Corps

Koerper, field

”Le corps conditionne le raisonnement.”

DÉFINITION 4.1. *Un corps K est un anneau commutatif possedant au moins deux elements $0_K \neq 1_K$ et tel que tout element non-nul est inversible:*

$$K^\times = K - \{0_K\}.$$

Ex: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

$\mathbb{Z}$ n'est pas un corps: 2 n'est pas inversible ds $\mathbb{Z}$

$\mathbb{Z}^\times = \{\pm 1\}$

THÉORÈME 4.3. *Soit $q \geqslant 1$ un un entier, alors l'anneau des classes de congruences modulo q $(\mathbb{Z}/q\mathbb{Z}, +, .)$ est un corps ssi q est premier (q a exactement deux diviseurs distincts 1 et q)*

NOTATION 4.1. *Soit $p \geqslant 2$ un nombre premier, le corps fini a p elements $(\mathbb{Z}/p\mathbb{Z}, +, .)$ est note $\mathbb{F}_p$.*

PROPOSITION 4.3 (Petit Theoreme de Fermat). *Soit $p \geqslant 2$ un nombre premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps a p elements. Pour tout $x \in \mathbb{F}_p$ on a*

$$x^p = x.$$

$\forall x \in \mathbb{F}_p \quad x^p - x = 0_{\mathbb{F}_p}$

PROPOSITION 4.4. *Soit p un nombre premier alors pour tout $x, y \in \mathbb{F}_p$ on a*

$$(x+y)^p = x^p + y^p.$$

THÉORÈME 4.1. *Soit K un corps alors tout ideal $I \subset K$ est soit $I = \{0_K\}$ ou bien $I = K$.*

Reciproquement, soit A un anneau commutatif possedant au moins deux elements alors si ses ideaux sont $\{0_K\}$ ou bien K alors K est un corps.

THÉORÈME 4.2. *Soit K un corps, B un anneau et $\varphi \in \mathrm{Hom}_{Ann}(K, B)$ un morphisme d'anneaux. Alors si φ n'est pas nul ($\varphi \neq \underline{0}_B$) φ est injectif:*

$$\varphi : K \hookrightarrow B.$$

En particulier K s'identifie alors a son image $\varphi(K)$ qui est un sous-corps de B.

Caractéristique d'un corps

$$Car(K) = p \geq 0$$

$$Ker(Can_K) = p\mathbb{Z} \subset \mathbb{Z}$$

THÉORÈME 4.5. *Soit K un corps, alors sa caracteristique* $\mathrm{car}(K)$ *vaut soit* 0 *soit un nombre premier* p.

(1) On a $\mathrm{car}(K) = 0$ *si et seulement si*

$$\mathrm{Can}_K(\mathbb{Z}) = \{n_K = n.1_K,\ n \in \mathbb{Z}\} =: \mathbb{Z}_K \subset K$$

est un sous-anneau isomorphe a $\mathbb{Z}$*; alors* K *contient un sous-corps isomorphe a* $\mathbb{Q}$,

$$\mathbb{Q}_K = \mathrm{Frac}(\mathbb{Z}_K) = \{\frac{a_K}{b_K},\ a \in \mathbb{Z},\ b \in \mathbb{Z} - \{0\}\}$$

le corps des fractions de $\mathbb{Z}_K$*. De plus tout sous-corps* $K' \subset K$ *isomorphe a* $\mathbb{Q}$ *est en fait* $\mathbb{Q}_K$.

(2) *On a* $\mathrm{car}(K) = p \geqslant 2$ *un nombre premier si et seulement si*

$$\mathrm{Can}_K(\mathbb{Z}) = \{n_K = n.1_K,\ n \in \mathbb{Z}\} =: \mathbb{F}_{p,K} \subset K$$

est isomorphe au corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Tout sous-corps $K' \subset K$ *isomorphe a* $\mathbb{F}_p$ *est egal a* $\mathbb{F}_{p,K}$ *et* K *ne contient aucun autre corps isomorphe a* $\mathbb{F}_q$ *avec* $q \neq p$ *premier ou isomorphe a* $\mathbb{Q}$.

Dans ce cas, l'application de Frobenius

$$\mathrm{frob}_p : x \in K \mapsto x^p \in K$$

est un morphisme de corps injectif; en particulier

$$\forall x, y \in K (x + y)^p = x^p + y^p$$

et on a (Petit Theoreme de Fermat)

