit $V = \{f \in \mathcal{D}^2 \mid \forall x \in \mathbb{R}, f''(x) + f(x) = 0\}$. Démontrer que V est un sous-espace vectoriel de $\mathcal{D}^2$. Vérifier que les fonctions cos et sin sont des éléments de V. Peut-on trouver $f \in V$ telle que $f(0) = 2$ et $f(\pi/2) = -1$?

5.19 **Définition (combinaison linéaire).** Soit E un espace vectoriel sur un corps $\mathbb{K}$, soit X un sous-ensemble quelconque de E. Une *combinaison linéaire* d'éléments de X est un vecteur qui peut s'écrire sous la forme $\lambda_1 v_1 + \cdots + \lambda_n v_n$ où $\lambda_1, \ldots, \lambda_n$ sont des scalaires et $v_1, \ldots, v_n$ sont des éléments de X.

Une combinaison linéaire est donc un vecteur que l'on peut obtenir à partir des vecteurs de l'ensemble de départ au moyen d'additions et de multiplications par des scalaires.

Du fait des axiomes qui définissent la structure d'espace vectoriel (voir définition 5.9), tout vecteur obtenu à partir des vecteur de X au moyen d'additions et de multiplications par des scalaires peut être écrit comme une combinaison linéaire. Par exemple si $x, y, z \in X$, le vecteur $3(x + 5(2y + z))$ n'a pas la forme demandée par la définition 5.19, mais on a $3(x+5(2y+z)) = 3x+(3\times 5\times 2)y+(3\times 5)z = 3x+30y+15z$ qui est de la bonne forme.

5.20 **Définition (sous-espace engendré).** Soit E un espace vectoriel et soit X un sous-ensemble de E. On appelle sous-espace de E engendré par X l'ensemble $\mathrm{Vect}(X)$ des combinaisons linéaires d'éléments de X.

5.21 Il est facile de constater que $\mathrm{Vect}(X)$ est bien un sous-espace vectoriel de E, même si ce n'est pas demandé explicitement par la définition. En effet $\mathrm{Vect}(X)$ n'est pas vide puisqu'il contient 0 qui est la combinaison linéaire vide (obtenue en prenant $n = 0$ dans la définition 5.19), de plus il est stable par combinaisons linéaires d'après la remarque précédente.

5.22 **Théorème.** *Soit E un espace vectoriel et soit X un sous-ensemble de E. L'ensemble* $\mathrm{Vect}(X)$ *est le plus petit sous-espace vectoriel de E contenant X, c'est-à-dire que si V est un sous-espace vectoriel de E et si $X \subseteq V$ alors* $\mathrm{Vect}(X) \subseteq V$.

Démonstration. Soit v un élément de $\mathrm{Vect}(X)$. Par définition v est un combinaison linéaire $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$ d'éléments de X. Par hypothèse les v_i sont éléments de V donc leur combinaison linéaire v est élément de V d'après la définition d'un sous-espace vectoriel. □

Ce théorème signifie que le sous-espace vectoriel engendré par X peut être vu soit de façon explicite par les combinaisons linéaires, soit par sa propriété caractéristique d'être le plus petit sous-espace contenant X. Les deux visions sont utiles et l'une ou l'autre est utilisée selon le contexte.

5.23 **Définition (somme de sous-espaces).** Soit E un espace vectoriel et soient U et V deux sous-espaces de E. La *somme* de U et V est l'ensemble $U + V := \{u + v \mid u \in U, v \in V\}$.

5.24 **Exercice.** Montrer que la pour tous sous-espaces vectoriels U et V d'un espace E on a $U + V = \mathrm{Vect}(U \cup V)$.

5.25 **Exercice.** Montrer que l'intersection de deux sous-espaces vectoriels est un sous-espace vectoriel.

5.26 **Définition (somme directe).** Deux sous-espaces vectoriels U et V d'un espace vectoriel sont dits *en somme directe* si leur intersection $U \cap V$ ne contient que le vecteur nul. Dans ce cas, la somme $U + V$ est notée $U \oplus V$.

5.27 **Théorème.** *Soient U et V deux sous-espaces d'un espace vectoriel E qui sont en somme directe. Pour tout vecteur $x \in U \oplus V$ il existe un unique couple (u, v) de vecteurs tels que $u \in U$, $v \in V$ et $x = u + v$.*

Démonstration. L'existence d'une décomposition $x = u + v$ est immédiate par définition de la somme de sous-espaces vectoriels. Pour l'unicité, considérons deux décompositions $x = u+v$ et $x = u'+v'$ et montrons qu'elles doivent être identiques. Pour cela remarquons que l'on a $0 = x - x = (u+v) - (u'+v') = (u-u') + (v-v')$ donc $u - u' = v' - v$. Comme u et u' sont dans U, leur différence $u - u'$ est dans U. De même la différence $v' - v$ est dans V. Comme ces deux différences sont égales, elles sont élément de $U \cap V$, or cet ensemble ne contient que 0 donc $u - u' = 0$ et $v' - v = 0$, d'où on déduit $u = u'$ et $v = v'$. □

La définition de somme et de somme directe et ce théorème de décomposition se généralisent au cas d'un nombre quelconque de sous-espaces : si $(V_i)_{i\in I}$ est une famille de sous-espaces vectoriels de E, la somme $\sum_{i\in I} V_i$ est l'ensemble $\mathrm{Vect}\big(\bigcup_{i\in I} V_i\big)$. Cette somme est directe si pour tous $i, j \in I$ distincts on a $V_i \cap V_j = \{\emptyset\}$, on la note alors $\bigoplus_{i\in I} V_i$.

5.3 Applications linéaires

Les fonctions entre espaces vectoriels qui respectent la structure d'espace vectoriel sont appelées *applications linéaires*.

