

Modules sur un anneau

DÉFINITION 6.1. Soit $(A, +, \cdot)$ un anneau, un A -module (à gauche) est un groupe commutatif $(M, +)$ muni d'une loi de multiplication externe

$$\bullet * \bullet : \begin{array}{ccc} A \times M & \mapsto & M \\ (a, m) & \mapsto & a * m \end{array}$$

(appelée multiplication par les scalaires) ayant les propriétés suivantes:

(1) Associativité: $\forall a, a' \in A, m \in M,$

$$(a \cdot a') * m = a * (a' * m).$$

(2) Distributivité: $\forall a, a' \in A, m, m' \in M,$

$$(a + a') * m = a * m + a' * m, \quad a * (m + m') = a * m + a * m'.$$

(3) Neutralité de 1_A : $\forall m \in M,$

$$1_A * m = m.$$

Rmq: $\forall m \in M \quad (-1_A) * m = -m.$

$$(1_A + (-1)_A) * m = 0_A * m = 0_M = m + (-1)_A * m$$

Exemples: A est un A -module sur lui-même
on définit la multiplication externe
comme étant la multiplication usuelle

$$\begin{aligned} A \times A &\longrightarrow A \\ (a, a') &\longrightarrow a \cdot a' \end{aligned}$$

— $I \subset A$ un idéal (à gauche) de A
tq $\forall m \in I \quad a \in A \quad a \cdot m = m' \in I$

Module libre (de rang $d \geq 1$)

$$M = A^d = A \times \dots \times A \quad d \text{ fois.}$$

$$m = (a_i)_{i=1 \dots d} \quad m' = (a'_i)_{i=1 \dots d}$$

$$m + m' = (a_i + a'_i)_{i=1 \dots d}$$

$$(a_1, a_2, \dots, a_d) + (a'_1, \dots, a'_d) := (a_1 + a'_1, \dots, a_d + a'_d)$$

$$\cdot \quad \mathcal{O}_{A^d} = (\mathcal{O}_A, \dots, \mathcal{O}_A)$$

multiplication externe (par les scalaires)

$$a \in A \quad m = (a_1, \dots, a_d) \in A^d$$

$$a * m = (a.a_1, \dots, a.a_d)$$

On voit que A^d muni de cette multiplication externe est un A -module

le A -module de rang d .
libre

— $(M, +)$ est un gpe commutatif
alors M est automatiquement un $\mathbb{Z}$ -module
la loi externe étant

$$k \in \mathbb{Z}, m \in M \longrightarrow k * m = \underbrace{m + \dots + m}_{k \text{ fois}} \text{ si } k \geq 1 \\ = -(\underbrace{m + \dots + m}_{|k| \text{ fois}}) \text{ si } k < 0$$

$$\text{et } 0.m = 0_M$$

- $X = \text{ens}$ A anneau

$$\mathcal{F}(X; A) = \{ f: X \rightarrow A \}$$

est un grp commutatif pour +

$$f + g: x \mapsto f(x) +_A g(x)$$

c'est un A -module en posant pour

$$a \in A \quad f \in \mathcal{F}(X; A) \quad a \cdot f: x \mapsto a \cdot_A f(x)$$

- $A[x]$ = l'anneau des polynômes à coeffs ds A (A est commutatif)

$$A[x] = \left\{ P(x) = a_0 + a_1x + \dots + a_dx^d \mid d \geq 0, a_0, \dots, a_d \in A \right\}$$

$A[x]$ est un A -module:

$$a \in A \quad P(x) \in A[x] \quad \begin{matrix} a * P(x) \\ a \cdot P(x) \end{matrix} = \begin{matrix} a \cdot a_0 + a \cdot a_1x + \dots + a \cdot a_dx^d \end{matrix}$$

- A commutatif. $M_2(A) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in A \right\}$

$$a \in A \quad m = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in M_2(A)$$

$$a * m = \begin{pmatrix} aa' & ab' \\ ac' & ad' \end{pmatrix}$$

$M_2(A)$ est un A module.

REMARQUE 5.1.1. On defini de maniere analogue la notion de A -module a droite a partir d'une multiplication externe "a droite"

$$\bullet *_d \bullet : \begin{array}{ccc} M \times A & \mapsto & M \\ (m, a) & \mapsto & m *_d a \end{array}$$

verifiant des proprietes analogues notamment l'associativite

$$\forall a, a' \in A, m \in M, m *_d (a.a') = (m *_d a) *_d a'.$$

Sous-module

DÉFINITION 6.3. Soit M un A -module. Un sous-module $N \subset M$ d'un A -module M est un sous-groupe de $(M, +)$ qui est stable pour la multiplication par les scalaires:

$$\forall a \in A, n \in N, a * n \in N.$$

On a donc $\forall n, n' \in N, a, a' \in A$

$$a * n + a' * n' \in N$$

PROPOSITION 6.1. (Critère de sous-module) Soit $N \subset M$ un sous-ensemble d'un A -module M alors N est un sous-module de M ssi

$$(6.1.1) \quad \forall a \in A, n, n' \in N, a * n + n' \in N.$$

^
non vide

Exemples $\{0_M\} \subset M$: le sous-module nul.

- sous-module engendré par $m \in M$

$A * m = \{ a * m \mid a \in A \}$ est un sous- A -module de M

$$- M = A^d \quad d \geq 1$$

$$\Delta A = \left\{ (a, a, \dots, a) = a * (\underbrace{1_A, \dots, 1_A}_{d \text{ fois}}) \right. \\ \left. a \in A \right\}$$

$$= A \cdot \underline{1}_A \quad \underline{1}_A = (\underbrace{1_A, \dots, 1_A}_{d \text{ fois}})$$

$$- A[X] \supset A[X]_{\leq d} = \left\{ P(X) \in A[X] \right. \\ \left. \deg P \leq d \right\}$$

$$A[x]_{\leq d} = \{a_0 + a_1x + \dots + a_dx^d \mid a_0, \dots, a_d \in A\}$$

c'est un sous- A -module de $A[x]$.

Module engendré par un
ensemble

PROPOSITION 6.2. Soit $(M, +, *)$ un A -module et M_1, M_2 des sous-modules alors

$$M_1 \cap M_2 \subset M$$

est un sous-module et plus généralement soit $(M_i)_{i \in I}$ une collection de sous-modules alors

$$\bigcap_{i \in I} M_i \subset M$$

est un sous-module.

Preuve: $M_1, M_2 \subset M$ des ssmodules
on montre que $M_1 \cap M_2$ vérifie le critère
de ss-module:

soient $m, m' \in M_1 \cap M_2$, $a \in A$ on veut $a * m$
 $a * m + m' \in M_1 \cap M_2$ mais comme M_1 et
 M_2 sont des sous-modules

$$a * m + m' \in M_1, \quad a * m + m' \in M_2$$

$$\Rightarrow a * m + m' \in M_1 \cap M_2$$



DÉFINITION 6.4. Soit $X \subset M$ un sous-ensemble d'un A -module, le module engendré par X est le plus petit sous-module de M contenant X (l'intersection de tous les sous-modules contenant X):

$$\langle X \rangle_A := \bigcap_{\substack{X \subset N \subset M \\ N \text{ } A\text{-mod}}} N.$$

PROPOSITION 6.3. Soit $X \subset M$ un ensemble alors $\langle X \rangle_A$ est soit le module nul $\{0_M\}$ si X est vide, soit l'ensemble des combinaisons linéaires d'éléments de X à coefficients dans A :

$$\langle X \rangle_A = \text{CL}_A(X) := \left\{ \sum_{i=1}^n a_i * x_i, \ n \geq 1, \ a_1, \dots, a_n \in A, \ x_1, \dots, x_n \in X \right\}.$$

Preuve $= a_1 * x_1 + \dots + a_n * x_n$

Si $X = \emptyset$ $\{0_M\}$ contient $\emptyset$ et c'est le + petit sous-module de cette forme.

