Introduction aux espaces vectoriels de dimension finie sur un corps commutatif

Alain Wazner. Pour Hélène, Léo et Corentin

Anneaux : définition, quelques exemples, caractéristique d'un anneau. Corps : définition

Définition

Soit $(A,+)$ **un groupe commutatif** dont on note 0 le neutre, si sur A est définie une opération $\times$, alors $(A,+,\times)$ est un anneau si et seulement si

- $\times$ est distributive par rapport $+$ c'est à dire $\boxed{\forall x,y,z \in A\ x\times(y+z) = x\times y + x\times z}$ $\boxed{\forall x,y,z \in A\ (y+z)\times x = y\times x + z\times x}$
- $\times$ a un neutre noté 1 c'est à dire $\boxed{\forall x \in A\ 1\times x = x\times 1 = x}$

$(A,+,\times)$ est dit un anneau commutatif si et seulement si $\times$ est une loi d'opération commutative.

Nota :

- Pour un ensemble A, la notion d'anneau est dépendante des opérations qu'on y définit, **par commodité** on écrit «A est un anneau» une fois que ses deux opérations sont clairement définies.

- Comme $\forall x, y \in A$

  $$x \times y = x \times (y + 0) = x \times y + x \times 0$$

  nous déduisons que $x \times y = x \times y + x \times 0$ puis que $x \times 0 = 0,\ \forall x \in A$. De

  $$y \times x = (y + 0) \times x = y \times x + 0 \times x$$

  nous déduisons que $0 \times x = 0,\ \forall x \in A$. Finalement

  $$\boxed{\forall x \in A,\ 0 \times x = x \times 0 = 0}$$

  On dit que 0 est **un élément absorbant** pour la multiplication.
- Si $1 = 0$ alors $(\forall x \in A)\ x = 1.x = 0.x = 0 \Rightarrow A = \{0\}$: $(A, +, \times)$ est **l'anneau trivial** $(\{0\}, +, \times)$ avec les «tables de loi» $0 + 0 = 0$ et $0 \times 0 = 0$. Dans la suite nous ne considérons que des anneaux non triviaux, c'est à dire des anneaux sur lesquels $1 \neq 0$.
- Un élément $x \in A$ est dit inversible s'il existe $y \in A$ tel que $x \times y = y \times x = 1$. On appelle $\mathcal{U}_A$ l'ensemble des éléments inversibles de A. $(\mathcal{U}_A, \times)$ est un groupe «multiplicatif». Comme 0 est **absorbant** si $(A, +, \times)$ **n'est pas trivial** alors $0 \notin \mathcal{U}_A$.

Quelques exemples

$\mathbb{Z}$, l'ensemble des entiers relatifs, muni des opérations d'addition et de multiplication est un

anneau commutatif.
On appelle $\mathcal{B}$ l'ensemble à deux éléments $\mathcal{B} = \{0, 1\}$ sur lequel on définit les opérations $+$ et $\times$ par

- $0 + 0 = 0$
- $1 + 1 = 1$
- $1 + 0 = 0 + 1 = 1$

et par

- $0 \times 0 = 0$
- $1 \times 1 = 1$
- $1 \times 0 = 0 \times 1 = 0$

$\mathcal{B}$ est un anneau commutatif appelé **anneau de Boole**.
Si A est un anneau commutatif on appelle ensemble des matrices d'ordre 2 à coefficients sur A l'ensemble des tableaux d'éléments de A : $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$.
On note $M_2(A)$ cet ensemble.
On définit une addition $+$ sur $M_2(A)$ par $\begin{pmatrix} a & c \\ b & d \end{pmatrix} + \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \begin{pmatrix} a + a' & c + c' \\ b + b' & d + d' \end{pmatrix}$ alors $(M_2(A), +)$ est un groupe commutatif de neutre $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
On définit une multiplication sur A par $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \times \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \begin{pmatrix} a \times a + c \times b' & a \times c' + c \times d' \\ b \times a' + d \times b' & b \times c' + d \times d' \end{pmatrix}$
$(A, +, \times)$ est un anneau non commutatif dont le

neutre pour $\times$ est $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Caractéristique d'un anneau

