Mat 301

Chapitre 1 : Rappel d'algèbre linéaire

Déf. On appelle famille d'éléments d'un ensemble E la donnée d'un ensemble I (dont les éléments sont appelés indices) et d'une application de I dans E.

Le cas qui va nous intéresser principalement est le cas où I est fini (famille "finie"), et on prendra en général $I = \{1, \dots, n\}$, $n \in \mathbb{N}^*$.

Exemple de notation :

$\mathcal{F}a = (x_1, x_2, x_3)$ avec $\begin{array}{l} x_1 = (1,0) \\ x_2 = (2,-3) \\ x_3 = (-1,1) \end{array}$ est une famille de $\mathbb{R}^2$

indexée par $\{1,2,3\}$. Elle correspond formellement à $I = \{1,2,3\}$ et

$$\begin{array}{l} I \longrightarrow \mathbb{R}^2 \\ 1 \to (1,0) \\ 2 \to (2,-3) \\ 3 \to (-1,1) \end{array}$$

Déf : Soit E un $\mathbb{K}$-espace vectoriel. On dit que une famille B de vecteurs de E est une base de E ssi tout vecteur de E s'écrit de manière unique comme combinaison linéaire de vecteurs de B.

Cas de la dimension finie : Si E possède une base finie $B = (e_1, \dots, e_n)$ alors $\forall x \in E$ $\exists! \, x_1, \dots, x_n \in \mathbb{K}$ tq. $x = x_1 e_1 + \dots + x_n e_n$

$x_1, \dots, x_n$ sont uniques et s'appellent les coordonnées de x dans la base B.

$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ s'appelle la matrice de coordonnées ou le vecteur colonne des coordonnées de x.

Exemple $(2,3)$ a pour coordonnées $\begin{pmatrix} 2 \\ 3 \end{pmatrix}$ dans la base canonique de $\mathbb{R}^2$

Proposition : Une base de E est exactement une famille libre et génératrice de E.

Preuve – exercice – (rappel) ▨

Proposition : Si E possède une base finie, alors toutes les bases de E ont le même cardinal, appelé la dimension de E.

Preuve – voir cours – rappel) ▨

Proposition : Si $\dim E = n$, une famille B est une base de E

ssi $\operatorname{card} B = n$ et B est libre

ssi $\operatorname{card} B = n$ et B est génératrice

Définition (somme des s.e.v) : Soit E un $\mathbb{K}$-e.v.

Soient F, G des s.e.v. de E. On note

$$F+G=\{f+g,\ f\in F,\ g\in G\}$$
$$(=\{x\in E \mid \exists f\in F,\ \exists g\in G \text{ t.q. } x=f+g\})$$

Proposition : Dans ce cas, $F+G$ est un s.e.v. de E et $\boxed{F+G=\text{vect}(F\cup G)}$

Exemples :

Propositions : Avec ces notations, si B_F est une base de F, B_G est une base de G, alors $B_F\cup B_G$ est une famille génératrice de $F+G$

Preuve : (rappel) - exercice - $\blacksquare$

On va s'intéresser au cas où l'union des bases est une base. (**)

Définition : Soient $F_1, \dots, F_n$ des s.e.v. de E.

On dit que la somme $F_1+\dots+F_n$ est directe ssi tout vecteur de $F_1+\dots+F_n$ s'écrit de manière unique comme somme d'éléments de $F_1,\dots,F_n$

$$\forall x\in F_1+\dots+F_n,\ \exists!\, f_1\in F_1,\dots,\exists!\, f_n\in F_n \text{ t.q. } x=f_1+\dots+f_n$$

Exemple :

$$F+G=F\oplus G$$

$E=\mathbb{R}^3$, $F=\text{vect}((0,0,1))$, $G=\text{vect}((1,0,1),(0,1,1))$

On peut vérifier (exercice) que

$$E=F+G=F\oplus G \quad \blacksquare$$

$F+G=\text{vect}(F\cup G)$
$=\text{vect}((0,0,1),(1,0,1),(0,1,1))=E$ car base

on peut prendre l'union des bases de F et G montrer que c'est une base de E (libre + bon cardinal) et d'après une proposition F et G seront en somme directe

$\Rightarrow E=F\oplus G$ au plus court

$E=\mathbb{R}^3$

$F_1=\text{vect}((1,0,0))$

$F_2=\text{vect}((1,1,0))$

$F_3=\text{vect}((0,0,1))$

On vérifie que $E=F_1+F_2+F_3=F_1\oplus F_2\oplus F_3$

Plus généralement, il est facile de montrer à l'aide des définitions la proposition suivante :

Proposition : Si E est un e.v. de base $B=(e_1,\dots,e_n)$ alors
$$E = vect(e_1) \oplus \dots \oplus vect(e_n).$$

Preuve : exercice $\blacksquare$

De même, on a :

Proposition : Des sev. $F_1,\dots,F_n$ de E sont en somme directe ssi la réunion des bases $B_1,\dots,B_n$ de $F_1,\dots,F_n$ est une base de $F_1+\dots+F_n$.

Démo : idée de la preuve

Supposons que $F_1,\dots,F_n$ sont en somme directe.

Prenons $B_1,\dots,B_n$ des bases de $F_1,\dots,F_n$.

Soit $x \in F_1+\dots+F_n$ $(=F_1\oplus\dots\oplus F_n)$

On veut montrer que x s'écrit de manière unique comme c.l. des vecteurs de $B_1\cup\dots\cup B_n$.

Comme la somme $F_1+\dots+F_n$ est directe, on sait que x s'écrit de manière unique comme somme
$$x = f_1+\dots+f_n \text{ d'éléments } f_1\in F_1,\dots,f_n\in F_n.$$

Chaque f_i, $i=1,\dots,n$, s'écrit de manière unique comme c.l. des vecteurs de $B_1,\dots,B_n$.

Donc x s'écrit comme c.l. de vecteurs $B_1\cup\dots\cup B_n$.

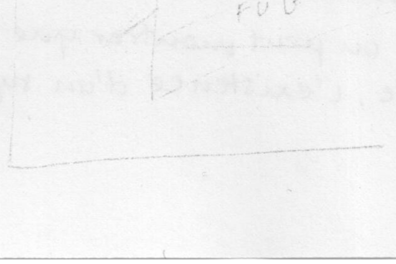
L'unicité résulte du fait que si on prend une autre c.l. de vecteurs de $B_1\cup\dots\cup B_n$ égale à x, en regroupant les termes de $B_1,\dots$, les termes de B_n, on obtient une écriture de x comme somme de vecteurs de $F_1,\dots F_n$.

$$x = (x_{1,1}e_{1,1}+\dots+x_{1,k_1}e_{1,k_1}) + (x_{2,1}e_{2,1}+\dots+x_{2,k_2}e_{2,k_2}) + \dots + (x_{n,1}e_{n,1}+\dots+x_{n,k_n}e_{n,k_n})$$

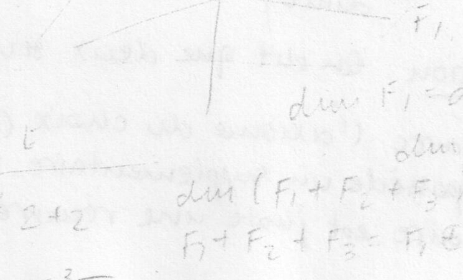
Réciproque : exercice $\blacksquare$

Proposition : Soit E un ev. de dimension finie, $F_1,\dots,F_n$ des sev. de E.
Alors $F_1,\dots,F_n$ sont en somme directe ssi
$$\dim(F_1+\dots+F_n) = \dim F_1+\dots+\dim F_n$$

Exemple :



$\dim F = 2$
$\dim G = 2$
$\dim(F+G) = 3 \neq 2+2$
$F+G \neq F\oplus G$



$\dim F_1 = \dim F_2 = \dim F_3 = 1$
$\dim(F_1+F_2+F_3) = 3$
$F_1+F_2+F_3 = F_1\oplus F_2\oplus F_3$

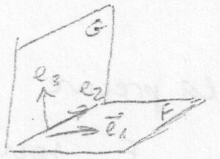
Démonstration : $F_1 + \dots + F_n = F_1 \oplus \dots \oplus F_n \iff \dim(F_1 + \dots + F_n) = \dim F_1 + \dots + \dim F_n$

$\Rightarrow$ Supposons $F_1 + \dots + F_n = F_1 \oplus \dots \oplus F_n$.

D'après le résultat précédent, si $B_1, \dots, B_n$ sont des bases de $F_1, \dots, F_n$, alors $B_1 \cup \dots \cup B_n$ est une base de $F_1 + \dots + F_n$.

On a alors — "union" ou concaténation des familles (pas d'ensemble)

$$\dim(F_1 + \dots + F_n) = \operatorname{card}(B_1 \cup \dots \cup B_n)$$
$$= \operatorname{card}(B_1) + \dots + \operatorname{card}(B_n)$$
$$= \dim F_1 + \dots + \dim F_n$$



$B_1 = (e_1, e_2)$ base de F
$B_2 = (e_2, e_3)$ base de G
$B_1 \cup B_2 = (e_1, e_2, e_2, e_3)$ n'est pas une base de $F+G$

$\Leftarrow$ Supposons $\dim(F_1 + \dots + F_n) = \dim F_1 + \dots + \dim F_n$ (1)

Soit $B_1 \dots B_n$ des bases de $F_1, \dots, F_n$.

On veut montrer que $B_1 \cup \dots \cup B_n$ est une base de $F_1 + \dots + F_n$.

D'après (1), $\operatorname{card}(B_1 \cup \dots \cup B_n) = \operatorname{card} B_1 + \dots + \operatorname{card} B_n$ (union de famille)

$= \dim F_1 + \dots + \dim F_n$ (B_i base de F_i)

$= \dim(F_1 + \dots + F_n)$ (hyp. (1))

De plus, $\operatorname{vect}(B_1 \cup \dots \cup B_n) = \operatorname{vect}(B_1) + \dots + \operatorname{vect}(B_n)$

$= F_1 + \dots + F_n$

i.e. $B_1 \cup \dots \cup B_n$ est génératrice de $F_1 + \dots + F_n$.

Cela caractérise le fait que $B_1 \cup \dots \cup B_n$ est une base de $F_1 + \dots + F_n$.

Cas de deux sev. :

Proposition : Soit F, G deux sev de E. Alors

$$F + G = F \oplus G \iff F \cap G = \{0\}$$

démo : rappel - exercice $\boxed{}$

Proposition Soient F, G deux sev d'un ev E de dimension finie.

Alors $E = F \oplus G \iff \begin{cases} E = F + G \\ F \cap G = \{0\} \end{cases} \iff \begin{cases} \dim F + \dim G = \dim E \\ F \cap G = \{0\} \end{cases} \iff \begin{cases} \dim F + \dim G = \dim E \\ E = F + G \end{cases}$

démo : rappel - exo $\boxed{}$

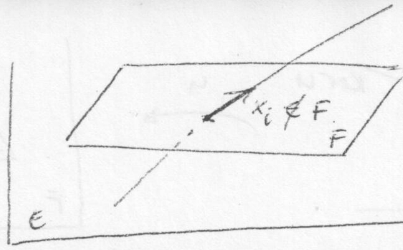
Rmq Cette résultat est du même esprit que les caractérisations d'une base.

somme	famille
$E = F \oplus G$	base
$F \cap G = \{0\}$	libre
$F + G = E$	génératrice
$\dim F + \dim G = \dim E$	cardinal $= \dim E$

Définition : On dit que deux sev F, G de E sont supplémentaires ssi on a $E = F \oplus G$

Rmq : avec l'axiome du choix ($\iff$ lemme de Zorn) on peut montrer que tout sev possède un supplémentaire. En dimension finie, l'existence d'un supplémentaire est juste une récurrence.

