III. Espaces vectoriels

Dans toute la suite, E désigne un espace vectoriel sur $\mathbb{K}$.

3. Parties génératrices

Soit A une partie non vide de E. On note $\mathrm{Vect}(A)$ l'ensemble des des vecteurs $u \in E$ pouvant s'écrire

$$u = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n$$

avec $n \in \mathbb{N}^*$, $a_1, \ldots, a_n \in A$ et $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$.

Proposition. $\mathrm{Vect}(A)$ est un sous-espace vectoriel.

Preuve.
Soit $a \in A$. On a $0.a = \vec{0}$ donc $\vec{0} \in \mathrm{Vect}(A)$. Soit $u, v \in \mathrm{Vect}(A)$ et $\lambda \in \mathbb{K}$. Par définition il existe un entier n, des vecteurs $a_1, \ldots, a_n \in A$ et des scalaires $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ tels que $u = \alpha_1 a_1 + \cdots + \alpha_n a_n$. De même, il existe $m \in \mathbb{N}^*$, $b_1, \ldots, b_m \in A$ et $\beta_1, \ldots, \beta_m \in \mathbb{K}$ tels que $v = \beta_1 b_1 + \cdots + \beta_m b_m$. Alors

$$u + \lambda v = \alpha_1 a_1 + \cdots + \alpha_n a_n + (\lambda\beta_1) b_1 + \cdots + (\lambda\beta_m) b_m$$

donc $u + \lambda v \in \mathrm{Vect}(A)$.

Définition.
$\mathrm{Vect}(A)$ est appelé le **sous-espace engendré** par A.
Soit F un sous-espace vectoriel. Si $\mathrm{Vect}(A) = F$ on dit que A est une **partie génératrice** (ou une **famille génératrice**) de F ou que A **engendre** F.

Notation.
Si $A = \{a\}$ contient un seul élement on note $\mathbb{K}a = \mathrm{Vect}(a) = \{\lambda a \mid \lambda \in \mathbb{K}\}$.

Remarques.
- $\mathrm{Vect}(A)$ est le plus petit sous-espace vectoriel contenant A.
- Si $A \subset B$ alors $\mathrm{Vect}(A) \subset \mathrm{Vect}(B)$. En particulier, si A est une partie génératrice de E et si B contient A alors B est aussi une partie génératrice de E.
- On considère souvent un ensemble fini : si $A = \{a_1, \ldots, a_n\}$. Alors

$$\mathrm{Vect}(A) = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_1, \ldots, \lambda_n \in \mathbb{K}\}.$$

Exemple 1. Les vecteurs $(1,0), (0,1)$ engendrent $\mathbb{R}^2$. En effet, si $(x,y) \in \mathbb{R}^2$, on peut écrire

$$(x,y) = x(1,0) + y(0,1).$$

$\{(1,0), (0,1), (1,1)\}$ engendre également $\mathbb{R}^2$ car

$$(x,y) = x(1,0) + y(0,1) + 0(1,1).$$

Il y a plusieurs façons d'écrire (x,y) comme combinaison linéaire de ces 3 vecteurs, en voici une deuxième :

$$(x,y) = \frac{x-y}{2}(1,0) + \frac{y-x}{2}(0,1) + \frac{x+y}{2}(1,1).$$

Exemple 2.
Proposition. L'ensemble $\mathcal{F}$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ est un espace vectoriel. Le vecteur nul de $\mathcal{F}$ est la fonction identiquement nulle : $\forall x \in \mathbb{R},\ f_0(x) = 0$.
Les solutions de l'équation différentielle $y'' + y = 0$ sont $y(x) = \lambda \cos(x) + \mu \sin(x), \lambda, \mu \in \mathbb{R}$. C'est le sous-espace vectoriel de $\mathcal{F}$ engendré par les fonctions $x \mapsto \cos(x)$ et $x \mapsto \sin(x)$.

Exemple 3 : $E = \mathbb{K}[X]$ avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
$\mathbb{K}[X]$ est l'ensemble des polynômes à coefficients dans $\mathbb{K}$: un polynôme $P \in \mathbb{K}[X]$ s'écrit

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \qquad (*)$$

avec $a_0, a_1, \ldots, a_n \in \mathbb{K}$.
Deux polynômes P et Q sont égaux si et seulement si tous leurs coefficients sont égaux.
Exemple : si $aX^2 + bX + c = 2X + 3$ alors $a = 0, b = 2, c = 3$ (identification des coefficients).

