LEÇONS 151 ET 162

Dimension d'un espace vectoriel

Référence : [RW06, p. 206 et p. 352].

Soit $\mathbf{k}$ un corps, et V un $\mathbf{k}$-espace vectoriel. Soit $(x_i)_{i\in I}$ une famille de vecteurs de V. Une *combinaison linéaire* des x_i est une somme

$$\sum_{i\in I} \lambda_i x_i$$

avec les $\lambda_i \in \mathbf{k}$ tous nuls sauf un nombre fini.

La famille $(x_i)_{i\in I}$ est dite *génératrice* si tout vecteur de V est une combinaison linéaire des x_i.

La famille $(x_i)_{i\in I}$ est dite *libre* si la seule combinaison linéaire des x_i nulle est celle avec tous les λ_i nuls. Dans le cas contraire on dit que la famille est *liée*.

Un espace vectoriel est dit *finiment engendré* s'il admet une partie génératrice finie. On trouve souvent dans les livres la terminologie "de dimension finie" pour cette notion, mais ce serait pour l'instant un léger abus de langage, puisque l'objet de ce qui suit est de définir la notion de dimension d'un espace vectoriel.

Une *base* de V est une famille libre et génératrice.

Convention : la famille vide est libre, et engendre l'espace vectoriel trivial $\{0\}$.

Une façon de résumer ces définitions : La famille (x_i) est génératrice, libre, une base, ssi l'application

$$\begin{array}{ccc} \bigoplus_{i\in I} \mathbf{k} & \to & E \\ (\lambda_i) & \mapsto & \sum_i \lambda_i x_i \end{array}$$

est respectivement surjective, injective, bijective.

Proposition 1. *Soit V un espace vectoriel finiment engendré. Alors toute partie génératrice de V contient une partie génératrice finie.*

Preuve. Soit F une partie génératrice finie, et G une partie génératrice quelconque. On peut exprimer chaque $x \in F$ comme une combinaison linéaire des éléments de G : un choix d'une telle combinaison étant fait, notons $G_x \subseteq G$ l'ensemble (fini) des éléments de G avec un coefficient non nul. Alors

$$G' = \bigcup_{x\in F} G_x \subseteq G$$

est la sous-famille génératrice finie cherchée. □

Proposition 2. *Soit V un espace vectoriel, et $x_1, \dots, x_n$ des vecteurs de V. Soit $y_1, \dots, y_m$ des vecteurs qui sont chacun combinaison linéaire des x_i. Si $m > n$, alors la famille $(y_j)_{1\leqslant j\leqslant m}$ est liée.*

En particulier, si V admet une partie génératrice finie de cardinal n, alors toute partie libre de V est finie de cardinal au plus n.

Preuve. On procède par récurrence sur n, le cas $n = 0$ (famille vide) étant clair. Par hypothèse, on peut exprimer les y_j comme des combinaisons linéaires :

$$\begin{cases} y_1 & = a_{1,1}x_1 + \cdots + a_{1,n}x_n \\ & \cdots \\ y_m & = a_{m,1}x_1 + \cdots + a_{m,n}x_n. \end{cases}$$

Si les $a_{j,n}$ sont tous nuls on conclut directement par l'hypothèse de récurrence. Sinon quitte à réordonner on peut supposer $a_{m,n} \neq 0$, et en posant $\lambda_i = \frac{a_{i,n}}{a_{m,n}}$ on peut appliquer l'hypothèse de récurrence aux $m-1$ vecteurs $y_1 - \lambda_1 y_m, \dots, y_{m-1} - \lambda_{m-1} y_m$ qui sont combinaisons des $n-1$ vecteurs $x_1, \dots, x_{n-1}$. La combinaison linéaire nulle non triviale entre les $(y_j - \lambda_j y_m)_{1 \leqslant j \leqslant m-1}$ fournit une combinaison linéaire nulle non triviale entre les $(y_j)_{1 \leqslant j \leqslant m}$. □