Idée : ajouter des droites en somme directe

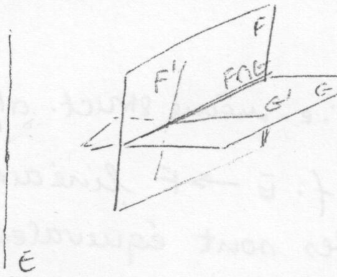


On utilise souvent des supplémentaires (à la place des bases) dans les formules sur les dimensions. Par exemple :

Proposition : Soient F, G des sev de E de dimension finie.

On a $\dim(F+G) = \dim F + \dim G - \dim(F \cap G)$

idée de preuve : prendre F' un supplémentaire de $F \cap G$ dans F, G' un supplémentaire de $F \cap G$ dans G et montrer que $F + G = F' \oplus (F \cap G) \oplus G'$



Exercice ▨

Chapitre 2 : Applications linéaires et matrices.

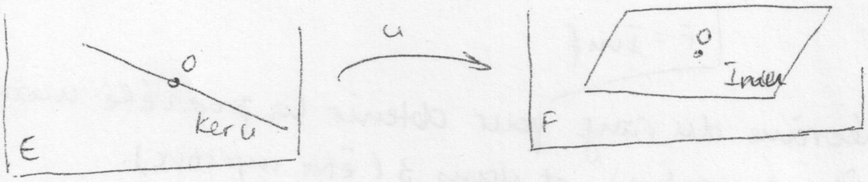
Soient E, F deux ev, $u : E \to F$ une application linéaire.

On définit $\operatorname{Ker} u = \{x \in E \mid u(x) = 0\}$ $(= u^{-1}(\{0\}))$

$\operatorname{Im} u = \text{"}\{u(x) \mid x \in E\}\text{"} = \{y \in F \mid \exists\, x \in E \text{ tq } y = u(x)\}$ $(= u(E))$

Fait : $\operatorname{Ker}(u)$ est un sev de E

$\operatorname{Im}(u)$ est un sev de F démo : rappel - exo ▨



Proposition : (**) Avec ces notations,

1) $\operatorname{Ker} u = \{0\} \Leftrightarrow u$ est injective

2) $\operatorname{Im} u = F \Leftrightarrow u$ est surjective démo : rappel - exo ▨

Proposition : Avec ces notations, u est bijective $\Leftrightarrow$ l'image d'au moins une base de E est une base de F
$\Leftrightarrow$ l'image de toute base de E est une base de F.

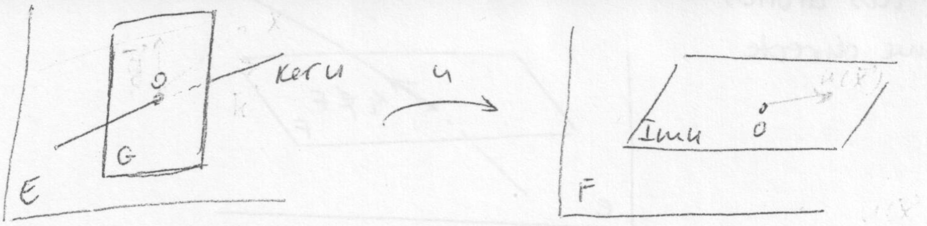
démo : rappel - exo ▨

Cas de la dimension finie

Théorème du rang : Soit $u : E \to F$ linéaire, E de dimension finie. Alors

$$\dim E = \dim(\operatorname{Ker} u) + \underbrace{\dim(\operatorname{Im} u)}_{=: \operatorname{rg}(u)}$$

Idée de preuve:



$A = B \oplus C$
$\Rightarrow \dim A = \dim B + \dim C$

Soit G un supplementaire de $\mathrm{Ker}\, u$ dans E. On a:

$$E = \mathrm{Ker}\, u \oplus G.$$

On aura donc (prop précédente) $\dim E = \dim \mathrm{Ker}\, u + \dim G$

Il reste à montrer $\dim G = \dim(\mathrm{Im}\, u)$

Cela vient du fait

$$u_{|G}^{|\mathrm{Im}\,u} : G \to \mathrm{Im}\, u \quad \text{est un isomorphisme (i.e. est bijective)}$$
$$x \mapsto u(x) \quad \text{de } G \text{ sur } \mathrm{Im}\, u.$$

démo : exercice ■

▷ Toute ev. de dimension n est isomorphe à $\mathbb{R}^n$ (i.e. même struct. algébrique)

Corollaire: Soit E, F des e.v. de dimension finie, $f : E \to F$ linéaire.
Si $\dim E = \dim F$, alors les propriétés suivantes sont équivalentes:

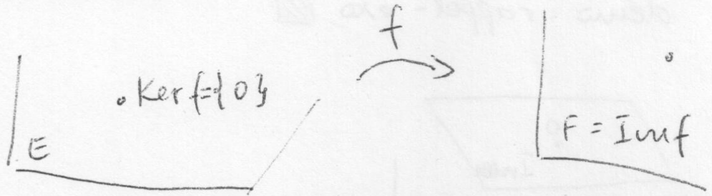
1) f est bijective (donc isomorphisme)

2a) f est injective (exercice - cours - au dernier)

2b) $\mathrm{Ker}\, f = \{0\}$

3a) f est surjective

3b) $\mathrm{Im}\, f = F$



Preuve: appliquer le théorème du rang pour obtenir la propriété manquante dans 2 (être surjective) et dans 3 (être injective).

Rappel : exercice ■

On utilisera régulièrement ce résultat dans le cas où $F = E$, i.e. $f : E \to E$ est un endomorphisme.

Exemple Soit $f : \mathbb{R}^3 \to \mathbb{R}^3$ (linéaire) tq. $\mathrm{mat}_{B_{can}} f = \begin{pmatrix} 1 & 2 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

i.e. tq $\left| \begin{array}{l} f((1,0,0)) = (1,0,0) \\ f((0,1,0)) = (2,-1,0) \\ f((0,0,1)) = (0,1,1) \end{array} \right.$

i.e. tq $\forall (x,y,z) \in \mathbb{R}^3 \quad f((x,y,z)) = (x+2y, -y+z, z)$

$$\overset{\|}{\left(f(x(1,0,0)+y(0,1,0)+z(0,0,1)\right)}$$

CL de $f(e_1), f(e_2), f(e_3)$, $\overset{\|}{\underline{\left\{ x\, f(1,0,0) + y\, f(0,1,0) + z \cdot f(0,0,1) \right\}}} = \mathrm{Im} f$

$\mathrm{Im} f = \mathrm{vect}\,((1,0,0),(2,-1,0),(0,1,1))$

Les coordonnées de ces vecteurs sont échelonnées, ils forment une base de $\mathbb{R}^3$. Cela montre que $\mathrm{Im} f = \mathbb{R}^3$ donc f est surjective.

Le corollaire conclut que f est bijective.

<u>Autre preuve:</u> $\mathrm{Ker} f = \left\{ (x,y,z) \in \mathbb{R}^3 \text{ tq } \begin{cases} x + 2y = 0 \\ -y + z = 0 \\ z = 0 \end{cases} \right\}$

Ce système déjà est un système d'équations échelonnée et de rang 3. Donc $0 = (0,0,0)$ est sa seule solution.

Donc $\mathrm{Ker} f = \{0\}$ et f est injective. Le corollaire conclut que f est bijective.

<u>Matrices d'applications linéaires</u>

Soit E un ev de dimension finie, $\mathcal{B} = (e_1, \dots, e_n)$ une base de E.

Si $x = x_1 e_1 + \dots + x_n e_n$, $x_1, \dots, x_n \in \mathbb{K}$.

On note $\mathrm{mat}_{\mathcal{B}}\, x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ la matrice colonne des coordonnées de x dans $\mathcal{B}$.

(notation non conventionnelle)

On notera $\mathcal{M}_{n,1}(\mathbb{K})$ ou $\mathbb{K}^{1,n}$ l'ensemble (espace vectoriel) des matrices colonnes à n lignes.

<u>Exemple</u>: $\mathrm{mat}_{\mathcal{B}_{can}}(1,-2,1) = \begin{pmatrix} 1 \\ -2 \\ +1 \end{pmatrix}$

base canonique de $\mathbb{R}^3$

Soit $f: E \to F$ une application linéaire,

$\mathcal{B}_E = (e_1, \dots, e_m)$ une base de E ($\dim E = m$)

$\mathcal{B}_F = (f_1, \dots, f_n)$ une base de F ($\dim F = n$)

Alors:

<u>Fait</u>: f est entièrement déterminée par la donnée de $f(e_1) \dots f(e_m)$

donc par les matrices colonnes $\mathrm{mat}_{\mathcal{B}_F} f(e_1), \dots, \mathrm{mat}_{\mathcal{B}_F} f(e_m)$.

Dans l'exemple précédent, f est entièrement déterminée par

$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, matrices coordonnées dans $\mathcal{B}_{can}$ de $f((1,0,0))$, $f((0,1,0))$, $f((0,0,1))$.

Définition : Avec ces notations, la matrice de $\mathbb{K}^{n,m}$ (à n lignes et m colonnes) dont les colonnes sont ces m vecteurs colonnes s'appelle la matrice de f dans les bases B_E, B_F. On la notera $\text{mat}_{B_F}^{B_E} f$ (notation non conventionnelle, usuellement $\text{mat}_{B_E, B_F} f$)

Exemple : Il y a une unique application linéaire de $\mathbb{R}^2$ dans $\mathbb{R}^3$ tq.

$$\text{mat}_{\text{can}_{\mathbb{R}^3}} f((1,0)) = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \qquad \text{mat}_{\text{can}_{\mathbb{R}^3}} f((0,1)) = \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}.$$

C'est l'application

$$f : \mathbb{R}^2 \to \mathbb{R}^3$$
$$(x,y) \to (-x+2y, x-y, y)$$

et sa matrice dans les bases canoniques $\text{can}_{\mathbb{R}^2}$ et $\text{can}_{\mathbb{R}^3}$ de $\mathbb{R}^2$ et $\mathbb{R}^3$ est

$$\text{mat}_{\text{can}_{\mathbb{R}^3}}^{\text{can}_{\mathbb{R}^2}} f = \begin{pmatrix} -1 & 2 \\ 1 & -1 \\ 0 & 1 \end{pmatrix} \quad (\in \mathbb{K}^{3,2})$$

On peut écrire (brouillon, mais si possible pas dans une copie...)

$$\text{mat}_{B_F}^{B_E} f = \begin{array}{c} \begin{array}{ccc} f(e_1) & & f(e_m) \end{array} \\ \begin{pmatrix} \big[\ \ \big] & \dots & \big[\ \ \big] \end{pmatrix} \\ \begin{array}{ccc} \uparrow & & \uparrow \\ \text{mat } f(e_1) & & \text{mat } f(e_m) \\ (f_1, \dots, f_n) & & (f_1, \dots, f_n) \end{array} \end{array} \begin{array}{c} f_1 \\ \vdots \\ f_n \end{array}$$

Les opérations sur les applications linéaires se traduisent par des opérations sur les matrices.