Si $X \neq \emptyset$ On considère

$$CL_A(X) = \left\{ a_1 * x_1 + \dots + a_n * x_n \quad \begin{array}{l} a_i \in A \quad x_i \in X \\ n \geq 1 \end{array} \right\}$$

il contient X : $x \in X \quad x = 1_A * x$

$CL_A(X)$ est un ss module de M :

Critère : $m, m' \in CL_A(X) \quad a \in A$

$$m = a_1 * x_1 + \dots + a_n * x_n, \quad m' = a'_1 * x'_1 + \dots + a'_n * x'_n$$

alors $a * m + m' =$

$$\begin{aligned} & a * (a_1 * x_1 + \dots + a_n * x_n) + a'_1 * x'_1 + \dots + a'_{n'} * x'_{n'} \\ = & a * (a_1 * x_1) + \dots + a * (a_n * x_n) + a'_1 * x'_1 + \dots + a'_{n'} * x'_{n'} \\ = & (a \cdot a_1) * x_1 + \dots + (a \cdot a_n) * x_n + a'_1 * x'_1 + \dots + a'_{n'} * x'_{n'} \end{aligned}$$

= est un CL à $n+n'$ termes d'éléments

de X : $x_1, \dots, x_n, x'_1, \dots, x'_{n'}$

multipliés par des elts de A : $a \cdot a_1, \dots, a \cdot a_n$
 $a'_1, \dots, a'_{n'}$

$$\Rightarrow a * m + m' \in CL_A(X)$$

$CL_A(X)$ est un ss module contenant

$$X \Rightarrow \langle X \rangle_A \subset CL_A(X)$$

Pour conclure il reste à vérifier que
si N est un ss module contenant X
alors il contient toute combinaison
linéaire

d'elts de X a coeffs dans A :

$$\forall x_1, \dots, x_n \in X \subset N, \quad a_1, \dots, a_n \in A$$

comme N est stable par $+$ et $*$ on a que

$$a_1 * x_1 + \dots + a_n * x_n \in N$$

$$\Rightarrow X \subset N \text{ alors } CL_A(X) \subset N \quad \square$$

DÉFINITION 6.5. Si $\langle X \rangle_A = M$, on dit que X est une famille génératrice de M .

DÉFINITION 6.6. Un A -module M est de type fini si il possède une famille génératrice qui est finie.

Explicitement: il existe $n \geq 1$ et
 $e_1, \dots, e_n \in M$ tq tout $m \in M$ peut
s'écrire $m = a_1 * e_1 + \dots + a_n * e_n$
avec $a_1, \dots, a_n \in A$.

Exemple: $A^d = \{ (a_1, a_2, \dots, a_d) \mid a_i \in A \}$

A^d est de type fini: on prend

$$B_d = \{ e_1, \dots, e_d \} \subset A^d$$

$$e_1 = (1_A, 0_A, \dots, 0_A),$$

$$e_2 = (0_A, 1_A, 0_A, \dots, 0_A) \dots e_d = (0_A, \dots, 0_A, 1_A)$$

B_d engendre A^d : soit $(a_1, \dots, a_d) \in A^d$
on a

$$\begin{aligned}(a_1, \dots, a_d) &= a_1 * e_1 + a_2 * e_2 + \dots + a_d * e_d \\ &= (a_1, 0_A, \dots, 0_A) + (0_A, a_2, 0_A, \dots, 0_A) + \dots + \\ &\quad + (0_A, \dots, 0_A, a_d)\end{aligned}$$

B_d est appelée Base canonique de A^d .

- $A[x]$ est engendré comme A -module
par les monômes

$$\{1_A, x, x^2, \dots, x^d, x^{d+1}, \dots\}$$

- $A[x]_{\leq d}$ est engendré par

$$\{1_A, x, \dots, x^{d-1}, x^d\}$$

- $A = \mathbb{Z} \quad M = \mathbb{Z}^2$

$\mathbb{Z}^2$ est engendré par $\{(1,0), (0,1)\}$

et si $a, b, c, d \in \mathbb{Z}$ tq

$ad - bc = \pm 1$ alors $\mathbb{Z}^2$ est engendré

par $\{(a,b), (c,d)\}$.

Morphismes

DÉFINITION 5.7. Soit A un anneau et M, N des A -modules, un morphisme de A -modules entre M et N est un morphisme de groupes **additifs**

$$\varphi : M \mapsto N$$

qui est compatible avec les lois de multiplications externes $*_M$ et $*_N$:

$$\forall a \in A, m \in M, \varphi(a *_M m) = a *_N \varphi(m).$$

Rmq: on a $\forall a, a' \in A \quad m, m' \in M$

$$\varphi(a *_M m +_M a' *_M m') = a *_N \varphi(m) +_N a' *_N \varphi(m')$$

Plus généralement si on a $m_1, \dots, m_i \in M$
 $a_1, \dots, a_i \in A$

$$\varphi(a_1 *_M m_1 + \dots + a_i *_M m_i) = a_1 *_N \varphi(m_1) + \dots + a_i *_N \varphi(m_i)$$

LEMME 5.1. (Critere d'application lineaire) Soit $\varphi : M \mapsto N$ une application entre deux A -modules alors φ est un morphisme (ie. est A -lineaire) si et seulement si

$$(5.1.2) \quad \forall a \in A, m, m' \in M, \varphi(a *_M m + m') = a *_N \varphi(m) + \varphi(m').$$

Preuve: si on prend $a = 1_A$ ou a

$$\varphi(1_A * m + m') = 1_A * \varphi(m) + \varphi(m')$$

$$\varphi(m + m') = \varphi(m) + \varphi(m')$$

$\Rightarrow \varphi$ est un morphisme de groupes additifs

$$\Rightarrow \varphi(0_M) = 0_N$$

$$\varphi(a * m + 0_H) = a * \varphi(m) + \varphi(0_H)$$

$$- \varphi(a * m) = a * \varphi(m)$$

- φ vérifie: morphisme de gpc
et compatibilité avec $*$

φ est un morphisme de A -modules.

Réciproquement si φ est un morphisme de A -modules

$$\begin{aligned}\varphi(a * m + m') &= \varphi(a * m) + \varphi(m') \\ &= a * \varphi(m) + \varphi(m').\end{aligned}$$



Noyau - Image

PROPOSITION 5.4. Soit $\varphi : M \mapsto N$ un morphisme de A -modules et $M' \subset M$ et $N' \subset N$ des sous-modules alors

$$\varphi(M') \subset N \text{ et } \varphi^{(-1)}(N') \subset M$$

sont des sous-modules de M et N respectivement. En particulier

$$\ker(\varphi) = \varphi^{(-1)}(\{0_N\}) \subset M \text{ et } \operatorname{Im}(\varphi) = \varphi(M) \subset N$$

sont des sous A -modules.

Preuve pour $\varphi^{(-1)}(N')$: soit $a \in A$ $m, m' \in \varphi^{(-1)}(N')$
 $N' \subset N$ ss-module.

$$\text{on a } \varphi(m) = n, \varphi(m') = n' \in N'$$

$$\Rightarrow a * n + n' \in N' \quad (N' \text{ est un ss module})$$

$$a + n + n' = a + \varphi(m) + \varphi(m') \in N'$$

$$= \varphi(a + m + m')$$

$$\Rightarrow a + m + m' \in \varphi^{(-1)}(N')$$

$\varphi^{(-1)}(N')$ est un ssmodule de M .