5.28 **Définition (application linéaire).** Soient E et F deux espaces vectoriels sur un même corps $\mathbb{K}$. Une fonction $f : E \to F$ est dite *linéaire* si elle préserve les deux opérations des espaces vectoriels, c'est-à-dire si pour tous $v, v' \in E$ et $\lambda \in \mathbb{K}$ on a

$$f(v + v') = f(v) + f(v'), \qquad\qquad f(\lambda v) = \lambda f(v).$$

Les expressions *application linéaire* et *morphisme (d'espaces vectoriels)* sont synonymes.

5.29 *Exemple.* Soit $a \in \mathbb{R}$. L'application $f : \mathbb{R} \to \mathbb{R}$ telle que $f(x) = ax$ pour tout x est linéaire. Son graphe dans $\mathbb{R}^2$ est une droite de pente a (orthogonale au vecteur $(a, -1)$) passant par 0.

5.30 *Exemple.* Les applications $f : x \mapsto x^2$ et $g : x \mapsto x+1$ (de $\mathbb{R}$ dans $\mathbb{R}$) ne sont *pas* linéaires. En effet, on a par exemple $f(1) = 1$ et $f(2) = 4$ donc $f(2 \times 1) \neq 2 \times f(1)$. De même on a $g(1) = 2$ et $g(2) = 3$ donc $g(2 \times 1) \neq 2 \times g(1)$.

5.31 *Exemple.* Soient $a, b \in \mathbb{R}$. L'application $f : \mathbb{R}^2 \to \mathbb{R}$ telle que $f(x, y) = ax + by$ pour tous x, y est linéaire. Son graphe est un plan passant par l'origine, orthogonal au vecteur $(a, b, -1)$.

5.32 *Exemple.* Soit E l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ qui sont infiniment dérivables. L'application $D : E \to E$ qui à chaque fonction f associe sa dérivée f' est linéaire. De même, l'évaluation en un point $a \in \mathbb{R}$, représentée par la fonction $E_a : E \mapsto \mathbb{R}$ telle que $E_a(f) = f(a)$ pour tout f, est une application linéaire.

5.33 **Théorème.** *Soient E et F deux espaces vectoriels sur un même corps $\mathbb{K}$. L'ensemble $\mathcal{L}(E, F)$ des applications linéaires de E dans F, muni des opérations usuelles, est un espace vectoriel sur $\mathbb{K}$.*

Démonstration. Les opérations d'addition et de multiplication par un scalaire sont définies point par point, c'est-à-dire que pour toutes fonctions f et g de E dans F, pour tout scalaire $\lambda \in \mathbb{K}$ et tout vecteur $x \in E$ on a par définition

$$(f+g)(x) = f(x) + g(x) \qquad\qquad (\lambda f)(x) = \lambda(f(x))$$

donc les propriétés des opérations voulues par la définition d'un espace vectoriel sont satisfaites dans l'ensemble F^E des fonctions de E dans F. Il reste simplement à montrer que $\mathcal{L}(E, F)$ est un sous-espace vectoriel de E^F, c'est-à-dire que la somme de deux applications linéaires est une application linéaire et que le produit d'un application linéaire par un scalaire est une application linéaire. Ces propriétés se vérifient très simplement en appliquant les définitions. □

5.34 **Exercice.** Soit E, F et G des espaces vectoriels sur un corps $\mathbb{K}$. Soient $f : E \to F$ et $g : F \to G$ des applications linéaires. Démontrer que la composée $g \circ f : E \to G$ est linéaire.

5.35 **Exercice.** Soient E et F des espaces vectoriels sur un corps $\mathbb{K}$. Soit $f : E \to F$, une application linéaire. Supposons que f est bijective. Démontrer que son inverse f^{-1} est aussi linéaire.

5.36 **Définition (image, noyau).** Soit $f : E \to F$ une application linéaire entre deux espaces vectoriels E et F sur un corps $\mathbb{K}$. L'*image* de f est l'ensemble des images par f des vecteurs de E :

$$\operatorname{Im}(f) := \{w \in F \mid \exists v \in E, f(v) = w\}.$$

Le *noyau* de f est l'ensemble

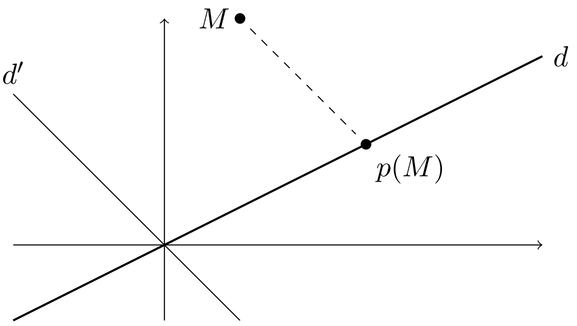
$$\operatorname{Ker}(f) := \{v \in E \mid f(v) = 0\}.$$

La notation Ker vient du fait que « noyau », dans ce contexte, se dit « kernel » en anglais.

5.37 *Exemple.* Reprenons le cas d'une application linéaire $f(x) = ax$ de $\mathbb{R}$ dans $\mathbb{R}$. Si a n'est pas nul, alors pour tout réel y on a $f(y/a) = y$ donc f est surjective, c'est-à-dire que son image est $\mathbb{R}$. De plus, pour tout x, on a $f(x) = 0$ si et seulement si $ax = 0$ si et seulement si $x = 0$ donc 0 est le seul élément dont l'image est 0, c'est-à-dire que le noyau de f est le singleton $\{0\}$.

5.38 *Exemple.* La fonction $g : \mathbb{R}^2 \to \mathbb{R}^2$ définie par $g(x, y) = (x, 0)$ peut être vue géométriquement comme la projection orthogonale sur l'axe des abscisses. Il est clair que l'image de g est l'ensemble des points $(x, 0)$ pour toutes les valeurs possibles de x, c'est-à-dire que $\operatorname{Im}(g) = \{(x, 0) \mid x \in \mathbb{R}\}$, autrement dit l'image de g est l'axe des abscisses. De plus un vecteur (x, y) est envoyé sur 0 par g si et seulement si on a $x = 0$, c'est-à-dire que $\operatorname{Ker}(g) = \{(0, y) \mid y \in \mathbb{R}\}$, autrement dit le noyau de g est l'axe des ordonnées.