Propriétés : 1) Soit $f : E \to F$ B_E base de E, B_F base de F (finies)

On a : $\boxed{\forall x \in E \quad \text{mat}_{B_F} f(x) = \text{mat}_{B_F}^{B_E} f \cdot \text{mat}_{B_E} x}$

Exemple :

$$f : \mathbb{R}^2 \to \mathbb{R}^3$$
$$(x,y) \to (-x+y, x-2y, 2x+3y)$$

$f((1,1)) = (0,-1,5)$ s'écrit matriciellement $\begin{pmatrix} -1 & 1 \\ 1 & -2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 5 \end{pmatrix}$

$$\text{mat}_{\text{can}_{\mathbb{R}^3}}^{\text{can}_{\mathbb{R}^2}} f \cdot \text{mat}_{\text{can}_{\mathbb{R}^2}} (1,1) = \text{mat}_{\text{can}_{\mathbb{R}^3}} f(1,1)$$

Rappel sur la règle de produit matriciel :

$$\begin{array}{cc} & \begin{pmatrix} \boxed{1} \\ 1 \end{pmatrix} \\ \begin{pmatrix} \boxed{-1 \quad 1} \\ 1 \quad -2 \\ 2 \quad 3 \end{pmatrix} & \begin{pmatrix} \boxed{0} \\ -1 \\ 5 \end{pmatrix} \end{array}$$

Faire ce calcul mentalement

!! réserver au brouillon

2) Soient $f : E \to F$, $g : F \to G$ linéaires, B_E, B_F, B_G des bases de E, F, G.

On a $\boxed{\mathrm{mat}_{B_G}^{B_E}(g \circ f) = \mathrm{mat}_{B_G}^{B_F} g \cdot \mathrm{mat}_{B_F}^{B_E} f}$

Preuve de ces 2 propositions : exercice ▨

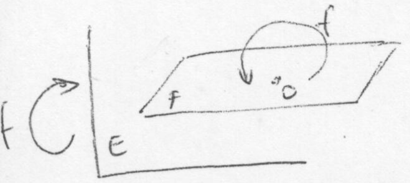
Cas d'un endomorphisme

Si $E = F$, on essaie en général de prendre $B_E = B_F$

Dans ce cas, on écrit $\mathrm{mat}_{B_E}^{B_E} f = \mathrm{mat}_{B_E} f$.

*** Sous-espace invariant par un endomorphisme

Définition : Soit $f : E \to E$ un endomorphisme. On dit qu'un sev F de E est stable ou invariant par f si $f(F) \subset F$.



Fait fondamental : Si F est stable par f, alors f induit par restriction un endomorphisme de F :
$$f_{|F} : F \to F \qquad \text{(vérifier la linéarité est trivial)}$$
$$x \mapsto f(x)$$

Objectif : Étant donnée $f : E \to E$, trouver des sev stables, si possible :
- de petites dimensions
- en somme directe
- de somme E.

** Des sev stables induisent des formes matricielles "simples".

Soit $f : E \to E$ endomorphisme, F un sev stable, G un supplémentaire de F dans E, B_F, B_G des bases de F, G.

Ainsi $B = B_F \vee B_G$ est une base de E. La matrice de f a alors la forme suivante.

$$\mathrm{mat}_{B_F \vee B_G} f = \begin{array}{c} \begin{array}{cc} f(B_F) & f(B_G) \end{array} \\ \left(\begin{array}{c|c} \mathrm{mat}_{B_F} f_{|F} & * \\ \hline 0 & * \end{array}\right) \end{array} \begin{array}{c} B_F \\ \vdots \\ B_G \end{array}$$

Preuve : exercice ▨

Cette matrice est dite triangulaire par bloc.

$f : E \to E$ endomorphisme, $F \subset E$ stable par f

$(f_{|F}^{|F} =)\ f_{|F} : F \to F$ endomorphisme

B_F base de F, B_G base d'un supplémentaire G de F dans E, $B = B_F \vee B_G$.

$$E = F \oplus G.$$

$$\text{mat}_B f = \begin{array}{c} \begin{array}{cc} \scriptstyle f(B_F)\ p & \scriptstyle q\ f(B_G) \end{array} \\ \left(\begin{array}{c|c} \text{mat}_{B_F} f_{|F} & * \\ \hline \underset{q\times p}{0} & * \end{array}\right) \end{array} \begin{array}{l} p\ \ B_F \\ q\ \ B_G \end{array}$$

triangulaire par bloc, avec $\begin{cases} p = \dim F \\ q = \dim G \\ p+q = \dim E \end{cases}$

$\text{mat}_B f \in M_q(\mathbb{K}) \qquad \text{mat}_{B_F} f_{|F} \in M_p(\mathbb{K})$

Soit $f : E \to E$ endomorphisme.
Soit $E = F_1 \oplus \dots \oplus F_k$ une décomposition de E en somme directe telle que $\forall i = 1 \dots k$, F_i est stable par f.
Soient $B_1, \dots, B_k$ des bases de $F_1, \dots, F_k$.
Soit $B = B_1 \vee \dots \vee B_k$. C'est une base de E (théorème).

On a

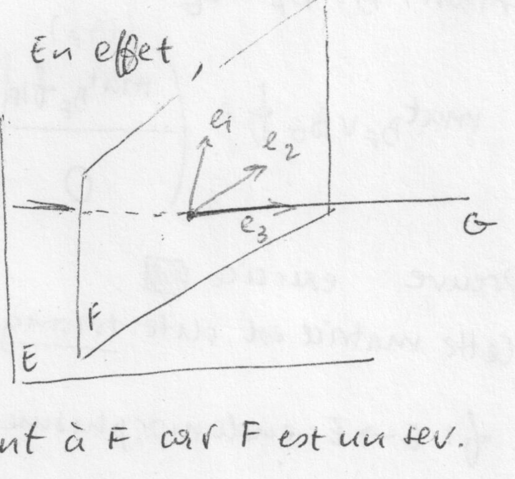
$$\text{mat}_B f = \begin{array}{c} \begin{array}{cccc} \scriptstyle f(B_1) & \scriptstyle f(B_2) & \dots & \scriptstyle f(B_k) \end{array} \\ \left(\begin{array}{c|c|c|c} \text{mat}_{B_1} f_{|F_1} & & 0 & \\ \hline & \text{mat}_{B_2} f_{|F_2} & & 0 \\ \hline 0 & & \ddots & \\ \hline & 0 & & \text{mat}_{B_k} f_{|F_k} \end{array}\right) \end{array} \begin{array}{l} B_1 \\ B_2 \\ \vdots \\ B_k \end{array} \Bigg) B$$

matrice diagonale par bloc.
Réciproquement, si un endomorphisme a une matrice diagonale par bloc dans une certaine base, on en déduit une décomposition de E en une somme directe de sev stables.

Exemple Soit $f : E \to E$, E $\mathbb{R}$-ev de dim 3, $B = (e_1, e_2, e_3)$ une base de E

tq. $$\text{mat}_B f = \begin{array}{c} \begin{array}{ccc} \scriptstyle f(e_1) & \scriptstyle f(e_2) & \scriptstyle f(e_3) \end{array} \\ \left(\begin{array}{cc|c} -1 & 0 & 0 \\ 1 & 1 & 0 \\ \hline 0 & 0 & 2 \end{array}\right) \end{array} \begin{array}{l} e_1 \\ e_2 \\ e_3 \end{array}$$

On voit que $F = \text{vect}(e_1, e_2)$ est stable par f. En effet,



$f(e_1) = -e_1 + e_2 \in F$

$f(e_2) = e_2 \in F$

Donc $\nearrow$ l'image de toute CL de e_1, e_2 est CL de e_1, e_2 donc dans F

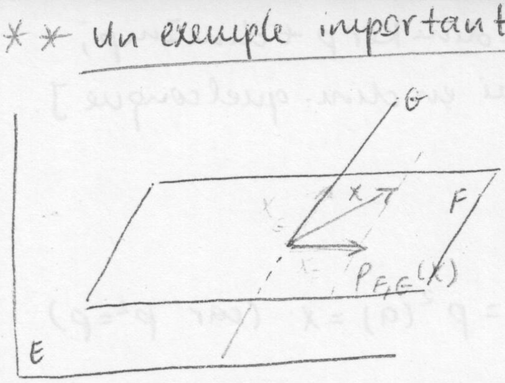
retour aux déf.

thm ou déf d'un sev $\searrow$ l'image de toute C.L. de e_1, e_2 est C.L. de vecteurs de F, donc appartient à F car F est un sev.

De même la droite $G = \text{vect}(e_3)$, supplémentaire de F dans E est stable par f.

$f(e_3) = 2e_3 \in G$.

** Un exemple important d'endomorphisme : les projections linéaires



Soit $E = F \oplus G$ une décomposition en somme directe d'un ev. E.

Tout vecteur x de E s'écrit de manière unique $x = x_F + x_G$ avec $x_F \in F$, $x_G \in G$ [définition de $\oplus$]

Définition : Avec ces notations, l'application $p_{F,G} : E \to E$, $x = x_F + x_G \mapsto x_F$ s'appelle la projection (linéaire) sur F parallèlement à / le longueur de G.

Fait : Cette application est linéaire

démo : exercice ▨ *** très important à faire.

Remarque : L'écriture $x = x_F + x_G$ donne $x = p_{F,G}(x) + p_{G,F}(x)$.

Donc $id = p_{F,G} + p_{G,F}$.

Propriété : Avec ces notations,

1) $\operatorname{Ker} p_{F,G} = G$

2) $\operatorname{Im} p_{F,G} = F$

3) $p_{F,G}^2 = p_{F,G}$ (on note $p^2 = p \circ p$)

Démo : 1) $\supset$: Soit $x \in G$. Alors $x = \underset{\in F}{0} + \underset{\in G}{x}$ donc $p_{F,G}(x) = 0$.

$\subset$: Soit $x \in \operatorname{Ker} p_{F,G}$. On écrit $x = \underset{\in F}{x_F} + \underset{\in G}{x_G}$. On a $p_{F,G}(x) = x_F = 0$.

Donc $x = x_G \in G$.

2) $\subset$: Soit $y \in \operatorname{Im} p_{F,G}$. Soit $x \in E$ tq. $y = p_{F,G}(x)$. On écrit $x = \underset{\in F}{x_F} + \underset{\in G}{x_G}$.

On a $y = x_F \in F$. [On peut aussi dire : "clair par déf. de $p_{F,G}$" : toutes les images par $p_{F,G}$ sont dans F]

$\supset$: Soit $x \in F$. Alors $x = p_{F,G}(x)$ car $x = \underset{\in F}{x} + \underset{\in G}{0}$

3) Soit $x = \underset{\in F}{x_F} + \underset{\in G}{x_G} \in E$. On a $p_{F,G}^2(x) = p_{F,G}(p_{F,G}(x)) = p_{F,G}(x_F) = x_F$

car $x_F = \underset{\in F}{x_F} + \underset{\in G}{0}$

La dernière propriété caractérise les projections linéaires.

Proposition : Soit $p : E \to E$ un endomorphisme tel que $p \circ p = p$.

Alors p est la projection linéaire sur $\operatorname{Im} p$ parallèlement à $\operatorname{Ker} p$.

Démonstration : Vérifions $E = \operatorname{Ker} p \oplus \operatorname{Im} p$.

[Rmq : si $\dim E$ est finie, on peut utiliser $\dim E = \dim \operatorname{Ker} p + \dim \operatorname{Im} p$, le théorème du rang. Mais la proposition est vrai en dim. quelconque].

*** $\operatorname{Ker} p \cap \operatorname{Im} p = \{0\}$: Soit $x \in \operatorname{Im} p \cap \operatorname{Ker} p$.

Soit $a \in E$ tq $x = p(a)$ [existe car $x \in \operatorname{Im} p$)

On a $p(x) = 0$ car $x \in \operatorname{Ker} p$ et $p(x) = p(p(a)) = p^2(a) = x$ (car $p^2 = p$)

On a montré $x = 0$.