Proposition. $\mathbb{K}[X]$ est un espace vectoriel sur $\mathbb{K}$.
Soit $A = \{1, X, X^2, \ldots, X^n, \ldots\} = \{X^k \mid k \in \mathbb{N}\}$. En regardant $(*)$ on voit qu'un polynôme $P \in \mathbb{R}[X]$ s'écrit comme une combinaison linéaire d'éléments de A. Donc A est une famille génératrice de $\mathbb{R}[X]$.

4. Somme, somme directe, supplémentaire.

Soit F et G deux sous-espaces vectoriels de E. On définit $F + G$ comme l'ensemble des vecteurs w de E pouvant s'écrire $w = u + v$ avec $u \in F$ et $v \in G$:

$$F + G = \{u + v \in E \mid u \in F, v \in G\}.$$

Proposition. $F + G$ est un sous-espace vectoriel de E, qui s'appelle la **somme** de F et G.

Preuve. $\vec{0} \in F$ et $\vec{0} \in G$ donc $\vec{0} = \vec{0} + \vec{0} \in F + G$.
Soit w_1, w_2 deux vecteurs de $F + G$ et $\lambda \in \mathbb{K}$. Il existe $u_1, u_2 \in F$ et $v_1, v_2 \in G$ tels que $w_1 = u_1 + v_1$ et $w_2 = u_2 + v_2$. Donc

$$w_1 + w_2 = \underbrace{(u_1 + u_2)}_{\in F} + \underbrace{(v_1 + v_2)}_{\in G} \in F + G.$$

De plus

$$\lambda w_1 = \underbrace{(\lambda u_1)}_{\in F} + \underbrace{(\lambda v_1)}_{\in G} \in \ F + G.$$

Donc $F + G$ est un sous-espace vectoriel.

Remarque. $F \subset F + G$ car si $u \in F$ alors $u = u + \vec{0}$ et $\vec{0} \in G$. De même $G \subset F + G$. Donc $F \cup G \subset F + G$. Mais en général, $F \cup G$ <u>n'est pas</u> un sous-espace vectoriel.

Théorème. Soit A, B deux parties de E. Soit F le sous-espace vectoriel engendré par A et G le sous-espace vectoriel engendré par B. Alors $F + G$ est engendré par $A \cup B$.

Preuve. A est une partie de F et on a vu que $F \subset F+G$, donc $A \subset F+G$. De même $B \subset F+G$. Puisque $F+G$ est un sous-espace vectoriel, toute combinaison linéaire d'éléments de $A \cup B$ appartient à $F+G$, donc $\mathrm{Vect}(A \cup B) \subset F+G$.

Réciproquement, si $w \in F+G$ alors il existe $u \in F$ et $v \in G$ tels que $w = u+v$. Par définition u s'écrit comme une combinaison linéaire de vecteurs de A et v s'écrit comme une combinaison linéaire d'éléments de B, donc $w = u+v$ s'écrit comme une combinaison linéaire d'éléments de $A \cup B$. Donc $F+G \subset \mathrm{Vect}(A \cup B)$.

Conclusion : $F+G = \mathrm{Vect}(A \cup B)$.

Définition. Soit F et G deux sous-espaces vectoriels de E.
On dit que F et G sont en **somme directe** si tout vecteur w de $F+G$ s'écrit de façon unique sous la forme $w = u+v$ avec $u \in F$ et $v \in G$. On écrit alors $F \oplus G$.
On dit que F et G sont **supplémentaires** ou que G est un **supplémentaire** de F si $F \oplus G = E$ (c'est-à-dire F et G sont en somme directe et $F+G = E$).

Théorème. Les sous-espaces vectoriels F et G sont en somme directe si et seulement si $F \cap G = \{\vec{0}\}$.

Par conséquent F et G sont supplémentaires si et seulement si $F+G = E$ et $F \cap G = \{\vec{0}\}$.

Preuve. Supposons que F et G sont en somme directe. On a $\vec{0} \in F$ et $\vec{0} \in G$, donc $\vec{0} \in F \cap G$. Soit $u \in F \cap G$. On peut écrire

$$u = \underbrace{u}_{\in F} + \underbrace{\vec{0}}_{\in G} = \underbrace{\vec{0}}_{\in F} + \underbrace{u}_{\in G}.$$

Par unicité de la décomposition, on a $u = \vec{0}$. Donc $F \cap G = \{\vec{0}\}$.

Réciproquement supposons que $F \cap G = \{\vec{0}\}$. Soit $u, u' \in F$ et $v, v' \in G$ tels que $u+v = u'+v'$. Alors $u-u' = v'-v$. De plus $u-u' \in F$ et $v'-v \in G$, donc si on pose $w = u-u' = v'-v$ on a $w \in F \cap G = \{\vec{0}\}$. On en déduit que $w = \vec{0}$, donc $u = u'$ et $v = v'$. Par conséquent, tout vecteur de $F+G$ s'écrit de façon unique comme somme d'un vecteur de F et d'un vecteur de G, autrement dit F et G sont en somme directe.