Si $(A, +, \times)$ est un anneau dont 1 est le neutre pour $\times$ et -1 est l'opposé de 1 pour $+$. Si $n \in \mathbb{Z}$ on pose : si $n \geq 0$ alors $n.1 = \underbrace{1 + \cdots + 1}_{n\ fois}$, si $n < 0$ alors $n.1 = \underbrace{(-1) + \cdots + (-1)}_{-n\ fois}$ alors l'application $\phi \ : \ \begin{cases} (\mathbb{Z}, +) & \to & (A, +) \\ n & \mapsto & n.1 \end{cases}$ est un morphisme de groupe dont le noyau est un sous-groupe de $\mathbb{Z}$ soit $c\mathbb{Z}$ avec $c \in \mathbb{N}$. c **est la caractéristique de** A : $c = 0$ si et seulement si ϕ est un isomorphisme, si $c > 0$ alors c est le plus petit entier n tel que $n.1 = 0$.

Définition d'un corps

Définition Soit $(K, +, \times)$ un **anneau** alors $(K, +, \times)$ est un corps si seulement si $(K, +, \times)$ est l'anneau trivial **ou** $K = \mathcal{U}_K \cup \{0\}$.
Dans la suite nous ne considérons que des **corps** $(K, +, \times)$ **non triviaux** (c'est à dire dont l'anneau $(K, +, \times)$ appelé **anneau sous-jacent** est non trivial).
Définition La caractéristique du corps $(K, +, \times)$

est celle de l'anneau sous-jacent $(K, +, \times)$, c'est un nombre premier.

Preuve : Sur **l'anneau** non trivial $(K, +, \times)$ on a : $\forall p, q \in \mathbb{N}$ $(p.1) \times (q.1) = (pq).1$ puisque

$$\begin{aligned}
(p.1) \times (q.1) &= \left(\underbrace{1 + \cdots + 1}_{p}\right) \times \left(\underbrace{1 + \cdots + 1}_{q}\right) \\
&= \underbrace{\left(\underbrace{1 + \cdots + 1}_{q}\right) + \cdots + \left(\underbrace{1 + \cdots + 1}_{q}\right)}_{p} \\
&= \left(\underbrace{1 + \cdots + 1}_{p \times q}\right) \\
&= (pq).1
\end{aligned}$$

Si la caractéristique de c de l'anneau $(K, +, \times)$ est le produit de $c = p \times q$ avec $1 < p < c$ et $1 < q < c$ (c'est à dire que c n'est pas un nombre premier) alors $0 = c.1 = p.1 \times q.1$: le produit $p.1 \times q.1$ est nul, $p.1$ et $q.1$ ne sont pas nuls (puisque $q < c$ et $p < c$ et que c la **caractéristique** de K est le plus petit entier k tel que $k.1 = 0$). Mais K est un corps et donc $p.1 \neq 0$ a un inverse que nous notons i et $p.1 \times q.1 = 0 \Rightarrow i \times p.1 \times q.1 = i \times 0 = 0 \Rightarrow q.1 = 0$ ce qui contredit $q.1 \neq 0$.

Espace vectoriel sur un corps commutatif

Introduction

À un groupe commutatif $(E, +)$ on ajoute une opération externe notée . dont l'opérande est à valeur sur un corps commutatif $(K, +, \times)$ (**attention ! Le + sur K n'est pas à priori le + sur E**) et si $x \in E, \lambda \in K$ on note $\lambda.x$ le résultat de cette opération. On dit que $(E, +, .)$ est un espace vectoriel sur K si les propriétés suivantes sont vraies :

- $(\forall x \in E)\ 1.x = x$
- $(\forall \lambda, \mu \in K)\ (\forall x \in E)\ (\lambda + \mu).x = \lambda.x + \mu.x$
- $(\forall \lambda \in K)\ (\forall x, y \in K)\ \lambda.(x + y) = \lambda.x + \lambda.y$
- $(\forall \lambda, \mu \in K)\ (\forall x \in E)\ \lambda.(\mu.x) = (\lambda \times \mu).x$
  Les éléments de E sont appelés vecteurs et on a $\forall \lambda,\ \lambda.0 = 0$: En effet $\lambda.(x + 0) = \lambda.x$ soit $\lambda.x + \lambda.0 = \lambda.x$ donc $\lambda.0 = \lambda.x - \lambda.x = 0$.

