”Le corps conditionnne le raisonnement.”

Theorie des Corps

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:*

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

Rmq : si K est un anneau avec au moins 2 elts 0_K n'est jamais inversible.

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

$\mathbb{R}(X) = \left\{ \frac{P(X)}{Q(X)} \;\; P, Q \in \mathbb{R}[X] \right\}$ corps des fractions rationnelles à coefs dans $\mathbb{R}$

THÉORÈME 4.1. *Soit $q \geqslant 2$ un nombre premier (les seuls diviseurs de q sont 1 et q) alors l'anneau des classes de congruences modulo q $(\mathbb{Z}/q\mathbb{Z}, +, .)$ est un corps (fini de cardinal q).*

Rmq: si q est composé $q = q_1 q_2$ $q_i \geq 2$ alors $\mathbb{Z}/q\mathbb{Z}$ n'est pas un corps car $q_1 \pmod q$ et $q_2 \pmod q$ sont $\neq 0 \pmod q$ mais $q_1 \pmod q \cdot q_2 \pmod q = q_1 q_2 \pmod q = 0(q)$ $q_1(q)$ et $q_2 \pmod q$ ne peuvent pas être inversible.

Notation: le corps $\mathbb{Z}/q\mathbb{Z}$ et note $\mathbb{F}_q$.

PROPOSITION 4.1. *Soit K un corps, B un anneau et $\varphi \in \mathrm{Hom}_{Ann}(K, B)$ un morphisme. Alors si φ n'est pas nul ($\varphi \neq \underline{0}_B$) φ est injectif:*

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

Preuve : et donc $\varphi(K)$ est un sous-anneau de B isomorphe à K

Soit $\varphi : K \to B$ tq $\varphi \neq \underline{0}_B$

il existe $a \in K$ tq $\varphi(a) \neq 0_B$

en particulier $a \neq 0_K$ et comme K est un corps a est inversible

Construction de Corps

PROPOSITION 4.2. *Soit A un anneau integre (en particulier commutatif) , alors il existe un corps K et un morphisme d'anneau injectif*

$$\iota : A \hookrightarrow K$$

(de sorte qu'on peut considerer A comme un sous-anneau de K en identifiant A a $\iota(A) \subset K$) et tel que K a la propriete de minimalite suivante: pour tout corps K' et tout morphisme injectif

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

il existe un morphisme (necessairement injectif)

$$\iota'_K : K \hookrightarrow K'$$

prolongeant le morphisme ι' (ainsi A et K peuvent etre vus comme des sous-anneaux de K').

DÉFINITION 4.3. *Le corps K s'appelle le corps des fractions de A et se note* $\mathrm{Frac}(A)$.

$\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$

Rmq: "prolonge": $\iota'_K : K \to \cdot$

non nul.

Définition 4.4. *soit A un anneau commutatif. Un ideal $I \subset A$ est maximal si $I \neq A$ et si il est maximal pour l'inclusion parmi tous les ideaux de A distincts de A:*

$$\forall J \subset A, J \text{ ideal de } A,\ I \subset J \Longrightarrow J = I \text{ ou } J = A$$

Théorème 4.2. *L'anneau commutatif A/I est un corps ssi I est un ideal maximal.*

Rmq: si q est premier, $q>1$, $q\mathbb{Z}$ est maximal

$q_1, q_2 \geq 2$, $q_1 q_2 \mathbb{Z}$ n'est pas maximal ($q_1 q_2 \mathbb{Z} \subset q_1\mathbb{Z} \neq \mathbb{Z}$, $\subset q_2\mathbb{Z}$)

Rmq: les ideaux maximaux existent toujours (peu necessiter l'axiome du choix)

Preuve:

Caractéristique d'un Corps

K corps : morphisme canonique

$$\begin{aligned} Can_K : \mathbb{Z} &\longrightarrow K \\ n &\longrightarrow n.1_K = n_K \end{aligned}$$