.....



Rappel: soit φ un morphisme de A -
module alors

φ est injectifssi $\ker \varphi = \{0_M\}$.

PROPOSITION 5.5. Soient $\varphi : L \mapsto M$ et $\psi : M \mapsto N$ des morphismes de A -modules alors

- $\psi \circ \varphi : L \mapsto N$ est un morphisme de A -modules.
- Si $\varphi : L \mapsto M$ est bijectif alors $\varphi^{-1} : M \mapsto L$ est un morphisme de A -modules.

NOTATION 5.1. On note

$$\mathrm{Hom}_{A\text{-mod}}(M, N), \quad \mathrm{Isom}_{A\text{-mod}}(M, N),$$

$$\mathrm{End}_{A\text{-mod}}(M) = \mathrm{Hom}_{A\text{-mod}}(M, M),$$

$$\mathrm{Aut}_{A\text{-mod}}(M) = \mathrm{GL}_{A\text{-mod}}(M) = \mathrm{Isom}_{A\text{-mod}}(M, M)$$

les ensembles de morphismes, morphismes bijectifs (ou isomorphismes), d'endomorphismes et d'automorphismes des A -modules M et N .

COROLLAIRE 5.2. L'ensemble $\mathrm{Aut}_{A\text{-mod}}(M) \subset \mathrm{Bij}(M)$ est un sous-groupe de $\mathrm{Bij}(M)$. Plus précisément $\mathrm{Aut}_{A\text{-mod}}(M)$ est un sous-groupe de $\mathrm{Aut}_{Gr}(M)$.

PROPOSITION 5.6. Soient M et N des A -modules alors $\text{Hom}_{A\text{-mod}}(M, N)$ a une structure naturelle de groupe commutatif. Si de plus A est commutatif alors $\text{Hom}_{A\text{-mod}}(M, N)$ a une structure naturelle de A -module.

Preuve: on defini une addition sur $\text{Hom}_{A\text{-mod}}(M, N)$
en posant pour φ, ψ de tels morphisme

$$\varphi + \psi : m \in M \longrightarrow \varphi(m) + \psi(m) \in N$$

$$\varphi + \psi \in \text{Hom}_{A\text{-mod}}(M, N).$$

$$\forall a \in A \quad m, m' \in M$$

$$(\varphi + \psi)(a * m + m') = \varphi(a * m + m') + \psi(a * m + m')$$

$$= a * \varphi(m) + \varphi(m') + a * \psi(m) + \psi(m')$$

$$= a * (\varphi(m) + \psi(m)) + \varphi(m') + \psi(m')$$

$$= a * (\varphi + \psi)(m) + (\varphi + \psi)(m')$$

Supposons A commutatif: on définit une multiplication externe sur $\text{Hom}_{A\text{-mod}}(\Pi, N)$

$$\forall a \in A \quad \varphi \in \text{Hom}_{A\text{-mod}}(\Pi, N)$$

$$a \star \varphi: m \longrightarrow a \star \varphi(m)$$

On veut montrer que $a \star \varphi$ est A -linéaire.

$$\forall a' \in A \quad m, m' \in \Pi \quad \text{on a}$$

$$(a * \varphi)(a' + m + m') \stackrel{?}{=} a' * (a + \varphi)(m) + (a + \varphi)(m')$$

$$\begin{aligned} (a * \varphi)(a' + m + m') &= a * (\varphi(a' + m + m')) \\ &= a * (a' * \varphi(m) + \varphi(m')) \end{aligned}$$

$$= a * (a' * \varphi(m)) + a * \varphi(m')$$

$$= (a \cdot a') * \varphi(m) + (a + \varphi)(m')$$

$$\stackrel{a' \cdot a}{\text{A is commutative}}$$

$$\begin{aligned}
 &= (a' \circ a) * \varphi(m) + (a \pm \varphi)(m') \\
 &= a' * (a \pm \varphi)(m) + a \pm \varphi(m')
 \end{aligned}$$



Algebre des Endomorphismes d'un A-module

PROPOSITION 5.6. Soient M et N des A -modules alors $\text{Hom}_{A\text{-mod}}(M, N)$ a une structure naturelle de groupe commutatif. Si de plus A est commutatif alors $\text{Hom}_{A\text{-mod}}(M, N)$ a une structure naturelle de A -module.

$$\psi, \varphi: M \rightarrow N$$

$$\psi + \varphi: m \rightarrow \varphi(m) + \psi(m)$$

$$a \in A \quad \varphi: M \rightarrow N$$

$$a * \varphi: m \rightarrow a \cdot \varphi(m)$$

$$N = M \quad \text{Hom}_A(M, M) = \text{End}_A(M)$$

est munis d'une composition

$$\varphi, \psi: M \rightarrow M$$

$$\varphi \circ \psi: M \rightarrow M$$

est encore A -linéaire $\varphi \circ \psi \in \text{End}_A(M)$

$$(\text{End}_A(M), +, \cdot, \underline{0}_M, \text{Id}_M)$$

forme un anneau.

Si de plus A est commutatif alors
 $\text{End}_A(M)$ est aussi un A -module.

On vérifie que la loi de multiplication
externe est associative par la composition
0.

$$a \in A \quad \varphi, \psi: M \rightarrow M$$

$$\begin{aligned} a * (\varphi \circ \psi): m &\rightarrow a. \varphi(\psi(m)) \\ &= \varphi(a. \psi(m)) \\ &= \varphi \circ (a + \psi)(m) \end{aligned}$$

"Associativité":

$$a * (\varphi \circ \psi) = (a + \varphi) \circ \psi = \varphi \circ (a + \psi)$$

DÉFINITION 5.8. soit A un anneau commutatif. Une A -algebre associative est un anneau $(B, +, \cdot_B)$ muni d'une structure de A -module, note $*$: $A \times B \mapsto B$ verifiant en plus des axiomes habituels

– Distributivite par rapport a la multiplication:

$$\forall a \in A, b, b' \in B, a * (b \cdot_B b') = (a * b) \cdot_B b' = b \cdot_B (a * b').$$

Associativité

THÉORÈME 5.1. *Soit M un A -module. L'ensemble $\text{End}_{A\text{-mod}}(M)$ des endomorphismes de M comme A -module est un sous-anneau de $(\text{End}_{\text{Gr}}(M), +, \circ)$ dont le groupe des unités est le groupe des automorphismes*

$$\text{End}_{A\text{-mod}}^{\times}(M) = \text{Aut}_{A\text{-mod}}(M) = \text{GL}_{A\text{-mod}}(M).$$

$\text{End}_{A\text{-mod}}(M)$ est l'anneau des endomorphismes de (du A -module) M .

De plus, si A est commutatif, $\text{End}_{A\text{-mod}}(M)$ possède une structure naturelle de A -module qui en fait une A -algèbre et $\text{End}_{A\text{-mod}}(M)$ est appelée

Algèbre des endomorphismes de (du A -module) M .

Espaces Vectoriels

*“An attempt at visualizing the Fourth Dimension:
Take a point, stretch it into a line,
curl it into a circle, twist it into a sphere,
and punch through the sphere.”*

DÉFINITION 5.9. Soit K un corps, un K -espace vectoriel (K -ev) V est simplement un K -module. Les éléments de V sont appelés vecteurs de V .

Exemples : K est un EV sur lui-même.