5.39 *Exemple.* On peut généraliser l'exemple précédent à n'importe quelle projection.



Considérons deux droites d et d' passant par l'origine et définissons la fonction p comme étant la projection sur d parallèlement à d'. Par un raisonnement de géométrie élémentaire on peut établir que la fonction p est une application linéaire du plan dans lui-même. Son image est la droite d par construction, son noyau est l'ensemble des points envoyés sur l'origine, c'est-à-dire l'axe de projection d'.

Notons que si la droite d ne passait pas par l'origine, alors la projection ne serait pas une application linéaire, notamment parce que le vecteur nul (c'est-à-dire l'origine) ne serait pas envoyé sur lui-même. En revanche le fait que d' passe par l'origine est sans importance puisqu'on ne considère que sa direction ; le noyau de la projection est simplement la parallèle à d' passant par l'origine.

5.40 *Exemple.* Soit E l'espace vectoriel de toutes les fonctions de $\mathbb{R}$ dans $\mathbb{R}$ et soit $\phi : E \to E$ l'opération qui à chaque fonction $f : \mathbb{R} \to \mathbb{R}$ associe la fonction $\phi(f) : \mathbb{R} \to \mathbb{R}$ telle que $\phi(f)(x) = f(x) + f(-x)$. Alors on peut facilement se rendre compte que l'image de ϕ est l'ensemble des fonctions paires (c'est-à-dire telles que $f(-x) = f(x)$) et que son noyau est l'ensemble des fonctions impaires (c'est-à-dire telles que $f(-x) = -f(x)$).

5.41 **Exercice.** Démontrer que le noyau et l'image d'une application linéaire $f : E \to F$ sont des sous-espaces vectoriels de E et F respectivement.

5.42 **Théorème.** *Une application linéaire f est injective si et seulement si* $\mathrm{Ker}(f) = \{0\}$.

Démonstration. Supposons que f est injective. Comme on a toujours $f(0) = 0$ par linéarité, pour tout $v \in E$ on a $f(v) = 0$ si et seulement si $f(v) = f(0)$ si et seulement si $v = 0$ par injectivité, donc $\mathrm{Ker}(f) = \{0\}$. Réciproquement, supposons $\mathrm{Ker}(f) = \{0\}$ et considérons deux vecteurs $v, w \in E$ tels que $f(v) = f(w)$. Par linéarité on a $f(v - w) = f(v) - f(w) = 0$ donc $v - w \in \mathrm{Ker}(f)$, par conséquent $v - w = 0$ donc $v = w$, ce qui prouve que f est injective. □

5.43 **Théorème.** *Une application linéaire f à valeurs dans un espace vectoriel F est surjective si et seulement si* $\mathrm{Im}(f) = F$.

Démonstration. Par définition. □

Ainsi le noyau et l'image donnent des indications générales sur les propriétés des applications linéaires. On verra par la suite qu'ils permettent de décrire des propriétés bien plus précise que la simple surjectivité ou injectivité.

5.44 **Définition (endomorphisme).** Un *endomorphisme* d'un espace vectoriel E est une application linéaire de E dans lui-même.

5.45 **Définition (isomorphisme).** Un *isomorphisme* d'une espace vectoriel E dans un espace vectoriel F est une application linéaire qui est bijective.

5.4 Indépendance linéaire

5.46 **Définition (indépendance linéaire).** Une famille finie de vecteurs $v_1, \ldots, v_n$ d'un espace vectoriel E sur un corps $\mathbb{K}$ est *linéairement indépendante* ou *libre* si pour toute famille de scalaires $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$,

$$\lambda_1 v_1 + \ldots \lambda_n v_n = 0 \qquad \text{implique} \qquad \lambda_1 = \cdots = \lambda_n = 0.$$

Un famille infinie de vecteurs est linéairement indépendante si toute sous-famille finie cette famille est linéairement indépendante.

Une famille de vecteurs qui n'est pas linéairement indépendante est appelée *linéairement dépendante* ou *liée*.

5.47 C'est-à-dire que des vecteurs $v_1, \ldots, v_n$ sont indépendants si la seule manière d'obtenir 0 en les combinant linéairement est de tous les multiplier par 0. Une conséquence importante est que dans ce cas toute combinaison linéaire de $v_1, \ldots, v_n$ s'écrit de façon unique sous la forme $\lambda_1 v_1 + \cdots + \lambda_n v_n$.

Illustrons cela sur des exemples. Attention à bien distinguer le vecteur $0 \in E$ et le scalaire $0 \in \mathbb{K}$ dans la définition ci-dessus et dans les exemples suivants.

5.48 *Exemple.* Dans $\mathbb{R}^2$, les trois vecteurs $(1,0), (0,1), (1,1)$ ne sont pas indépendants. En effet, on a $1(1,0)+1(0,1)+(-1)(1,1) = (0,0)$ or $(0,0)$ est le vecteur nul de $\mathbb{R}^2$ et les coefficients $1, 1, -1$ ne sont pas nuls.

Par contre les deux vecteurs $(1,0), (0,1)$ sont indépendants. En effet, si $\lambda_1(1,0) + \lambda_2(0,1) = (0,0)$, alors on a $(\lambda_1, \lambda_2) = (0,0)$ donc $\lambda_1 = \lambda_2 = 0$.

5.49 **Exercice.** Démontrer que trois vecteurs $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ de $\mathbb{R}^2$ ne peuvent jamais être linéairement indépendants.

5.50 **Exercice.** Démontrer que les fonctions cos et sin, en tant que vecteurs de l'espace $\mathcal{D}^2$ (voir l'exercice 5.18) sont linéairement indépendantes.