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

$$p \geq 0$$

Définition 4.6. *L'entier p s'appelle la caracteristique du corps K et se note*

$$\mathrm{car}(K) \geqslant 0$$

$$\ker(\mathrm{Can}_K) = \mathrm{car}(K).\mathbb{Z}$$

Cas $p = 0$

$\ker(\mathrm{Can}_K) = \{0\} \iff \mathrm{Can}_K$ est injectif

et donc $\mathrm{Can}_K : \mathbb{Z} \hookrightarrow K$, $n \longmapsto n.1_K$

K contient un ss-anneau isomorphe a $\mathbb{Z}$

K est infini

mais en plus si K contient $\mathbb{Z}$

$$n \in \mathbb{Z} \longrightarrow n_K \in K$$

de plus K contient $\mathbb{Q}$

$$\frac{a}{b} \in \mathbb{Q} \longrightarrow \frac{a_K}{b_K} = a_K \cdot b_K^{-1} \in K$$

Cas $p \geq 1$ ⚠ exclure $p=1$

LEMME 4.2. *Si* $\mathrm{car}(K) > 0$ *alors* $\mathrm{car}(K) = p$ *est un nombre premier.*

Preuve: supposons par l'absurde que $p = q_1 \cdot q_2$ $q_1, q_2 \geq 2$

alors on $p_K = p \cdot 1_K = 0_K$ ($p \in \ker(\mathrm{Can}_K)$)

$p_K = (q_1 \cdot q_2)_K = q_{1K} \cdot q_{2K} = 0_K$

K est un corps donc intègre donc

q_{1K} ou q_{2K} est $= 0_K$

Supposons que $q_{1K} = 0_K$

$\Rightarrow q_1 \in \ker(\mathrm{Can}_K) = p\mathbb{Z}$

q_1 est un multiple de p mais comme

$q_2 \geq 2 \Rightarrow q_1 < p = q_1 q_2$

absurde.

□

LEMME 4.3. *L'anneau* $\mathrm{Can}_K(\mathbb{Z}) = \mathbb{Z}.1_K$ *est un corps fini de cardinal* p *isomorphe au corps* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Recap: $\mathrm{Car}(K).\mathbb{Z} = \ker(\mathrm{Can}_K)$

- si $\mathrm{Car}(K) = 0 \Rightarrow K \supset \mathbb{Q}$
- si $\mathrm{Car}(K) = p \geq 2$ premier

$K \supset \mathrm{Can}_K(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

On dit que $\mathbb{Q}$ ou $\mathbb{F}_p$ est le sous-corps premier de K

Preuve : si $n, k \in \mathbb{Z}$

$$\mathrm{Can}_K(n + pk) = n_K + p_K \cdot k_K$$

mais $p_K = O_K = n_K$

l'image de n par Can_K ne dépend que la classe $n + p\mathbb{Z}$.

Can_K définit une application

$$\mathbb{Z}/p\mathbb{Z} \longrightarrow K$$

$$n \pmod p \longrightarrow n_K$$

et cette application est un morphisme d'anneau non-nul (car $1(p) \to 1_K \neq 0$)

Ce morphisme et injectif et son image c'est $\mathrm{Car}_K(\mathbb{Z})$ □

Lemme 4.4. *Un anneau commutatif integre et fini est un corps.*

Preuve: Exercice. □

Définition 4.7. *Le corps $\mathbb{Q} \subset K$ (si $\mathrm{car}(K) = 0$) ou bien $\mathbb{F}_p \subset K$ (si $\mathrm{car}(K) = p > 0$) s'appelle le sous-corps premier de K.*

Arithmetique des Corps de caracteristique >0

Frobenius

Proposition 4.3. *Soit K un corps de caracteristique $p > 0$ alors l'application*

$$\bullet^p : \begin{array}{ccc} K & \mapsto & K \\ x & \mapsto & x^p \end{array}$$

est un morphisme d'anneaux non-nul (donc necessairement injectif).