- $\{0_K\}$

- $d \geq 1 \quad K^d = \{(x_1, \dots, x_d) \mid x_i \in K\}$

$$\begin{aligned} v + w &= (x_1, \dots, x_d) + (y_1, \dots, y_d) \\ &= (x_1 + y_1, \dots, x_d + y_d) \end{aligned}$$

$$\lambda \in K \quad \lambda \cdot v = (\lambda x_1, \lambda x_2, \dots, \lambda x_d)$$

- Si V et W sont 2 K-ev

$$V \times W = \{ (v, w) \mid v \in V, w \in W \}$$

$$- (v, w) + (v', w') = (v +_V v', w +_W w')$$

$$- \lambda(v, w) = (\lambda \cdot_v v, \lambda \cdot_w w)$$

$$0_{V \times W} = (0_V, 0_W).$$

- X est

$$\mathcal{F}(X; K) = K^X = \{f: X \rightarrow K\}$$

est un K -ev.

- si V est un K -ev

$$\mathcal{F}(X; V) = V^X = \{f: X \rightarrow V\}$$

$$f + g: x \mapsto f(x) +_V g(x)$$

$$\lambda. f: x \mapsto \lambda \cdot f(x).$$

DÉFINITION 5.10. Soit V un K -espace vectoriel, un sous-espace vectoriel (SEV) de V est un sous- K module $W \subset V$.

PROPOSITION 5.7 (Critere de SEV). Un sous-ensemble $U \subset V$ d'un K -ev est un SEV ssi

$$\forall \lambda \in K, v, v' \in U, \lambda.v + v' \in U.$$

Ex: $\{0_V\}, V \subset V$

- $v \in V \quad K.v = \{ \lambda.v \mid \lambda \in K \} \subset V$

c'est un SEV.

- $V' \subset V, W' \subset W$ sont des ssev alors

$V' \times W' \subset V \times W$ est un sev.

- $\{(x_1, \dots, x_d) \in K^d \text{ tq } x_1 + \dots + x_d = 0_K\} \subset K^d$
est un sev.

- $\{(x_1, \dots, x_d) \in K^d \text{ tq } x_1 + \dots + x_d = 1_K\} \subset K^d$
n'est pas un sev. $0_{K^d} \notin \uparrow$

- $x_0 \in X \quad \{f \in \mathcal{F}(X, V) \mid f(x_0) = 0_V\} \subset \mathcal{F}(X, V)$
est un SEV.

- $\mathcal{F}(\mathbb{R}; \mathbb{R}) \supset$ fct paires et un sev

$$f: \mathbb{R} \rightarrow \mathbb{R} \quad \text{tq} \quad \forall x \quad f(-x) = f(x) \quad .$$

$\supset$ fct impaires et un sev.

$$f: \mathbb{R} \rightarrow \mathbb{R} \quad \text{tq} \quad \forall x \quad f(-x) = -f(x)$$

DÉFINITION 5.11. Soient V et W deux K -espaces vectoriels; un morphisme $\varphi : V \mapsto W$ de K -modules est appelé une application K -linéaire.

PROPOSITION 5.8 (Critère d'application linéaire). Une application entre espaces vectoriels $\varphi : V \mapsto W$ est linéaire ssi

$$\forall \lambda \in K, v, v' \in V, \varphi(\lambda.v + v') = \lambda.\varphi(v) + \varphi(v').$$

$$\varphi(\lambda_1.v_1 + \dots + \lambda_n.v_n) = \lambda_1.\varphi(v_1) + \dots + \lambda_n.\varphi(v_n)$$

$$\varphi \text{ est linéaire: } \ker \varphi = \{v \in V \mid \varphi(v) = 0_W\}$$

PROPOSITION 5.9. Si $\varphi : V \mapsto W$ est une application lineaire, le noyau

$$\ker \varphi = \{v \in V, \varphi(v) = 0_W\} \subset V$$

et l'image

$$\operatorname{Im} \varphi := \{\varphi(v), v \in V\} \subset W$$

sont des sous-espaces vectoriels de V et de W respectivement.

PROPOSITION 5.10. Soit $\varphi : V \mapsto W$ est une application lineaire, alors φ est injective ssi

$$\ker \varphi = \{0_V\}.$$

Exemples $V = K^d$ $W = K$ $i=1, \dots, d$

$$e_i^*: (x_1, \dots, x_d) \longrightarrow x_i$$

$e_i^*(v)$ = i-ième coord de v est linéaire

$$\ker e_i^* = \left\{ (x_1, \underset{\substack{\uparrow \\ \text{i-ième position}}}{0_K}, \dots, x_d) \mid x_1, \dots, x_d \in K \right\}$$

$$\varphi: K^2 \longrightarrow K^2 \text{ at lineaire}$$

$$(x, y) \longrightarrow (2x+y, x+y)$$

$$\ker \varphi = \{0_2\} \quad \operatorname{Im} \varphi = K^2$$

NOTATION 5.3. *On notera*

$$\mathrm{Hom}_{K\text{-ev}}(V, W), \mathrm{Isom}_{K\text{-ev}}(V, W),$$

$$\mathrm{End}_{K\text{-ev}}(V) = \mathrm{Hom}_{K\text{-ev}}(V, V), \mathrm{Aut}_{K\text{-ev}}(V) \text{ ~~est égal à~~ } = \mathrm{Isom}_{K\text{-ev}}(V, V)$$

les ensembles des applications lineaires, applications lineaires bijectives (ou isomorphismes), d'endomorphismes et d'automorphismes des K -espaces vectoriels V et W .

Pour simplifier on ecrira souvent

$$\mathrm{Hom}_K(V, W), \mathrm{Isom}_K(V, W), \mathrm{End}_K(V), \mathrm{Aut}_K(V)$$

PROPOSITION 5.11. *L'ensemble des automorphismes du K -ev V ,*

$$\text{Aut}_{K\text{-ev}}(V) = \text{Isom}_{K\text{-ev}}(V, V)$$

est un groupe pour la composition. On l'appelle également le groupe linéaire de V et on le note

$$\text{Aut}_K(V) =: \text{GL}(V).$$

PROPOSITION 5.11. *La composée de deux applications K -lineaires est K -linéaire : pour $\varphi \in \text{Hom}_K(U, V)$ et $\psi \in \text{Hom}_K(V, W)$ linéaires, alors $\psi \circ \varphi : U \mapsto W$ est K -linéaire et si φ est bijective alors $\varphi^{-1} : V \mapsto U$ est encore linéaire.*

Une combinaison linéaire de deux applications linéaires est linéaire: $\forall \varphi, \phi : U \mapsto V$ et $\forall \lambda \in K$, l'application

$$\lambda \cdot \underbrace{\varphi}_{\Psi} + \underbrace{\phi}_{\Psi} : u \in U \mapsto \lambda \varphi(u) + \phi(u) \in V$$

est K -linéaire.

THÉORÈME 5.2. *L'ensemble des application lineaires $\text{Hom}_K(V, W)$ a une structure naturelle de K -ev.*

L'ensemble des endomorphismes de V , $\text{End}_K(V)$ muni de l'addition et de la composition a une structure naturelle de K -algebre. Son groupe des unites est le groupe $\text{End}_{K\text{-ev}}(V)^\times = \text{Aut}_{K\text{-ev}}(V)$ des applications K -lineaires bijectives. C'est un sous-groupe de $\text{Bij}(V)$.

Formes lineaires

DÉFINITION 5.12. Une application lineaire de $\ell : V \mapsto K$ est également appelée une forme lineaire. L'espace des formes lineaires $\text{Hom}_K(V, K)$ est également note

$$\text{Hom}_K(V, K) = V^*.$$

On appelle également cet espace le dual de V .

$$\text{Ex: } S: (x_1, \dots, x_d) \longrightarrow x_1 + \dots + x_d$$

$$e_i^*: (x_1, \dots, x_d) \longrightarrow x_i.$$

SEV engendre par un
ensemble

PROPOSITION 5.12 (Les SEV sont stables par intersection). *Soit W_i , $i \in I$ une famille de SEV de V indexes par un ensemble I alors leur intersection*

$$\bigcap_{i \in I} W_i \subset V$$

est un SEV de V .