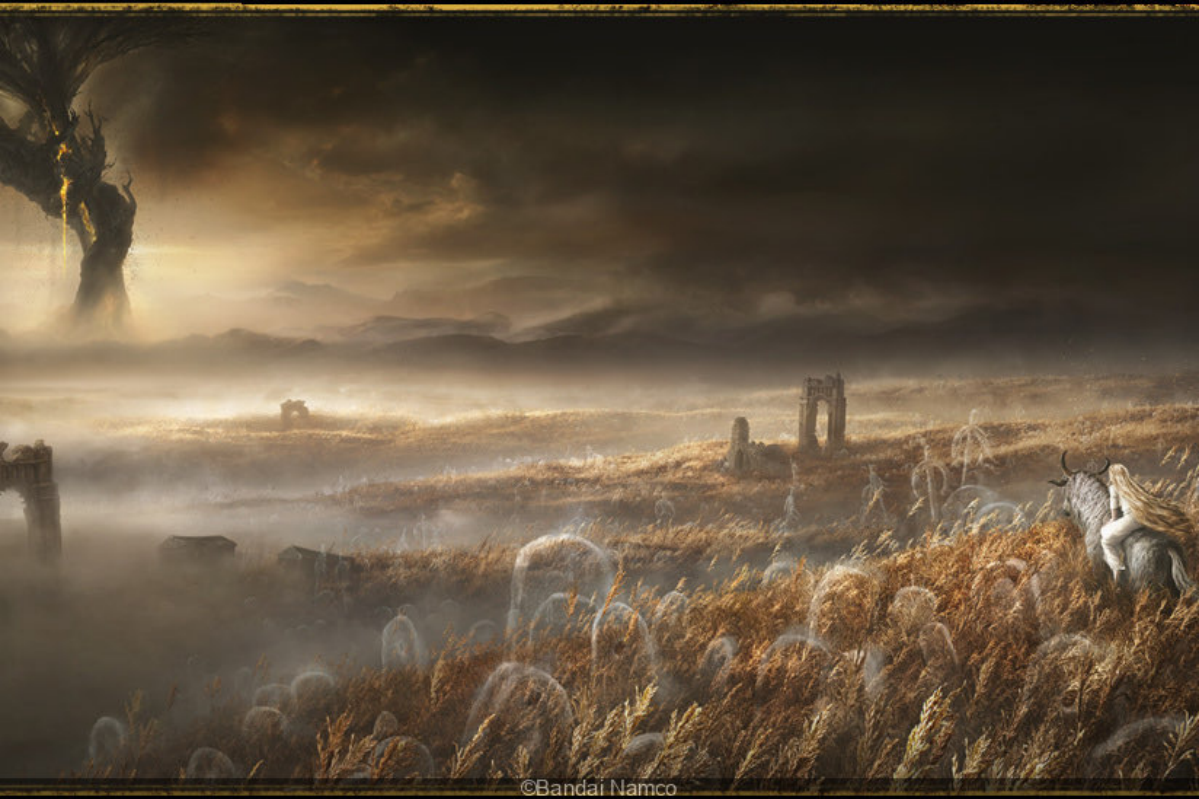
$$x \in \mathbb{F}_{p,K} \iff x^p = x. \tag{4.3.1}$$

Par le PTF : la direction $\Leftarrow$

$$x^p = x \implies x \in \mathbb{F}_{p,K}$$

On dit que le polynome de d° p $X^p - X$ a déjà p racine (les elts de $\mathbb{F}_{p,K}$) et un poly de d° p ont un corps a au plus

p racines $\Longrightarrow$ $\mathbb{F}_{p^k}$ est exactement l'ensemble des racines de $X^p - X$.


©Bandai Namco

Corps de fractions

Définition 4.2. *Un anneau A non-nul, commutatif, tel que $\forall a, b \in A$ on ait*

$$a.b = 0 \iff a = 0 \text{ ou } b = 0$$

est dit integre.

Théorème 4.4. *Soit A un anneau integre (en particulier commutatif) , alors il existe un corps $\mathrm{Frac}(A)$ et un morphisme d'anneau injectif*

$$\iota : A \hookrightarrow \mathrm{Frac}(A)$$

(de sorte qu'on peut considerer A comme un sous-anneau de $\mathrm{Frac}(A)$ en identifiant A a son image $\iota(A) \subset \mathrm{Frac}(A)$).

De plus $\mathrm{Frac}(A)$ a la propriete de minimalite suivante: pour tout corps K et tout morphisme injectif

