§1. Panorama algèbre
Espaces vectoriels

I. Panorama algèbre

$\boxed{\text{Ensembles}}$

$\boxed{\text{Groupes}}$ ens + 1 loi + prop

$(\mathbb{Z},+)$ $(\mathbb{R}^*,\times)$ .....

$(\mathbb{R}^n,+)$ — pas de 2ème loi

vects

2 opérations ?

2 lois + prop ....

$x \times y$

pour + : groupe

$\boxed{\text{Anneaux}}$

≠ (prop × ...

$\boxed{\text{Corps}}$ tous les élts (sauf neutre de +) sont sym. pour ×

1 loi + 1 op. externe (produit par un scalaire) $\lambda \cdot \vec{u}$) — vect.

nombre vect

pour + groupe

$\boxed{\text{Espaces vectoriels}}$

+ opération externe

$\cdot : \underbrace{\mathbb{K}}_{\text{corps}} \times \underset{\text{vects}}{E} \longrightarrow E$

corps → ens. de "nombres" / scalaires

$\mathbb{R}$ $\mathbb{C}$ $\mathbb{Z}/p\mathbb{Z}$

ex :

Anneaux $(\mathbb{Z},+,\times)$ $n \in \mathbb{Z}$ $\frac{1}{n} \notin \mathbb{Z}$

$(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$ n pas premier

Corps $(\mathbb{R},+,\times)$ / $(\mathbb{C},+,\times)$

$(\mathbb{Q},+,\times)$

$(\mathbb{Z}/p\mathbb{Z}, \oplus, \otimes)$ p premier

$(\mathbb{R}^n,+,\cdot)$ $\mathbb{R}$-ev $(\mathbb{K}=\mathbb{R})$

(polynômes à coefs ds $\mathbb{R}$, +, ·) $\mathbb{R}$ ev

$\mathbb{R}[X]$

$(\mathbb{Z}/p\mathbb{Z}[X], \oplus, \cdot)$ $\mathbb{Z}/p\mathbb{Z}$ ev

(poly → coefs ds $\mathbb{Z}/p\mathbb{Z}$)

→ sert à l'arithmétique → crypto / codes → cf cours crypto ...

II. Espaces vectoriels.

Dans toute la suite, $\mathbb{K}$ désigne un corps $\to (\mathbb{R}, +, \times)$

$\to (\mathbb{C}, +, \times)$

$\to (\mathbb{Z}/p\mathbb{Z}, \oplus, \otimes)$

$\vdots$

le plus général ... corps à p^n élts $\neq \mathbb{Z}/p^n\mathbb{Z}$ (pas un corps ...)

$\downarrow$

$\mathbb{F}_{p^n}$

1) Généralités.

* déf : Soit E un ensemble (de vecteurs)

et $+$: lci sur E

$\cdot$: loi de comp. externe sur E

$\cdot : \mathbb{K} \times E \longrightarrow E$

$(E, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel ($\mathbb{K}$ev) si :

i) $(E, +)$ groupe commutatif.

ii) les relations suivantes (pseudo-distributivité) sont vraies :

$\lambda \cdot \vec{u}$

$\lambda \in \mathbb{K}$: $+$ a), $\times$ b)

$\vec{u} \in E$: $+$ (sur les vects) c)

distributivité de ces 3 op / $\cdot$

a) $\forall \lambda, \mu \in \mathbb{K}$, $\vec{u} \in E$

$$(\lambda + \mu) \cdot \vec{u} = \lambda \cdot \vec{u} + \mu \cdot \vec{u}$$

b) $\forall \lambda, \mu \in \mathbb{K}$, $\vec{u} \in E$

$$(\lambda \times \mu) \cdot \vec{u} = \lambda \cdot (\mu \cdot \vec{u})$$

c) $\forall \lambda \in \mathbb{K}$, $\vec{u}, \vec{v} \in E$

$$\lambda \cdot (\vec{u} + \vec{v}) = \lambda \cdot \vec{u} + \lambda \cdot \vec{v}$$

iii) $1 \cdot \vec{u} = \vec{u} \quad \forall \vec{u} \in E$

$1 \in \mathbb{K}$ — neutre de $\times$ de $\mathbb{K}$

$\downarrow$ déf

$\forall \lambda \in \mathbb{K} \quad 1 \times \lambda = \lambda \times 1 = \lambda$