Proposition 3. *Soit V un espace vectoriel, G une partie génératrice, et $L \subseteq G$ une partie libre maximale parmi les parties libres de G. Alors L est une base de V.*

Preuve. Soit $x \in G$. Montrons que x est combinaison linéaire d'élément de L. Si $x \in L$, c'est clair, et sinon $L \cup \{x\}$ est liée par hypothèse de maximalité. Il existe une relation linéaire non triviale entre les éléments de la famille $L \cup \{x\}$, et le coefficient devant x doit être non nul, sinon on aurait une relation linéaire entre les éléments de la famille libre L, absurde. On en déduit que x est combinaison linéaire de vecteurs dans L, et ceci étant vrai pour tout $x \in G$ avec G génératrice, c'est vrai également pour tout $x \in V$. □

Théorème 4 (Base incomplète)**.** *Soit V un espace vectoriel finiment engendré, L une partie libre, et G une partie génératrice. Alors il existe une base B de V telle que*

$$L \subseteq B \subseteq L \cup G.$$

De plus B, et donc également L, sont finies.

Preuve. Par la proposition 1, quitte à passer à une sous-famille on peut supposer G finie, de cardinal n. Alors la proposition 2 assure que toute partie libre de V est de cardinal au plus n, en particulier L est finie.

On considère l'ensemble des parties libres contenant L de la partie génératrice $G \cup L$: cet ensemble de parties est non vide (il contient la partie L) et fini (car $G \cup L$ est fini), donc il contient une partie maximale B, qui est une base par la proposition 3. Enfin B est de cardinal au plus n, à nouveau par la proposition 2. □

Corollaire 5. *Soit V un espace vectoriel finiment engendré. Alors V admet une base, et toutes les bases de V sont finies de même cardinal.*

Preuve. L'existence d'une base est donnée par le théorème 4, en complétant la famille L vide à l'aide la famille génératrice $G = V$. Si B et B' sont des bases de cardinaux respectifs n et n', la proposition 2 donne successivement $n \leqslant n'$ et $n \geqslant n'$, et donc l'égalité. □

Le cardinal commun de toutes les bases s'appelle la *dimension* de V.

Algèbre linéaire sur $\mathbf{Z}$

[Coh93, p. 67-75], [NQ92, p. 212-220], notes Coste, notes Belabas.

Lemme 6. *Soit $a, b \in \mathbf{Z}$. Alors il existe une matrice $M \in \mathrm{SL}_2(\mathbf{Z})$ tel que*

$$\begin{pmatrix} a & b \end{pmatrix} M = \begin{pmatrix} 0 & d \end{pmatrix}$$

où d est un PGCD de a, b.

Preuve. Si $a = 0$ on prend $M = I_2$, et si $b = 0$ on prend $M = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Sinon on trouve une relation de Bézout $au + bv = d$ grâce à l'algorithme d'Euclide ("étendu"). En posant $a = a'd$, $b = b'd$, on a donc $a'u + b'v = 1$, et

$$M = \begin{pmatrix} b' & u \\ -a' & v \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$$

convient. □

Corollaire 7. *Soit $a_1, \dots, a_n \in \mathbf{Z}$ de PGCD égal à d. Alors il existe une matrice $P \in \mathrm{SL}_n(\mathbf{Z})$ tel que*

$$\begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} P = \begin{pmatrix} 0 & \dots & 0 & d \end{pmatrix}$$

Preuve. Par récurrence. □

Exemple 8. Considérons le vecteur (2 3 5). En utilisant le procédé du lemme 6 on obtient :

$$(2\ 3) \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} = (0\ 1), \qquad (1\ 5) \begin{pmatrix} 5 & -4 \\ -1 & 1 \end{pmatrix} = (0\ 1).$$