Le deuxième point du théorème découle directement du premier point et de la définition de supplémentaire.

Exemple. Soit $F = \{(a,0) \mid a \in \mathbb{R}\}$ et $G = \{(0,b) \mid b \in \mathbb{R}\}$. Ce sont deux sous-espaces vectoriels de $\mathbb{R}^2$. On a $F+G = \mathbb{R}^2$ car si $(x,y) \in \mathbb{R}^2$ on peut écrire $(x,y) = (x,0)+(0,y)$ avec $(x,0) \in F$ et $(0,y) \in G$.

Cette écriture est unique : si $(x,y) = (a,0)+(0,b)$ alors $(a,0)+(0,b) = (a,b)$ donc $a = x$ et $b = y$. Donc F et G sont en somme directe.

On peut aussi utiliser le théorème précédent. Soit $u \in F \cap G$. Comme $u \in F$ il existe $a \in \mathbb{R}$ tel que $u = (a,0)$. De même il existe $b \in \mathbb{R}$ tel que $u = (0,b)$. On a $(a,0) = (0,b)$ donc $a = b = 0$. On en déduit que $F \cap G = \{\vec{0}\}$, donc $F \oplus G = \mathbb{R}^2$.

Soit $\vec{\imath} = (1,0)$. On peut écrire $(a,0) = a(1,0) = a\vec{\imath}$ donc $F = \mathrm{Vect}(\vec{\imath}) = \mathbb{R}\vec{\imath}$. De même G est engendré par $\vec{\jmath} = (0,1)$. Par l'avant dernier théorème, $(\vec{\imath}, \vec{\jmath})$ engendre $\mathbb{R}^2$.

Par contre $F \cup G$ n'est pas un sous-espace vectoriel car $(1,0) \in F$, $(0,1) \in G$ mais $(1,1) = (1,0)+(0,1)$ n'appartient pas à $F \cup G$

5. Parties libres

Définition.
Soit A une partie non vide de E. On dit que A est une **partie libre** si quels que soient les vecteurs $a_1, \ldots, a_n \in A$ et les scalaires $\lambda_1, \ldots, \lambda_n$, la relation

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n = 0$$

entraîne $\lambda_1 = 0, \lambda_2 = 0, \ldots, \lambda_n = 0$.

On dit aussi que les éléments de A sont **linéairement indépendants.**
Une partie qui n'est pas libre est dite **liée**.

Exemple 1. Soit $u = (1,0,2)$ et $v = (1,3,1)$ des vecteurs de $\mathbb{R}^3$ et $\lambda, \mu \in \mathbb{R}$.
On a $\lambda u + \mu v = (\lambda + \mu, 3\mu, 2\lambda + \mu)$, donc si $\lambda u + \mu v = 0$ alors
$$\begin{cases} \lambda + \mu &= 0 \\ 3\mu &= 0 \\ 2\lambda + \mu &= 0 \end{cases}$$
Ce système a une unique solution $\lambda = 0, \mu = 0$, donc u, v sont linéairement indépendants.

Soit $w = (2,6,2)$. Les vecteurs v et w sont liés car $2v - w = 0$.

Exemple 2.
On a vu que l'ensemble des solutions de $y'' + y = 0$ est le sous-espace vectoriel engendré par $x \mapsto \cos x$ et $x \mapsto \sin x$. Montrons que ces deux fonctions (vues en tant que vecteurs) sont linéairement indépendantes.

Soit $\lambda, \mu \in \mathbb{R}$ tels que $\forall x \in \mathbb{R}, \lambda \cos x + \mu \sin x = 0$. En particulier pour $x = 0$ on doit avoir $\lambda = 0$. Et pour $x = \frac{\pi}{2}$ on obtient $\mu = 0$. Donc $\{\cos, \sin\}$ est une famille libre.

Exemple 3.
Soit f_1, f_2 et f_3 les fonctions de $\mathbb{R}$ dans $\mathbb{R}$ définies par $f_1(x) = \cos^2(x)$, $f_2(x) = \sin^2(x)$, $f_3(x) = \cos(2x)$. La famille $\{f_1, f_2, f_3\}$ est liée car $\cos(2x) = \cos^2(x) - \sin^2(x)$, autrement dit $f_1 - f_2 - f_3 = 0$.