$\exists$

ex :

$(\mathbb{R}^n, +, \cdot)$ $\mathbb{R}$ev

$((\mathbb{Z}/p\mathbb{Z})^m, \oplus, \cdot)$ $\mathbb{Z}/p\mathbb{Z}$ ev

$\vdots$

$(\mathbb{Z}^m, +, \cdot)$

$\to (\mathbb{Z}^m, +)$ groupe commut. ✓

$\to \cdot : \lambda \cdot \vec{u} \in \mathbb{Z}^m$

$\lambda \in \mathbb{Z}$ — pas un corps....

② Sous-espaces vectoriels.

Ici $(E,+,\cdot)$ est un $\mathbb{K}$ev.

$(G,*)$ groupe

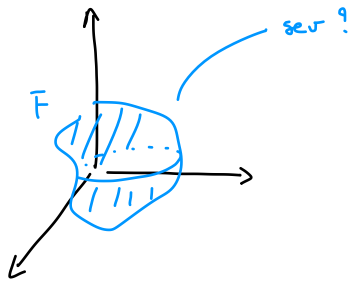
Déf $H \subseteq G$ tq $(H,*)$ groupe

Prop. caract. $H \subseteq G$
→ $H \neq \emptyset$
→ stable par $*$ et sym.

* déf : $F \subseteq E$ est un sous-espace vectoriel de $(E,+,\cdot)$ (distrib...) si $(F,+,\cdot)$ est un $\mathbb{K}$ev (F sev de $(E,+,\cdot)$)

bien définies sur F

ex : $(\mathbb{R}^3,+,\cdot)$



$+$ Ici $\forall \vec{u},\vec{v} \in F$ $\quad \vec{u}+\vec{v} \in F$

$\cdot$ Ici $\forall \lambda \in \mathbb{K}$ $\quad \vec{u} \in F$ $\quad \lambda\cdot\vec{u} \in F$

distributivités

$1\cdot\vec{u} = \vec{u} \quad \forall \vec{u} \in F \subset E$ ...

reste vrai, car vrai ds E ...

Prop (caractérisation)

$F \subseteq E$ est un sev ssi :

i) $F \neq \emptyset$

ii) Version longue

$\forall \vec{u},\vec{v} \in F \quad \vec{u}+\vec{v} \in F$

$\forall \lambda \in \mathbb{K}$, $\vec{u} \in F \quad \lambda\cdot\vec{u} \in F$

F stable par $+$ et $\cdot$

$\Longleftrightarrow$

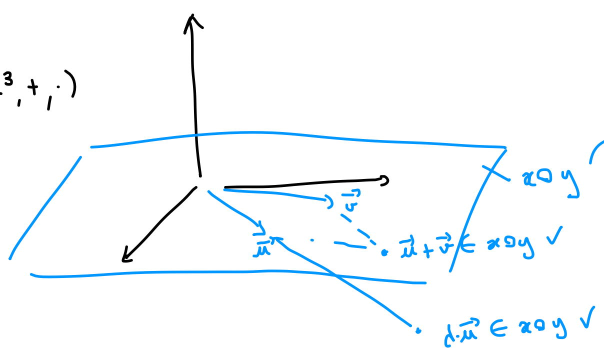
Version courte

ii) $\forall \vec{u},\vec{v} \in F,\ \forall \lambda,\mu \in \mathbb{K}$

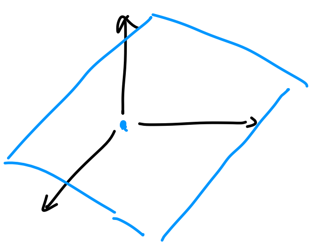
$\underbrace{\lambda\cdot\vec{u}+\mu\cdot\vec{v}}_{\text{combinaison linéaire de } \vec{u} \text{ et } \vec{v}} \in F$