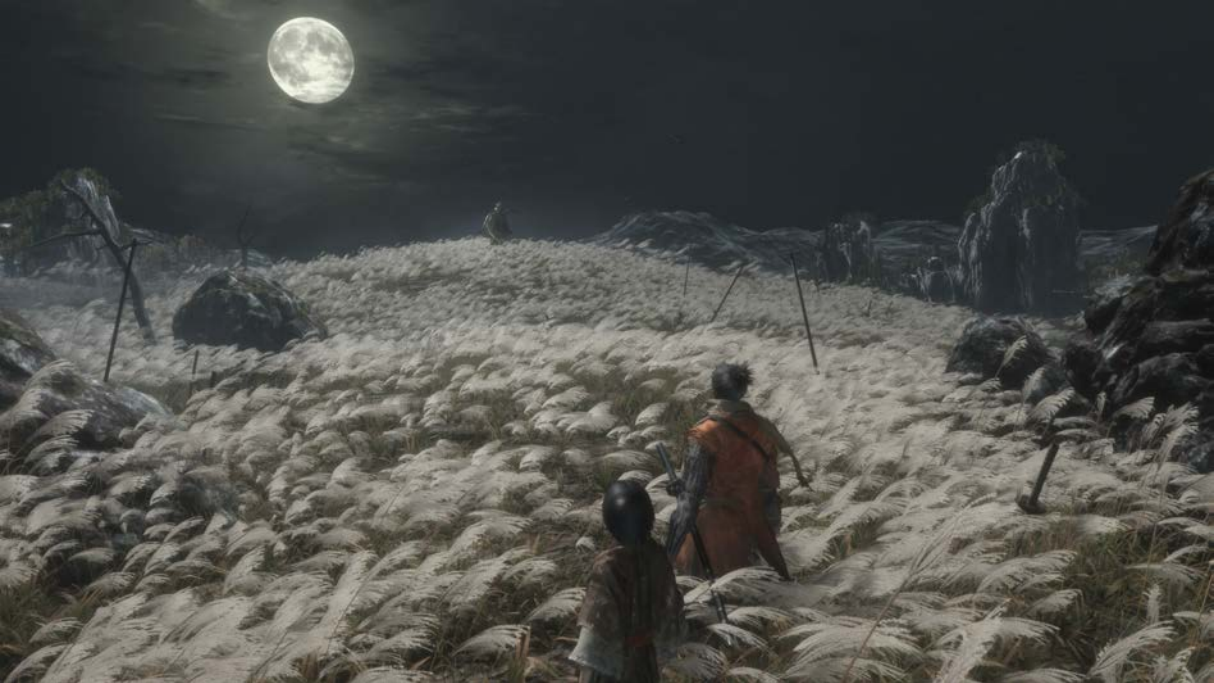
$$\iota' : A \hookrightarrow K,$$

il existe un morphisme (necessairement injectif)

$$\iota'_{\mathrm{Frac}(A)} : \mathrm{Frac}(A) \hookrightarrow K$$

prolongeant le morphisme ι' (ainsi A et $\mathrm{Frac}(A)$ peuvent etre vus comme des sous-anneaux de K).

$\mathcal{P}_{(A\times A-\{0\})} \supset \mathrm{Frac}(A) = \left\{ \frac{a}{b} = \{(c,d) \text{ avec } \substack{c\in A \\ d\in A-\{0\}} \ ad=bc\} \right\}$



Construction de $\mathbb{C}$

THÉORÈME 5.1. *Soit K un corps et $M_2(K)$ l'algebre des matrices 2×2 a coefficients dans K. Soit $\Delta \in K - K^2$ un element de K qui n'est pas un carre: $\forall x \in K,\ x^2 \neq \Delta$ et*

$$I_\Delta := \begin{pmatrix} 0 & \Delta \\ 1 & 0 \end{pmatrix}.$$

Alors la matrice I_Δ verifie

$$I_\Delta^2 = \Delta \mathrm{Id}_2 = \begin{pmatrix} \Delta & 0 \\ 0 & \Delta \end{pmatrix}$$

Soit

$$K[I_\Delta] := K.\mathrm{Id}_2 + K.I_\Delta = \left\{ Z = x.\mathrm{Id}_2 + y.I_\Delta = \begin{pmatrix} x & \Delta y \\ y & x \end{pmatrix},\ x, y \in K \right\} \subset M_2(K)$$

l'ensemble des combinason lineaires des matrices Id_2 et I_Δ. Alors $K[I_\Delta]$ a les proprietes suivantes:

(1) L'ecriture d'un element Z sous la forme $Z = x.\mathrm{Id}_2 + y.I_\Delta$ est unique.

(2) $K[I_\Delta]$ muni du produit de matrices est un sous-anneau commutatif de $M_2(K)$ contenant l'anneau des matrices scalaires $K.\mathrm{Id}_2$ et c'est meme un corps : toute matrice non-nulle de $K[I_\Delta]$ est inversible dans $K[I_\Delta]$.

(3) Plus precisemment soit

$$Z = x\mathrm{Id}_2 + y.I_\Delta = \begin{pmatrix} x & \Delta y \\ y & x \end{pmatrix}$$

$\det Z = x^2 - \Delta y^2$

alors

$$\det(Z) = x^2 - \Delta y^2$$

et si $\det(Z) \neq 0$ (alors Z est inversible) on a

$$Z^{-1} = \frac{1}{x^2 - \Delta y^2}(x.\mathrm{Id}_2 - yI_\Delta) = \begin{pmatrix} \frac{x}{x^2-\Delta y^2} & \Delta \frac{-y}{x^2-\Delta y^2} \\ \frac{-y}{x^2-\Delta y^2} & \frac{x}{x^2-\Delta y^2} \end{pmatrix} \in K[I_\Delta].$$

Exemple: $K = \mathbb{R}$ $\Delta = -1 \neq \square$

$\mathbb{R}[I_{-1}] \simeq \mathbb{C}$.

Modules sur un Anneau

Espace Vectoriel sur un Corps

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

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

(appellee multiplication par les scalaires) ayant les proprietes suivantes:

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

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

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

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

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

$$1_A * m = m.$$

Si $A = K$ est un corps alors M s'appelle egalement un K-espace vectoriel (K-EV) et les elements de M sont les vecteurs de M.

Rmq : $-m = -1_A * m$

Exemples : Actum A-module

- $\{0_A\}$ actum A-module
- $I \subset A$ ideal $\Rightarrow I$ = A-module

$\varphi : A \to B$

$\ker \varphi$ = A-module.