Combinaisons linéaires, parties libres, parties génératrices, notions ensemblistes de bases

Définition : Soit E un espace vectoriel sur un corps K, on dit que $x \in E$ est combinaison linéaire des vecteurs $x_1, x_2, \ldots, x_n \in E$ si $\exists \lambda_1, \ldots, \lambda_n \in K$ tels que $x = \sum_{i=1}^{n} \lambda_i x_i$.

Nota : On ne définit de combinaison linéaire que pour un nombre **fini** de vecteurs.

Définition : Une partie $F \subset E$ est une partie géneratrice de E si et seulement tout $x \in E$ est combinaison linéaire (**finie**) d'éléments de E.

Exemple : E est une partie génératrice de E puisque tout x est égal à $1.x$.

Définition : Une partie $F \subset E$ est une partie libre de E si et seulement si les seules combinaisons linéaires nulles de vecteurs de F sont les combinaisons linéaires à coefficients tous nuls.

Exemple : Soit $x \neq 0 \in E$ alors $\{x\}$ est une partie libre. En effet $\forall \lambda \neq 0,\ \lambda x \neq 0$ puisque $\lambda^{-1}.(\lambda.x) = (\lambda^{-1}.\lambda).x = 1.x = x$ si $\lambda.x = 0$ alors $\lambda^{-1}.(\lambda.x) = \lambda^{-1}.0 = 0$ ce qui donne $x = 0$.

Définition : Une partie $\mathcal{B}$ de E est une base si elle est libre et génératrice.

On suppose que E n'est pas réduit à $\{0\}$ alors la partie $\mathcal{B} \subset E$ est une base si et seulement si tout $x \in E\backslash\{0\}$ est de manière unique combinaison linéaire d'éléments de $\mathcal{B}$.

Preuve : Si $\mathcal{B} \subset E$ est une base et si

$$x = \sum_{i \in I\ fini} \lambda_i b_i = \sum_{j \in J\ fini} \mu_j b_j$$

avec $\forall i \in I \forall j \in J,\ b_i \in \mathcal{B}, b_j \in \mathcal{B}$ alors

– Si $I \cap J = \emptyset$ alors

$$0 = x - x = \sum_{i \in I} \lambda_i b_i + \sum_{j \in J} (-\mu_j) b_j$$

c.a.d. $0 = \sum_{k \in I \bigsqcup J} \gamma_k b_k$ avec $\gamma_k = \lambda_k$ si $k \in I$ et $\gamma_k = -\mu_k$ si $k \in J$ et comme $\mathcal{B}$ est une partie libre ceci entraîne $\gamma_k = 0, \ \forall k \in I \bigsqcup J$ soit $\lambda_i = 0, \ \forall i \in I$ et $\mu_j = 0, \ \forall j \in J$ soit $x = 0$. **On en déduit que si $x \neq 0$ alors** $I \cap I \neq \emptyset$.

– On a alors

$$I \cup J = (I \backslash I \cap J) \bigsqcup (I \cap J) \bigsqcup (J \backslash I \cap J)$$

et si

$$x = \sum_{i \in I \ fini} \lambda_i b_i = \sum_{j \in J \ fini} \mu_j b_j$$

alors

$$\begin{aligned} 0 &= x - x \\ &= \textstyle\sum_{i \in I \backslash I \cap J} \lambda_i b_i + \sum_{k \in I \cap J} (\lambda_k - \mu_k) b_k \\ &\quad + \textstyle\sum_{j \in J \backslash I \cap J} (-\mu_j) b_j \end{aligned}$$

et comme $\mathcal{B}$ est une partie libre ceci entraîne :
1 $\lambda_i = 0, \ \forall i \in I \backslash I \cap J$
2 $\lambda_k - \mu_k = 0, \ \forall k \in I \cap J$ soit $\lambda_k = \mu_k$, $\forall k \in I \cap J$
3 $-\mu_j = 0, \ \forall j \in J \backslash I \cap J$ soit $\mu_j = 0$, $\forall j \in J \backslash I \cap J$

ce qui revient à dire que les combinaisons linéaires $\sum_{i\in I}\lambda_i b_i$ et $\sum_{j\in J}\mu_j b_j$ sont **la combinaison linéaire** $\sum_{k\in I\cap J}\lambda_k b_k$.