Définition 4.8. *Soit K un corps de caracteristique p, le morphisme d'anneau precedent s'appelle le morphisme de Frobenius (ou simplement le Frobenius) de K se note*

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

En particulier

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

Preuve: on veut mq

$$x^p \cdot y^p = (x \cdot y)^p$$

$$(x \cdot y)^p = \underbrace{xy \cdot xy \cdot xy \cdot \ldots \cdot xy}_{p \text{ fois}}$$

$$\overset{\uparrow}{=}$$

Ket commutatif $(xy)^p = x^p \cdot y^p$.

$$(x+y)^p = \underbrace{(x+y)\cdot(x+y)\cdot\ldots\cdot(x+y)}_{p \text{ fois}}$$

Comme K est commutatif on a la formule du binôme de Newton

$$= \sum_{k=0}^{p} C_p^k \cdot x^k \cdot y^{p-k}$$

$$C_p^k = \frac{p!}{k!(p-k)!}$$

$$= y^p + \sum_{k=1}^{p-1} C_p^k x^k y^{p-k} + x^p$$

- si $1 \leq k \leq p-1$ l'entier

C_p^k est divisible par p :

$$C_p^k = \frac{p!}{k!.(p-k)!} = \frac{p \cdot (p-1)!}{k!.(p-k)!}$$

$k! = 1 \cdot 2 \cdot \ldots \cdot (k-1) \cdot k$

$(p-k)! = 1 \cdot 2 \cdot \ldots \cdot (p-k-1) \cdot (p-k)$

et comme $k < p$ $k!$ n'est pas divisible par ce nb premier p.

de même comme $p-k < p$ $(p-k)!$ n'est pas divisible par p.

$$C_p^k = p \cdot \frac{(p-1)!}{k!(p-k)!} \in \mathbb{N}$$

Comme $k!.(p-k)!$ divise $p.(p-1)!$

et est premier avec p

$k!.(p-k)!$ divise $(p-1)!$

$$C_p^k = p \cdot \underbrace{\frac{(p-1)!}{k!(p-k)!}}_{\in \mathbb{N}} \quad 1 \leq k \leq p-1$$

$$\in p\,\mathbb{N}$$

dans le corps K $\quad 1 \leq k \leq p-1$

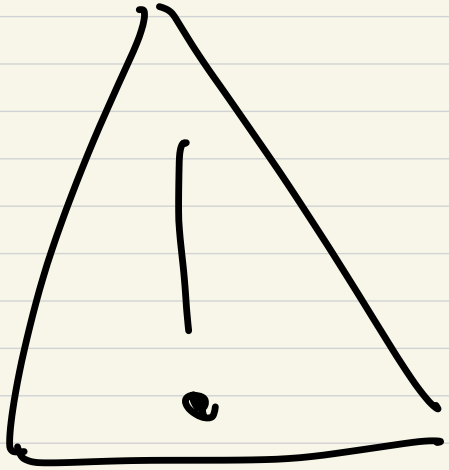
$$C_p^k x^k y^{p-k} = C_p^k \cdot 1_K \cdot x^k y^{p-k} = (C_p^k)_K \, x^k y^{p-k}$$

$$C_p^k x^k y^{p-k} = O_K$$

$$(x+y)^p = y^p + (p-1)\cdot O_K + x^p$$

$$= x^p + y^p$$

□



en general $x^p \neq x$

(si K est un corps de caractéristique p general)

Petit Thm de Fermat :

si $x \in \mathbb{F}_p$ (son image ds K)

alors on a $x^p = x$

de manière équivalente : $\forall n \in \mathbb{Z}$

$n^p - n$ est divisible par p

Si K est un corps de caractéristique p et $x \in K$ alors

$$x^p = x \quad \text{ssi} \quad x \in \mathbb{F}_p \left(\text{l'image de } \mathbb{Z} \text{ par } \text{Can}_K \right)$$

Calcul en car $= p > 0$

$x \in K \quad x \neq 0_K$ alors pour $n \in \mathbb{Z}$

$$n.x = \underbrace{x + \dots + x}_{n \text{ fois}} = 0_K \overset{\text{ssi}}{\equiv} n \in p\mathbb{Z}$$

$$n.x = n.1_K.x = (\underbrace{1_K + \dots + 1_K}_{n}).x = \underbrace{n.1_K}_{n_K}.x$$

$$= \underbrace{x + \dots + x}_{n \text{ fois}} = 1_K.x + \dots + 1_K.x \quad \text{Car}_K(n)$$

Théorème 4.3 (Petit Theoreme de Fermat). *Soit K un corps de caracteristique positive p et $\mathrm{frob}_p : K \mapsto K$ le Frobenius. Pour tout $x \in \mathbb{F}_p = \mathbb{Z}.1_K$ on a*

$$\mathrm{frob}_p(x) = x^p = x.$$

Si $x \in \mathbb{F}_p \Rightarrow x^p = x$

Preuve : preuve $x = n.1_K$ avec $n \in \mathbb{Z}$
et faire une recurrence sur n..