5.51 **Exercice.** Démontrer que les vecteurs 1 et i dans $\mathbb{C}$ vu comme espace vectoriel sur $\mathbb{R}$ sont linéairement indépendants.

5.52 On peut reformuler l'indépendance linéaire dans quelques cas simples :

- la famille vide est toujours linéairement indépendante ;
- une famille réduite à un seul vecteur est indépendante, sauf si ce vecteur est nul ;
- deux vecteurs forment une famille libre si et seulement si ils ne sont pas colinéaires (c'est-à-dire proportionnels).

Cette dernière propriété se généralise à une famille quelconque en disant qu'une famille est linéairement indépendante si et seulement si aucun de ses éléments n'est combinaison linéaire des autres. En particulier, une famille qui contient le vecteur nul n'est jamais linéairement indépendante.

5.53 *Exemple.* Soit $E = \mathbb{K}[X]$, l'ensemble des polynômes d'indéterminée X à coefficients dans $\mathbb{K}$. C'est un espace vectoriel sur $\mathbb{K}$. La famille

$$M := \{1, X, X^2, \ldots, X^n, \ldots\}$$

des monômes de $\mathbb{K}[X]$ est une famille infinie de vecteurs linéairement indépendante. En effet, si $\{X^{i_1}, X^{i_2}, \dots, X^{i_n}\}$ est un sous-ensemble fini de M, alors l'équation $\lambda_{i_1} X^{i_1} + \lambda_{i_2} X^{i_2} + \cdots + \lambda_{i_n} X^{i_n} = 0$ implique que $\lambda_{i_1} = \cdots = \lambda_{i_n} = 0$.

5.54 **Définition (base d'un espace vectoriel).** Soit E un espace vectoriel sur un corps $\mathbb{K}$. Une base de E est une famille $(v_i)_{i \in I}$ de vecteurs qui est libre et génératrice pour E (c'est-à-dire que $\mathrm{Vect}(\{v_i \mid i \in I\}) = E$).

5.55 *Exemple.* Dans l'espace vectoriel $\mathbb{R}^2$, les vecteurs $(1, 0)$ et $(0, 1)$ forment une base. C'est même la base dite *canonique* : c'est la plus simple et sa définition est naturelle.

La famille de vecteurs $\{(1, 1), (1, -1)\}$ est aussi une base de $\mathbb{R}^2$. En revanche, la famille à trois éléments $\{(1, 0), (0, 1), (1, 1)\}$ n'est pas une base de $\mathbb{R}^2$ parce que ce n'est pas une famille libre, et la famille réduite au seul vecteur $(1, 0)$ n'est pas une base parce qu'elle n'est pas génératrice pour $\mathbb{R}^2$.

5.56 *Exemple.* L'ensemble des monômes $\{X^n \mid n \in \mathbb{N}\}$ est la base canonique de $\mathbb{R}[X]$. L'ensemble de polynômes $\{(X + 1)^n \mid n \in \mathbb{N}\}$ est aussi une base de $\mathbb{R}[X]$.

5.57 **Théorème.** *Soit E un espace vectoriel sur un corps $\mathbb{K}$, soit $(v_i)_{i \in I}$ une famille de vecteurs de E. Les conditions suivantes sont équivalentes :*

1. *La famille $(v_i)_{i \in I}$ est une base de E.*
2. *La famille $(v_i)_{i \in I}$ est une famille libre maximale, c'est-à-dire que toute famille qui contient tous les v_i est au moins un vecteur de plus est nécessairement liée.*
3. *La famille $(v_i)_{i \in I}$ est une famille génératrice minimale, c'est-à-dire qu'une famille obtenue à partir de $(v_i)_{i \in I}$ en supprimant au moins un vecteur ne peut pas être génératrice.*
4. *Tout vecteur $w \in E$ s'écrit de façon unique comme une combinaison linéaire d'éléments de la famille $(v_i)_{i \in I}$.*

Démonstration. On commence par le cas d'une famille finie $(v_1, \dots, v_n)$.

1 implique 2. Supposons que $(v_1, \dots, v_n)$ est une base de E et considérons un vecteur v_{n+1} quelconque. Comme $(v_1, \dots, v_n)$ est une famille génératrice de E on peut écrire $v_{n+1} = \lambda_1 v_1 + \cdots + \lambda_n v_n$ pour une certaine famille $(\lambda_1, \dots, \lambda_n)$. En posant $\lambda_{n+1} = -1$ on a alors $\lambda_1 v_1 + \cdots + \lambda_{n+1} v_{n+1} = 0$ or la famille $(\lambda_1, \dots, \lambda_{n+1})$ n'est pas nulle (puisque $\lambda_{n+1} \neq 0$) donc la famille $(v_1, \dots, v_{n+1})$ n'est pas libre.

2 implique 3. Supposons que $(v_1, \dots, v_n)$ est une famille libre maximale. Soit w un vecteur quelconque de E. Si w n'était pas combinaison linéaire de $(v_1, \dots, v_n)$ alors la famille $(v_1, \dots, v_n, w)$ serait libre, or c'est impossible par hypothèse, donc la famille $(v_1, \dots, v_n)$ est génératrice. De plus, un sous-famille $(v_1, \dots, v_{n-1})$ ne peut pas être génératrice puisque, par indépendance linéaire, v_n n'est pas combinaison linéaire de $(v_1, \dots, v_{n-1})$. La famille est donc génératrice minimale.