- $A^d = \{(a_1, \dots, a_d) \quad a_i \in A\}$

et un A-module

$$\vec{a} = (a_1, \dots, a_d)$$

$$a * \vec{a} = (aa_1, \dots, aa_d)$$

A^d = A-module libre de rang d

(free, frei) dimension

- $X = Ens$

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

qtum A-module

$a * f : x \in X \to a.f(x)$

$$\mathcal{F}(X; A) = A^X \quad \text{et si } X = \{1, 2, \dots, d\}$$

$$A^X = A^d$$

- M = gpe abélien

M est un $\mathbb{Z}$-module

$$k * m = \begin{cases} m + m + \dots + m & (k \text{ fois si } k \geq 0 \\ (-m) + \dots + (-m) & (k \text{ fois si } k \leq 0) \end{cases}$$

Réciproquement si M a un structure de $\mathbb{Z}$-module alors cette structure

coincide avec la structure canonique de $\mathbb{Z}$-mod provenant du fait que M est un gpe commutatif.

$\rightsquigarrow$ $\mathbb{Z}$-module $\Leftrightarrow$ gpe commutatif

$\varphi : A \to B$ morphisme d'anneaux

$\ker \varphi$ est un A-mod.

- B a une structure de A-module

$$a * b := \varphi(a) \cdot_B b$$

Anneau des Polynomes : A commutatif

$$A[X] = \{ P(X) = a_d X^d + a_{d-1} X^{d-1} + \dots + a_1 X + a_0 \}$$

$$d \geq 0, \quad a_d, a_{d-1}, \dots, a_0 \in A \}$$

$A[X]$ un A-module

$$a \cdot P(X) = a \cdot a_d X^d + a \cdot a_{d-1} X^{d-1} + \dots + a \cdot a_0$$

$D \geq 0$ $A[X]_{\leq D} = \{ P(X) = a_D X^D + \dots + a_1 X + a_0$

$a_D, a_{D-1}, \dots, a_0 \}$

$=$ polynômes de $d^\circ \leq D$

$A[X]_{\leq D}$ n'est pas un anneau (sauf si $D=0$)

mais c'est un A-module.

$M_2(A)$ est un A-module :

$$\lambda * \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$$

Rmq $M_2(A) \underset{A\text{-mod}}{\simeq} A^4$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow (a, b, c, d)$$

En fait $M_2(A)$ est une A-algebre

DÉFINITION 6.2. *Soit A un anneau commutatif. Une A-algebre est un anneau $(B, +_B, .B)$ possedant une structure de A-module qui verifie la propriete d'associativite suivante pour les deux multiplications:*

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

Autre exemple:

$A[X]$ est une A-algebre.

Sous-Module
(sous-espace vectoriel)

DÉFINITION 6.3. *Soit A un anneau commutatif et 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 $\forall n, n' \in N,\ a, a' \in A$

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

Si $A = K$ est un corps, N est un sous-espace vectoriel (SEV) de M.

PROPOSITION 6.1. *(Critere de sous-module/ de SEV) Soit $N \subset M$ un sous-ensemble non vide d'un A-module M alors N est un sous-module de M ssi*

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

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

$-1_A * n = -n$ et donc $\forall n, n' \in N$

$n + (-1)_A * n = n' - n \in N \Longrightarrow N$ est un ssgpe de $(M,+)$

$\Rightarrow 0_M \in N$ et $\forall a \in A \; n \in N$

$$a * n = a + n + 0_M \in N$$

□

Exemples $\{0_M\} \subset M$ est un ss module

- $\forall m \in M \quad A * m = \{a * m \quad a \in A\}$ est un ss module

- $\forall m, m' \in M \quad A*m + A*m'$

$$= \left\{ a*m + a'*m' \;\middle|\; a, a' \in A \right\} \subset M$$

est un ss-module.

- $M = A^d$ $\quad b_1, \dots, b_d \in A$

$$K = \left\{ \vec{a} = (a_1, \dots, a_d) \in A^d \;\middle|\; b_1 . a_1 + \dots + b_d . a_d = 0_A \right\}$$

est un ss-A-mod de A^d

$K = \ker \varphi$ avec

$$\varphi : A^d \longrightarrow A$$
$$(a_1, \dots, a_d) \longmapsto b_1 . a_1 + \dots + b_d . a_d$$

φ est un morphisme de A-mods

et $K = \ker \varphi$ et est "donc" un A-mod.

- $0 \leqslant D \leqslant D'$

$$A[X]_{\leqslant D} \subset A[X]_{\leqslant D'} \subset A[X]$$

et une chaîne de ss modules.

Sous-Module Engendré

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 generalement soit $(M_i)_{i \in I}$ une collection de sous-modules alors

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

est un sous-module.

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

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

Rmq: si $X = \emptyset \longrightarrow \langle \emptyset \rangle_A = \{0_M\}$

PROPOSITION 6.3. *Soit M un A-module sur un anneau commutatif A et $X \subset M$ un sous-ensemble de M alors $\langle X \rangle_A$ est soit le module nul $\{0_M\}$ si X est vide, soit l'ensemble des combinaisons lineaires d'elements de X a coefficients dans A:*

$$\langle X \rangle_A = \mathrm{CL}_A(X) := \{\sum_{i=1}^{n} a_i * x_i,\ n \geqslant 1,\ a_1, \cdots, a_n \in A,\ x_1, \cdots, x_n \in X\}.$$

Preuve: Il faut voir que $Cl_A(X)$ est un ss-module de M (critere de ss module)