F stable par combinaisons linéaires

ex : $E = (\mathbb{R}^3,+,\cdot)$

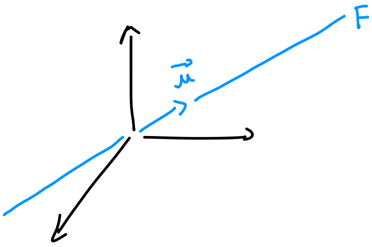


stable par $+$, $\cdot$) → sev



plan quelconque (contenant $\vec{0}$!) — sev car stable par $+$, $\lambda\cdot\vec{u}$

$\vec{u}+\vec{v}$



$\overset{\text{ensemble}}{\#/\#}\ \{\vec{u}\}$ pas un sev

A"

$\lambda \vec{u} + \mu \cdot \vec{u} = (\lambda+\mu)\vec{u} \notin \{\vec{u}\}$ ....

$\neq \vec{u}$

sous-espace vectoriel engendré par A → droite de vecteur directeur $\vec{u}$: F sev

↓

Vect(A)

* **déf**: si $A \subseteq E$ (partie quelconque)

On appelle <u>sous-espace vectoriel engendré</u> par A (noté <u>Vect(A)</u>) le plus petit sous-espace vectoriel de E contenant A.

$A \rightsquigarrow \text{Vect}(A)$

ajouter les élts pour rendre stable par $+$, $\cdot$

Prop Vect(A) : ensemble des comb. linéaires d'éléments de A

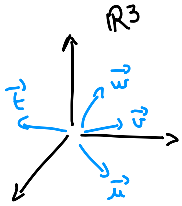
$$\text{Vect}(A) = \{\lambda_1 \cdot \vec{u}_1 + \dots + \lambda_n \cdot \vec{u}_n \ ; \ \lambda_i \in \mathbb{K},\ \vec{u}_i \in A\}$$

* **déf**: une famille de n vecteurs $\{u_1, \dots, u_n\}$ est une <u>famille génératrice</u> de E si :

→ l'espace vect. qu'elle engendre est E

ie → $\text{Vect}\{u_1 \dots u_n\} = E$

ex:



familles génératrices :

→ $(\vec{i}, \vec{j}, \vec{k})$, $\vec{i} = \begin{pmatrix}1\\0\\0\end{pmatrix}$, $\vec{j} = \begin{pmatrix}0\\1\\0\end{pmatrix}$, $\vec{k} = \begin{pmatrix}0\\0\\1\end{pmatrix}$

→ 3 vects non coplanaires

→ 4 vects non coplanaires – génératrice ✓

famille libre ← "1 vect. en trop"... peut être écrit comme c.l. des autres

groupes

$(\mathbb{Z}, +)$

$A = \{1\}$ générateur

$A' = \{2, 3\}$ "

"libres"

bases

nbe d'élts varie...

~~dimension~~

* déf : une famille $\{\vec{u}_1 \dots \vec{u}_m\}$ est libre si

(famille pas libre → liée)

* intuition : aucun vect. n'est c.l. des autres

$\forall \alpha_1 \dots \alpha_m \in \mathbb{K}$

$\alpha_1 \cdot \vec{u}_1 + \dots + \alpha_m \cdot \vec{u}_m = \vec{0} \underset{\text{faux}}{\Longrightarrow} \alpha_1 = \dots = \alpha_m = 0$

(S)

résoudre 1 syst. lin $m \times m$

↓

Gauss $(\mathcal{O}(m^3))$

↘ ∃ solution de (S) avec $\alpha_i \neq 0$

diviser (S) par α_i

↓

$\vec{u}_i = -\left(\frac{\alpha_1}{\alpha_i} \vec{u}_1 + \dots + \frac{\alpha_m}{\alpha_i} \cdot \vec{u}_i\right)$

tester chaque vect.....