$E = \operatorname{Im} p + \operatorname{Ker} p$: Soit $x \in E$

On a $x = \underbrace{p(x)}_{\in \operatorname{Im} p} + (x - p(x))$

Or $p(x - p(x)) \underset{\text{lin.}}{=} p(x) - p(p(x)) = p(x) - p^2(x) \overset{p^2=p}{=} p(x) - p(x) = 0$

Donc $x - p(x) \in \operatorname{Ker} p$. Cela conclut la preuve de la somme directe

Il reste à vérifier que p est la projection sur $\operatorname{Im} p$ parallèlement à $\operatorname{Ker} p$

Soit $x \in E$. On a $x = \underbrace{p(x)}_{\in \operatorname{Im} p} + \underbrace{(x - p(x))}_{\in \operatorname{Ker} p}$

Cela montre que $p(x) = p_{\operatorname{Im} p, \operatorname{Ker} p}(x)$ $\square$

Matrice d'une projection dans une base adaptée :

Soit p une projection linéaire de E sur F parallèlement à G.

Si B_F, B_G des bases de F, G, alors

$$\operatorname{mat}_{B_F \cup B_G} p = \begin{array}{cc} \begin{array}{cc} p(B_F) & p(B_G) \end{array} & \\ \left(\begin{array}{c|c} \begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix} & 0 \\ \hline 0 & \begin{matrix} 0 & & 0 \\ & \ddots & \\ 0 & & 0 \end{matrix} \end{array}\right) & \begin{array}{c} B_F \\ \\ B_G \end{array} \end{array}$$

matrice diagonale avec des 1 ou des 0 sur la diagonale

$p_{|F} : F \to F$, $x = x + 0 \mapsto x$ $\qquad p_{|F} = id_F$

Rmq : $id_E = p_{E,0}$ $\qquad 0 = p_{0,E}$ $\qquad (E = E \oplus \{0\})$

Rmq : La matrice précédente est diagonale par bloc, qui correspond à une décomposition de E en somme directe de sev. stables. On a en fait le résultat général suivant :

Proposition : Soit $f : E \to E$ un endomorphisme. Alors $\forall k \in \mathbb{N}$, $\operatorname{Ker} f^k$ et $\operatorname{Im} f$ sont stables par f.

Preuve pour $k = 1$: $\cdot$ $f(\operatorname{Ker} f) = \{0\} \subset \operatorname{Ker} f$

$\cdot$ $f(\operatorname{Im} f) \subset f(E) = \operatorname{Im} f$ $\square$

Cas général : exercice / TD ? / plus tard dans cours ?

Formules de changement de base

Soit E un ev de dimension finie, $u : E \to E$ un endomorphisme.

$B = (e_1, \dots, e_n)$, $B' = (e_1', \dots, e_n')$ deux bases de E.

Objectif : Trouver le lien entre $A = \mathrm{mat}_B f$ et $A' = \mathrm{mat}_{B'} f$.

On considère la composition suivante.

$$\begin{tikzcd} E \arrow[r, "id"] \arrow[rrr, bend right, "f = id \circ f \circ id"'] & E \arrow[r, "f"] & E \arrow[r, "id"] & E \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

$$\left[(E, B') \xrightarrow{id} (E, B) \xrightarrow{f} (E, B) \xrightarrow{id} (E, B') \right]$$

La formule de matrice de compositions des applications linéaires donne :

$$\underbrace{\mathrm{mat}^{B'}_{B'} f}_{A'} = \underbrace{\mathrm{mat}^{B}_{B'} id}_{P'} \cdot \underbrace{\mathrm{mat}^{B}_{B} f}_{A} \cdot \underbrace{\mathrm{mat}^{B'}_{B} id}_{P}$$

On a
$$P \cdot P' = \mathrm{mat}^{B'}_{B} id \cdot \mathrm{mat}^{B}_{B'} id = \mathrm{mat}^{B}_{B} (id \cdot id) = Id.$$

(Idem pour $P'P$)

Donc, $P' = P^{-1}$, ce qui donne

$\boxed{A' = P^{-1} A P}$ avec $P = \mathrm{mat}^{B'}_{B} id$

P s'appelle une matrice de changement de base.

$$\begin{array}{cccc} & e_1' = id(e_1') & \cdots & e_n' = id(e_n') & \\ P = & \left(\begin{array}{c} \vdots \\ \vdots \end{array} \right. & \cdots & \left. \begin{array}{c} \vdots \\ \vdots \end{array} \right) & \begin{array}{c} e_1 \\ \vdots \\ e_n \end{array} \end{array}$$

vecteur colonne de coord. de e' dans la base B — vecteur colonne des coord. de e'_n dans la base B.

P est en général donnée par le problème, et pour appliquer la formule, il faut (parfois) calculer P^{-1}.

Exemple : Soit $f : \mathbb{R}^2 \to \mathbb{R}^2$
$(x, y) \mapsto (2x + y, -x + y)$

Si on cherche la matrice de f dans la base $B' = ((1, -1), (-2, 1))$
$e_1' = (1, -1)$, $e_2' = (-2, 1)$

On peut appliquer la formule :

$$\text{mat}_{B'} f = \begin{pmatrix} 1 & -2 \\ -1 & 1 \end{pmatrix}^{-1} \underbrace{\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}}_{\overset{\shortparallel}{\text{mat}_{\text{can}} f}} \begin{pmatrix} \boxed{\begin{matrix} 1 \\ -1 \end{matrix}} & \boxed{\begin{matrix} -2 \\ 1 \end{matrix}} \end{pmatrix}$$

Remarque importante :

notons $A = \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}$ $C_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ $C_2 = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$ $P = (C_1\ C_2) = \begin{pmatrix} 1 & -2 \\ -1 & 1 \end{pmatrix}$

Le produit matriciel AP "a un sens" :

$$AP = \overset{\text{mat}_B f}{\overset{\shortparallel}{A}} (\overset{\text{mat}_B e'_i}{\overset{\shortparallel}{C_1}}\ C_2) = (\overset{\text{mat}_B f(e'_1)}{\overset{\shortparallel}{AC_1}}\ \ AC_2)$$

$$\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \boxed{\begin{matrix} 1 \\ -1 \end{matrix}} & \boxed{\begin{matrix} -2 \\ 1 \end{matrix}} \end{pmatrix} = \begin{pmatrix} \boxed{\begin{matrix} 1 \\ -2 \end{matrix}} & \boxed{\begin{matrix} -3 \\ 3 \end{matrix}} \end{pmatrix}$$

mat. de coord. de $f(e'_1)$ dans B.

$$\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \end{pmatrix}$$

En terme de coordonnées :

Soit $x \in E$, $\text{mat}_B x = X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ $\text{mat}_{B'} x = X' = \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$

Alors $\text{mat}_{B'} f(x) = A'X' = P^{-1}APX'$

$$PX' = \begin{array}{c} \begin{matrix} e'_1 & \cdots & e'_n \end{matrix} \\ \begin{pmatrix} C_1 & \cdots & C_n \end{pmatrix} \end{array}_{e_n}^{e_1} \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = \left(x'_1 C_1 + \cdots + x'_n C_n \right) = \overset{x'_1 e'_1 + \cdots + x'_n e'_n = x}{\begin{pmatrix} \\ \\ \end{pmatrix}}_{e_n}^{e_1} = X$$

$\boxed{PX' = X}$ ("P fait passer des coordonnées de la base B' aux coord. de la base B

$$A'X' = P^{-1}APX' = \overbrace{P^{-1}\underbrace{AX}_{\text{coord. de } f(x) \text{ dans } B}}^{\text{coord de } f(x) \text{ dans } B'}$$

(cela redémontre la formule de changement de bases)

Calcul de P^{-1} (si nécessaire)

On peut utiliser un algo de type Gauss

$$\begin{array}{ccc} P & \vdots & Id \\ & \downarrow & \\ Id & & P^{-1} \end{array}$$

(à faire au brouillon)

On peut aussi résoudre le système

$P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ $x_1, \ldots, x_n$ inconnus, $y_1, \ldots, y_n$ paramètres (par pivot de Gauss)

On a $P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \underset{\substack{\text{mult. par} \\ P^{-1} \text{ à gauche}}}{\iff} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P^{-1} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$

Exemple $P = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ $\forall x, y, y', x' \in \mathbb{R}$ $P\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$

$$\Leftrightarrow \begin{cases} 2x + y = x' & L_1 \\ x + y = y' & L_2 \end{cases}$$

$$\Leftrightarrow \begin{cases} x+y = y' & L_2 \\ -y' = x' - 2y' & L_1 - 2L_2 \end{cases} \Leftrightarrow \begin{cases} x = x' - y' \\ y = -x' + 2y' \end{cases}$$

$$\Leftrightarrow \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix} \text{ donc } P^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$$

Chapitre 3 : Déterminants

Rappel : On note $\boxed{M_n(\mathbb{K})}$ l'ensemble des matrices carrées $n \times n$ à coefficients dans $\mathbb{K}$ et $\boxed{GL_n(\mathbb{K})}$ l'ensemble des matrices carrées $n \times n$ à coefficients dans $\mathbb{K}$ inversibles. ("groupe linéaire")

$(M_n(\mathbb{K}), +, \times)$ est un anneau (non commutatif si $n \geq 2$)

$(M_n(\mathbb{K}), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel (de dimension n^2)

(pour $+, \cdot$ $M_2(\mathbb{R}) \simeq \mathbb{R}^{4,1} \simeq \mathbb{R}^4$

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

$(M_n(\mathbb{K}), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre (= anneau + ev + compatibilité entre les lois)

$(GL_n(\mathbb{K}), \times)$ est un groupe (non commutatif)
le groupe des inversibles de l'anneau $(M_n(\mathbb{K}), +, \times)$

On va définir une application

$$\det : M_n(\mathbb{K}) \to \mathbb{K}$$

qui va vérifier les propriétés suivantes

- det est une forme n-linéaire alternée en les lignes et les colonnes des matrices (voir plus loin)
- $\det M \neq 0$ ssi M est inversible, i.e. $M \in GL_n(\mathbb{K})$
- $\det GL_n(\mathbb{K}) \to \mathbb{K}^*$ est un morphisme de groupe.

On aura en fait un résultat plus général

$$\begin{cases} \det I_n = 1 \\ \forall M, N \in M_n(\mathbb{K}) \quad \det(MN) = \det M \cdot \det N \end{cases}$$

Soit $n \geq 1$. Si $A \in M_n(\mathbb{K})$, si $C_1, \dots, C_n$ sont les colonnes de A, $L_1, \dots, L_n$ sont les lignes de A, on notera

$$A = (C_1, \dots, C_n) = \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix}$$

Théorème : Il existe une unique application $f : M_n(\mathbb{K}) \to \mathbb{K}$ telle que :

1) $\forall i = 1 \dots n$, $\forall C_1, \dots, C_n$, $C_i' \in \mathbb{K}^{n,1}$ $\forall \alpha, \alpha' \in \mathbb{K}$

$$f((C_1, \dots, C_{i-1}\ \alpha C_i + \alpha' C_i'\ C_{i+1} \dots C_n)) =$$

$$\alpha f(C_1, \dots C_{i-1} C_i C_{i+1} \dots C_n))$$ "linéarité par rapport à la i^e-colonne"

$$+ \alpha' f((C_1 \dots C_{i-1} C_i' C_{i+1} \dots C_n))$$

On déduit que f est n-linéaire en colonnes.

2) $\forall C_1, \dots, C_n \in \mathbb{K}^n$, s'il existe $i \neq j \in \{1, \dots, n\}$ tels que $C_i = C_j$, alors

$$f((C_1, \dots, C_n)) = 0$$ On dit que f est alternée.