.....

$\Longleftarrow$ si x verifie $x^p = x$ alors

x est racine du polynome de $d^\circ p$

$P(X) = X^p - X$

$P(X)$ n'a pas plus de p racines distinctes

et $P(X)$ admet deja les elts de

$\mathbb{F}_p$ comme racine.

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.

Espaces Vectoriels

Définition 6.1. *Soit K un corps, un K-espace vectoriel (K-EV) V est simplement un K-module. Les elements de V sont appeles vecteurs de V.*

Ex: $\{0_K\}$

- K. et un K-ev ou la multiplication externe et interne sont elles ém.

Produit V et W sont des K-EV

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

a une structure de K-ev "produit"

$$(v,w) + (v',w') = (v+v', w+w')$$

$$k \in K \quad k.(v,w) = (k.v, k.w)$$

$k.v$: mult ext sur V

$k.w$: mult ext sur W

en appliquant à $V=W=K$ et en itérant on obtient pour $d>1$

$$K^d = \{ (x_1, x_2, \dots, x_d) = \vec{x} \quad x_i \in K \quad i = 1 \dots d \}$$

$$\vec{x} + \vec{x'} = (x_1 + x'_1, \dots, x_d + x'_d)$$

$$k \cdot \vec{x} = (k \cdot x_1, \dots, k \cdot x_d) \qquad O_{K^d} = \underline{O}_d = (0, \dots, 0)$$

$$\mathcal{F}(X,K) = \{ f : X \to K \}$$

$f+g : x \to f(x)+g(x)$ $\rightsquigarrow$ une structure de K-EV.

$k. : x \to k.f(x)$

$\mathcal{F}(X,V)$

$V = K\text{-}EV$

$\mathcal{F}(X, V) = \{f : X \to V\}$

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

$k.f : x \to k.f(x)$

Sous-Espace Vectoriel

Définition 6.2. *Soit V un K-espace vectoriel, un sous-espace vectoriel (SEV) de V est un sous-K module $W \subset V$.*

Proposition 6.1 (Critere de SEV). *Un sous-ensemble $U \subset V$ d'un K-EV est un SEV ssi*

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

Ex: $\{0_V\}, V \subset V$ sont des SEV

- $\vec{v} \in V \quad K.\vec{v} = \{k\vec{v} \quad k \in K\}$ est un SEV

- $\{(x_1, \dots, x_d) \quad x_i \in K \quad x_1 + \dots + x_d = 0_K\} \subset K^d$ est un SEV de K^d

- $\{(x_1, \dots, x_d) \quad x_1 + \dots + x_d = 1_K\} \subset K^d$ PAS un SEV!

$$\mathcal{F}(K,K) = \{ f : x \to f(x) \in K \}$$

$$\mathcal{F}(K,K)^+ = \{ f : K \to K \quad f(-x) = f(x) \}$$

$$\mathcal{F}(K,K)^- = \{ f : K \to K \quad f(-x) = -f(x) \}$$

sont des SEV.

Applications Linéaires

Définition 6.3. *Soient V et W deux K-espaces vectoriel, un morphisme $\varphi : V \mapsto W$ de K-modules est appele une application K-lineaire.*

Proposition 6.2 (Critere d'application lineaire). *Une application entre espaces vectoriels $\varphi : V \mapsto W$ est lineaire ssi*

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

Exemples $V = K^d = \{(x_1, \dots, x_d) \quad x_i \in K\}$

$e_1^* : \vec{x} = (x_1, \dots, x_d) \in K^d \to x_1 \in K$

$\vdots$

$e_i^* : \vec{x} = (x_1, \dots, x_i, \dots, x_d) \in K^d \to x_i \in K$

$\vdots$

e_d^* les $e_i^* : K^d \to K$ sont K-linéaires.