↓

⚠ complexité !

ex :

$$\begin{cases} u_1 = (1,1,-1,0) \\ u_2 = (1,0,0,-1) \\ u_3 = (0,1,-1,1) \end{cases}$$

libres ?

on suppose que $\alpha_1 \cdot \vec{u}_1 + \alpha_2 \cdot \vec{u}_2 + \alpha_3 \cdot \vec{u}_3 = \vec{0}$

$\Leftrightarrow \alpha_1 \cdot (1,1,-1,0) + \alpha_2 \cdot (1,0,0,-1) + \alpha_3 (0,1,-1,1) = \vec{0}$

pivot ← 1ère coord

$$\Leftrightarrow \begin{cases} \alpha_1 + \alpha_2 & = 0 \\ \alpha_1 \quad + \alpha_3 & = 0 & e_2 \leftarrow e_2 - e_1 \\ -\alpha_1 \quad - \alpha_3 & = 0 & e_3 \leftarrow e_3 + e_1 \\ -\alpha_2 + \alpha_3 & = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} \alpha_1 + \alpha_2 & = 0 \\ -\alpha_2 + \alpha_3 & = 0 & \leftarrow \text{pivot} \\ \cancel{\alpha_2 - \alpha_3 = 0} & & e_3 \leftarrow e_3 + e_2 \\ \cancel{-\alpha_2 + \alpha_3 = 0} & & e_4 \leftarrow e_4 - e_2 \end{cases}$$

identique

⟶ deviennent $0 = 0$

$$\Leftrightarrow \begin{cases} \alpha_1 + \alpha_2 = 0 \\ -\alpha_2 + \alpha_3 = 0 \end{cases}$$

3 inconnues
− 2 eq
―――――
1 param ↘ α_2

$$\Rightarrow \begin{cases} \alpha_1 = -\alpha_2 \\ \alpha_3 = \alpha_2 \end{cases}$$

famille liée : car infinité de sol avec $\alpha_i \neq 0 \dots$

* déf : si $\{u_1 \dots u_m\} \subseteq E$, le rang de $\{u_1 \dots u_m\}$ est la taille de la plus grande sous-famille libre.

rang $\{u_1 \dots u_m\}$

ex!

$$\begin{cases} u_1 = (1,1,-1,0) \\ u_2 = (1,0,0,-1) \\ u_3 = (0,1,-1,1) \end{cases}$$

⟶ liée → rang < nbre vects ...

↳ rang = 2   ($\{u_1, u_2\}$ libre)

* déf: si une famille de E est libre et génératrice, alors c'est une base de E.

* déf! si E admet une base finie, on dit que c'est un esp. vectoriel de dimension finie.

ex!

ev. de dim finie

$(\mathbb{R}^n, +, \cdot) \longrightarrow \{u_i = (0, \dots \overset{i}{1} \dots 0)\}$

vects à n coords.

$\left(\begin{array}{c}\text{poly} \\ d^\circ \leq n\end{array}, +, \cdot\right)$

$\downarrow$ $\mathbb{R}_n[X]$

$1, X \dots X^n$

ev. de dim ∞.

$(\text{polynômes}, +, \cdot) \xrightarrow{\text{base}} \underbrace{1, X, X^2, \dots\dots}_{\infty}$

$\mathbb{R}[X]$

$\downarrow$

degré ...

Théorème de la base incomplète

Dans un espace vectoriel de dim. finie toutes bases ont le même nombre d'élément → dimension de E dim(E).

Calcul du rang ⇝ par pivot de Gauss sur les coords car

$$\text{rang}\{u_1 \dots u_n\} = \text{rang}\{u_1 + \sum_{i=2}^{n} \alpha_i \cdot u_i, u_2 \dots u_n\}$$

Prop

$$\text{rang } \{u_1 \dots u_n\} = \dim\left(\overbrace{\text{Vect}(\{u_1 \dots u_n\})}^{\text{ev}}\right)$$

(3) Somme de sev.

Prop : E $\mathbb{K}$ev

F_1, F_2 deux sev (stable par c.l.)