3) $f(I_n) = 1$

On note $f = \det$. Plus précisement tout application de $M_n(\mathbb{K})$ dans $\mathbb{K}^*$ vérifiant 1 et 2 (i.e. toute forme n-linéaire alternée du $M_n((\mathbb{K}))$ est multiple de $\det$).

Ce théorème est admis.

On peut calculer un déterminant suivant deux formules :

- une formule utilise des permutations. C'est cette formule qui permet de montrer la plupart des théorèmes dans ce chapitre. On va la développer en cours.
- une formule de récurrence, par "développement suivant la première colonne".

$f : G \to G'$

f morphisme $\Leftrightarrow \forall a, b \in G \quad f(ab) = f(a) f(b)$

$\det : M_n(\mathbb{K}) \to \mathbb{K}$

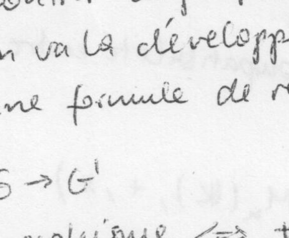
Permutations

Définition : On appelle permutation d'un ensemble X toute bijection de X dans X. L'ensemble de permutations de X est noté $S(X)$.

Notation : L'ensemble de permutations de $\{1, \dots, n\}$ est noté S_n.

$(S(X), \circ)$ est un groupe. Le neutre est id_X.

Une permutation $\sigma \in S_n$ est noté $\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$



Ex : $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\left| \begin{array}{l} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{array} \right.$

Définition : Si $i \neq j \in \{1, \dots, n\}$ on note $\tau_{i,j} = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix}$

$i \to j$
$j \to i$
$k \to k$ si $k \neq i, j$.

On l'appelle une transposition.

<u>Définition</u> : (cycle) Si $i_1, \dots, i_k \in \{1, \dots, n\}$ sont 2 à 2 distincts, on note

$$(i_1, \dots, i_k) : \left| \begin{array}{l} i_1 \to i_2 \\ i_2 \to i_3 \\ \vdots \\ i_{k-1} \to i_k \\ i_k \to i_1 \\ l \to l \text{ si } l \notin \{i_1, \dots, i_k\} \end{array} \right.$$

On l'appelle un k-cycle.

<u>Exemple</u> 1) Dans S_5, $(1\ 4\ 2)$

$$\left| \begin{array}{l} 1 \to 4 \\ 2 \to 1 \\ 3 \to 3 \\ 4 \to 2 \\ 5 \to 5 \end{array} \right.$$

2) Dans S_5, $\pi_{1,4} = (1\ 4)$

Toute transposition est un 2 cycle

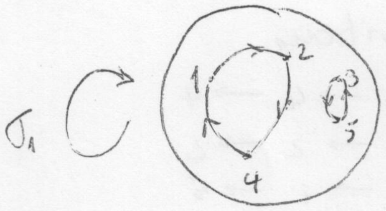
$$\begin{array}{l} 1 \to 4 \\ 4 \to 1 \\ 2 \to 2 \\ 3 \to 3 \\ 5 \to 5 \end{array}$$

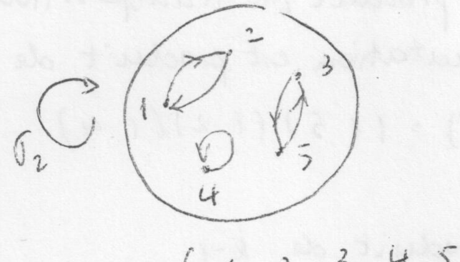
<u>Définition</u> : L'ensemble $\{i_1, \dots, i_k\}$ s'appelle le <u>support</u> du k-cycle $(i_1 \dots i_k)$.

Plus généralement, le support d'une permutation de X est le complementaire dans X de l'ensemble des éléments invariant par la permutation.

Si $\sigma \in S(X)$, $\operatorname{supp}(\sigma) := \{x \in X \mid \sigma(x) \neq x\}$

<u>Exemple</u> dans S_5





$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

$\operatorname{supp}(\sigma) = \{1, 2, 3, 4, 5\}$

$\operatorname{Fix}(\sigma) = \phi$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$\operatorname{supp}(\sigma) = \{1, 2, 3, 5\}$

$\operatorname{Fix}(\sigma) = \{4\}$

On a :

$$\sigma_1 = (1\ 2\ 4) \circ (3\ 5) = (3\ 5) \circ (1\ 2\ 4)$$

$$\sigma_2 = (1\ 2) \circ (3\ 5) = (3\ 5) \circ (1\ 2)$$

(vérification immediate à faire)

$$(1\ 2\ 4) \circ (3\ 5) \quad 1 \xrightarrow{(3\ 5)} 1 \xrightarrow{(1\ 2\ 4)} 2$$

$$2 \longrightarrow \quad \longrightarrow$$

$\vdots$

Fait : Toute permutation de S_n est la composée (le produit) de cycles de supports 2 à 2 disjoints.

idée de preuve : chercher les images successives des éléments de $\{1, \dots, n\}$ pour détecter les cycles. ▨

Fait : Des cycles de supports <u>disjoints</u> commutent dans S_n. (" $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$ ")

Exemple : Dans S_7 $(1\ 3\ 6\ 7) \circ (2\ 4\ 5) = (2\ 4\ 5) \circ (1\ 3\ 6\ 7)$

Preuve : exercice en bibliographie ▨

⚠ En général des permutations ne commutent pas.

Exemple : $(1\ 2) \circ (2\ 3)$:
$$1 \xrightarrow{(2\ 3)} 1 \xrightarrow{(1\ 2)} 2$$
$$2 \longrightarrow 3 \longrightarrow 3$$
$$3 \longrightarrow 2 \longrightarrow 1$$

$(1\ 2) \circ (2\ 3) = (1\ 2\ 3)$

$(2\ 3) \circ (1\ 2) = (1\ 3\ 2) \neq (1\ 2\ 3)$:
$$1 \xrightarrow{(1\ 2)} 2 \xrightarrow{(2\ 3)} 3$$
$$2 \longrightarrow 1 \longrightarrow 1$$
$$3 \longrightarrow 3 \longrightarrow 2$$

En effet, on a :

$$(1\ 2\ 3)^{-1} = ((1\ 2) \circ (2\ 3))^{-1} = (2\ 3)^{-1} \circ (1\ 2)^{-1} = (2\ 3) \circ (1\ 2) = (1\ 3\ 2)$$

car $\underbrace{\tau_{i,j} \circ \tau_{i,j}}_{\tau_{i,j}^2} = id$:
$i \to j \to i$
$j \to i \to j$
$k \to k \to k$ si $k \neq i, j$. donc $\tau_{i,j}^{-1} = \tau_{i,j}$.

Fait : Tout cycle est produit de transpositions

Corollaire : Toute permutation est produit de transpositions.

Exemple : $(1\ 4\ 2\ 5) = (1\ 5)(1\ 2)(1\ 4)$

$1 \longrightarrow 4 \longrightarrow 4 \longrightarrow 4$
$4 \longrightarrow 1 \longrightarrow 2 \longrightarrow 2$
$2 \longrightarrow 2 \longrightarrow 1 \longrightarrow 5$
$5 \longrightarrow 5 \longrightarrow 5 \longrightarrow 1$
$k \to k \to k \to k$ si $k \neq 1, 2, 4, 5$

tout k-cycle est produit de $k-1$ transpositions

Fait fondamental : Il existe un morphisme de groupe

$$\varepsilon : (S_n, \circ) \longrightarrow (\{+1, -1\}, \times)$$

qui vaut -1 sur toutes les transpositions de S_n.

C'est le seul morphisme "non trivial" i.e. différent de $1 : S_n \to \{-1, 1\}$, $\sigma \to 1$

On l'appelle la signature.

Admis

Exemple
$\varepsilon((1\ 5)) = -1$
$\varepsilon((1\ 2)) = -1$
$\varepsilon((1\ 4)) = -1$

donc $\varepsilon((1\ 4\ 2\ 5)) = \varepsilon((1\ 5)(1\ 2)(1\ 4))$
$= \varepsilon((1\ 5))\, \varepsilon((1\ 2))\, \varepsilon((1\ 4))$

ε morphisme

Donc $\varepsilon((1\ 4\ 2\ 5)) = (-1)^3 = -1$

La même preuve montre que tout k-cycle est de signature $(-1)^{k-1}$.

On dit que une permutation est <u>paire</u> si elle est de signature $+1$, <u>impaire</u> si elle est de signature -1.

<u>Exemple</u> : 1) $S_2 = \{ \underset{\begin{pmatrix}1&2\\1&2\end{pmatrix}}{id}, \underset{\begin{pmatrix}1&2\\2&1\end{pmatrix}}{(1,2)} \}$ $\qquad \varepsilon \left| \begin{array}{l} id \to 1 \\ (1\ 2) \to -1 \end{array} \right.$ $\qquad S_2 = \underbrace{\{id\}}_{\text{paire}} \cup \underbrace{\{(1,2)\}}_{\text{impaire}}$

(1,3) (1,2)

2) $S_3 = \{ \underset{+1}{id}, \underset{-1}{(1\ 2)}, \underset{-1}{(1\ 3)}, \underset{-1}{(2\ 3)}, \underset{+1}{(1\ 2\ 3)}, \underset{+1}{(1\ 3\ 2)} \}$ (ε)

$S_3 = \underbrace{\{id, (1\ 2\ 3), (1\ 3\ 2)\}}_{\text{paires}} \cup \underbrace{\{(1\ 2), (1\ 3), (2\ 3)\}}_{\text{impaires}}$

1) <u>Formule du déterminant par les permutations</u>

Soit $A = (a_{i,j}) \in M_n(\mathbb{K})$. On peut définir $\det A$ par

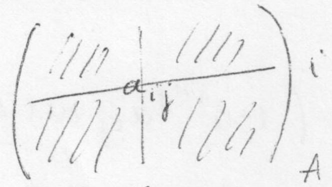
$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) \cdot a_{\sigma(1),1} \cdots a_{\sigma(n),n} \quad (n \text{ facteurs})$$

2) <u>Formule de développement du déterminant par rapport à la première colonne.</u>

On peut définir le déterminant par récurrence de la manière suivante :

- si $A = (a) \in M_1(\mathbb{K})$, $\det A = a$
- Soit $A = (a_{i,j})_{1 \le i,j \le n} \in M_n(\mathbb{K})$

On note $A_{i,j}$ la matrice de $M_{n-1}(\mathbb{K})$ obtenue en enlevant la i^e ligne et la j^e colonne de A.

$A =$ 

$$\det A = +a_{1,1} \det A_{i,j} - a_{2,1} \det A_{2,1} + \dots + (-1)^{1+n} a_{n,1} \det A_{n,1} = \sum_{i=1}^{n} (-1)^{i+1} a_{i,1} \det A$$

Exemples : On note $\det(\dots) = |\dots|$

1) $$\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} = (+1)\, a_{1,1} a_{2,2} + (-1)\, a_{2,1} a_{1,2} = a_{1,1} a_{2,2} - a_{2,1} a_{1,2}$$

$$\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix}_{1^{\text{ère}}\text{ col.}} = +a_{1,1} \cdot \det(a_{2,2}) - a_{2,1} \det(a_{1,2}) = a_{1,1} a_{2,2} - a_{2,1} a_{1,2}$$

2) $$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} = (+1) \underbrace{a_{1,1} a_{2,2} a_{3,3}}_{\sigma = id} + (+1) \underbrace{a_{2,1} a_{3,2} a_{1,3}}_{\sigma = (1\ 2\ 3)} + (+1) \underbrace{a_{3,1} a_{1,2} a_{2,3}}_{\sigma = (1\ 3\ 2)} + (-1) \underbrace{a_{2,1} a_{1,2} a_{3,3}}_{\sigma = (1\ 2)} + (-1) \underbrace{a_{3,1} a_{2,2} a_{1,3}}_{\sigma = (1\ 3)} + (-1) \underbrace{a_{1,1} a_{3,2} a_{2,3}}_{\sigma = (2\ 3)}$$

"règle de Sarrus"]

$$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} = a_{1,1}\begin{vmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} - a_{2,1}\begin{vmatrix} a_{1,2} & a_{1,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} + a_{3,1}\begin{vmatrix} a_{1,2} & a_{1,3} \\ a_{2,2} & a_{2,3} \end{vmatrix}$$

<u>Principe général</u> : On utilisera ces formules
- pour les preuves théoriques (surtout la première)
- si la matrice a beaucoup de coefficients nuls.

