L1S2 Informatique — Université de Tours
Notes de Cours 2018-2019
Emmanuel Chasseigne

Cours Numéro 7 — *Espaces Vectoriels*

(a) Notion de Corps — On rappelle que $(E, \star)$ est un groupe si la lci $\star$ est associative, qu'il existe un élément neutre et que tout élément admet un inverse pour $\star$. Le groupe est dit Abélien s'il est commutatif. Il existe une notion intermédiaire entre groupe et corps, la notion d'anneau que nous n'aborderons pas ici.

Définition — Soit $\mathbb{K}$ un ensemble muni de deux lci notées $+$ et $\times$. On dit que $(\mathbb{K}, +, \times)$ est un corps si:

(i) $(\mathbb{K}, +)$ est un groupe Abélien dont l'élément neutre est noté 0.
(ii) $(\mathbb{K}^*, \times)$ est un groupe Abélien, où $\mathbb{K}^* := \mathbb{K} \setminus \{0\}$, dont l'élément neutre est noté 1.
(iii) La loi $\times$ est distributive par rapport à la loi $+$.

Exemples : $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps fondamentaux utiles aussi bien en algèbre qu'en analyse. Néanmoins, chacun possède certaines caractéristiques spécifiques: toute suite de rationnel ne converge pas nécessairement dans $\mathbb{Q}$ alors que c'est vrai pour $\mathbb{R}$ et $\mathbb{C}$; tout polynôme admet toutes ses racines dans $\mathbb{C}$ alors que ce n'est pas toujours vrai pour $\mathbb{R}$ (ni $\mathbb{Q}$).

(b) Corps finis — les exemples ci-dessus concernent des corps infinis, mais on peut tout à fait construire des corps finis (c'est-à-dire avec un nombre fini d'éléments).

Le premier exemple est le corps $\mathbb{K} := \{0, 1\}$ muni des deux lci suivantes:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Il s'agit d'un corps à deux éléments, noté $\mathbb{F}_2$ ou encore $\mathbb{Z}/2Z$. On peut aussi construire un corps à 3 éléments de la même façon en calculant modulo 3, on obtient le corps $\mathbb{F}_3$.

En revanche, attention, si on considère les entiers modulo 4, $\mathbb{Z}/4\mathbb{Z} := \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, on voit qu'on a bien un groupe additif mais il ne s'agit pas d'un corps car $\bar{2} \times \bar{2} = \bar{0}$, et donc $\bar{2}$ n'est pas inversible.

Thorème — $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ *est un corps si et seulement si p est premier.*

Preuve. Il est assez facile de voir que $(\mathbb{Z}/p\mathbb{Z},+)$ a une structure de groupe quelque soit l'entier p, et que de plus la lci $\times$ est distributive sur la lci $+$. La seule question concerne l'inversibilité de tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$.

Or si p n'est pas premier, on peut alors écrire $p = p_1 \times p_2$ pour deux entiers $1 < p_1, p_2 < p$. Mais alors $\bar{p}_1\bar{p}_2 = \bar{p} = \bar{0}$. Or comme $\bar{p}_1$, $\bar{p}_2$ ne sont pas $\bar{0}$, c'est donc qu'ils ne sont pas inversibles. On n'a donc pas de structure de groupe multiplicatif pour $(\mathbb{Z}/p\mathbb{Z})^*$.

Réciproquement, si $(\mathbb{Z}/p\mathbb{Z})^*$ a une structure de groupe multiplicatif, alors si $p = p_1 \times p_2$ on voit que nécessairement, $p_1 = p$ ou $p_2 = p$ et donc p est premier.

(c) Structure d'espace vectoriel — Dans la suite, $(\mathbb{K},+,\times)$ est un corps et en pratique on prendra $\mathbb{K} = \mathbb{R}$ (plus rarement, $\mathbb{C}$).

Définition — *On dit que $E \neq \emptyset$ est un $\mathbb{K}$-espace vectoriel si E est muni d'une loi de composition interne notée $+$ et d'une loi de composition externe notée $\cdot$ vérifiant:*
(i) $(E,+)$ est un groupe abélien dont l'élément neutre est noté 0_E.
(ii) Pour tout $u \in E$, $1_{\mathbb{K}} \cdot u = u$.
(iii) Pour tous $\lambda, \mu \in \mathbb{K}$ et $u \in E$, $\lambda \cdot (\mu \cdot u) = (\lambda\mu) \cdot u$.
(iv) Pour tous $\lambda \in \mathbb{K}$ et $u, v \in E$, $\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v$.
(v) Pour tous $\lambda, \mu \in \mathbb{K}$ et $u \in E$, $(\lambda + \mu) \cdot u = \lambda \cdot u + \mu \cdot u$.