$Cl_A(X) \supset X$: $x \in X$ s'écrit $1_A * x \in Cl_A(X)$

$\Longrightarrow Cl_A(X) \supset \langle X \rangle_A$

Il reste à mq $\langle X \rangle_A$ contient $Cl_A(X)$

Soient $x_1, \dots, x_n \in X$ $a_1, \dots, a_n \in A$

alors $a_1 * x_1 + \dots + a_n * x_n \in Cl_A(X)$

mais comme $x_1, \dots, x_n \in X \Rightarrow a_i * x_i \in \langle X \rangle_A$

et donc $a_1 * x_1 + \dots + a_n * x_n \in \langle X \rangle_A$ □

Rmq : $X \subset M = A\text{-mod}$

engendré

$\langle X \rangle_{\mathbb{Z}}$ = ssgpe de M engendré par X

$\langle X \rangle_{\mathbb{Z}} \subsetneq \langle X \rangle_A$

c'est l'ensemble obtenu en considérant les CL d'elts de X à coef dans $\mathrm{Can}_A(\mathbb{Z}) \subsetneq A$

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

DÉFINITION 6.6. *Un A-module M est de type fini si il possede une famille generatrice qui est finie.*

tout elt de M est obtenu comme CL à coefs ds A d'un ensemble fini

Exemples

$A^d = \{(a_1, \dots, a_d) \quad a_i \in A\}$ et de t.f.

A^d est engendré par "la base canonique"

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

$$e_1^0 = (1_A, 0_A, \dots, 0_A), \quad e_2^0 = (0_A, 1_A, 0_A, \dots 0_A)$$

$$e_i^0 = (0_A, \dots 0_A, 1_A, 0_A, \dots 0_A)$$

$i^{ème}$ position

$$e_d^0 = (0_A, \quad , 0_A, 1_A)$$

$$\text{si effet } (a_1, \dots, a_d) \in A^d$$

$$\Leftrightarrow$$

$$a_1 * (1_A, 0_A, \dots, 0_A) + a_2 * (0_A, 1_A, \dots 0_A)$$

$$+ \dots + a_d * (0_A, 0_A, 1_A)$$

$$A[X] = \langle \underbrace{\{1, X, X^2, \dots, X^d, X^{d+1}, \dots\}}_{\text{les monomes unitaires de } A[X]} \rangle_A$$

$1 = X^0$

Base canonique de $A[X]$

$$P(X) = a_d \cdot X^d + \dots + a_0 \cdot 1$$

Rmq : la famille des monômes unitaires est infinie (indexée par $\mathbb{N}$). Ainsi $A[X]$ n'est pas de t.f.

$$A[X]_{\leq D} = \langle \{1, X, \dots, X^D\} \rangle_A$$

et de type fini de rang (rank) $D+1$

$$M_2(A) = \left\langle \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\} \right\rangle_A$$

$$= \langle \{ E_{11}, E_{12}, E_{21}, E_{22} \} \rangle$$

matrices elementaire

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \cdot E_{11} + b \cdot E_{12} + c \cdot E_{21} + d \cdot E_{22}$$

Morphismes de A-modules

Définition 6.7. *Soit A un anneau et M, N des A-modules, un morphisme de A-modules (encore appellee application A-lineaire) entre M et N est un morphisme de groupes*

$$\varphi : M \mapsto N$$

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

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

Si $A = K$ est un corps on parle plutot d'application lineaire entre K-EVs.

Rmq : image d'une CL. $a_1, \dots, a_k \in A$

$m_1, \dots, m_k \in M$

$$\varphi(a_1 \cdot m_1 + \dots + a_k \cdot m_k) = a_1 \cdot \varphi(m_1) + \dots + a_k \cdot \varphi(m_k)$$

LEMME 6.1. *(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*

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

Preuve : si φ verifie cela en prenant $a = 1_A$

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

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

$\rightsquigarrow$ φ est un morphisme de gpe comms

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

$$\varphi(a + m + 0_M) = a + \varphi(m) + 0_N$$

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

Reciproque ok

□

Noyau-Image

PROPOSITION 6.4. *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

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

sont des sous A-modules.

Preuve : (preimage) $N' \subset N$ ss-mod

on v mq $\varphi^{(-1)}(N') = \{ m \in M \ \ \varphi(m) \in N' \}$

est ss-module de M

Soit $m, m' \in \varphi^{(-1)}(N')$ et $a \in A$

ouvmq $\varphi(a \cdot m + m') \in N'$

et $\varphi(a \cdot m + m') = a \cdot \underbrace{\varphi(m)}_{N'} + \underbrace{\varphi(m')}_{N'} \in N'$ (car $N' = SS$ module)

....

□

Corollaire 6.1. *L'application A-lineaire $\varphi : M \mapsto N$ est injective ssi* $\ker(\varphi) = \{0_M\}$.

Espaces de Morphismes

NOTATION 6.1. *On note*

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

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

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

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

Si K est un corps et V, W sont des K-EVs on note ces ensembles

$$\mathrm{Hom}_K(M,N),\ \mathrm{Isom}_K(M,N),$$

$$\mathrm{End}_K(M) = \mathrm{Hom}_K(M,M),$$

$$\mathrm{Aut}_K(M) = \mathrm{Isom}_K(M,M).$$

PROPOSITION 6.5. *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.*
- *Soit $\lambda \in A$ alors l'application definie par*

$$\lambda * \psi : m \in M \mapsto \lambda *_N \psi(m) \in N$$

est un morphisme de A-modules entre M et N.