Pour se ramener à une telle matrice on utilisera le caractère multilinéaire alterné du déterminant et un algorithme de type algorithme de Gauss.

Exemples d'applications des propriétés du déterminant

1) $$\begin{vmatrix} 1 & 2 & 1 \\ 0 & -2 & 1 \\ 1 & 0 & 1 \end{vmatrix} \underset{\text{lin. \% 2e col}}{=} 2\begin{vmatrix} 1 & 1 & 1 \\ 0 & -1 & 1 \\ 1 & 0 & 1 \end{vmatrix} = 2\left(1\cdot\begin{vmatrix} -1 & 1 \\ 0 & 1 \end{vmatrix} + 1\begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix}\right) = 2(-1+2) = 2.$$

2) $$\begin{vmatrix} x+1 & 1 & -1 \\ -1 & 0 & 1 \\ 2x-1 & 1 & 1 \end{vmatrix} \underset{\text{lin \% 1ere col.}}{=} x\begin{vmatrix} 1 & 1 & -1 \\ 0 & 0 & 1 \\ 2 & 1 & 1 \end{vmatrix} + \begin{vmatrix} 1 & 1 & -1 \\ -1 & 0 & 1 \\ -1 & 1 & 1 \end{vmatrix}$$

3) $$\begin{vmatrix} 1 & 1 & -1 \\ -1 & 0 & 1 \\ -1 & 1 & 1 \end{vmatrix} \underset{\text{lin \% 1ere col}}{=} -\begin{vmatrix} -1 & 1 & -1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix} \underset{\text{alterné}}{=} 0$$

4) $$\begin{array}{c} \begin{vmatrix} 0 & 1 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix} \\ C_1 \; C_2 \; C_3 \end{array} = +0\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} - (-1)\begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} + (+1)\begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = -1+1=0$$

$$\det A = (-1)^{1+1} a_{11} \det A_{1,1} + \dots + (-1)^{n+1} a_{n1} \det A_{n,1} \qquad \left((-1)^{i+j} a_{ij} \det A_{ij}\right)$$

<u>Remarque</u> : Dans cette matrice, $C_1 - C_2 + C_3 = 0$, les colonnes sont liées. On verra que c'est un résultat général.

Le théorème principal (il existe une unique forme n-linéaire alternée valant 1 sur la matrice identité) se montre à l'aide de la formule par les permutations (théorème admis). De même l'équivalence des deux formules est admise.

<u>Remarque</u> : Si on itère le développement d'un déterminant suivant la première colonne, on trouve la formule par les permutations.

<u>Ex</u> $$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} = a_{1,1}\begin{vmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} - a_{2,1}\begin{vmatrix} a_{1,2} & a_{1,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} + a_{3,1}\begin{vmatrix} a_{1,2} & a_{1,3} \\ a_{2,2} & a_{2,3} \end{vmatrix}$$

$$= a_{1,1}(a_{2,2}a_{3,3} - a_{3,2}a_{2,3}) - a_{2,1}(\dots) + a_{3,1}(\dots)$$

donne la formule de Sarrus. (n! termes à la fin)

Propriétés du déterminant

1) $\det I_n = 1$ se retrouve à partir des deux modes de calcul :

Si on note $I_n = (a_{i,j})_{1 \le i,j \le n}$, avec $a_{i,j} = \begin{cases} 1 & \text{si } i=j \\ 0 & \text{sinon} \end{cases}$, les termes $a_{\sigma(1),1} \cdots a_{\sigma(n),n}$ de la formule des permutations sont tous nuls, sauf pour $\sigma(1)=1, \dots, \sigma(n)=n$.

(Si $\exists i$ tq $\sigma(i) \neq i$, alors $a_{\sigma(i),i} = 0$ donc $a_{\sigma(1),1} \cdots a_{\sigma(n),n} = 0$)

Donc $\det I_n = \varepsilon(id)\, a_{1,1} \cdots a_{n,n} = a_{1,1} \cdots a_{n,n}$. En développant $\det I_n$ par rapport à la première colonne on trouve

$$\det I_n = \begin{vmatrix} 1 & 0 \cdots 0 \\ 0 & \\ \vdots & I_{n-1} \\ 0 & \end{vmatrix} = +1 \det I_{n-1} - 0\,|*| + \dots + (-1)^{n+1}\, 0\, |*| = \det I_{n-1}$$

Comme $\det I_1 = \det(1) = 1$, par récurrence on a le résultat.

2) Les mêmes preuves donnent les résultats plus généraux. Le déterminant d'une matrice diagonale est égale au produit des termes diagonaux.

$$\begin{vmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{vmatrix} = a_1 \cdots a_n.$$

encore plus général :
Le déterminant d'une matrice triangulaire est égal au produit des termes diagonaux

$$\underset{\text{triangulaire supérieure}}{\begin{vmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{vmatrix}} = \underset{\text{triangulaire inférieure}}{\begin{vmatrix} a_1 & & 0 \\ & \ddots & \\ * & & a_n \end{vmatrix}} = a_1 \cdots a_n$$

Preuves : exercice ☒

Attention, pour les matrices triangulaires inférieures, il faut utiliser la formule des permutations. La formule de développement suivant la première colonne ne donne pas le résultat.

3) Le déterminant d'une matrice dont une colonne est nulle est égal à zéro.

$$\det(C_1 \cdots C_{i-1}\; 0\; C_{i+1} \cdots C_n) = 0 \qquad C_1, \dots, C_n \in \mathbb{K}^{n,1}.$$

Démonstration : Cela résulte de la linéarité du déterminant suivant n'importe quelle colonne.

$$\det(C_1 \cdots C_{i-1}\; \underset{\in\mathbb{R}}{0} \cdot \underset{\in\mathbb{K}^{n,1}}{0}\; C_{i+1} \cdots C_n) = \underset{\in\mathbb{R}}{0} \cdot \det(C_1 \cdots C_{i-1}\; 0 \cdots C_n) = 0$$

$$\underset{0\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}\cdots}{\parallel}$$

Ex
$$\begin{vmatrix} 1 & 0 & 2 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{vmatrix} = \det\left(\begin{pmatrix}1\\-1\\0\end{pmatrix}\begin{pmatrix}0\\0\\0\end{pmatrix}\begin{pmatrix}2\\0\\-1\end{pmatrix}\right) = \det\left(\begin{pmatrix}1\\-1\\0\end{pmatrix} 0 \cdot \begin{pmatrix}0\\0\\0\end{pmatrix}\begin{pmatrix}2\\0\\-1\end{pmatrix}\right) = 0 \det\left(\begin{pmatrix}1\\-1\\0\end{pmatrix}\begin{pmatrix}0\\0\\0\end{pmatrix}\begin{pmatrix}2\\0\\-1\end{pmatrix}\right) = 0.$$

4) Si on échange deux colonnes d'une matrice, on multiplie le déterminant de la matrice par -1.

$$\det(C_1 \dots C_i \dots C_j \dots C_n) = -\det(C_1 \dots C_j \dots C_i \dots C_n)$$

Démonstration : on a

$$0 \underset{alt}{=} \det(C_1 \cdots C_{i-1}\ \underline{C_i + C_j}\ C_{i+1} \cdots C_{j-1}\ \underline{C_i + C_j}\ C_{j+1} \cdots C_n)$$

$$= \det(C_1 \cdots C_i \cdots C_i + C_j \cdots C_n) + \det(C_1 \cdots C_j \cdots C_i + C_j \cdots C_n)$$

lin % à la $i^{ème}$ col.

$$= \det(C_1 \cdots C_i \cdots C_i \cdots C_n) + \det(C_1 \cdots C_i \cdots C_j \cdots C_n) +$$

lin % à la $j^{ème}$ col.

$$\det(C_1 \cdots C_j \cdots C_i \cdots C_n) + \det(C_1 \cdots C_j \cdots C_j \cdots C_n)$$

$$\underset{alt.}{=} \det(C_1 \cdots C_i \cdots C_j \cdots C_n) + \det(C_1 \cdots C_j \cdots C_i \cdots C_n).$$ Cela montre le résultat.

5) Si on permute les colonnes d'une matrice, on multiplie son déterminant par la signature de la permutation.

Si $\sigma \in S_n$, $\det(C_{\sigma(1)} \cdots C_{\sigma(n)}) = \varepsilon(\sigma) \det(C_1 \cdots C_n)$

Le résultat précédent est le cas particulier où σ est la transposition $\tau_{i,j}$.

Idée de preuve : écrire la permutation σ comme produit de transpositions, faire une suite d'échanges de colonnes 2 à 2 (correspondant aux transpositions), appliquer le résultat précédent, et vérifier que le signe qui apparaît à la fin de cette suite d'échanges est la signature de la permutation. ▨ récurrence sur le nombre de permutations.

Ex.

$$\begin{array}{c} \begin{vmatrix} 1 & 2 & 5 \\ 2 & 3 & 6 \\ 3 & 4 & 7 \end{vmatrix} \\ C_1\ C_2\ C_3 \end{array} = \begin{array}{c} \begin{vmatrix} 2 & 5 & 1 \\ 3 & 6 & 2 \\ 4 & 7 & 3 \end{vmatrix} \\ C_2\ C_3\ C_1 \end{array} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3) \qquad \varepsilon(\sigma) = 1.$$

$$\begin{array}{c} C_1\ C_2\ C_3\ C_4 \\ \begin{vmatrix} 1 & 5 & 9 & 13 \\ 2 & 6 & 10 & 14 \\ 3 & 7 & 11 & 15 \\ 4 & 8 & 12 & 16 \end{vmatrix} \end{array} = - \begin{array}{c} C_2\ C_3\ C_4\ C_1 \\ \begin{vmatrix} 5 & 9 & 13 & 1 \\ 6 & 10 & 14 & 2 \\ 7 & 11 & 15 & 3 \\ 8 & 12 & 16 & 4 \end{vmatrix} \end{array} \qquad \sigma = (1\ 2\ 3\ 4) \qquad \varepsilon(\sigma) = -1.$$

6) On ne change pas le déterminant d'une matrice si on additionne à la première colonne une C.L. des autres colonnes

$$\forall \lambda_2 \ldots \lambda_n \in \mathbb{K} \quad \det(C_1 + \lambda_2 C_2 + \ldots + \lambda_n C_n\ \ C_2 \ldots C_n) = \det(C_1\ C_2 \ldots C_n)$$

Démonstration : avec ces notations,

$$\det(C_1 + \lambda_2 C_2 + \ldots + \lambda_n C_n\ \ C_2 \ldots C_n) \underset{\text{lin \% à } 1^{ère} \text{ col}}{=} \det(C_1\ C_2 \cdots C_n) + \lambda_2 \underbrace{\det(C_2\ C_2 \ldots C_n)}_{=0} + \ldots + \lambda_n \underbrace{\det(C_n\ C_2 \ldots C_n)}_{=0} =$$

$$\underset{(alt.)}{=} \det(C_1\ C_2 \ldots C_n)$$

□

La même preuve se généralise à n'importe quelle autre colonne.

| On ne change pas le déterminant d'une matrice si on ajoute à une colonne une C.L. des autres colonnes.