D'où

$$(2\ 3\ 5) \begin{pmatrix} 3 & -1 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & -4 \\ 0 & -1 & 1 \end{pmatrix} = (2\ 3\ 5) \begin{pmatrix} 3 & -5 & 4 \\ -2 & 5 & -4 \\ 0 & -1 & 1 \end{pmatrix} = (0\ 0\ 1).$$

Noter que la matrice P obtenue n'est pas unique, par exemple on a aussi

$$(2\ 3\ 5) \begin{pmatrix} -4 & -3 & -1 \\ 1 & 2 & 1 \\ 1 & 0 & 0 \end{pmatrix} = (0\ 0\ 1).$$

Noter aussi que ce procédé de multiplications successives par matrices avec un bloc 2×2 n'est certainement pas l'algorithme le plus efficace.

Voici un analogue sur $\mathbf{Z}$ de la notion de matrice co-échelonnée en colonnes réduite :

Définition 9. Une matrice rectangulaire à m lignes et n colonnes à coefficients dans $\mathbf{Z}$ est sous *forme normale de Hermite* s'il existe $r \geqslant 0$ et une fonction strictement croissante de $[\![r+1, n]\!]$ vers $[\![1, m]\!]$ tel que les r première colonnes soient nulles, $m_{f(j),j} \geqslant 1$, $m_{i,j} = 0$ pour $i > f(j)$ et $0 \leqslant m_{f(j),k} < m_{f(j),j}$ pour tout $k > j$.

Les coefficients $m_{f(j),j} \geqslant 1$ sont appelés les pivots de la matrice, chaque colonne non nulle contient un tel pivot par définition. La définition signifie que tous les coefficients sous un pivot sont nuls, et ceux à droite d'un pivot sont positifs inférieurs au pivot.

Exemple 10. Les matrices

$$\begin{pmatrix} 6 & -8 & -9 \\ \boxed{2} & 1 & 0 \\ 0 & \boxed{4} & 3 \\ 0 & 0 & \boxed{3} \end{pmatrix}, \qquad \begin{pmatrix} 0 & \boxed{2} & 1 \\ 0 & 0 & -5 \\ 0 & 0 & \boxed{1} \end{pmatrix}, \qquad \begin{pmatrix} 0 & \boxed{1} \\ 0 & 0 \end{pmatrix}$$

sont sous forme normale de Hermite, avec les pivots encadrés.

Théorème 11. *Soit A une matrice rectangulaire $m \times n$ à coefficients dans $\mathbf{Z}$. Alors il existe une unique matrice B de taille $m \times n$ et une matrice $U \in \mathrm{GL}_n(\mathbf{Z})$ tel que $B = AU$ et B soit sous forme normale de Hermite.*

Preuve. On commence par regarder la dernière ligne de la matrice. Si elle n'est pas nulle, par le corollaire 7 on peut multiplier à droite par une matrice dans $\mathrm{SL}_n(\mathbf{Z})$ pour avoir un seul coefficient non nul en dernière position. Quitte à multiplier par la matrice diagonale avec des 1 sur la diagonale sauf un -1 en dernière position (qui est dans $\mathrm{GL}_n(\mathbf{Z})$), on peut supposer ce coefficient positif.

Supposons maintenant que les $k \geqslant 1$ dernières lignes donne une matrice $k \times n$ co-échelonnée en colonnes, avec premier pivot en position j. Si $j = 1$ ou $k = m$, la matrice est déjà co-échelonnée en colonne. Si $j > 1$ et $k < m$, on utilise le corollaire 7 et on trouve une matrice P dans $\mathrm{SL}_{j-1}(\mathbf{k})$ tel que en multipliant par une matrice diagonale par blocs : 1er bloc P, 2ème bloc identité, on obtient que les $k+1$ dernières lignes correspondent à une matrice co-échelonnée en colonnes.

Reste à normaliser pour obtenir une forme normale de Hermite. Pour chaque pivot $a_{f(j),j}$, et chaque $k > j$, on écrit une division euclidienne $a_{f(j),k} = qa_{f(j),j} + r$ avec $0 \leqslant r < a_{f(j),j}$. On remplace la colonne C_k par $C_k - qC_j$, ce qui remplace $a_{f(j),k}$ par r, et après avoir fait ces opérations pour chaque pivot et chaque colonne C_k à droite du pivot, on obtient une forme normale de Hermite.