PROPOSITION 6.3. *Si $\varphi : V \mapsto W$ est une application lineaire, le noyau*

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

et l'image

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

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

PROPOSITION 6.4. *Soit $\varphi : V \mapsto W$ est une application lineaire, alors φ est injective ssi*

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

$e_1^* : K^d \to K$

$\ker e_1^* = \{(0, x_2, \dots, x_d) \quad x_2, \dots, x_d \in K\}$

$\mathrm{Im}(e_1^*) = K$ $\quad$ e_1^* est injective ssi $d = 1$.

$S : K^d \to K$

$\vec{x} \longrightarrow x_1 + \dots + x_d$

S est linéaire

$\ker S = \{\vec{x} \text{ tq } x_1 + \dots + x_d = 0\}$

groupe linéaire.

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

NOTATION 6.2. *On notera*

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

$$\mathrm{End}_{K-EV}(V) = \mathrm{Hom}_{K-EV}(V,V),\ \mathrm{Aut}_{K-EV}(V) = \mathrm{GL}(V) = \mathrm{Isom}_{K-EV}(V,V)$$

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

On écrira aussi $\mathrm{Hom}_K(V,W)$ $\mathrm{End}_K(V)$

etc.....

Stabilité des applications linéaires

$\varphi : U \to V$ $\psi : V \to W$ linéaires

$\psi \circ \varphi$ est linéaire.

et si $\varphi : U \to V$ est bij alors

$\varphi^{-1} : V \to U$ est linéaire.

Si $\varphi : V \to W$ $\varphi' : V \to W$

$k \in K$ alors

$k.\varphi + \varphi' : \vec{v} \to k.\varphi(\vec{v}) + \varphi'(\vec{v})$

est linéaire (utilise que K est commutatif)

PROPOSITION 6.5. *La composee de deux applications K-lineaires est K-lineaire : pour $\varphi \in \mathrm{Hom}_K(U,V)$ et $\varphi \in \mathrm{Hom}_K(V,W)$ lineaires, alors $\psi \circ \varphi : U \mapsto W$ est K-lineaire et si φ est bijective alors $\varphi^{-1} : V \mapsto U$ est encore lineaire.*

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

$$\lambda.\varphi + \phi : u \in U \mapsto \lambda\varphi(u) + \phi(u) \in V$$

est K-lineaire.

THÉORÈME 6.1. *L'ensemble des application lineaires $\mathrm{Hom}_K(V,W)$ a une structure naturelle de K-EV.*

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

$\mathrm{Hom}_{K\text{-ev}}(V, W)$ a une structure naturelle de K-EV.

$\mathrm{Hom}_K(V, K) = V^*$ le dual de V

si $V = K^d$ $e_i^* \in V^*$

les vecteurs de V^* s'appellent les

<u>formes linéaires</u>

$\mathrm{End}_K(V) = \mathrm{Hom}_K(V,V)$ est un K-ev

et muni de la composition des AL

$\left(\mathrm{End}_K(V), +, \cdot_K, \circ, 0_V, \mathrm{Id}_V\right)$

a une structure d'anneau et m de

K-algebre.

L'algebre des endomorphismes de V

Sous-Espace Engendré

PROPOSITION 6.6 (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 6.4. *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*

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

Si $\mathscr{F} = \emptyset$ $\langle \mathscr{F} \rangle = \{0_V\}$

$\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$ $\quad n \geq 1 \quad \lambda_i \in K$

$x_i \in \mathscr{F}$

Cas particuliers : Somme / Somme directe

Si X, Y sont de SEV de V

on note $X + Y$ = "la somme de X et Y"

$= Vect(X, Y) \subset V$

LEMME 6.1. *On a*

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

Preuve : $\{x+y \quad x \in X, y \in Y\} \subset X+Y$?

vrai car si $x \in X, y \in Y$

$\cap$

$X+Y \qquad X+Y$

et comme $X+Y$ est un SEV $x+y \in X+Y$

$X+Y \subset \{x+y \quad x,y\}$ il suffit de

voir que $\{x+y \quad x,y\}$ est un SEV

car alors il contient X et Y et

donc contient $\text{Vect}(X,Y) = X+Y$.