DÉFINITION 5.13. *Soit $\mathcal{F} \subset V$ un sous-ensemble, on note*

$$\langle \mathcal{F} \rangle_K = \text{Vect}(\mathcal{F}) \subset V$$

le sous-espace vectoriel (le sous- K module) engendré par $\mathcal{F}$.

On rappelle qu'il s'agit de manière équivalente

- de l'intersection de tous les SEV contenant $\mathcal{F}$,*
- de l'ensemble des combinaisons linéaires d'éléments de $\mathcal{F}$ à coefficients dans K*

$$\langle \mathcal{F} \rangle_K = \left\{ \sum_{i=1}^n \lambda_i \cdot x_i, \ n \geq 1, \ \lambda_1, \dots, \lambda_n \in K, \ x_1, \dots, x_n \in \mathcal{F} \right\}.$$

Somme de SEVs:

DÉFINITION 5.14. Soient $X, Y \subset V$ des sous-espaces d'un espace vectoriel.
Leur somme

$$X + Y := \langle X \cup Y \rangle \subset V$$

est par définition le sous-espace vectoriel engendré par les vecteurs de X et de Y .

LEMME 5.2. On a

$$X + Y = \{x + y, x \in X, y \in Y\}.$$

Preuve: si $x \in X$ et $y \in Y$ $x + y \in \langle X \cup Y \rangle = X + Y$
- $\{x + y \mid x \in X, y \in Y\} \subset X + Y$
et on vérifie que $X + Y \subset \{x + y \mid x \in X, y \in Y\}$
il suffit de montrer que $\{x + y\}$ est un SEV

Somme Directe

NOTATION 5.4. Si $X \cap Y = \{0_V\}$, on dit que X et Y sont en somme directe et on écrit

$$X \oplus Y \subset V$$

$$\uparrow X \cap Y = \{0_V\}$$

pour leur somme.

Si de plus

$$X \oplus Y = V$$

on dit que V est somme directe de X et Y . On dit alors que X et Y sont des espaces supplémentaires (dans V).

PROPOSITION 5.13. Soit $V = X \oplus Y$ la somme directe de deux sous-espaces supplémentaires X et Y alors l'écriture de tout vecteur $v \in V \in X \oplus Y$ sous la forme

$$v = x + y, \quad x \in X, \quad y \in Y$$

est unique.

Preuve : on suppose que $V = X + Y$ et $X \cap Y = \{0_V\}$
soit $v \in V$ $v = x + y$ $x \in X$ $y \in Y$

et si $v = x' + y'$ $x' \in X$ $y' \in Y$ on va m

$$x = x' \text{ et } y = y'.$$

$$v - v = 0_V = x - x' + y - y'$$

$$\Leftrightarrow \begin{array}{c} x - x' \\ \oplus \\ X \end{array} = \begin{array}{c} y' - y \\ \oplus \\ Y \end{array} \quad \begin{array}{l} x - x' \in X \cap Y = \{0_V\} \\ x = x' \text{ et } y' = y \end{array}$$

Projections: Supposons $V = X \oplus Y$

On définit $\pi_X: V \longrightarrow x \in X \in X$

$\pi_Y: V \longrightarrow y \in Y$

où $v = x + y$ est l'unique décomp
de v en un vecteur de X et un vecteur de Y

Ex: mq π_X et π_Y sont linéaires de V vers
 X et Y respectivement.

Familles Génératrices

Familles Libres

Bases

Famille génératrice

DÉFINITION 5.15. Soit V un K -e.v. Un sous-ensemble $\mathcal{G} \subset V$ est une famille génératrice si

$$\text{Vect}(\mathcal{G}) = \langle \mathcal{G} \rangle_K = V,$$

ie. tout élément $v \in V$ peut s'écrire sous la forme d'une combinaison linéaire (finie) à coefficients dans K d'éléments de $\mathcal{G}$: pour tout $v \in V$ il existe $n \geq 1$, $x_1, \dots, x_n \in K$, $\mathbf{e}_1, \dots, \mathbf{e}_n \in \mathcal{G}$ tels que

$$(5.3.1) \quad v = \sum_{i=1}^n x_i \mathbf{e}_i.$$

Si V admet une famille génératrice finie, on dit que V est un K -module ou un K -ev de type fini.

Ex: $V = K^d$ une famille gen est donnée
par la base canonique

$$B^0 = \{e_1, e_2, \dots, e_d\}$$

$$e_1 = (1, 0, \dots, 0), \dots, e_d = (0, \dots, 0, 1)$$

$$v = (x_1, \dots, x_d) \quad v = x_1 \cdot e_1 + \dots + x_d \cdot e_d$$

B^0 est génératrice de K^d

— $d=3$ $K=\mathbb{R}$ $V=\mathbb{R}^3$

$\{(1,1,0) \ (1,0,1) \ (0,1,1)\}$ est une famille
génératrice de $\mathbb{R}^3$

— $d=3$ $K = \text{Corps de } \text{Car}(K)=2$ ($2_K=1_K+1_K=0_K$)
 $2\mathbb{Z} = \ker(\text{Can}_K)$

par exemple $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$

✓

$\{(1,1,0), (1,0,1), (0,1,1)\}$ n'est pas génératif
de K^3 .

$$(1,1,0) + (1,0,1) + (0,1,1) = (2,2,2) = 2(1,1,1)$$

$\neq 0$ si $K = \mathbb{R}$ $\text{Cor}(K) \neq 2$
 $= \underset{3}{0}$ si $\text{Cor}(K) = 2$

Dimension

DÉFINITION 5.16. Soit V un K -ev de type fini. Si V est non-nul, sa dimension est le cardinal minimum d'une famille génératrice finie de V :

$$\dim(V) := \min_{\mathcal{G} \text{ génératrice}} |\mathcal{G}|.$$

Par convention, la dimension de l'espace vectoriel nul $\{0_V\}$ est

$$\dim(\{0_V\}) = 0$$

(on peut prendre la famille vide comme famille génératrice).

On dira également " K -ev de dimension finie" à la place de " K -ev de type fini".

Un espace vectoriel qui n'est pas de type fini est dit de "dimension infinie".

Thm fondamental de l'algèbre linéaire

THÉORÈME 5.3. *Tout K -espace vectoriel de dimension finie $d = \dim V$ est isomorphe (comme K -ev) à l'espace vectoriel K^d (avec la convention que $\{0_K\} = K^0$). En d'autres termes V est isomorphe au K -module libre de rang $d = \dim(V)$, K^d .*

Rmq: Un tel résultat est complètement faux
si K n'est pas un corps.

Exemple: $A = \mathbb{Z}$ les $\mathbb{Z}$ -modules sont exactement
les gres commutatifs et la plupart ne sont
de ceux de type fini

pas isomorphes à $\mathbb{Z}^d$.

- Si M est un grpe commutatif fini $(\mathbb{Z}/q\mathbb{Z})$
 M est de type fini mais
 $M \not\cong \mathbb{Z}^d$ $d \geq 1$.