3 implique 4. Supposons que $(v_1, \dots, v_n)$ est une famille génératrice minimale et considérons un vecteur $w \in E$. Comme la famille est génératrice, il existe au moins une écriture $w = \lambda_1 v_1 + \cdots + \lambda_n v_n$. Supposons qu'il existe une autre écriture $w = \mu_1 v_1 + \cdots + \mu_n v_n$, distincte de la première. Il existe donc un i pour lequel $\lambda_i \neq \mu_i$; quitte à changer l'ordre des vecteurs on supposera que c'est n, donc que $\lambda_n \neq \mu_n$. Remarquons que l'on a $(\lambda_1 - \mu_1) v_1 + \cdots + (\lambda_n - \mu_n) v_n = w - w = 0$, on a donc $(\mu_n - \lambda_n)v_n = (\lambda_1 - \mu_1)v_1 + \cdots + (\lambda_{n-1} - \mu_{n-1})v_{n-1}$ d'où on peut déduire $v_n = \Sigma_{i=1}^{n-1}(\lambda_i - \mu_i)/(\mu_n - \lambda_n) \cdot v_i$ puisque $\mu_n - \lambda_n \neq 0$, c'est-à-dire que v_n est combinaison linéaire de $(v_1, \ldots, v_{n-1})$. En conséquence, $(v_1, \ldots, v_{n-1})$ est une famille génératrice, ce qui contredit l'hypothèse. Donc l'écriture $w = \lambda_1 v_1 + \cdots + \lambda_n v_n$ est unique.

4 implique 1. Supposons que tout vecteur $w \in E$ s'écrit de façon unique comme une combinaison linéaire de $(v_1, \ldots, v_n)$. L'existence d'une telle écriture pour tout vecteur signifie, par définition, que la famille est génératrice. Pour montrer que la famille est libre, supposons que l'on ait $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ pour une certaine famille $(\lambda_1, \ldots, \lambda_n)$. Comme on a $0v_1 + \cdots + 0v_n = 0$, par unicité de l'écriture on en déduit $\lambda_i = 0$ pour chaque i, donc la famille est libre.

On a donc établi l'équivalence entre les quatre énoncés, dans le cas fini. L'équivalence se généralise directement au cas général du fait de la définition de l'indépendance linéaire et des combinaisons linéaires dans le cas infini. □

5.58 **Exercice.** Soit $(v_1, \ldots, v_n)$ une base d'un espace vectoriel E. Démontrer que pour tout scalaire λ non nul, $(\lambda v_1, v_2, \ldots, v_n)$ est encore une base de E. En déduire que plus généralement, si $\lambda_1, \ldots, \lambda_n$ sont des scalaires non nuls, alors $(\lambda_1 v_1, \ldots, \lambda_n v_n)$ est encore une base de E.

5.59 **Exercice.** Démontrer que les deux vecteurs 1 et i de $\mathbb{C}$ forment une base de $\mathbb{C}$ considéré comme espace vectoriel sur $\mathbb{R}$.

5.60 *Exemple.* Les vecteurs $(1, 1)$ et $(-1, 1)$ de $\mathbb{R}^2$ forment un base de $\mathbb{R}^2$. En effet la condition 4 du théorème 5.57 est bien vérifiée puisque l'équation

$$(x_1, x_2) = y_1(1, 1) + y_2(-1, 1),$$

est équivalente au système d'équations linéaires

$$\begin{cases} x_1 = y_1 - y_2 \\ x_2 = y_1 + y_2 \end{cases}$$

et que ce système possède une unique solution qui est $y_1 = (x_1 + x_2)/2$, $y_2 = (x_2 - x_1)/2$.

5.61 **Exercice.** Soit E un espace vectoriel sur un corps $\mathbb{K}$. Soit $(e_1, \ldots, e_m)$ une famille de vecteurs de E qui sont linéairement indépendants. Soit V le sous-espace de E engendré par l'ensemble $\{e_1, \ldots, e_m\}$. Démontrer que $(e_1, \ldots, e_m)$ est une base de V. On pourra appliquer la condition 4 du théorème 5.57.

5.62 **Exercice.** Soit E un espace vectoriel et soient U et V des sous-espaces vectoriels de E tels que $E = U \oplus V$. Soient $(u_1, \ldots, u_m)$ une base de U et $(v_1, \ldots, v_n)$ une base de V. Démontrer que $(u_1, \ldots, u_m, v_1, \ldots, v_n)$ est une base de E.

5.5 Dimension finie

Dans le cas où un espace vectoriel a une base composée d'une famille finie de vecteurs, on dit que l'espace est *de dimension finie*. Dans ce cas, par le théorème de caractérisation des bases, tout vecteur peut s'écrire d'une unique façon comme combinaison linéaire des vecteurs de la base (c'est la condition 4). Les coefficients de cette combinaison linéaire sont appelés les *coordonnées* du vecteur dans la base considérée. On montre alors que tout peut se ramener à la manipulation des coordonnées, une fois qu'on a choisi une base.

5.63 **Lemme.** *Soit* $(e_1, \ldots, e_n)$ *une base d'un espace vectoriel* E *sur un corps* $\mathbb{K}$. *L'application* $C : E \to \mathbb{K}^n$ *qui à chaque vecteur* $v \in E$ *associe l'unique* n*-uplet* $(x_1, \ldots, x_n) \in \mathbb{K}^n$ *tel que* $v = x_1 e_1 + \cdots + x_n e_n$ *est une application linéaire bijective.*

Démonstration. Soient deux vecteurs $v, w \in E$, notons $C(v) = (x_1, \ldots, x_n)$ et $C(w) = (y_1, \ldots, y_n)$. On a par construction $v = x_1 e_1 + \cdots + x_n e_n$ et $w = y_1 e_1 + \cdots + y_n e_n$ donc $v + w = (x_1 + y_1)e_1 + \cdots + (x_n + y_n)e_n$, par définition de C et par unicité de l'écriture on a donc $C(v + w) = (x_1 + y_1, \ldots, x_n + y_n)$. Par le même argument on montre que pour tout scalaire λ on a $C(\lambda v) = (\lambda x_1, \ldots, \lambda x_n)$. On a donc établi que C est linéaire. Par unicité de l'écriture, comme $0e_1 + \cdots + 0e_n = 0$, on a $\mathrm{Ker}(C) = \{0\}$, donc C est injective d'après le théorème 5.42. Pour la surjectivité, il suffit de remarquer que tout vecteur $(x_1, \ldots, x_n) \in \mathbb{K}^n$ a pour antécédent la combinaison linéaire $x_1 e_1 + \cdots + x_n e_n$. □

Une des conséquences les plus utiles du théorème de caractérisation des bases concerne la définition des applications linéaires : une application linéaire est entièrement définie par son action sur une base.