Si une partie $\mathcal{B}$ de E est telle que tout $x \in E\backslash\{0\}$ est combinaison linéaire de ses éléments alors elle est par définition génératrice. Si tout $x \in E\backslash\{0\}$ est combinaison linéaire, de manière unique, de ses éléments alors $\mathcal{B}$ est une partie libre. **En effet, si $\mathcal{B}$ n'est pas une partie libre** alors il existe un ensemble I fini et une combinaison linéaire nulle, soit $\sum_{i\in I}\lambda_i b_i = 0$ où le sous-ensemble de K $\{\lambda_i/i \in I\}$ est différent de $\{0\}$ et $\forall i \in I,\ b_i \in \mathcal{B}$. Soit $\lambda_{i_0} \neq 0$ alors de $\sum_{i\in I}\lambda_i b_i = 0$ on déduit que

$$1.b_{i_0} = b_{i_0} = \sum_{i\in I\backslash\{i_0\}} \left(-\lambda_{i_0}^{-1} \times \lambda_i\right).b_i$$

b_{i_0} est combinaison linéaire d'éléments de $\mathcal{B}$ de manière non unique, ce qui est contradictoire.

Notion de dimension finie

Théorème : Si l'axiome du choix n'est pas contradictoire avec la théorie alors tout espace vectoriel admet une base.

Preuve : Soit $(K, +, \times)$ un corps, $(E, +, .)$ un K-espace vectoriel, non réduit à $\{0\}$, nous ordonnons l'ensemble $\mathcal{P}(E)$ des parties de E par l'inclusion,

nous considérons $\mathcal{L} \subset \mathcal{P}(E)$ l'ensemble des parties libres de E. $\mathcal{L}$ n'est pas vide car il contient au moins un singleton $\{x\}$ avec $x \neq 0$.
Si $\mathcal{C}$ est une partie totalement ordonnée de $\mathcal{L}$ alors $\mathcal{M} = \cup_{c\in\mathcal{C}} c$ est un majorant de $\mathcal{C}$, c'est aussi une partie libre de E :
En effet, si $\sum_{i=1}^{n} k_i e_i = 0$ avec $k_i \in K$ et $e_i \in \mathcal{M} = \cup_{c\in\mathcal{C}} c$ alors,
$(\forall i \in \{1,..,n\})(\exists c_i \in \mathcal{C}) e_i \in c_i$: les e_i sont des items d'au plus n parties libres c_i distinctes de $\mathcal{C}$, comme ces n parties sont totalement ordonnées par inclusion, la famille $(c_i)_{1\leq i\leq n}$ admet un plus grand élément c^* dans $\mathcal{C}$: autrement dit $\sum_{i=1}^{n} k_i e_i$ est une combinaison linéaire nulle sur la partie libre c^*, ce qui entraîne que $k_i = 0 \ \forall i \in \{1, ..., n\}$.
Ceci étant vrai pour toute combinaison linéaire sur $\mathcal{M}$, il suit que $\mathcal{M}$ **est une partie libre de** E.
$\mathcal{L}$ est donc une partie non vide et inductive de E et, par application du lemme de Zorn, il existe un élément $\mathcal{B}$ de $\mathcal{L}$ qui est maximal pour l'ordre de l'inclusion.
$\mathcal{B}$ est une base de E : Soit $x \in E$, si x est un vecteur de $\mathcal{B}$ il est égal à $1.x$ et c'est une combinaison linéaire de vecteurs de $\mathcal{B}$.
Si $x \notin \mathcal{B}$ alors la partie $\mathcal{B}' = \mathcal{B} \cup \{x\}$ n'est pas libre car si elle l'était $\mathcal{B}$ ne serait pas une partie libre maximale. Il existe alors une combinaison linéaire

nulle à coefficients non tous nuls de vecteurs de $\mathcal{B}'$, et le coefficient de x, item de $\mathcal{B}'$ n'est pas 0 car alors il existerait une combinaison linéaire nulle à coefficients non tous nuls de vecteurs de la partie libre $\mathcal{B}$. Si $\lambda x + \sum_{i=1}^{n} \lambda_i e_i = 0$ avec $\lambda \neq 0,\ e_i \in \mathcal{B}$ était cette combinaison linéaire alors $x = -\sum_{i=1}^{n} \frac{\lambda_i}{\lambda} e_i$ est combinaison linéaire de vecteurs de $\mathcal{B}$.
On a prouvé que $\mathcal{B}$ est une partie génératrice de E et, comme c'est déjà une partie libre : c'est une base de E.