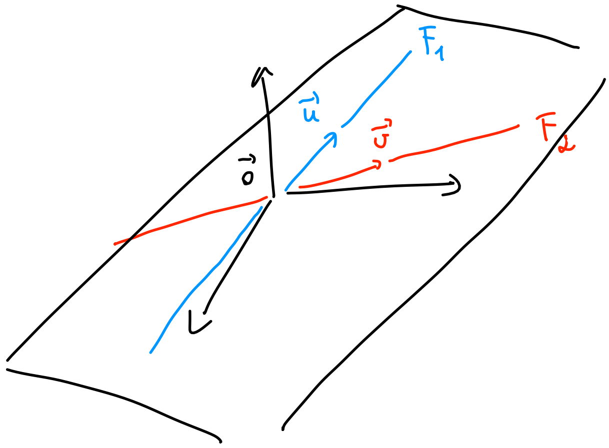
~~$F_1 \cup F_2$~~ pas sev sauf si $F_1 \subseteq F_2$ ou $F_2 \subseteq F_1$

$F_1 \cap F_2 \longrightarrow$ sev (stable par c.l.)

ex : $\mathbb{R}^3$

F_1 sev de dim 1 $\rightarrow$ droite $Vect\{\vec{u}\}$

F_2 sev de dim 1 $\rightarrow$ droite $Vect\{\vec{v}\}$



$F_1 \cup F_2 \longrightarrow$ union de 2 droites $\rightarrow$ pas un sev

$Vect(F_1 \cup F_2) = Vect(\{\vec{u}, \vec{v}\})$

$\rightarrow$ $\underline{\text{c.l. de } \vec{u} \text{ et } \vec{v}}$) plan engendré par $\vec{u}, \vec{v}$ si $\vec{u}, \vec{v}$ libres.

$\lambda.\vec{u} + \mu.\vec{v}$

$\in F_1$ $\in F_2$

$\vec{u}_1 + \vec{u}_2$

$\in F_1$ $\in F_2$

* **déf** : si F_1, F_2 sont des sev de E

$F_1 + F_2 = \{\vec{u}_1 + \vec{u}_2 \ ; \ \vec{u}_1 \in F_1, \ \vec{u}_2 \in F_2\}$ sev de E

$= Vect(F_1 \cup F_2)$

$$F_1 + F_2 = \{ \underbrace{\lambda \cdot \vec{u}_1}_{\in F_1} + \underbrace{\mu \cdot \vec{u}_2}_{\in F_2} \ ; \ \lambda, \mu \in \mathbb{K}, \ \vec{u}_1 \in F_1, \ \vec{u}_2 \in F_2 \}$$