Théorème.
Soit $u_1, \ldots, u_n$ des vecteurs linéairement indépendants et v un vecteur de E. Alors v est une combinaison linéaire de $u_1, \ldots, u_n$ si et seulement si $(u_1, u_2, \ldots, u_n, v)$ est une partie liée.

Preuve.
S'il existe des scalaires $\lambda_1, \ldots, \lambda_n$ tels que $v = \lambda_1 u_1 + \cdots + \lambda_n u_n$ alors $\lambda_1 u_1 + \cdots + \lambda_n u_n - v = 0$, donc les vecteurs $u_1, u_2, \ldots, u_n, v$ sont liés.

Réciproquement, supposons que $(u_1, u_2, \ldots, u_n, v)$ est une partie liée. Il existe $\mu_1, \ldots, \mu_n, \mu_{n+1} \in \mathbb{K}$ non tous nuls tels que $\mu_1 u_1 + \mu_2 u_2 + \cdots + \mu_n u_n + \mu_{n+1} v = 0$. Si $\mu_{n+1} = 0$ alors $\mu_1 u_1 + \mu_2 u_2 + \cdots + \mu_n u_n = 0$ donc $\mu_1 = \mu_2 = \cdots = \mu_n = 0$ car $u_1, \ldots, u_n$ sont linéairement indépendants, ce qui est une contradiction. Donc $\mu_{n+1} \neq 0$ et

$$v = -\frac{\mu_1}{\mu_{n+1}} u_1 - \frac{\mu_2}{\mu_{n+1}} u_2 - \cdots - \frac{\mu_n}{\mu_{n+1}} u_n.$$

Ainsi, v est une combinaison linéaire de $u_1, \ldots, u_n$.

6. Bases

Définition.
Soit A une partie de E. On dit que A est une **base** de E si A est à la fois une famille libre et une partie génératrice de E.

Exemple.
$\vec{\imath} = (1,0), \vec{\jmath} = (0,1)$ est une famille libre et génératrice de $\mathbb{R}^2$ donc c'est une base de $\mathbb{R}^2$.

Théorème.
$(e_1, \ldots, e_n)$ est une base de E si et seulement si tout vecteur u de E s'écrit de façon unique comme combinaison linéaire de $e_1, \ldots, e_n$.

Preuve.
On suppose que $(e_1, \ldots, e_n)$ est une base de E. Comme c'est une partie génératrice, pour tout $u \in E$ il existe $\lambda_1, \ldots, \lambda_n$ tels que $u = \lambda_1 e_1 + \cdots + \lambda_n e_n$. Supposons qu'on a aussi $u = \mu_1 e_1 + \cdots + \mu_n e_n$. Alors

$$u - u = (\lambda_1 - \mu_1)e_1 + \cdots + (\lambda_n - \mu_n)e_n = \vec{0}.$$

Comme $(e_1, \ldots, e_n)$ est une famille libre, tous les coefficients sont nuls, donc
$\lambda_1 = \mu_1, \lambda_2 = \mu_2, \ldots, \lambda_n = \mu_n$.

Réciproquement, on suppose que tout vecteur u s'écrit de façon unique comme combinaison linéaire de $e_1, \ldots, e_n$. Ceci implique tout d'abord que $(e_1, \ldots, e_n)$ est une famille génératrice. De plus $\vec{0} = 0e_1 + \ldots + 0e_n$. Par unicité, si $\lambda_1 e_1 + \cdots + \lambda_n e_n = \vec{0}$ alors $\lambda_1 = \cdots = \lambda_n = 0$, donc $(e_1, \ldots, e_n)$ est une famille libre. Par conséquent, c'est une base.

Définition.
On suppose que $(e_1, \ldots, e_n)$ est une base de E. Si $u \in E$ on peut écrire

$$u = x_1 e_1 + \cdots + x_n e_n.$$

Les scalaires $x_1, \ldots, x_n$ sont appelés les **coordonnées** de u dans la base $(e_1, \ldots, e_n)$.

Exemple fondamental : $\mathbb{R}^n$.
Soit e_k le vecteur de $\mathbb{R}^n$ dont toutes les coordonnées sont nulles sauf la k-ième qui vaut 1 :

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

Soit $u = (x_1, \ldots, x_n) \in \mathbb{R}^n$. Le vecteur u s'écrit de façon unique $u = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n$. Donc $(e_1, \ldots, e_n)$ est une base de $\mathbb{R}^n$ et $x_1, \ldots, x_n$ sont les coordonnées de u.