Théorème de la dimension finie : Soit $(E, +, .)$ un espace vectoriel sur $(K, +, \times)$, s'il existe une base $\mathcal{B}$ de E finie alors toute base est finie et a même nombre d'éléments que $\mathcal{B}$.
Preuve : Nous montrons le
Lemme : Soit $(E, +, .)$ un espace vectoriel sur $(K, +, \times)$, s'il existe une base $\mathcal{B}$ de E a n éléments alors toute partie libre de E a au plus n éléments (et est donc finie).
Pour prouver ce lemme nous allons utiliser un algorithme : l'algorithme du pivot dont l'introduction nécessite l'introduction de définitions nouvelles et d'un vocabulaire spécifique.
Nous considérons $(E, +, .)$ un espace vectoriel sur $(K, +, \times)$ dont $\mathcal{B} = \{b_1, \ldots, b_n\}$ **est une base**

finie et définissons à partir du corps K des espaces vectoriels admettant des bases finies.

- $(K, +, \times)$ est un espace vectoriel sur lui-même dont 1, le neutre pour $\times$ est une base, on peut appeler cet espace vectoriel l'espace vectoriel des scalaires.
- Si $n \in \mathbb{N}$ et $n > 1$ et si on définit sur K^n des opérations interne + et externe . suivantes : $\forall i / 1 \leq i \leq n,\ a_i, b_i \in K$

  $$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

  et $\forall \lambda \in K$

  $$\lambda.(a_1, \ldots, a_n) = (\lambda \times a_1, \ldots, \lambda \times a_n)$$

  alors $(K^n, +, .)$ est un espace vectoriel sur K dont le neutre pour + est $(0, \ldots, 0)$, on peut appeler cet espace vectoriel l'espace vectoriel des vecteurs d'ordres n.
- Si $p, q \in \mathbb{N}$ alors on appelle $M_{p,q}(K)$ l'ensemble des tableaux d'éléments de K à p lignes et q colonnes, on appelle **matrice à p lignes et q colonnes un élément** $M = (m_{i,j})_{1 \leq i,j \leq p} \in M_{p,q}(K)$. Si $p = q$ on note $M_p(K)$ à la place de $M_{p,p}(K)$ et on appelle **matrices carrées (et plus simplement matrices) d'ordre** p les éléments de $M_p(K)$. Si $(m_{i,j})_{1 \leq i,j \leq p}, (n_{i,j})_{1 \leq i,j \leq p} \in M_{p,q}(K)$

alors on pose :
– $(m_{i,j})_{1\leq i,j\leq p}+(n_{i,j})_{1\leq i,j\leq p} = (m_{i,j}+n_{i,j})_{1\leq i,j\leq p}$
– $\forall\lambda \in K,\ \lambda.(m_{i,j})_{1\leq i,j\leq p} = (\lambda \times m_{i,j})_{1\leq i,j\leq p}$
$(M_{p,q}(K), +, .)$ est un espace vectoriel isomorphe à $K^{p\times q}$ au moyen de

$$\Phi\ :\begin{cases} M_{p,q}(K) \longrightarrow K^{q\times p} \\ (m_{i,j})_{1\leq i,j\leq p} \mapsto (m_{1,1},\ldots,m_{1,q},\ldots,m_{p,1},\ldots,m_{p,q}) \end{cases}$$

ou de

$$\Psi\ :\begin{cases} M_{p,q}(K) \longrightarrow K^{p\times q} \\ (m_{i,j})_{1\leq i,j\leq p} \mapsto (m_{1,1},\ldots,m_{p,1},\ldots,m_{1,q},\ldots,m_{p,q}) \end{cases}$$