Discussion: Soit $G = \{e_1, \dots, e_d\}$ une famille
generatrice finie $d \geq 1$ (a priori $d \geq \dim V$)

Dive que G est generatrice:

$$\begin{array}{ccc} \text{CL}_G : & K^d & \longrightarrow V \\ & (x_1, \dots, x_d) & \longrightarrow x_1 \cdot e_1 + \dots + x_d \cdot e_d \end{array}$$

l'application CL_G est surjective.

l'application CL_g est lineaire:

$$\forall \lambda \in K \quad x = (x_1, \dots, x_d) \quad x' = (x'_1, \dots, x'_d)$$

$$CL_g(\lambda x + x') = CL_g(\lambda x_1 + x'_1, \dots, \lambda x_d + x'_d)$$

$$= (\lambda x_1 + x'_1) \cdot e_1 + \dots + (\lambda x_d + x'_d) \cdot e_d$$

$$= \lambda(x_1 \cdot e_1 + \dots + x_d \cdot e_d) + x'_1 \cdot e_1 + \dots + x'_d \cdot e_d$$

$$= \lambda CL_g(x) + CL_g(x')$$

Pour donner un isomorphisme entre
 K^d et V il suffit de trouver
 g telle que CLg soit injective.

g ↙
generatrice

DÉFINITION. Soit V un K -e.v. Un sous-ensemble fini

$$\mathcal{G} = \{\mathbf{e}_1, \dots, \mathbf{e}_d\} \subset V$$

est une famille generatrice (du K -ev V) ssi les conditions equivalentes suivantes sont satisfaites:

(1) On a

$$\text{Vect}(\mathcal{G}) = V.$$

(2) pour tous $v \in V$, il existe $x_1, \dots, x_d \in K$ tels que

$$v = x_1 \cdot \mathbf{e}_1 + \dots + x_d \cdot \mathbf{e}_d.$$

(3) L'application lineaire

$$CL_{\mathcal{G}} : \begin{array}{ccc} K^d & \mapsto & V \\ (x_1, \dots, x_d) & \mapsto & x_1 \cdot \mathbf{e}_1 + \dots + x_d \cdot \mathbf{e}_d \end{array}$$

est surjective.

Si V admet une famille generatrice finie ou dit que V est un K -ev de type fini ou est de dimension finie. On a alors

$$\dim_K V \leq d.$$

THÉORÈME. Soit $\mathcal{G} \subset V$ une famille génératrice de V de cardinal $d = \dim V$ alors l'application $CL_{\mathcal{G}}$ est injective et définit donc un isomorphisme

$$CL_{\mathcal{G}} : K^d \simeq V.$$

Preuve: soit $\mathcal{G}$ génératrice finie de cardinal $d = \dim V$ (toute famille de cardinal $\leq d-1$ n'est jamais génératrice)

On suppose $CL_{\mathcal{G}}$ n'est pas injective

il existe $(v_1, \dots, v_d) \neq (0, \dots, 0) \in K^d$ tq

$$CL_g(v_1, \dots, v_d) = v_1 \cdot e_1 + \dots + v_d \cdot e_d = 0_V$$

quitte à permute les indices ops $v_d \neq 0_K$

$$v_d e_d = -v_1 \cdot e_1 - v_2 \cdot e_2 \dots - v_{d-1} e_{d-1}$$

$v_d \neq 0_K$ donc est inversible : on a (divisant par v_d)

$$e_d = y_1 \cdot e_1 + \dots + y_{d-1} \cdot e_{d-1}$$

avec $y_1 = -v_1 \cdot v_d^{-1} \dots y_{d-1} = -v_{d-1} \cdot v_d^{-1}$

On va montrer $\{e_1, \dots, e_{d-1}\}$ engendre V

Contradiction.

Soit $v \in V$ $v = \pi_1 e_1 + \dots + \pi_{d-1} e_{d-1} + \pi_d \cdot e_d$

$$\begin{aligned} v &= \pi_1 e_1 + \dots + \pi_{d-1} e_{d-1} + \pi_d \cdot (y_1 \cdot e_1 + \dots + y_{d-1} e_{d-1}) \\ &= \pi'_1 e_1 + \dots + \pi'_{d-1} e_{d-1} \end{aligned}$$

en posant

$$x'_i = x_i + x_d y_i$$

v est CL des vecteurs $\{e_1, \dots, e_{d-1}\}$,

$\{e_1, \dots, e_{d-1}\}$ est génératrice
contradiction



COROLLAIRE 5.3 (Critere dimensionel d'isomorphisme). Soient V, W des K -ev de dimensions finie d_V et d_W alors V et W sont isomorphes ssi ils ont meme dimension:

$$V \simeq W \iff d_V = d_W.$$

Preuve : si $d_V = d_W = d$ il existe des isom

$$\varphi: K^d \xrightarrow{\sim} V \quad \psi: K^d \xrightarrow{\sim} W$$

et alors

$$\psi \circ \varphi^{-1}: V \xrightarrow{\varphi^{-1}} K^d \xrightarrow{\psi} W$$

est un isomorphisme.

Réciproquement supposons que

$$\varphi: V \xrightarrow{\sim} W \text{ on a alors } d_V = d_W$$

Soit $G = \{e_1, \dots, e_{d_V}\}$ une famille génératrice
de V de taille d_V alors

$\varphi(G) = \{\varphi(e_1), \dots, \varphi(e_{d_V})\}$ est génératrice
pour W .

En effet: soit $w \in W$ comme φ est un
isom: $V \rightarrow W$ et donc $\varphi \rightarrow$
il existe $v \in V$ tq $w = \varphi(v)$

comme φ est génératrice on peut écrire

$$v = x_1 e_1 + \dots + x_{d_V} e_{d_V} \text{ pour certains } x_1, \dots, x_{d_V} \in K$$

$$w = \varphi(v) = \varphi(x_1 e_1 + \dots + x_{d_V} e_{d_V})$$

$$= x_1 \varphi(e_1) + \dots + x_{d_V} \varphi(e_{d_V}) = w$$

$\Rightarrow \varphi(G)$ est génératrice. on a donc

$$d_W \leq |\varphi(G)| = |G| = d_V$$

On a mg $d_W \leq d_V$. On montre

$d_V \leq d_W$ en utilisant $\varphi^{-1}: W \xrightarrow{\sim} V$.
 et en échangeant les rôles de V et W

$$\Rightarrow d_v = d_w.$$

Familles Libres

$$g = \{e_1, \dots, e_d\} \subset V$$

$$\begin{aligned} CL_g: K^d &\longrightarrow V \\ (x_1, \dots, x_d) &\longrightarrow x_1 \cdot e_1 + \dots + x_d \cdot e_d \end{aligned}$$

On a trouve des conditions telles que

$$CL_g \text{ soit injective.}$$

$$\iff \ker(CL_g) = \{0_d\}$$

DÉFINITION 5.17. Un sous-ensemble fini $\mathcal{F} = \{\mathbf{e}_1, \dots, \mathbf{e}_f\} \subset V$ d'un espace vectoriel est une famille libre de V si et seulement si l'une des trois conditions équivalentes suivante est satisfaite:

(1) L'application linéaire

$$CL_{\mathcal{F}} : \begin{array}{ccc} K^f & \mapsto & V \\ (x_1, \dots, x_f) & \mapsto & x_1 \cdot \mathbf{e}_1 + \dots + x_f \cdot \mathbf{e}_f \end{array}$$

est injective.

(2) pour tous $x_1, \dots, x_f, x'_1, \dots, x'_f \in K$

$$x_1 \cdot \mathbf{e}_1 + \dots + x_f \cdot \mathbf{e}_f = x'_1 \cdot \mathbf{e}_1 + \dots + x'_f \cdot \mathbf{e}_f \implies x_1 - x'_1 = \dots = x_f - x'_f = 0_K.$$

(3) pour tous $x_1, \dots, x_f \in K$

$$x_1 \cdot \mathbf{e}_1 + \dots + x_f \cdot \mathbf{e}_f = 0_V \implies x_1 = \dots = x_f = 0_K.$$

Une famille $\mathcal{F}$ qui n'est pas libre est dit liée.