Cela permet un algorithme de Gauss "par colonnes".

$$\begin{array}{c} C_1\ C_2\ C_3 \\ \begin{vmatrix} 1 & 2 & -1 \\ -1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix} \end{array} = \begin{array}{c} C_1\ \ C_2 - 2C_1\ \ C_3 \\ \begin{vmatrix} 1 & 0 & -1 \\ -1 & 2 & 1 \\ 0 & 1 & 1 \end{vmatrix} \end{array} = \begin{array}{c} C_1\ \ C_2'\ \ C_3 + C_1 \\ \begin{vmatrix} 1 & 0 & 0 \\ -1 & 2 & 0 \\ 0 & 1 & 1 \end{vmatrix} \end{array} = 1 \cdot 2 \cdot 1 = 2$$

matrice triangulaire.

Corollaire : Le déterminant d'une matrice non inversible est nul.

Preuve : $(C_1, \dots, C_n)$ est non inversible <u>ssi</u> elle est de rang $< n$

<u>ssi</u> une colonne est C.L. des autres colonnes.

Pour se ramener à une telle matrice on utilisera le caractère multi-linéaire alterné du déterminant et un algorithme de type algorithme de Gauss.

Le déterminant de $(C_1 \dots C_n)$ ne change pas si on retranche à cette colonne la C.L. correspondante des autres colonnes, ce qui fait apparaître une colonne nulle. □

7) **Théorème** : Soit $A, B \in M_n(\mathbb{K})$. On a $\det(A \cdot B) = \det A \cdot \det B$

Démo : abstraite, admise □ - biblio

Corollaire : Le déterminant d'une matrice est nul <u>ssi</u> la matrice est non inversible

Preuve : Si A est non inversible, $\det A = 0$ par le corollaire précédent.

Si A est inversible, $1 = \det I_n = \det(A \cdot A^{-1}) = \det A \cdot \det(A^{-1})$

Donc $\det A \neq 0$. □

Cela donne aussi

Corollaire Si A est inversible, $\det A^{-1} = \dfrac{1}{\det A}$

8) **Rappel** : Si $A = (a_{i,j}) \in M_n(\mathbb{K})$, la transposée de A est ${}^tA = (b_{i,j})_{1 \le i,j \le n}$

avec $\forall i,j \quad b_{i,j} = a_{j,i}$

Autrement dit, les colonnes de ${}^tA$ sont les transposées des lignes de A.

$${}^t\begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix} = \left({}^tL_1 \dots {}^tL_n \right)$$

7. **Théorème** : Soit $A \in M_n(\mathbb{K})$ $\quad \det {}^tA = \det A$.

La preuve s'obtient à l'aide de la formule des permutations, admise.

Conséquence : On peut faire les mêmes opérations sur les lignes que celles sur les colonnes.

En particulier, on a les formules suivantes

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij} \qquad \text{pour tout } j \in \{1 \dots n\}$$

$$= \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A_{i,j} \qquad \text{pour tout } i \in \{1 \dots n\}$$

La première formule est le développement du déterminant suivant la j^e colonne, la seconde est le développement suivant la i^e ligne.

Exemple

$$\begin{vmatrix} 1 & 2 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 2 \end{vmatrix} \underset{\substack{\text{dev. \% } \\ 2^e \text{ ligne}}}{=} -0 \begin{vmatrix} 2 & -1 \\ 0 & 2 \end{vmatrix} + 1 \begin{vmatrix} 1 & -1 \\ -1 & 2 \end{vmatrix} + 0 \begin{vmatrix} 1 & 2 \\ -1 & 0 \end{vmatrix} = 1$$

$(-1)^{2+3}$

$$\underset{\substack{\text{dev. \% } 3^e \\ \text{colonne} \\ (1^{ère} \text{ formule pour } j=3)}}{=} (-1) \begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix} - 0 \begin{vmatrix} 1 & 2 \\ -1 & 0 \end{vmatrix} + 2 \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} = -1 + 2 = 1$$

Remarque : $(-1)^{i+j}\det A_{ij}$ est appelé le cofacteur de a_{ij} dans la matrice A.

Applications du déterminant

1) Mineurs et rang d'une matrice

Déf^n : Soit $A \in \mathbb{K}^{n,m}$ $(= M_{n,m}(\mathbb{K}))$. On appelle matrice extraite de A toute matrice obtenue en enlevant des lignes et/ou des colonnes de A. Plus précisement, si $I, J \subset \{1, \dots, n\}$, on note $A_{I,J}$ la matrice extraite de A qui conserve les lignes indexés dans I et les colonnes indexés dans J (après renormalisation des indices dans $\{1, \dots, \operatorname{card} I\}$, $\{1, \dots, \operatorname{card} J\}$)

Exemple :
$$A = \begin{pmatrix} 1 & -1 & 0 \\ 2 & 1 & -1 \\ -1 & 0 & 2 \\ 3 & -1 & 1 \end{pmatrix} \in \mathbb{R}^{4,3} \quad \text{si } I = \{2,4\} \quad J = \{2,3\} : A_{I,J} = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

Remarque : si $A \in M_n(\mathbb{K})$, $i,j \in \{1, \dots, n\}$ alors $A_{ij} = A_{\{1,\dots,n\}\setminus\{i\}, \{1,\dots,n\}\setminus\{j\}}$ c'est une matrice extraite de A.

Définition : Soit $A \in \mathbb{K}^{n,m}$. On appelle mineur de A tout déterminant d'une matrice carrée extraite de A.

Dans l'exemple précédent, $\begin{vmatrix} 1 & -1 \\ -1 & 1 \end{vmatrix} = 0$ est un mineur de A.

On appelle taille d'un mineur la taille (nombre de lignes ou de colonnes) de la matrice extraite associée.

Théorème : le rang d'une matrice est égal à la plus grande taille d'un mineur non nul. Autrement dit si $A \in \mathbb{K}^{n,m}$, on a $\operatorname{rg}(A) = r$ ssi

- il existe un mineur de A de taille r non nul
- tous les mineurs de A de taille $\geq r+1$ sont nuls.

La preuve montre le résultat suivant plus précis.

Théorème : si $A \in \mathbb{K}^{n,m}$ alors $\operatorname{rg}(A) = r$ ssi
- il existe un mineur de A de taille r non nul
- tous les mineurs de A de taille $r+1$ sont nuls.

Exemple : $A = \begin{pmatrix} 1 & -1 & 2 \\ -1 & 0 & -1 \\ 0 & 1 & -1 \\ 2 & -1 & 3 \end{pmatrix}$

On vérifie que:
- le mineur $\begin{vmatrix} -1 & 0 \\ 0 & 1 \end{vmatrix} = -1$ est non nul donc $\operatorname{rg} A \geq 2$.
- tous les mineurs $\begin{vmatrix} 1 & -1 & 2 \\ -1 & 0 & -1 \\ 0 & 1 & -1 \end{vmatrix}$, $\begin{vmatrix} 1 & -1 & 2 \\ -1 & 0 & -1 \\ 2 & 1 & 3 \end{vmatrix}$, $\begin{vmatrix} 1 & -1 & 2 \\ 0 & 1 & -1 \\ 2 & -1 & 3 \end{vmatrix}$, et $\begin{vmatrix} -1 & 0 & -1 \\ 0 & 1 & -1 \\ 2 & -1 & 3 \end{vmatrix}$ de taille 3 sont nuls.

Donc $\operatorname{rg} A = 2$.

Remarques 1) Si on note $A = (C_1\ C_2\ C_3)$, on a $C_1 - C_2 - C_3 = 0$.
Cette rélation est aussi valable pour les colonnes des 4 mineurs de taille 3 de A. Cela explique que ces 4 mineurs sont nuls. Cela explique aussi que $\operatorname{rg}(A) < 3$.

2) Ce résultat a des applications théoriques. Il peut être utile pour des matrices de petites tailles (≤ 4) mais il est trop couteux en calculs pour des matrices de grande taille. La méthode la plus pratique pour calculer le rang est l'algo de Gauss.

La preuve du théorème est admise. Elle repose sur l'utilisation de deux lemme

Lemme 1 : Soit $A \in \mathbb{K}^{n,m}$ avec $n \geq m$. S'il existe un mineur de A de taille m non nul, alors $rg(A) = m$.

idée de preuve : On se ramène au cas où le mineur de taille m non nul est formé des m premières lignes.

$$A = \underbrace{\begin{pmatrix} \boxed{A_{\{1..m\}\{1..m\}}} \\ \\ \end{pmatrix}}_{m} {\scriptstyle n}$$ i.e correspondant à $B = A_{\{1,\dots,m\}\{1,\dots,m\}}$ la matrice extraite

Comme $\det B \neq 0$, les colonnes de B sont indépendantes. Donc les colonnes de A sont indépendantes (argument ① de l'exemple précédent). Donc $rg A = m$. □

Lemme 2 (majoration du rang) : Soit $A \in \mathbb{K}^{n,m+1}$, $n \geq m+1$. S'il existe un mineur de A de taille m non nul et si tous les mineurs de A de taille $m+1$ sont nuls, alors $rg(A) = m$.

idée de preuve : On se ramène au cas où la matrice extraite $B = A_{\{1..m\},\{1..m\}}$ est de déterminant non nul.

$$A = \begin{array}{c} \begin{matrix} C_1 \dots C_m & C_{m+1} \end{matrix} \\ \underbrace{\begin{pmatrix} \boxed{B} & \boxed{} \\ \boxed{} & \boxed{} \end{pmatrix}}_{m+1} {\scriptstyle n} \end{array}$$

L'annulation des mineurs de taille $m+1$ et le fait que $\det_B \neq 0$ montre que la matrice colonne formée des m premières lignes de C_{m+1}, et d'une ligne i, $i \geq m+1$, de C_{m+1} (en noir sur la figure) est C.L. des matrices colonnes correspondantes sur $C_1 \dots C_m$. On montre que les C.L. obtenues entre ces colonnes ne dépendent pas du choix de la ligne $i \geq m+1$. On en déduit que C_{m+1} est C.L. de $C_1 \dots C_m$. Comme $C_1 \dots C_m$ sont indépendantes par le lemme 1, on en déduit que $vect(C_1 \dots C_{m+1}) = vect(C_1 \dots C_m)$ est de dimension m. □

Corollaire : Si $A = (C_1 \dots C_m) = (L_1 \dots L_n) \in \mathbb{K}^{n,m}$ alors

$$rg(A) \underset{déf}{=} \dim vect(C_1 \dots C_m) = \dim vect(L_1 \dots L_n)$$

démo : A et ${}^tA$ ont les mêmes mineurs.

Exemple :
$$rg\begin{pmatrix} 1 & -1 \\ -2 & 2 \\ -1 & 1 \\ 1 & 0 \end{pmatrix} = rg\begin{pmatrix} 1 & -2 & -1 & 1 \\ -1 & 2 & 1 & 0 \end{pmatrix} = 2$$

$$\dim vect\left(\begin{pmatrix} 1 \\ -2 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 1 \\ 0 \end{pmatrix}\right)$$

$$\dim vect\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -2 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \dim vect\left((1,-1), (-2,2), (-1,1), (1,0)\right)$$

$$\begin{vmatrix} -1 & 1 \\ 1 & 0 \end{vmatrix} = -1 \neq 0.$$

2) ~~Éléments~~ Comatrice et inverse d'une matrice (inversible)

Soit $A \in M_n(\mathbb{K})$, $A = (a_{i,j})_{1 \leq i,j \leq n}$. On note $comA$ la matrice de $M_n(\mathbb{K})$ dont les coefficients sont les cofacteurs de A, précisément

on calcule la comatrice que pour des matrices carrées

$$comA = (b_{i,j}) \text{ avec } b_{i,j} = (-1)^{i+j} \det A_{i,j}.$$ On l'appelle commatrice de A.