Pour les distinguer, on appelle les élément de E des vecteurs et les éléments de $\mathbb{K}$ des scalaires. De plus, on convient en général de simplifier l'ecriture de la loi externe en notant simplement $\lambda \cdot u = \lambda u$.

Exemple 1 — On prend $E = \mathbb{R}^2$ et $\mathbb{K} = \mathbb{R}$. Si $u\binom{x}{y}$, $v\binom{x'}{y'}$ et $\lambda \in \mathbb{R}$ on pose

$$(u+v)\begin{pmatrix} x + x' \\ y + y' \end{pmatrix}, \quad \lambda u \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}.$$

Alors il est facile de vérifier que E est un $\mathbb{R}$-espace vectoriel.

Exemple 2 — On considère l'ensemble E des fonctions continues sur $\mathbb{R}$. Alors E est un $\mathbb{R}$-espace vectoriel.

Exemple 3 — L'ensemble des suites numériques constitue un $\mathbb{R}$-espace vectoriel.

(d) Sous-espace vectoriel — On dit que F est un sous-ev d'un $\mathbb{K}$-ev E si $F \subset E$ et les lois de E induisent sur F une structure de $\mathbb{K}$-ev. On a un critère assez simple.

Proposition — *Soit E un $\mathbb{K}$-ev. Alors $F \subset E$ est un sev si et seulement si $F \neq \emptyset$ et*

$$\text{pour tous } u, v \in F,\ \lambda \in \mathbb{K}, \quad u + \lambda v \in F\,.$$

Exemples — L'ensemble des suites réelles tendant vers zéro est un sous-espace vectoriel de l'ensemble des suites réelles ; l'ensemble des fonctions continues et paires est un sev de l'ensemble des fonctions continues. La droite d'équation $y = x$ est un sev du plan $\mathbb{R}^2$ vu comme $\mathbb{R}$-ev.

Conséquence: l'intersection de sev est un sev.

(e) Famille, bases — Une base est une famille de vecteurs spécifiques de E qui permet de coder n'importe quel vecteur par combinaison linéaire, de façon unique.

Définition — *On dit qu'une famille $A \subset E$ est libre si pour tout $n \in \mathbb{N}$ et $\lambda_1 ... \lambda_n \in \mathbb{K}$, $\sum \lambda_i x_i = 0$ implique $\lambda_1 = ... = \lambda_n = 0$.*

On dit qu'une famille $A \subset E$ est génératrice si tout vecteur $u \in E$ s'écrit comme une compbinaison linéaire finie de vecteurs de la famille A.

On dit que A est une base de E si c'est une famille à la fois libre et génératrice.

Dans le cas où la famille A est finie, de cardinal n, on dit que E est un espace vectoriel de dimension finie, n. A noter que toute base est de même cardinal (cf. cours d'algèbre linéaire).

Exemple — Dans $\mathbb{R}^2$, $A := \left\{ \binom{1}{0}, \binom{0}{1} \right\}$ est une base. $\mathbb{R}^2$ est donc un espace vectoriel de dimension 2 sur $\mathbb{R}$.

Attention, il existe des espaces vectoriels de dimension infinie comme les ensemble de fonctions ou les suites réelles. Par exemple, la famille des suites où on place un 1 en position n

$$A := \left\{ e_n := (0, 0..., 0, 1, 0, ...) \, , \; n \in \mathbb{N} \right\}$$

constitue une base de l'ensemble des suites. C'est une famille infinie et on ne peut construire une base de taille finie.

(f) Applications linéaires, matrices — Une application linéaire est une application qui respecte la structure d'espace vectoriel.

Définition — Soient E et F deux $\mathbb{K}$-espaces vectoriels. On dit que $f : E \to F$ est linéaire si pour tous $x, y \in E$, $\lambda \in \mathbb{K}$, $f(x + \lambda y) = f(x) + \lambda f(y)$.

Exemple — l'application $f : \mathbb{R}^2 \to \mathbb{R}$ donnée par $f(x, y) = x + 2y$ est linéaire mais pas $f(x, y) = x^2 + \cos(y)$.

On peut représenter toute application linéaire par une matrice dès qu'on choisit une base de chaque espace vectoriel en plaçant en colonne les images des vecteurs de la base de départ en fonction de la base d'arrivée:

$$\mathrm{Mat}(f) := \begin{pmatrix} f(e_1) & \cdots & f(e_n) \end{pmatrix} .$$

La matrice obtenue dépend évidemment du choix des bases, mais l'application est un objet intrinsèque. On renvoit au cours d'algèbre linéaire pour plus de détails.