Soient x,x',y,y' $\lambda \in K$

$$\lambda(x+y)+(x'+y') = \underbrace{(\lambda x+x')}_{\in X} + \underbrace{(\lambda y+y')}_{\in Y} \quad \square$$

NOTATION 6.3. *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 6.6. *Si X et Y sont en somme directe alors l'ecriture de tout vecteur $v \in X \oplus Y$ sous la forme*

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

est unique.

Preuve : si $v \in X \oplus Y$ si $v = x+y = x'+y'$

on veut mq $x = x'$ et $y = y'$?

On a $x+y = x'+y' \iff x - x' = y' - y$

$\in X$ $\in Y$

$\in X \cap Y$

$$x - x' \in X \cap Y$$

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

$$\Rightarrow x = x' \ \& \ y = y'$$

□

Exo: $V = X \oplus Y$

$\pi_X : V = X \oplus Y \longrightarrow X$

$v = x + y \longrightarrow x$

mq π_X est linéaire de V vers X

- calculer $\mathrm{Im}(\pi_X)$ et $\ker(\pi_X)$
- Mq $\pi_X \circ \pi_X = \pi_X$ (Idempotente)

= projection sur X // lement a Y.

- pareil pour π_y :

- Mq $V = X \oplus Y \simeq X \times Y = \{(x,y) \begin{matrix} x \in X \\ y \in Y \end{matrix}\}$

Familles Generatrices libres, bases

DÉFINITION 6.6. *Soit V un K-e.v. Un sous-ensemble $\mathscr{G} \subset V$ est une famille generatrice si*

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

ie. tout element $v \in V$ peut s'ecrire sous la forme d'une combinaison lineaire 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

$$v = \sum_{i=1}^{n} x_i \mathbf{e}_i. \tag{6.2.1}$$

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

Ex: K^d $d \geq 1$ K^d est de type fini

K^d est engendré par la famille de d elts

$e_1 = (1, 0, \ldots, 0)$ $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_d = (0, 0, \ldots, 1)$

si $(x_1, x_2, \dots, x_d) \in K^d$

$\overrightarrow{x}$

$$\vec{x} = x_1.(1,0,\dots,0) + x_2.(0,1,0,\dots,0)$$

$$+ \dots + x_d.(0,\dots,0,1)$$

$$= x_1 e_1 + \dots + x_d e_d .$$

$\mathcal{F}(\mathbb{R},\mathbb{R})$ n'est pas de type fini

- $\mathbb{R} \supset \mathbb{Q}$

  $\mathbb{R}$ est un $\mathbb{Q}$-ev

  $\mathbb{R}$ n'est pas un $\mathbb{Q}$-ev de type fini.

- $\mathbb{R} \supset \mathbb{R}$ $\mathbb{R}$ est un $\mathbb{R}$-ev

  $\mathbb{R}$ est de type fini (comme $\mathbb{R}$-ev)

  $\forall x \in \mathbb{R}$ $x = x \cdot 1_{\mathbb{R}}$.

Définition 6.7. *Soit V un K-EV de type fini. Si V est non-nul, sa dimension le minimum du cardinal des familles generatrices finies 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 peux prendre la famille vide comme famille generatrice).

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

THÉORÈME 6.2. *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.*

Rmq C'est totalement faux si K est un anneau general ~~m~~ tres joli

pares: $\mathbb{Z}$. les $\mathbb{Z}$-modules sont les gpes commutatifs et il y a des tas de gpes commutatifs qui ne sont pas de la forme $\mathbb{Z}^d$ de type fini

Par exemple un gpe commutatif fini.