Preuve : mq $\lambda * \psi : M \to N$ est un morphisme de A-mods

on veut mq $\forall a \forall m, m'$

$$\lambda * \psi(a * m + m') \overset{?}{=} a * (\lambda * \psi)(m) + (\lambda * \psi)(m')$$

$$\lambda * \psi(a * m * m') = \lambda * (\psi(a * m * m'))$$
$$= \lambda * (a * \psi(m) * \psi(m'))$$
$$= \lambda * a * \psi(m) * \lambda * \psi(m')$$

Acomm

$$= a * \lambda * \psi(m) * \lambda * \psi(m')$$
$$= a * (\lambda * \psi)(m) * (\lambda * \psi)(m')$$

....

□

THÉORÈME 6.1. *Soient M et N des A-modules alors $\mathrm{Hom}_{A-mod}(M,N)$ a une structure naturelle de A-module.*

L'espace des endomorphismes de M,

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

a une structure naturelle de A-algebre. (pour la composition)

L'ensemble des element inversibles de l'anneau $\mathrm{End}_{A-mod}(M)$ est l'ensemble des automorphismes de M,

$$\mathrm{End}_{A-mod}(M)^{\times} = \mathrm{Aut}_{A-mod}(M) \subset \mathrm{Bij}(M)$$

est un sous-groupe de $Aut_{Gr}(M) \subset \mathrm{Bij}(M)$.

On note egalement ce groupe

$$\mathrm{Aut}_{A-mod}(M) = \mathrm{GL}_A(M)$$

et on l'appelle le groupe lineaire du A-module M.

Preuve : on a vu que $\mathrm{Hom}_A(M,N)$ est équipé d'une multiplication par A

Si φ et $\psi \in \mathrm{Hom}_A(M,N)$ on veut mq

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

est A-linéaire.

on veut mq $(\varphi+\psi)(a+m) = a+(\varphi+\psi)(m)$

//

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

- $\underline{\Theta}_N$ est un morphisme de A-mod.

on sait que $\lambda*\varphi : m \to \lambda\varphi(m)$ est A-linéaire

on vérifie l'associativité et la distributivité de $*$ sur $\mathrm{Hom}_A(N,N)$ ...

$M = N$: $\mathrm{Hom}_A(M,M) = \mathrm{End}_A(M)$

est muni de la composition $\circ$

on vérifie que $(\mathrm{End}_A(M), +, \circ, 0_M, \mathrm{Id}_M)$

est un anneau.

Pour voir que c'est une A-algebre

on doit vérifie que

$\forall\ \varphi, \psi \in \mathrm{End}_A(M) \quad \forall \lambda \in A$

$$\lambda * (\varphi \circ \psi) = (\lambda * \varphi) \circ \psi = \varphi \circ (\lambda * \psi)$$