Remarque.
On suppose que $(e_1, \ldots, e_n)$ est une base de E. Soit u, v deux vecteurs de E. On note $x_1, \ldots, x_n$ les coordonnées de u et $y_1, \ldots, y_n$ les coordonnées de v dans cette base. Alors les coordonnées de $u + v$ sont $x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n$ et les coordonnées de λu sont $\lambda x_1, \ldots, \lambda x_n$.
Autrement dit, les opérations sur les coordonnées se font comme dans $\mathbb{R}^n$.

Théorème.
Soit F et G des sous-espaces vectoriels tels que $F \oplus G = E$. Si $(e_1, \ldots, e_p)$ est une base de F et $(f_1, \ldots, f_q)$ est une base de G alors $(e_1, \ldots, e_p, f_1, \ldots, f_q)$ est une base de E.

Preuve.
Soit $u \in E$. Il existe $v \in F$ et $w \in G$ tels que $u = v + w$. Le vecteur v est combinaison linéaire de $e_1, \ldots, e_p$ et le vecteur w est combinaison linéaire de $f_1, \ldots, f_q$, donc u peut s'écrire comme combinaison linéaire de $e_1, \ldots, e_p, f_1, \ldots, f_q$, autrement dit $(e_1, \ldots, e_p, f_1, \ldots, f_q)$ est une famille génératrice de E.

Soit $\lambda_1, \ldots, \lambda_p, \mu_1, \ldots, \mu_q$ tels que

$$\lambda_1 e_1 + \cdots + \lambda_p e_p + \mu_1 f_1 + \cdots + \mu_q f_q = \vec{0}.$$

$v = \lambda_1 e_1 + \cdots + \lambda_p e_p$ appartient à F et $w = \mu_1 f_1 + \cdots + \mu_q f_q$. Comme $\vec{0} = \vec{0} + \vec{0}$ est l'unique décomposition de $\vec{0}$ selon la somme directe $F \oplus G$, on a $v = w = \vec{0}$. Comme $(e_1, \ldots, e_p)$ est une base de F, $v = \vec{0}$ implique que $\lambda_1 = \lambda_2 = \cdots = \lambda_p = 0$. De même, comme $(f_1, \ldots, f_q)$ est une base de G, $\mu_1 = \mu_2 = \cdots = \mu_q = 0$. On en déduit que $(e_1, \ldots, e_p, f_1, \ldots, f_q)$ est une famille libre.

Conclusion : $(e_1, \ldots, e_p, f_1, \ldots, f_q)$ est une base de E.

Théorème de la base incomplète.
Soit $u_1, u_2, \ldots, u_p$ des vecteurs de E linéairement indépendants. Soit $v_1, v_2, \ldots, v_q$ des vecteurs qui engendrent E. Alors il existe un entier $n \geq p$ et une base $(e_1, e_2, \ldots, e_n)$ de E telle que
- $e_i = u_i$ si $1 \leq i \leq p$,
- e_i est l'un des vecteurs $v_1, \ldots, v_q$ si $i > p$.

Preuve.
1er cas : pour tout i le vecteur v_i appartient au sous-espace engendré par $u_1, \ldots, u_p$. On a donc $\mathrm{Vect}(v_1, \ldots, v_q) \subset \mathrm{Vect}(u_1, \ldots, u_p)$. Comme $\mathrm{Vect}(v_1, \ldots, v_q) = E$, on en déduit que $\mathrm{Vect}(u_1, \ldots, u_p) = E$. On sait déjà que $(u_1, \ldots, u_p)$ est une famille libre donc c'est une base. C'est le théorème avec $n = p$.

2ème cas : il existe i_1, $1 \leq i_1 \leq q$, tel que $v_{i_1} \notin \mathrm{Vect}(u_1, \ldots, u_p)$. Par le théorème du paragraphe 5 (page 4), les vecteurs $u_1, \ldots, u_p, v_{i_1}$ sont linéairement indépendants.

On pose $u_{p+1} = v_{i_1}$ et on recommence la preuve avec $(u_1, \ldots, u_{p+1})$ et $(v_1, \ldots, v_q)$.
Si on est de nouveau dans le 2ème cas, alors il existe i_2 tel que $v_{i_2} \notin \mathrm{Vect}(u_1, \ldots, u_p, u_{p+1})$ et nécessairement $i_2 \neq i_1$ car $u_{p+1} = v_{i_1}$. On pose $u_{p+2} = v_{i_2}$ et on recommence.

Le processus s'arrête en un nombre fini d'étapes (au plus q) puisqu'à chaque fois on prend un vecteur différent parmi $v_1, \ldots, v_q$. Appelons k le nombre d'étapes. À ce moment-là, on est nécessairement dans le premier cas, donc $(u_1, \ldots, u_p, u_{p+1} \ldots, u_{p+k})$ est une base. C'est le théorème avec $n = p + k$.