Ex: $\mathbb{Z}/q\mathbb{Z}$. $\mathbb{Z}/q\mathbb{Z} = \mathbb{Z}.1_{\mathbb{Z}/q\mathbb{Z}}$

$\mathbb{R}$ n'est pas de type fini comme $\mathbb{Q}$-ev:

Supposons $\mathbb{R}$ est un $\mathbb{Q}$-ev de t.f.

$$\mathbb{R} \simeq \mathbb{Q}^d \quad d \geq 1$$

$$|\mathbb{R}| = |\mathbb{Q}^d|$$

$\mathbb{Q}$ est dénombrable $|\mathbb{Q}| = |\mathbb{N}|$

le produit $|\mathbb{Q}^d| = |\mathbb{N}| \Rightarrow |\mathbb{R}| = |\mathbb{N}|$ ← Contradiction

□

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

$CL_g : K^d \longrightarrow V$

$\vec{x} = (x_1, \dots, x_d) \longrightarrow x_1 e_1 + x_2 e_2 + \dots + x_d e_d = v \in V$

$CL_g(\vec{x})$

$CL_g(\bullet)$ est linéaire.

$$CL_g(\lambda\vec{x} + \vec{x'})$$

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

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

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

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

Dire que G est génératrice

$\Longleftrightarrow$ CL_G est surj.

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

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

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

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

(on veut mq CLg est injective)

Famille Libre

$$\mathcal{F} = \{e_1, \dots, e_p\} \subset V$$

$$CL_{\mathcal{F}} : K^p \longrightarrow V$$

$$\vec{x} = (x_i)_{i \leq p} \longrightarrow x = x_1 \cdot e_1 + \dots + x_p \cdot e_p$$

Image $CL_{\mathcal{F}}(K^p) = \langle \mathcal{F} \rangle \subset V$

$CL_{\mathcal{F}}$ et injective ?

$CL_{\mathcal{F}}$ inj ?

Si $\vec{x}$ et $\vec{x'}$ sont tq $V = x_1 e_1 + \dots + x_p e_p$

$= x'_1 e_1 + \dots + x'_p e_p$

$\Rightarrow x_1 = x'_1, \dots, x_p = x'_p$

$\Rightarrow x_1 - x'_1 = \dots = x_p - x'_p = 0_K$

L'écriture de V comme CL d'elts de $\mathcal{F}$ est unique.

Cl_f inj ?

$\ker(Cl_f) = \{0_{K[f]}\}$

si $\vec{x}$ tq $x_1 e_1 + \dots + x_g e_g = 0_V$

$\Rightarrow x_1 = x_2 = \dots = x_g = 0_V$.

Définition 6.8. *Un sous-ensemble fini* $\mathscr{F} = \{\mathbf{e}_1, \cdots, \mathbf{e}_f\} \subset V$ *d'un espace vectoriel est une famille libre de* V *si et seulement si l'une des trois conditions equivalentes suivante est satisfaite:*

(1) L'application lineaire

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

est injective.

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

$$x_1.\mathbf{e}_1 + \cdots + x_f.\mathbf{e}_f = x'_1.\mathbf{e}_1 + \cdots + x'_f.\mathbf{e}_f \Longrightarrow x_1 - x'_1 = \cdots = x_f - x'_f = 0_K.$$

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

$$x_1.\mathbf{e}_1 + \cdots + x_f.\mathbf{e}_f = 0_V \Longrightarrow x_1 = \cdots = x_f = 0_K.$$

Une famille $\mathscr{F}$ *qui n'est pas libre est dit liee.*

Exemple Base Canonique

K^d $e_1 = (1, 0, \dots, 0), \dots, e_d = (0, \dots, 0, 1)$

est libre.

K^3 $v_1=(1,1,0)$ $v_2=(0,1,1)$ $v_3=(1,0,1)$

Soient $x_1, x_2, x_3 \in K$ tq

$$x_1v_1 + x_2v_2 + x_3v_3 = (0,0,0)$$

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

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

$$\begin{cases} x_1 + \quad + x_3 = 0 \\ x_1 + x_2 \quad = 0 \\ \quad x_2 + x_3 = 0 \end{cases}$$

$x_2 = -x_3$

$2 = 2_K = 2 \cdot 1_K$

Si Con $K \neq 2$

$2_K \neq 0_K$ donc inversible

$$\begin{matrix} x_1 + x_3 = 0 \\ x_1 - x_3 = 0 \end{matrix} \Longrightarrow 2x_1 = 0$$