Exemple : soit $e \in V - \{0_V\}$ alors

$\{e\}$ est libre : supposons que $x \cdot e = 0_V$
 si $x \neq 0$ x est inversible $x^{-1} \cdot x \cdot e = 0_V$
 $= e$

Exemple: la base canonique

$$V = K^d \quad B^o = \{e_1^o, \dots, e_d^o\}$$

$$e_1^o = (1, 0, \dots, 0) \quad \dots \quad e_d^o = (0, \dots, 0, 1)$$

B^o est libre: si

$$\begin{aligned} x_1 \cdot e_1^o + \dots + x_d e_d^o &= 0_{K^d} \Rightarrow x_1 = x_2 = \dots = x_d \\ &= (x_1, x_2, \dots, x_d) = (0, \dots, 0) \quad = 0 \end{aligned}$$

Example: $\{(1,1,0), (0,1,1), (1,0,1)\} \subset K^3$

- si $\text{car}(K) \neq 2$ alors cette famille est libre:

$$x_1(1,1,0) + x_2(0,1,1) + x_3(1,0,1) = (0,0,0)$$

$$\Rightarrow x_1 + x_3 = 0 \quad x_1 + x_2 = 0 \quad x_2 + x_3 = 0$$

$$\Rightarrow 2x_1 + x_2 + x_3 = 0 \Rightarrow 2x_1 = 0$$

$$2_K \text{ est inversible} \Rightarrow 2^{-1} 2x_1 = 0 = x_1$$

Si $\text{Car}(K) = 2$

$$(1, 1, 0) + (0, 1, 1) + (1, 0, 1) = (2, 2, 2) \\ = (0, 0, 0)$$

la famille est liée.

PROPOSITION 5.15. Une famille a l elements $\mathcal{F} = \{\mathbf{e}_1, \dots, \mathbf{e}_l\} \subset V$ est liée ssi il existe $i \in \{1, \dots, l\}$ tel que $\mathbf{e}_i$ peut s'exprimer comme combinaison lineaire des autres elements de $\mathcal{F}$:

$$\exists i \leq l, \mathbf{e}_i \in \text{Vect}(\mathcal{F} - \{\mathbf{e}_i\}) = \text{Vect}(\{\mathbf{e}_j, j \neq i\}).$$

On a alors

$$W = \text{Vect}(\mathcal{F}) = \text{Vect}(\mathcal{F} - \{\mathbf{e}_i\}).$$

Preuve: si $\mathcal{F}$ est liée: il existe

$x_1, \dots, x_l \in K$ non-tous nuls tq

$$x_1 \mathbf{e}_1 + \dots + x_l \mathbf{e}_l = \mathbf{0}_V$$

Supposons que $x_l \neq 0_K$ on a

$$x_l \mathbf{e}_l = - (x_1 \mathbf{e}_1 + \dots + x_{l-1} \mathbf{e}_{l-1})$$

$x_\ell \neq 0$ x_ℓ est inversible ds K

$$x_\ell^{-1} \cdot x_\ell \cdot e_\ell = e_\ell = y_1 e_1 + \dots + y_{\ell-1} e_{\ell-1}$$

$$y_i = -x_i \cdot x_\ell^{-1}$$

$$\Rightarrow e_\ell \in \text{Vect}(\{e_1, \dots, e_{\ell-1}\})$$

THÉORÈME 5.4 (Majoration du cardinal d'une famille libre). Soit V un espace vectoriel non-nul de dimension d et $\mathcal{F} = \{v_1, \dots, v_f\} \subset V$ une famille finie et libre; alors $f \leq d$.

Preuve: les vecteurs $v_1, \dots, v_f$ sont distincts

si $v_i = v_j$ pour $j \neq i$ alors

v_j est CL des autres $v_j = \lambda_i v_i$.

On fait une récurrence sur d .

Si $d=1$ $V=K.e$ $e \neq 0_V$ on veut mq

$$f=1.$$

Notons que $v_i \neq 0_V$ sinon $v_i=0$ sera
CL non trivial de

$$0_V = 1.v_1 + 0.v_2 + \dots + 0.v_f$$

de m $v_i \neq 0_V$ pour tout $i=1, \dots, f$.

Si $v_i \neq 0$ on a $v_i = x_i e$ avec $x_i \neq 0$

supposons que $f \geq 2$ on aura

$$v_2 = x_2 e = x_2 \cdot x_1^{-1} \cdot x_1 \cdot e = x_2 \cdot x_1^{-1} \cdot v_1$$

$x_1 \neq 0 \Rightarrow x_1$ est inversible.

v_2 est CL non triviale de

$$v_1, v_3, \dots, v_{f-1}$$

$$v_2 = x_2 x_1^{-1} v_1 + 0 \cdot v_3 + \dots + 0 v_{f-1} \quad \text{contradiction}$$

si $\dim V = 1$ $|F| \leq 1$.

- Supposons que si W est un K -ev de $\dim \leq d-1$
le cardinal d'une famille libre de W
est $\leq d-1$.

- Soit V de $\dim d \geq 2$.

Soit G une famille génératrice de V
de cardinal d

$$g = \{e_1, \dots, e_d\}.$$

$$\forall i=1, \dots, f \text{ il existe } (x_{i,j})_{j \leq d} \neq 0$$

$$v_i = x_{i,1}e_1 + \dots + x_{i,d}e_d$$

$$\text{Comme } v_f \neq 0_V \text{ il existe } j_0 \neq 0$$

$$x_{f,j_0} \neq 0_K \quad (\text{quitte à renuméroter})$$

$$\text{ops } j_0 = d : x_{f,d} \neq 0$$

et est inversible.

$$v'_i = v_i - (x_{i,d}/x_{g,d}) v_g \quad i=1, \dots, g$$

$$\text{On a } v'_g = v_g - (x_{g,d}/x_{g,d}) v_g = v_g - v_g = 0_v$$

en general

$$v'_i = x'_{i,1} e_1 + \dots + x'_{i,d-1} e_{d-1} + \\ (x_{i,d} - (x_{i,d}/x_{g,d}) x_{g,d}) e_d$$

on obtient que pour $i=1, \dots, f-1$
 v_i' est CL des vecteur $\{e_1, \dots, e_{d-1}\}$

$$v_f' = 0_V$$

la famille $F' = \{v_1', \dots, v_{f-1}'\} \subset V'$

$$V' = \text{Vect}(\{e_1, \dots, e_{d-1}\})$$

$$\dim V' \leq d-1$$

la famille $\overline{\sigma}'$ est libre : si pour $\lambda_1, \dots, \lambda_{g-1} \in K$
on a $\lambda_1 v_1' + \dots + \lambda_{g-1} v_{g-1}' = 0_V$
en utilisant l'expression de v_i' en fonction
des v_i on obtient que

$$\lambda_1 v_1 + \dots + \lambda_{g-1} v_{g-1} + \lambda_g v_g = 0_V \quad \text{pour}$$

un certain $\lambda_g \in K$

Comme $\{v_1, \dots, v_g\}$ est libre

$$\Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_{g-1} = \lambda_g = 0_K$$

$\Rightarrow \{v'_1, \dots, v'_{g-1}\}$ est libre.