Soient $\mathcal{B} = \{b_1,\ldots,b_n\}$ et $\mathcal{P} = \{x_1, x_2,\ldots,x_{n+1}\}$ inclus dans E nous montrons que $\mathcal{P}$ n'est pas une partie libre. Posons $\forall i \in [1, n+1] \cap \mathbb{N}$, $x_i = \sum_{j=1}^{n} a_{i,j}b_j$ et considérons **la matrice** $(a_{i,j})_{1\leq i\leq n+1,\ 1\leq j\leq n}$: il est à noter que $(a_{i,j})_{1\leq i\leq n+1,\ 1\leq j\leq n}$ **n'est pas la matrice de la partie $\mathcal{P}$ dans la base $\mathcal{B}$** puisque sa définition découle d'ordres implicites sur les vecteurs de $\mathcal{B}$ et de $\mathcal{P}$ obtenus par les indexation : $i \mapsto b_i$ et $j \mapsto x_j$; En effet, puisque nous considérons les vecteurs b_i et x_j **dans leur ensemble**, toute matrice obtenue à partir de $(a_{i,j})_{1\leq i\leq n+1,\ 1\leq j\leq n}$ par permutation de lignes et colonnes pourrait aussi être nommée de cette manière. $(a_{i,j})_{1\leq i\leq n+1,\ 1\leq j\leq n}$ est un élément de $M_{n+1,n}(K)$, obtenu en fixant un ordre sur les **partie finies $\mathcal{B}$ et $\mathcal{P}$** auquel nous allons **appli-**

quer un algorithme dont voici une description en «pseudo-langage algorithmique» :
nous entendons par là la description du fonctionnement d'un automatisme réalisé par une machine programmable imaginaire (autrement dit une **machine virtuelle**) supposée pouvoir réaliser des calculs suivant un langage compréhensible par un lecteur humain, ce qui nécessite d'introduire quelques éléments du dit pseudo-langage algorithmique.

- Chaque instruction est terminée par ;
- L'affectation : A :=B ;
  Si A et B sont des objets de même nature, B pouvant être une expression comme $x^2 + 1$, $A := B$ signifie : Le contenu de A (sa valeur) est remplacé par le contenu de B.
- L'instruction conditionnelle :
  Si $<$ *condition* $>$ **alors**
  $instruction_1$;
  $\vdots$
  $instruction_n$;
  sinon
  $autre\_instruction_1$;
  $\vdots$
  $autre\_instruction_m$;
  finsi ;
  Si $<$ *condition* $>$ est vraie alors la machine

virtuelle exécute les n premières instructions, sinon la machine virtuelle exécute les m autres instructions.

- La boucle itérative :
  Pour $i := m$ à n
  $instruction_1$;
  $\vdots$
  $instruction_p$;
  finpour ;
  Exécuter itérativement ($m - n + 1$ fois) une suite de p instructions.
- La fonction
  - Appeler une fonction :
    Par exemple :
    $n := 30;$
    $z := f(n);$
    f dépend de n et est déclarée en début d'algorithme (voir Déclarer une fonction).
  - Déclarer une fonction : dans la liste des instructions figure au moins une affectation de la variable que l'on retourne (dans l'exemple z).
    Fonction f(*liste_de_paramètres*)
    $instruction_1$;
    $\vdots$
    $instruction_n$;

Retourner z ;
finfonction ;
Parmi les instructions du corps de fonction peuvent figurer des appels à d'autres fonctions ou à f elle-même, f est dans ce dernier cas dite récursive, comme c'est le cas de la fonction factorielle qui suit :
Fonction factorielle(n)
Si $n = 0$ **alors**
$f := 1$;
sinon
$f := n \times factorielle(n-1)$;
finsi ;
Retourner f ;
finfonction ;

- **STOP** ; : arrêt de l'algorithme sans enchaîner les instructions suivantes.
- Commentaires : tout ce qui est écrit entre /* et */ n'est pas exécutable et a valeur de notes ou commentaires. Par exemple : /* ceci est un commentaire */

Voici l'algorithme du pivot : A étant une matrice $l_i(A)$ désignera son i-ème vecteur ligne.

/*$\mathcal{B} = \{b_1, \ldots, b_n\}$ est une base de E et $\mathcal{P} = \{x_1, x_2, \ldots, x_{n+1}\}$ une partie de E à $n+1$ éléments. $\forall i \in [1, n+1] \cap \mathbb{N},\ x_i = \sum_{j=1}^{n} a_{i,j} b_j$ et $A = (a_{i,j})_{1 \leq i \leq n+1,\ 1 \leq j \leq n}$ */

Fonction $Pivot(A, n)$/* $A \in M_{n+1,n}(K)$*/

$B := A$;

Si $n = 1$ **alors**

Retourner B ;

STOP ;

finsi ;

/*$B = (b_{i,j})_{1 \leq i \leq n+1,\ 1 \leq j \leq n} = (a_{i,j})_{1 \leq i \leq n+1,\ 1 \leq j \leq n}$ */