$\Longrightarrow x_1 = 0 \quad x_3 = 0 \quad x_2 = 0$

Si $Car(K)=2$ $\quad x_1-x_3=0 \Rightarrow x_1=x_3$

$x_1+x_2=0=x_1-x_2 \quad x_1=x_2$

$$v_1+v_2+v_3=(2,2,2)=(0,0,0)$$

Famille non libre.

$$x_3 = -x_3 \Leftrightarrow 2x_3 = 0$$

($x = -x$ si $\mathrm{Car}(K) = 2$)

Si $\mathrm{Car}(K) \neq 2$ la famille est libre.

- Si $\mathrm{Car}(K) = 2$ la famille n'est pas libre

PROPOSITION 6.8. *Une famille a l elements $\mathscr{F} = \{\mathbf{e}_1, \cdots, \mathbf{e}_l\} \subset V$ est liee ssi il existe $i \in \{1, \cdots, l\}$ tel que $\mathbf{e}_i$ peut s'exprimer comme combinaison lineaire des autres elements de $\mathscr{F}$:*

$$\exists i \leqslant l,\ \mathbf{e}_i \in \mathrm{Vect}(\mathscr{F} - \{\mathbf{e}_i\}) = \mathrm{Vect}(\{\mathbf{e}_j,\ j \neq i\}).$$

On a alors

$$W = \mathrm{Vect}(\mathscr{F}) = \mathrm{Vect}(\mathscr{F} - \{\mathbf{e}_i\}).$$

Preuve : Si $\mathcal{F}$ est liee il existe

$(x_1, \cdots, x_l) \neq (0, \cdots, 0)$ tq

$x_1 e_1 + \cdots + x_l e_l = 0_V$

comme $\vec{x} \neq \vec{0}$ il existe $i \in \{1, \cdots, l\}$ tq

$x_i \neq 0$ quitte à renumeroter les e_i

ops $i = l$ $\quad x_l \neq 0$

$$x_1 e_1 + \dots + x_{l-1} e_{l-1} + x_l e_l = 0$$

$$(-x_l) e_l = x_1 e_1 + \dots + x_{l-1} e_{l-1}$$

$-x_l \neq 0$ donc inversible

$$e_l = \frac{x_1}{-x_l} e_1 + \dots + \frac{x_{l-1}}{-x_l} e_{l-1}$$

e_ℓ est CL de $\{e_1, \dots, e_{\ell-1}\}$

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

$\mathrm{Vect}(\mathcal{F}) = \mathrm{Vect}(\mathcal{F} - \{e_\ell\})$

$\Longleftarrow$ $e_\ell \in \mathrm{Vect}(\{e_1, \dots, e_{\ell-1}\})$ alors

il existe $x_1, \dots, x_{\ell-1} \in K$ tq

$$e_l = x_1 e_1 + \dots + x_{l-1} e_{l-1}$$

$$0 = x_1 e_1 + \dots + x_{l-1} e_{l-1} + (-1) e_l$$

Comme $-1 \neq 0$

$F = \{e_1, \dots, e_l\}$ est liée.

□

THÉORÈME. *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 $\{0_K\} = K^0$).*

Preuve: Soit $\mathcal{G} \subset V$ une famille generatrice de taille $d = \dim(V)$ ce $\mathcal{G} = \{e_1, \dots, e_d\}$

$CL_{\mathcal{G}} : K^d \longrightarrow V$ est surjective

on veut mq c'est injectif.

Cad G est libre.

Si G était liée alors il existerait

$i \in \{1, \dots, d\}$ tq

$e_i \in Vect(G - \{e_i\})$

$Vect(G - \{e_i\}) = Vect(G) = V$

V serait engendré par $d-1$ éléments

ce qui contredit la déf de $\dim V$.

- G est libre

$Cl_G : K^d \to V$ est un isom.

□

Corollaire : Soient V et W des K-ev de dim finies alors

$$V \simeq W \text{ ssi } \dim V = \dim W$$

(en particulier $\mathbb{R}^2 \not\simeq \mathbb{R}^3$ comme $\mathbb{R}$-ev.)