$$\lambda * (\varphi \circ \psi)(m) = \lambda * \varphi(\psi(m))$$

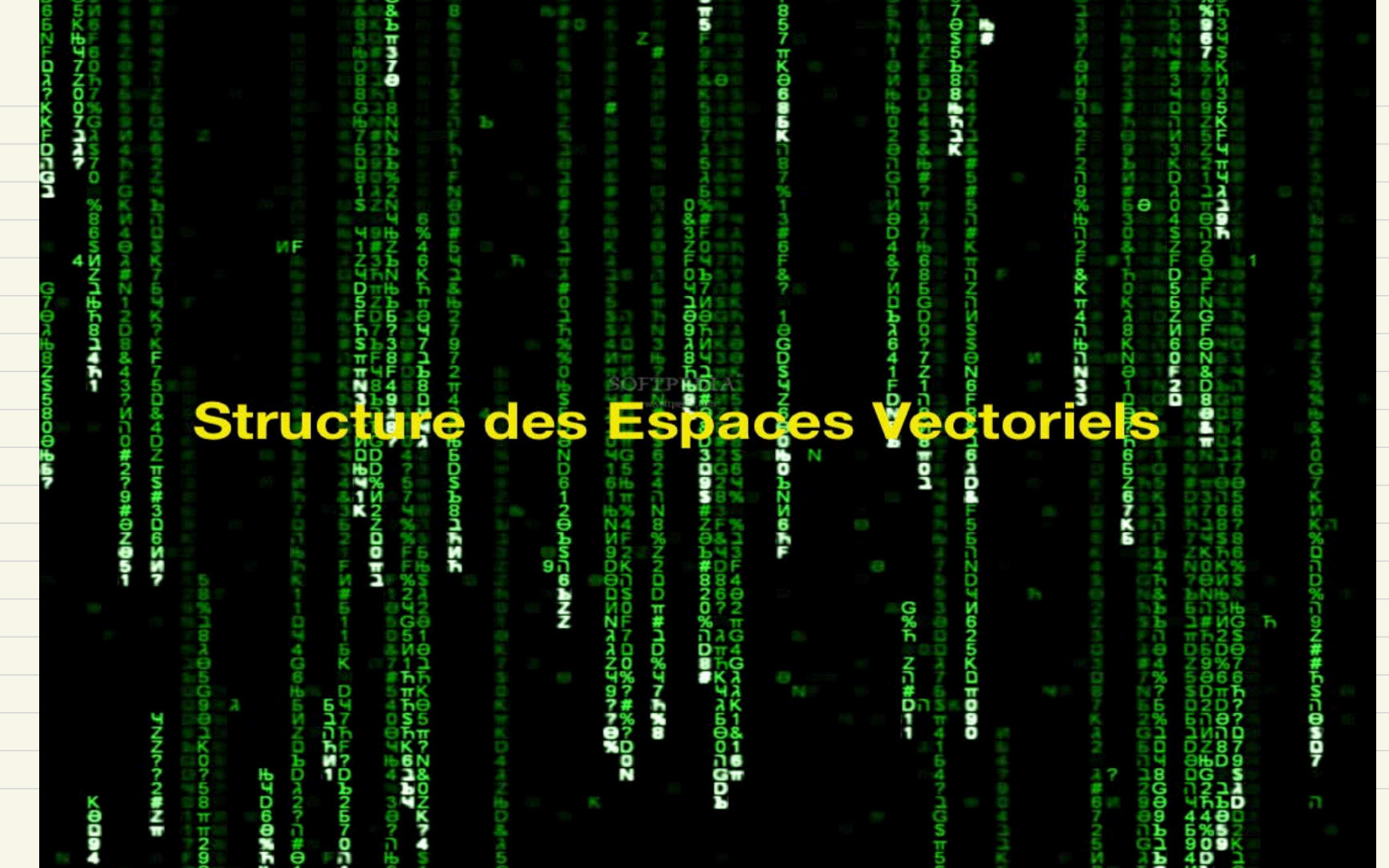
$$= (\lambda * \varphi) \circ \psi(m)$$

$$= \lambda * \varphi(\psi(m)) = \varphi(\lambda * \psi(m))$$

$$= \varphi \circ (\lambda * \psi)(m)$$

...

□


Structure des 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."

$A = K$ un corps

A-module = K-espace vectoriel K-EV

sous-A-module = sous K-espace vectoriel K-SEV

morphisme = application linéaire.

si V K-EV $v \in V$ = vecteur de V

$\lambda \in K$ = scalaire.

PROPOSITION 7.2 (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 7.3. *Soit $\mathscr{F} \subset V$ un sous-ensemble, on note*

$$\langle \mathscr{F} \rangle_K = \mathrm{Vect}(\mathscr{F}) \subset V$$

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

On rappelle qu'il s'agit de maniere equivalente

- *de l'intersection de tous les SEV contenant $\mathscr{F}$,*
- *de l'ensemble des combinaisons lineaires d'elements de $\mathscr{F}$ a coefficients dans K*

$$\langle \mathscr{F} \rangle_K = \{ \sum_{i=1}^{n} \lambda_i . x_i,\ n \geqslant 1,\ \lambda_1, \cdots, \lambda_n \in K,\ x_1, \cdots, x_n \in \mathscr{F} \}.$$

finies

Exemple : Somme de deux SEV

DÉFINITION 7.4. *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 definition le sous-espace vectoriel engendre par les vecteurs de X et de Y.

LEMME 7.1. *On a*

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

Preuve : on a que $\{x+y \quad x \in X, y \in Y\}$ contient X et Y si on montre que c'est un sev on aura $X+Y \subset \{\ \}$ et reciproquement

on montre que $\{x+y\ldots\} \subset \langle X \cup Y \rangle_K$

- $\{x+y\}$ est un SEV :

$\forall \lambda \in K$ $x+y$ $x'+y'$ on a

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

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

$\in X$ $\in Y$ (sont des SEV)

si $x \in X$ $y \in Y$ allora $x+y \in \langle X \cup Y \rangle_K$

$\{x+y\} \subset \langle X \cup Y \rangle_K$.

□

Somme Directe

DÉFINITION 7.5. *Si $X \cap Y = \{0_V\}$, on dit que X et Y sont en somme directe et on ecrit*

$$X \oplus Y \subset V$$

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 supplementaires (dans V).

PROPOSITION 7.3. *Soit $V = X \oplus Y$ la somme directe de deux sous-espaces supplementaires X et Y alors l'ecriture de tout vecteur $v \in V \in X \oplus Y$ sous la forme*

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

est unique.

Preuve: soit $v \in V = X \oplus Y$ supposons

$$v = x + y = x' + y'$$

alors $x+y=x'+y' \iff x-x'=y'-y$

$\uparrow$ $\uparrow$

X Y

$x-x'=y-y' \in X \cap Y = \{0_V\}$

$x-x'=y-y'=0_V \quad x=x' \quad y=y'$

Définition 7.7. *Soit V un K-e.v. Un sous-ensemble $\mathscr{G} \subset V$ est une famille generatrice si*

$$\mathrm{Vect}(\mathscr{G}) = \langle \mathscr{G} \rangle_K = V,$$

ie. tout element $v \in V$ peut s'ecrire sous la forme d'une combinaison lineaire (finie) a coefficients dans K d'elements de $\mathscr{G}$: pour tout $v \in V$ il existe $n \geqslant 1$, $x_1, \cdots, x_n \in K$, $\mathbf{e}_1, \cdots, \mathbf{e}_n \in \mathscr{G}$ tels que

$$v = \sum_{i=1}^{n} x_i \mathbf{e}_i. \tag{7.4.1}$$

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

DÉFINITION 7.8. *Soit V un K-ev de type fini. Si V est non-nul, sa dimension est le cardinal minimum d'une famille generatrice finie de V:*

$$\dim(V) := \min_{\mathscr{G} \text{ generatrice}} |\mathscr{G}|.$$

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

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

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

On dira egalement "K-ev de dimension finie" a la place de " K-ev de type fini".