Unicité : Si B et B' sont deux formes normales de Hermite, on montre leur égalité colonne par colonne, en partant de la colonne de droite (celle avec le pivot le plus bas), en exprimant chaque colonne de B' comme une combinaison linéaire des colonnes de B. □

Application 12 (Trouver une base)**.** Avec les notations du théorème, les colonnes non nulles de la matrices B forment une base du groupe abélien libre engendré par les colonnes de A. On pourra méditer l'exemple simple donné par

$$A = \begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

où l'on peut constater qu'aucune des colonnes initiales ne formait une base.

Application 13 (Tester l'appartenance à un groupe)**.** Soit

$$B = \begin{pmatrix} 6 & -8 & -9 \\ \boxed{2} & 1 & 0 \\ 0 & \boxed{4} & 3 \\ 0 & 0 & \boxed{3} \end{pmatrix} \qquad V = \begin{pmatrix} -7 \\ 1 \\ -1 \\ 3 \end{pmatrix}.$$

Le vecteur V est-il combinaison entière des colonnes C_i de la matrice B ?

Réponse : on cherche V sous la forme $V = a_1C_1 + a_2C_2 + a_3C_3$. On trouve successivement $a_3 = 1$, $a_2 = -1$, $a_1 = 1$, et on vérifie que le premier coefficient -7 colle avec ces contraintes.

Application 14 (Résoudre un système linéaire à coefficient entier)**.** On veut résoudre l'équation $2x + 3y + 5z = 0$. Sous forme matricielle :

$$(2\ 3\ 5) \begin{pmatrix} x \\ y \\ z \end{pmatrix} = (0).$$

On met la matrice $A = (2\ 3\ 5)$ sous forme normale de Hermite $AU = B$:

$$(2\ 3\ 5) \begin{pmatrix} -4 & -3 & -1 \\ 1 & 2 & 1 \\ 1 & 0 & 0 \end{pmatrix} = (0\ 0\ 1)$$

Les colonnes de U forment une base de $\mathbf{Z}^3$. Les 2 premières colonnes de la matrice U forment une base de l'espace Sol des solutions, c'est à dire

$$\text{Sol} = \left\{ \mathbf{Z} \begin{pmatrix} -4 \\ 1 \\ 1 \end{pmatrix} + \mathbf{Z} \begin{pmatrix} -3 \\ 2 \\ 0 \end{pmatrix} \right\} \simeq \mathbf{Z}^2.$$

Application 15 (Compléter une base)**.** On veut compléter le vecteur (2 3 5) en une base de $\mathbf{Z}^3$ (c'est possible car les coefficients sont premiers entre eux dans leur ensemble). On considère cette fois l'inverse de la matrice qui amène à la forme normale de Hermite :

$$\begin{pmatrix} 0 & 0 & 1 \\ -1 & -1 & -3 \\ 2 & 3 & 5 \end{pmatrix} \begin{pmatrix} -4 & -3 & -1 \\ 1 & 2 & 1 \\ 1 & 0 & 0 \end{pmatrix} = I_3$$

Les 3 lignes de la première matrice donnent la base souhaitée.

Leçons concernées :

- 122 Anneaux principaux. Applications.
- 126 Exemples d'équations en arithmétique.
- 142 PGCD et PPCM, algorithme de calcul. Applications.
- 162 Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

Références

[Coh93] H. Cohen. *A course in computational algebraic number theory*. Springer, 1993.

[NQ92] P. Naudin & C. Quitté. *Algorithmique algébrique*. Masson, 1992.

[RW06] J.-P. Ramis & A. Warusfel. *Mathématiques Tout-en-un pour la Licence, Niveau L1*. Dunod, 2006.