Si $\exists i \in [1, n+1] \cap \mathbb{N} / l_i(B) = 0$ **alors**

Retourner B ;

STOP ;

sinon

Si $b_{1,1} = 0$ **alors**

$B := permuter\_colonnes(B)$; /*permuter_colonnes est une fonction qui permute les colonnes de la matrice B -dont aucune ligne n'est identiquement nulle- de façon à ce la matrice obtenue a pour coefficient de premières ligne et colonne un coefficient non nul. Après l'appel de permuter_colonnes $b_{1,1} \neq 0$*/

Pour $j := 2$ à $n+1$

$l_j(B) := l_j(B) - (b_{1,j} \times b_{1,1}^{-1}).l_1(B)$;

finpour ;

/*Après ces n affectations les coefficients $b_{1,j}$ avec $j \geq 2$ de la première colonne de B* deviennent $b_{1,j} - (b_{1,j} \times b_{1,1}^{-1}).b_{1,1}$ soit 0*/
$B := matrice\_extraite(B, n)$; /*matrice_extraite(B,n) est une fonction qui renvoie la matrice extraite de B -qui a n lignes et n colonnes- obtenue en supprimant les premières ligne et colonne de B*/
$n := n - 1$;
$B := Pivot(B, n)$;/*Appel récursif de la fonction Pivot*/
Retourner B ;
STOP ;
finsi ;
finfonction ;

Description de l'algorithme Pivot : Si une ligne de la matrice initiale A est nulle et $\mathcal{P}$ n'est pas une partie libre, sinon le coefficient de la première ligne et première colonne de A n'est pas nulle (à permutation de colonne près). A l'issue des **éliminations** exprimées par les n instructions $l_j(B) := l_j(B) - (b_{1,j} \times b_{1,1}^{-1}).l_1(B)$, $A = A_0$ devient la matrice écrite par blocs $A_1 = \begin{pmatrix} a_{11} & v \\ 0 & B \end{pmatrix}$ $a_{11} \in K\backslash\{0\}$ et $B \in M_{n,n-1}(K)$. L'appel récursif de Pivot appliquée à B amorce une récurrence : si une ligne de B est nulle l'algorithme Pivot s'arrête sinon (à permutation de colonnes près) le coefficient de premières lignes et colonnes de B n'est pas nul et les $n-1$ éliminations qui suivent transforment A_1 en A_2 écrite par blocs $A_2 = \begin{pmatrix} a_{11} & v & \\ 0 & b_{11} & w \\ 0 & 0 & C \end{pmatrix}$......

Cet algorithme s'arrête puisqu'il décrémente n et que $n = 1$ déclenche l'instruction STOP, s'il s'arrête pour une valeur de n au moins égale à 2 alors **l'élimination triangulaire** (on retranche d'abord un multiple de la première ligne, puis de la deuxième...) et la **condition d'arret** (une ligne nulle) **équivallent à l'existence d'une combinaison linéaire nulle à coefficients non tous nuls des x_j qui ne constituent pas une**

partie libre. Si n décrémente jusqu'à la valeur 1 alors **l'élimination triangulaire** (on retranche d'abord un multiple de la première ligne, puis de la deuxième...enfin la n-ième) transforme A en une matrice $A_n = \begin{pmatrix} M \\ l \end{pmatrix}$ M est une matrice d'ordre n **triangulaire supérieure à diagonale non nulle ce qui entraîne que sa dernière ligne est à coefficients nuls sauf le dernier**, l est une ligne dont tous les coefficients sont nuls sauf le dernier : on peut alors **annuler l en lui retranchant un multiple de la dernière ligne de l**. On a obtenu une combinaison linéaire nulle des x_j : **Cette combinaison linéaire est à coefficients non tous nuls puisque on n'a pas retranché au cours de l'algorithme la dernière ligne dont le coefficient multiplicateur est alors 1.** Ceci démontre le lemme.

Preuve du théorème de la dimension finie : Soit B une base finie (de cardinal n) d'un espace vectoriel E et B' une autre base alors B' est fini (dans le cas contraire $n+1$ éléments de B' sont liés et B' n'est pas une base). Par deux applications du lemme qui précède B' a au plus n éléments et B a au plus autant d'éléments que B' : B et B' ont donc même cardinal n.