F' est libre ds un espace V' de $\dim \leq d-1$
par récurrence $|F'| = g-1 \leq d-1$

$$\Rightarrow g \leq d.$$



Bases

DÉFINITION 5.18. Soit V un espace vectoriel de dimension finie. Une famille $\mathcal{B} = \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ est une base de V si l'une des conditions équivalentes suivantes est vérifiée:

- (1) $\mathcal{B}$ est génératrice et libre,
- (2) L'application combinaison linéaire de $\mathcal{B}$,

$$CL_{\mathcal{B}} : K^d \mapsto V$$

est un isomorphisme,

- (3) Pour tout $v \in V$ il existe un unique uplet $(x_1, \dots, x_d) \in K^d$ tel que v s'écrit sous la forme

$$v = x_1 \cdot \mathbf{e}_1 + \dots + x_d \cdot \mathbf{e}_d.$$

Alors $d = \dim V$.

Exemple : $\mathcal{B}_d^o = \{e_1^o, \dots, e_d^o\} \subset K^d$.

THÉORÈME 5.5. Soit V un K -ev de dimension d alors V possède une base et toute base $\mathcal{B}$ de V vérifie

$$(5.3.3) \quad |\mathcal{B}| = \dim(V).$$

Preuve : soit B une famille génératrice
de cardinal $d = \dim V$.

On a vu que comme B est gen de taille
minimal alors B est libre.

et donc B est une base.

Reciproquement si B est une base de
cardinal d
 $CL_B : K^d \cong V$

et $\dim V = \dim K^d = d$ (la base canonique
de K^d est une base
de cardinal d)



THÉORÈME 5.6 (Extraction et Completion). Soit V un K -ev non nul. **de dim finie.**

- (1) (Extraction) Soit $\mathcal{G} \subset V$ une famille generatrice alors il existe une base $\mathcal{B}$ de V contenue dans $\mathcal{G}$. Si de plus $|\mathcal{G}| = d$ alors $\mathcal{G}$ est deja une base.
- (2) (Completion) Soit $\mathcal{L} \subset V$ une famille libre alors il existe une base $\mathcal{B}$ de V contenant $\mathcal{L}$. Si $|\mathcal{L}| = d$ alors $\mathcal{L}$ est deja une base.

Preuve: Soit $\mathcal{G}$ generatrice on sait que
 $|\mathcal{G}| \geq d = \dim V$

$\mathcal{G}$ contient au moins un vecteur $\neq 0_V$
 $\{e\}$ forme une famille libre $\subset \mathcal{G}$

Soit B une famille libre contenue dans G de cardinal $|B|$ maximal parmi les famille libre contenues ds G
(on sait que si $F \subset G$ est libre $|F| \leq d$)

On sait que $|B| \leq d$.

On va mq B est generatrice

$$B = \{e_1, \dots, e_{d'}\} \quad d' = |B| \leq d$$

2 cas: $d' = |G|$ alors $B = G$ et B génératrice
 $\Rightarrow$ c'est une base

- $d' < d$. Supposons que B n'est pas génératrice:

$$\text{Vect}(B) = W \neq \text{Vect}(G) = V$$

donc il existe $e \in G$ tq $e \notin W$

$\forall x_1, \dots, x_{d'} \in K$ alors

$$x_1 e_1 + \dots + x_{d'} e_{d'} \neq e$$

Mq $B \cup \{e\}$ est libre (ou aura une contradiction)
 $B \cup \{e\} \subset G$ et de taille $> |B|$

Supposons que

$$\lambda_1 e_1 + \dots + \lambda_{d'} e_{d'} + \lambda e = 0_V$$

- si $\lambda = 0_K$ on arait $\lambda_1 e_1 + \dots + \lambda_{d'} e_{d'} = 0_V$
 $\Rightarrow \lambda_1 = \dots = \lambda_{d'} = 0$ car B est libre.

- si $\lambda \neq 0_K$ λ est inversible

Impossible

$$e = -\lambda_1/\lambda e_1 + \dots + -\lambda_{d'}/\lambda e_{d'}$$

La preuve du Thm donne:

Thm de la base incomplète: Si V de dim finie
 $\mathcal{L} \subset V$ est libre et $\mathcal{B} \subset V$ est une base
alors il existe $\mathcal{L}' \subset \mathcal{B}$ d'libre
tq $\mathcal{L} \cup \mathcal{L}'$ forme une base de V .

Idee de la preuve: α libre B une
base alors $\alpha \cup B$ est une famille
generatrice contenant α
on va prendre la plus petite des
familles gen de $\alpha \cup B$ contenant α
et mq c'est une base.

Sous-Espace vectoriel et dimension

THÉORÈME 5.8 (Bases et SEV). Soit V un espace vectoriel de dimension finie, et $W \subset V$ un sous-espace vectoriel alors W est de dimension finie et

(1) ~~W est de dimension finie~~ $\dim(W) \leq \dim(V)$.

(2) Si $\dim(W) = \dim(V)$ alors $W = V$.

(3) Si $\mathcal{B}_W$ est une base de W alors il existe une base $\mathcal{B}_V$ de V contenant $\mathcal{B}_W$.

Preuve: Soit $\alpha \subset W$ une famille libre
on a que $|\alpha| \leq \dim V$. Soit $\alpha \subset W$
libre et de cardinal maximal (parmi
les famille libre de W)
On montre alors que α est

generatrice de W : sinon on prend
 $e \in W \setminus \text{Vect}(\alpha)$ et on mg
 $\alpha \cup \{e\}$ et libre.

- on a alors $\dim W \leq \dim V$.

□

- Un sous-espace vectoriel de dimension 1 est appelle *droite vectorielle*.
- *Un sous-espace vectoriel de dimension 2 est appelle* plan vectoriel.
- *Un sous-espace vectoriel de dimension $\dim(V) - 1$ est appelle* hyperplan vectoriel.

EVs de dimension infinie

DÉFINITION 5.20. Soit V un K -e.v. Un sous-ensemble $\mathcal{G} \subset V$ est une famille génératrice si

$$\text{Vect}(\mathcal{G}) = V,$$

ie. tout élément $v \in V$ peut s'écrire sous la forme d'une combinaison linéaire (finie) d'éléments de $\mathcal{G}$: il existe $d \geq 1$, $\mathbf{e}_1, \dots, \mathbf{e}_d \in \mathcal{G}$, $x_1, \dots, x_d \in K$, tels que

$$(5.4.1) \quad v = x_1 \mathbf{e}_1 + \dots + x_d \mathbf{e}_d.$$

DÉFINITION 5.21. Soit V un K -e.v., un sous-ensemble $\mathcal{L} \subset V$ est une famille libre si tout sous-ensemble fini $\mathcal{L}' \subset \mathcal{L}$ est libre: si $\mathcal{L}' = \{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ (les éléments tous distincts), on a

$$(5.4.2) \quad x_1 \mathbf{e}_1 + \dots + x_d \mathbf{e}_d = 0_V \iff x_1 = \dots = x_d = 0_K.$$

DÉFINITION 5.22. Une base algébrique $\mathcal{B} \subset V$ est une famille libre et génératrice.

PROPOSITION 5.16. Soit $\mathcal{B} \subset V$ une base algébrique. Alors tout élément v de V est representable comme combinaison linéaire finie d'éléments de $\mathcal{B}$ et une telle représentation est unique.

THÉORÈME 5.9 (Existence de bases sous l'axiome du choix). *Dans une théorie des ensembles contenant l'axiome du choix, tout espace vectoriel sur un corps K possède une base et toutes les bases de V ont même cardinal: pour toutes bases $\mathcal{B}, \mathcal{B}'$ il existe une bijection*

$$\mathcal{B} \simeq \mathcal{B}'.$$

La dimension de V est de cardinal d'une base:

$$\dim(V) = |\mathcal{B}|.$$

Preuve: On utilise le lemme suivant équivalent à l'axiome du choix.

LEMME DE ZORN. *Soit E un ensemble ordonné tel que tout sous-ensemble $A \subset E$ totalement ordonné possède un majorant alors E possède un élément maximal.*