5.64 **Théorème.** *Soient* E *et* F *des espaces vectoriels. Soient* $(e_1, \ldots, e_n)$ *une base de* E *et* $(v_1, \ldots, v_n)$ *des vecteurs de* F. *Il existe une unique application linéaire* $f : E \to F$ *telle que pour chaque* i *on ait* $f(e_i) = v_i$.

Démonstration. Pour l'existence, on considère l'application C des coordonnées (donnée par le lemme précédent). L'application $f_c : \mathbb{K}^n \to F$ définie par $f_c(x_1, \ldots, x_n) = x_1 v_1 + \cdots + x_n v_n$ est clairement linéaire et la fonction $f_c \circ C$ a la propriété voulue puisque pour chaque i on a $C(e_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$ avec le 1 en i-ème position et donc $f_c(C(e_i)) = v_i$.

Pour l'unicité, soit une application linéaire $g : E \to F$ telle que $g(e_i) = v_i$ pour chaque i, montrons que $g = f_c \circ C$. Pour simplifier, posons $f = f_c \circ C$. Il suffit donc de montrer que $f - g$ est l'application nulle. Pour chaque i, on a par construction $f(e_i) = v_i$ et par hypothèse $g(e_i) = v_i$, donc $(f - g)(e_i) = 0$. Tout vecteur $v \in E$ peut s'écrire $x_1 e_1 + \cdots + x_n e_n$ et on a donc $(f - g)(v) = x_1(f - g)(e_1) + \cdots + x_n(f - g)(e_n) = x_1 0 + \cdots + x_n 0 = 0$, ainsi $f - g = 0$ et $f = g$. □

On va maintenant établir le premier théorème fondamental des espaces vectoriels de dimension finie, selon lequel deux bases finies d'un même espace vectoriel ont toujours le même nombre d'éléments. C'est ce nombre d'éléments que l'on appelle la *dimension* de l'espace.

5.65 **Lemme.** *Si un espace vectoriel* E *a une famille génératrice de* n *vecteurs, alors toute famille de strictement plus de* n *vecteurs de* E *est liée.*

Démonstration. On démontre par récurrence sur n la propriété « pour tout espace vectoriel E et toute famille génératrice $(g_1, \ldots, g_n)$ de E, pour tout $m > n$, toute famille $(v_1, \ldots, v_m)$ de vecteurs de E est liée ». Le cas $n = 0$ correspond à $E = \{0\}$ et le résultat est alors vrai puisqu'une famille qui contient le vecteur nul est toujours liée.

Pour l'étape de récurrence, supposons le résultat vrai pour un entier $n \in \mathbb{N}$ donné. Soient $(g_1, ..., g_{n+1})$ une famille génératrice d'un espace vectoriel E et $(v_1, ..., v_m)$ une famille de vecteurs de E, avec $m > n+1$. Pour tout i tel que $1 \leq i \leq m$, il existe une décomposition $v_i = x_{i,1}g_1 + \cdots + x_{i,n+1}g_{n+1}$ (pas nécessairement unique). On distingue alors deux cas.

Si pour chaque i on a $x_{i,n+1} = 0$, alors on a $v_i \in \mathrm{Vect}(g_1, ..., g_n)$ pour chaque i. Par hypothèse de récurrence, appliquée à l'espace $\mathrm{Vect}(g_1, ..., g_n)$ et la famille génératrice $(g_1, \ldots, g_n)$, on en déduit que la famille $(v_1, \ldots, v_m)$ est liée.

Sinon il existe un i tel que $x_{i,n+1} \neq 0$. Quitte à renuméroter les éléments de la famille $(v_1, \ldots, v_m)$, on peut supposer $i = m$ donc $x_{m,n+1} \neq 0$. On a alors $g_{n+1} = (1/x_{m,n+1})(v_m - x_{m,1}g_1 - \cdots - x_{m,n}g_n)$. Pour chaque $i < m$ on a donc

$$\begin{aligned} v_i &= x_{i,1}g_1 + \cdots + x_{i,n}g_n + \frac{x_{i,n+1}}{x_{m,n+1}}(v_m - x_{m,1}g_1 - \cdots - x_{m,n}g_n) \\ v_i - \frac{x_{i,n+1}}{x_{m,n+1}}v_m &= x_{i,1}g_1 + \cdots + x_{i,n}g_n - \frac{x_{i,n+1}}{x_{m,n+1}}(x_{m,1}g_1 + \cdots + x_{m,n}g_n). \end{aligned}$$

Posons alors $w_i = v_i - (x_{i,n+1}/x_{m,n+1})v_m$ pour chaque $i < m$, de sorte que l'on a $w_i \in \mathrm{Vect}(g_1, \ldots, g_n)$. Par hypothèse de récurrence, on en déduit que la famille $(w_1, \ldots, w_{m-1})$ est liée, il existe donc une famille $(\lambda_1, \ldots, \lambda_{m-1})$ dont les éléments ne sont pas tous nuls et telle que $\lambda_1 w_1 + \cdots + \lambda_{m-1}w_{m-1} = 0$. En remplaçant chaque w_i par sa définition, on en déduit un λ_m tel que $\lambda_1 v_1 + \cdots + \lambda_m v_m = 0$, ce qui prouve que la famille $(v_1, \ldots, v_m)$ est liée. □

5.66 **Théorème (unicité de la dimension).** *Soit E un espace vectoriel. Supposons qu'il existe une base de E constituée de n vecteurs. Alors toute base de E est constituée de n vecteurs. Cet entier n est appelé* dimension *de E et est noté* $\dim E$.