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

THÉORÈME 7.2. *Tout K-espace vectoriel de dimension finie $d = \dim V$ est isomorphe (comme K-ev) a 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.*

Très différent du cas des A-module

Parlons des $\mathbb{Z}$-modules = groupes commutatifs

$\mathbb{Z}^d$ est un $\mathbb{Z}$-module libre de type fini

mais $\mathbb{Z}/q\mathbb{Z}$ ou tout gp com fini est un $\mathbb{Z}$-module mais n'est pas libre $\simeq \mathbb{Z}^d$.

On peut classifier les $\mathbb{Z}$-modules de type fini et tout $\mathbb{Z}$-mod de type fini est un produit de $\mathbb{Z}^d$ et de $\mathbb{Z}/q\mathbb{Z}$'s

V = K-EV de dim finie

G génératrice $G = \{e_1, \dots, e_d\}$ $d \geq \dim V$

génératrice

$CL_G : K^d \longrightarrow V$

$(x_1, \dots, x_d) \longrightarrow x_1 \cdot e_1 + \dots + x_d \cdot e_d$

Par déf de G = génératrice CL_G est surjective

LEMME 7.2. *L'application CL_g est lineaire.*

Preuve: $\lambda \in K$ $\vec{x}=(x_1,\dots,x_d)$ $\vec{y}=(y_1,\dots,y_d) \in K^d$

$$CL_g(\lambda\vec{x}+\vec{y}) = \sum_{i=1}^{n} (\lambda x_i + y_i).e_i$$

$$= \sum \lambda x_i . e_i + \sum y_i . e_i$$

$$= \lambda \sum x_i e_i + \sum y_i e_i$$

$$= \lambda . CL_g(\vec{x}) + CL_g(\vec{y})$$

□

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

$$\mathscr{G} = \{\mathbf{e}_1, \cdots, \mathbf{e}_d\} \subset V$$

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

(1) On a

$$\mathrm{Vect}(\mathscr{G}) = V.$$

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

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

(3) L'application lineaire

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

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

$$\dim_K V \leqslant d.$$

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

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

Preuve : $\mathcal{G} = \{e_1, \dots, e_d\}$ $d = \dim V$

Si $CL_{\mathcal{G}}$ n'est pas injective : $\ker CL_{\mathcal{G}} \neq \{0_{K^d}\}$

$\exists (v_1, \dots, v_d) \in K^d - \{0_{K^d}\}$ tq

$$v_1 \cdot e_1 + \dots + v_d \cdot e_d = 0_V$$

il existe $i \in \{1, \dots, d\}$ tq $v_i \neq 0$

ops $i = d$ $v_d \neq 0_K$

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

et $v_d \neq 0_K$ v_d at inversable

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

e_d at CL de $\{e_1, \dots, e_{d-1}\}$

$\Rightarrow \{e_1, \dots, e_{d-1}\}$ est génératrice de V

$\Rightarrow$ Contradiction.

Soit $v \in V$ $\quad v = x_1 e_1 + \dots + x_{d-1} e_{d-1} + x_d e_d$

$$v = x_1 e_1 + \dots + x_{d-1} \cdot e_{d-1}$$
$$+ x_d \frac{v_1}{v_d} \cdot e_1 + \dots + x_d \frac{v_{d-1}}{v_d} \cdot e_{d-1}$$
$$v = \left(x_1 - x_d \frac{v_1}{v_d}\right) \cdot e_1 + \dots + \left(x_{d-1} - x_d \frac{v_{d-1}}{v_d}\right) e_{d-1}$$

□

$\Rightarrow CL_g$ est injective donc un isomorphisme $K^d \otimes V$.

Corollaire 7.1 (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 $d_V = d_W = d$ on a

$$\Phi : K^d \xrightarrow{\sim} V \qquad \Psi : K^d \xrightarrow{\sim} W$$

et $\Psi \circ \Phi^{-1} : V \to W$ est un isomorphe

- Si $V \xrightarrow{\sim} W$ on a $K^{d_V} \xrightarrow{\sim} V \xrightarrow{\sim} W \xrightarrow{\sim} K^{d_W}$

$K^{d_V} \xrightarrow{\sim} K^{d_W} \Rightarrow d_V = d_W$

$\varphi : V \simeq W$ soit G_V une famille gen de V
de taille d_V

$\varphi(G_V) = \{\varphi(e_1), \dots, \varphi(e_{d_V})\}$ est
génératrice de W

soit $w \in W$ $w = \varphi(v)$

$$= \varphi\left(\sum_{i=1 \dots d_V} x_i e_i\right) = \sum x_i \varphi(e_i)$$

$\Rightarrow d_V \geq d_W$

en inversant V et W on montre que

$$d_W \geq d_V \Rightarrow d_V = d_W.$$

$\square$