sev

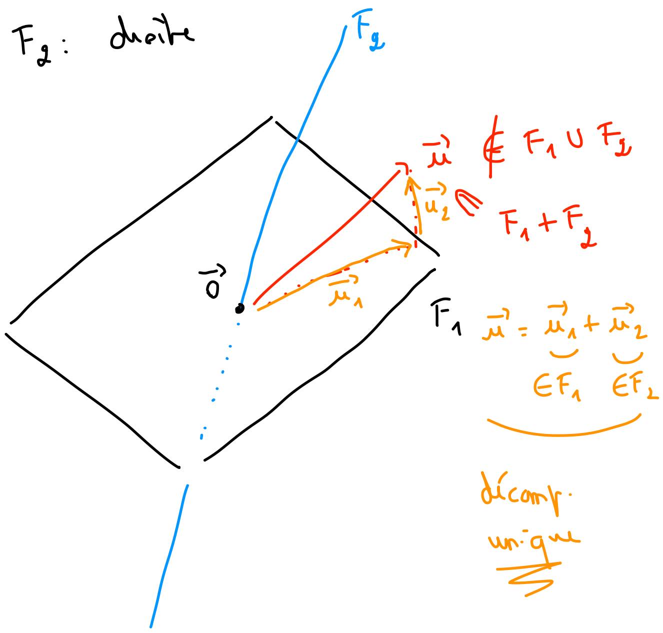
$\cap$ ✓

$\cup$

ex : ds $\mathbb{R}^3$

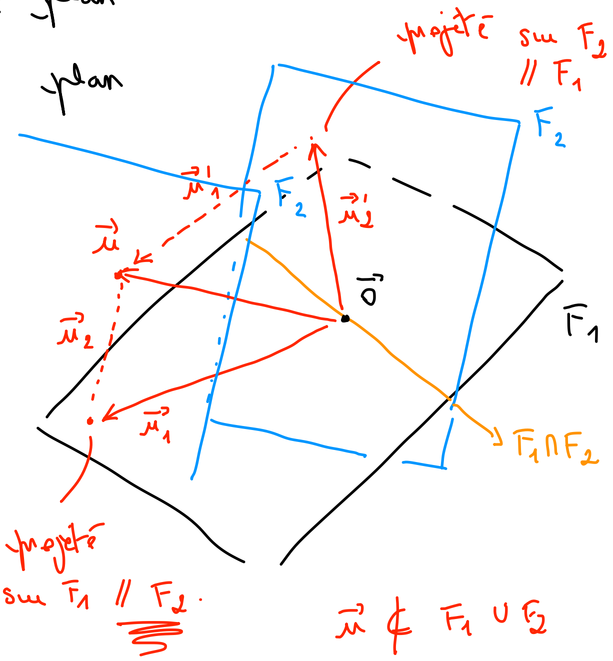
F_1 : plan

F_2 : droite



F_1 : plan

F_2 : plan



$\vec{u} \notin F_1 \cup F_2$

$\vec{u} \in F_1 + F_2$ ✓

$\vec{u} = \vec{u}_1 + \vec{u}_2 = \underbrace{\vec{u}_1'}_{\in F_1} + \underbrace{\vec{u}_2'}_{\in F_2}$

décomp. non unique

$F_1 + F_2 = \mathbb{R}^3$

sev supplémentaires

$F_1 \cap F_2 = \{\vec{0}\}$ — dim 0.

$F_1 + F_2 = \mathbb{R}^3$

F_1 : dim 2, F_2 : dim 2

$\dim(F_1 \cap F_2) = 1$

* **déf** : la somme de deux sev F_1, F_2 est dite directe si

$$F_1 \cap F_2 = \{\vec{0}\}$$

On la note : $F_1 \oplus F_2$

Dans ce cas $\forall \vec{u} \in F_1 \oplus F_2 \quad \exists! \ \vec{u}_1 \in F_1, \ \vec{u}_2 \in F_2$ tq $\vec{u} = \vec{u}_1 + \vec{u}_2$

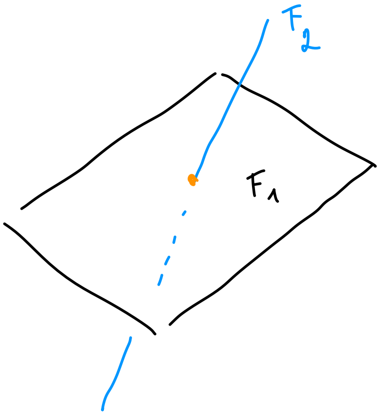
Prop. une base de $F_1 \oplus F_2$ est l'union

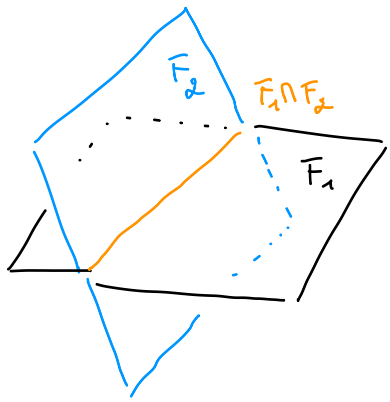
→ d'une base de F_1

→ et une base de F_2

Prop. si F_1, F_2 deux sev de E si somme directe $F_1 \oplus F_2$

$$\dim(F_1+F_2) + \underbrace{\dim(F_1 \cap F_2)}_{0} = \dim F_1 + \dim F_2$$





$F_1 + F_2 = \mathbb{R}^3 \longrightarrow \dim 3$