Démonstration. Soient $(e_1, \ldots, e_m)$ et $(f_1, \ldots, f_n)$ deux bases d'en espace vectoriel E. Par définition, la famille $(e_1, \ldots, e_m)$ est génératrice de E et la famille $(f_1, \ldots, f_n)$ est libre, on a donc $n \leq m$, puisque si on avait $n > m$, par le lemme 5.65 la famille $(f_1, \ldots, f_n)$ serait liée. En appliquant le même argument en échangeant le rôle des familles $(e_1, \ldots, e_m)$ et $(f_1, \ldots, f_n)$, on en déduit que l'on a aussi $m \leq n$. Par conséquent on a $m = n$. □

La dimension $\dim E$ d'un espace vectoriel E est donc par définition le cardinal de chacune de ses bases. S'il n'existe pas de base de cardinal fini, alors on dit que E est de *dimension infinie.*

5.67 On peut noter qu'un espace vectoriel est de dimension nulle si et seulement si il est réduit au seul vecteur nul 0, c'est-à-dire que $\dim(E) = 0$ si et seulement si $E = \{0\}$. Bien sûr, E n'est pas vide, puisqu'un espace vectoriel n'est jamais vide.

5.68 **Théorème (de la base incomplète).** *Soient E un espace vectoriel de dimension n, $(g_1, \ldots, g_m)$ une famille génératrice de E et $(v_1, \ldots, v_k)$ une famille libre de E. Alors $k \leq n$ et il existe des vecteurs $v_{k+1}, \ldots, v_n \in \{g_1, \ldots, g_m\}$ tels que $(v_1, \ldots, v_n)$ soit une base de E.*

Démonstration. D'après le théorème 5.66, le fait que la famille $(v_1, \ldots, v_k)$ soit libre implique $k \leq n$, donc $n - k$ est un entier positif. On procède par alors par récurrence sur $n - k$.

Le cas initial correspond à $n-k=0$ donc $n=k$. Comme toute famille de strictement plus de n vecteurs de E est liée, la famille libre $(v_1,\dots,v_k)$ est maximale, c'est donc une base d'après le théorème 5.57.

Pour l'étape de récurrence, supposons que le résultat soit vrai pour tous n,k tels que $n-k=p$ pour un entier p donné, et considérons un couple n,k avec $n-k=p+1$. Si la famille $(v_1,\dots,v_k)$ était génératrice de E, alors ce serait une base et on aurait $k=n$ d'après le théorème 5.66, ce qui contredit $n-k=p+1$. Par conséquent la famille n'est pas génératrice de E, or la famille $(g_1,\dots,g_n)$ est génératrice de E donc il existe un vecteur $v_{k+1}\in\{g_1,\dots,g_n\}$ qui n'est pas combinaison linéaire de $(v_1,\dots v_k)$. La famille $(v_1,\dots,v_{k+1})$ est donc libre et on a $n-(k+1)=n-k-1=p+1-1=p$, on peut donc lui appliquer l'étape de récurrence, ce qui donne une base $(v_1,\dots,v_n)$ de E. □

Ce théorème peut aussi être démontré sans l'hypothèse de dimension finie pour E, mais il se démontre alors de façon beaucoup plus abstraite (en utilisant l'axiome du choix) et n'est utile que dans des situations elles aussi très abstraites. Dans ce cours, on n'aura besoin que du cas fini.

5.69 **Corollaire.** *De toute famille génératrice d'un espace vectoriel de dimension finie on peut extraire une base.*

Démonstration. Il suffit d'appliquer le théorème de la base incomplète à la famille génératrice considérée et à la famille vide, qui est toujours libre. □

La dimension est en quelque sorte la bonne notion de « taille » pour un espace vectoriel. En effet, considérer le cardinal d'un espace vectoriel a en général peu d'intérêt (tous les espaces vectoriels se dimension finie ont le même cardinal dès que le corps de base est infini), mais considérer la dimension permet de retrouver des propriétés similaires à celles que l'on connaît sur le cardinal des ensembles finis.

5.70 **Théorème.** *Soit E un espace vectoriel de dimension finie et soit $V\subseteq E$ un sous-espace vectoriel de E. Alors*

— *V est de dimension finie et* $\dim V\le\dim E$ *;*
— *si* $\dim V=\dim E$ *alors $V=E$.*

Démonstration. Toute famille libre $(v_1,\dots,v_k)$ dans V est une famille libre de E puisque V est un sous-espace de E. Comme E est de dimension finie, on a alors toujours $k\le\dim E$. Considérons alors une telle famille libre $(v_1,\dots,v_k)$ de cardinal le plus grand possible. Il s'agit donc d'une famille libre maximale de V (sinon on pourrait ajouter un vecteur et avoir une famille libre de cardinal $k+1$), donc c'est une base de V d'après le théorème 5.57. Par conséquent V est de dimension finie et on a $\dim V=k\le\dim E$. Par le théorème de la base incomplète, on peut compléter la base $(v_1,\dots,v_k)$ de V en une base $(v_1,\dots,v_n)$ de E, or si $k=n$ les deux familles sont égales donc la base $(v_1,\dots,v_k)$ de V est génératrice de E et par conséquent $V=E$. □

5.71 **Théorème.** *Soit E un espace vectoriel et soient U et V deux sous-espaces vectoriels de E de dimension finie. Alors*

— *$U\cap V$ est de dimension finie et* $\dim(U\cap V)\le\min(\dim U,\dim V)$,
— *$U+V$ est de dimension finie et* $\dim(U+V)=\dim U+\dim V-\dim(U\cap V)$,
— *si U et V sont en somme directe, alors* $\dim(U\oplus V)=\dim U+\dim V$.

Démonstration. Le fait que $U \cap V$ soit de dimension finie et inférieure à $\dim U$ et à $\dim V$ est une conséquence immédiate du théorème précédent, puisque $U \cap V$ est un sous-espace vectoriel de U et aussi de V.

Dans le cas de la somme $U + V$, considérons une base $(e_1, \ldots, e_m)$ de $U \cap V$ (qui est donc de dimension finie). Comme U est de dimension finie et $U \cap V \subseteq U$, on peut étendre cette base en une base $(e_1, \ldots, e_n)$ de U avec $n \geq m$, grâce au théorème de la base incomplète. De même, on peut l'étendre en une base $(e_1, \ldots, e_m, v_1, \ldots, v_p)$ de V, avec $p \geq 0$. Par construction, la famille $(e_1, \ldots, e_n, v_1, \ldots, v_p)$ est génératrice de $U + V$.

Pour montrer qu'elle est libre, considérons une combinaison linéaire $x_1 e_1 + \cdots + x_n e_n + y_1 v_1 + \cdots + y_p v_p = 0$ et montrons que les coefficients sont tous nuls. Posons $u = x_1 e_1 + \cdots + x_n e_n$ et $v = y_1 v_1 + \cdots + y_p v_p = 0$ de sorte que l'hypothèse est $u + v = 0$ alors on a $u = -v$ or par construction $v \in V$ et $u \in U$ donc $v \in U \cap V$. Par conséquent v peut s'écrire $z_1 e_1 + \cdots + z_m e_m$ puisque $(e_1, \ldots, e_m)$ est une base de $U \cap V$. On a donc $v = z_1 e_1 + \cdots + z_m e_m + 0 v_1 + \cdots + 0 v_p = 0 e_1 + \cdots + 0 e_m + y_1 v_1 + \cdots + y_p v_p$, or la décomposition de v dans la base $(e_1, \ldots, e_n, v_1, \ldots, v_p)$ est unique donc on a $y_1 = \cdots = y_p = 0$. On en déduit que $v = 0$ donc $u = 0$ et par conséquent $x_1 e_1 + \cdots + x_n e_n = 0$, or la famille $(e_1, \ldots, e_n)$ est libre donc $x_1 = \cdots = x_n = 0$.

Ainsi la famille $(e_1, \ldots, e_n, v_1, \ldots, v_p)$ est libre, c'est donc une base de $U + V$. On en déduit que $\dim(U + V) = n + p$ or par construction on a $\dim U = n$, $\dim V = m + p$ et $\dim(U \cap V) = m$ donc on a bien $\dim(U + V) = n + p = n + (m + p) - m = \dim U + \dim V - \dim(U \cap V)$.

Le cas de la somme directe est une conséquence immédiate puisque dans ce cas on a $U \cap V = \{0\}$ donc $\dim(U \cap V) = 0$. L'exercice 5.62 permet aussi d'obtenir le résultat directement. □

5.72 **Exercice.** Soient E un espace vectoriel de dimension finie et U un sous-espace vectoriel de E. Montrer qu'il existe un sous-espace vectoriel V de E tel que $E = U \oplus V$. Un tel sous-espace est un *supplémentaire* de U dans E.

La dimension permet aussi de donner des propriétés des applications linéaires. Une mesure instructive dans ce cas est la dimension de l'image d'une application linéaire.

5.73 **Définition (rang).** Le rang d'une application linéaire f est $\dim(\operatorname{Im} f)$, la dimension de son image. On le note aussi $\operatorname{rg} f$.

5.74 **Théorème (du rang).** *Soit $f : E \to F$ une application linéaire entre deux espaces vectoriels. Si E est de dimension finie, alors* $\dim E = \dim(\operatorname{Im} f) + \dim(\operatorname{Ker} f)$.

Démonstration. Par le théorème 5.70, $\operatorname{Ker} f$ est de dimension finie, on peut donc en considérer une base $(v_1, \ldots, v_m)$. De plus, comme E est de dimension finie, il existe une base $(e_1, \ldots, e_n)$ de E et $\operatorname{Im} f$ est engendré par $(f(e_1), \ldots, f(e_n))$ et on peut donc extraire de cette famille une base $(f(w_1), \ldots, f(w_q))$ de sorte que $(w_1, \ldots, w_q)$ soit une famille libre de E. On montre alors que la famille $(v_1, \ldots, v_m, w_1, \ldots, w_q)$ est une base de E. Pour tout $v \in E$, il existe des scalaires $\lambda_1, \ldots, \lambda_q$ tels que $\lambda_1 f(w_1) + \cdots + \lambda_q f(w_q) = f(v)$. Le vecteur $v - \lambda_1 w_1 - \cdots - \lambda_q w_q$ appartient donc à $\operatorname{Ker} f$, ce qui montre que $v_1, \ldots, v_m, w_1, \ldots, w_q$ engendre E. Ces vecteurs sont indépendants car si $\lambda_1 v_1 + \cdots + \lambda_m v_m + \mu_1 w_1 + \cdots + \mu_q w_q = 0$, alors en appliquant f à cette égalité on obtient $\mu_1 f(w_1) + \cdots + \mu_q f(w_q) = 0$, donc $\mu_1 = \cdots = \mu_q = 0$ puisque $(f(w_1), \ldots, f(w_q))$ est libre. On en déduit $\lambda_1 v_1 + \cdots + \lambda_m v_m = 0$

donc $\lambda_1 = \ldots = \lambda_m = 0$ puisque $(v_1, \ldots, v_n)$ est libre. Par conséquent $\dim E = m + q = \dim(\operatorname{Ker} f) + \dim(\operatorname{Im} f)$. $\square$

Enfin, on sait par le théorème 5.33 que l'ensemble des applications linéaires entre deux espaces vectoriels donnés est un espace vectoriel. On peut en fait observer que si E et F sont de dimensions finies, alors $\mathcal{L}(E, F)$ aussi et que sa dimension est $\dim E \times \dim F$. Pour établir cette propriété, on passe par la notion de matrice, qui est l'objet du chapitre suivant.