Exemple $\quad \text{com}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Proposition : Avec ces notations, on a $\quad A \cdot {}^t\text{com}A = \begin{pmatrix} \det A & & 0 \\ & \ddots & \\ 0 & & \det A \end{pmatrix} = \det A \cdot I_n$

idée de preuve : On effectue le produit matriciel $A \cdot {}^t\text{com}A$ (resp ${}^t\text{com}A \cdot A$).
On trouve

- sur la diagonale des coefficients égaux au développement de $\det A$ suivant une colonne (resp. une ligne), donc égaux à $\det A$.
- hors de la diagonale des coefficients égaux au développement du déterminant d'une matrice ayant deux fois la même colonne (resp. deux fois la même ligne), donc égaux à 0. □

Corollaire : Si $A \in M_n(\mathbb{K})$ est inversible, alors $A^{-1} = \dfrac{1}{\det A} \, {}^t\text{com}A \quad (\det A \neq 0)$.

Exemple : Si $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ est inversible, $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} = \dfrac{1}{ad-bc} \, {}^t\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \dfrac{1}{ad-bc}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$

(vérification facile !)

Remarque : En pratique, numériquement pour des matrices de taille ≥ 3, on n'utilise pas cette formule pour calculer l'inverse d'une matrice. (mais un algo de type Gauss).

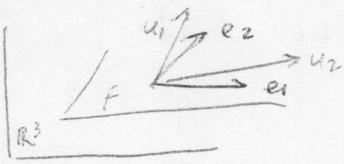
3) Déterminant d'une famille de vecteurs dans une base.

Soit E un ev de dimension n. Soit B une base de E. Soient $(u_1, \dots, u_n)$ une famille de n vecteurs de E. On appelle déterminant de cette famille de vecteurs dans la base B, noté $\det_B(u_1 \dots u_n)$, le déterminant de la matrice

$$\text{mat}_B(u_1 \dots u_n) = (\text{mat}_B u_1 \; \dots \; \text{mat}_B u_n).$$

Exemple : Dans le plan $F = \{(x,y,z) \in \mathbb{R}^3 \mid x+y-z=0\}$ muni de la base

$$B = (\underset{e_1}{(1,-1,0)}, \underset{e_2}{(1,0,1)}), \quad \det_B(\underset{u_1}{(1,1,2)}, \underset{u_2}{(1,-1,0)}) = \begin{array}{c|cc|c} & u_1 & u_2 & \\ & -1 & 1 & e_1 \\ & 2 & 0 & e_2 \end{array} = -2$$



Attention : Ce déterminant ne dépend pas seulement de la famille $(u_1, \dots, u_n)$ il dépend aussi de B.

E base B, $\dim E = n$, $\quad \mathcal{F} = (v_1, \dots, v_n)$ famille de vecteurs de E.

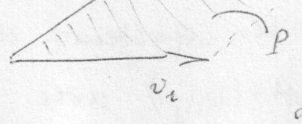
$$\det_B \mathcal{F} = \det_B(v_1 \dots v_n) = \det \text{mat}_B \mathcal{F} = \det(\text{mat}_B v_1 \dots \text{mat}_B v_n)$$

Exemple $\quad \det_{can}((1,1,1),(-1,0,1),(2,1,0)) = \begin{vmatrix} 1 & -1 & 2 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix}$

⚠ Ce nombre ne dépend pas seulement de $\mathcal{F}$, il dépend aussi de B.

idée : la valeur absolue du déterminant d'une famille de vecteurs $(v_1, \dots, v_n)$ correspond au volume du parallélépipède.

$$P = \left\{ \sum_{i=1}^{n} \lambda_i v_i \;,\; 0 \leq \lambda_i \leq 1 \text{ pour tout } i \right\}$$



la base B fixe l'unité de volume

$\det_B B = \det I_n = 1.$

Fait: Si B, B' sont deux bases de E telles que $\det_B B' = 1$ alors pour toute famille de vecteurs $\mathcal{F}$ de E de cardinal $\dim E$ on a $\det_B \mathcal{F} = \det_{B'} \mathcal{F}$

Démo: $\boxed{\mathrm{mat}_{B'} \mathcal{F} = \mathrm{mat}_{B'}^{B}\, \mathrm{id} \cdot \mathrm{mat}_B \mathcal{F}}$ (formule de changement de base pour les coordonnées

et $\boxed{\det(A \cdot B) = \det A \cdot \det B}$ □

Théorème: Soit E de dimension n, B une base de E. Soit $\mathcal{F} = (v_1, \dots, v_n)$ une famille de vecteurs de E. On a

$$(v_1 \dots v_n) \text{ est libre} \Leftrightarrow \det_B(v_1 \dots v_n) \neq 0.$$

démo: Cela résulte du fait que $(v_1 \dots v_n)$ est libre dans E ssi $(\mathrm{mat}_B v_1 \dots \mathrm{mat}_B v_n)$ est libre dans l'espace des vecteurs colonnes $\mathbb{K}^{n,1}$.

En effet, $\varphi : E \to \mathbb{K}^{n,1}$, $(v_1 \dots v_n) \mapsto (\mathrm{mat}_B v_1 \dots \mathrm{mat}_B v_n)$ est un isomorphisme d'espaces vectoriels.

Montrons pourquoi c'est un isomorphisme.

- $\dim E = \dim \mathbb{K}^{n,1} = n$
- φ est linéaire (vérification immédiate)
- φ est injective: le seul vecteur de coordonnées nulles est le vecteur nul □.

4) Déterminant d'un endomorphisme

Le cas d'un endomorphisme est différent, on va définir le déterminant d'un endomorphisme (qui sera indépendant du choix d'une base).

Soit E de dimension n, B, B' deux bases de E.

Soit f un endomorphisme de E. Alors

$$\mathrm{mat}_{B'} f = P^{-1}\, \mathrm{mat}_B f \cdot P \quad \text{où} \quad P = \mathrm{mat}_B^{B'}\, \mathrm{id}$$

Donc $\det(\mathrm{mat}_{B'} f) = \det P^{-1} \cdot \det(\mathrm{mat}_B f) \cdot \det P$

Or $\det P^{-1} = \dfrac{1}{\det P}$ donc $\det(\mathrm{mat}_{B'} f) = \det(\mathrm{mat}_B f)$

On a montré:

Définition/Théorème: Avec ces notations, $\det \mathrm{mat}_B f$ ne dépend pas du choix de B.

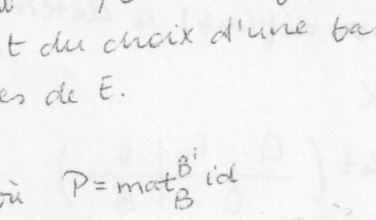
On l'appelle déterminant de l'endomorphisme f, noté $\det f$.

idée: $\det f$ est le "coefficient" multiplicateur du volume lorsqu'on applique f.

Précisément:

Si $\mathcal{F} = (v_1 \dots v_n)$ est une famille de vecteurs de E, on a:

$$\det_B \underbrace{f(\mathcal{F})}_{=\,(f(v_1) \dots f(v_n))} = \det f \cdot \det_B \mathcal{F}$$



Remarque: Le signe d'un déterminant correspond à une "orientation" de l'espace vectoriel.

Propriétés du déterminant (+ ce qu'on a vu)

9) On a montré qu'on ne modifie pas un déterminant si on ajoute à une colonne une c.L des autres colonnes (resp. lignes). En faisant une suite de tel opérations, on peut montrer:

fait : 1) On ne change pas le déterminant d'une matrice si on ajoute aux colonnes une c.l. des colonnes suivantes.

2) On ne change pas le déterminant d'une matrice si on ajoute aux colonnes une c.l. des colonnes précédentes.

3) On ne change pas le déterminant d'une matrice si on ajoute aux colonnes autre que C_i une multiple de C_i.

Exemples :

1. $\det(\underline{C_1} + C_2 + C_3, \underline{C_2} + C_3, \underline{C_3}) = \det(C_1, C_2, C_3)$
2. $\det(\underline{C_1}, \underline{C_2} - C_1, \underline{C_3} + 2C_1 - C_2) = \det(C_1, C_2, C_3)$
3. $\det(\underline{C_1} + C_2, \underline{C_2}, \underline{C_3} - C_2) = \det(C_1, C_2, C_3)$ démo : exercice ▨

théorème : 10) Déterminant d'une matrice triangulaire par bloc (avec blocs diagonaux carrés).

Soit $M = \begin{array}{cc} & \begin{array}{cc} k & l \end{array} \\ & \left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array}\right) \end{array}\begin{array}{c} k \\ l \end{array} \in M_n(\mathbb{K})$ avec $A \in M_k(\mathbb{K})$, $B \in M_l(\mathbb{K})$, $C \in \mathbb{K}^{k,l}$
(0 la matrice nulle de $\mathbb{K}^{l,k}$)

avec $k + l = n$.

On a $\det M = \det A \cdot \det B$.

idée de preuve : On peut revenir à la formule des permutations, constater que beaucoup de termes sont nuls (ceux correspondant à des permutations $\sigma \in S_n$ t.q. $\exists i \in \{1 \ldots k\}$ tq $\sigma(i) \in \{k+1, \ldots, k+l\}$) puis factoriser. On peut aussi utiliser le théorème qui caractérise (ou définit) le déterminant. On considère

$$\phi : \underset{M_k(\mathbb{K})}{(\mathbb{K}^{k,1})^k} \longrightarrow \mathbb{K}$$
$$(C_1 \ldots C_k) \to \det\left(\begin{array}{c|c} C_1 \ldots C_k & C \\ \hline 0 & B \end{array}\right)$$

(on voit $\det M$ comme une application en les colonnes de A)

On constate que c'est une forme k-linéaire alternée. On a vu (théorème-définition du déterminant) qu'alors $\exists \lambda \in \mathbb{K}$ tq $\phi = \lambda \det$ i.e.

$$\phi(C_1 \ldots C_k) = \det\left(\begin{array}{c|c} C_1 \ldots C_k & C \\ \hline 0 & B \end{array}\right) = \lambda \det(C_1 \ldots C_k)$$

Pour déterminer λ, on prend $C_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \ldots C_k = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$. On a

$$\det\left(\begin{array}{c|c} \begin{matrix} 1 & & 0 \\ 0 & \ddots & \vdots \\ 0 & & 1 \end{matrix} & C \\ \hline 0 & B \end{array}\right) = \lambda \det\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} = \lambda$$

Par ailleurs, en développant k fois suivant la première colonne, on a

$$\begin{array}{c} \left(\begin{array}{c|c} \begin{matrix} 1 & & 0 \\ 0 & \ddots & \vdots \\ 0 & & 1 \end{matrix} & C \\ \hline 0 & B \end{array}\right) \\ \begin{array}{cc} k & l \end{array} \end{array} = \begin{array}{c} \left|\begin{array}{c|c} \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} & C' \\ \hline 0 & B \end{array}\right| \\ \begin{array}{cc} k-1 & l \end{array} \end{array} = \ldots = |B| = \det B$$

Ceci montre $\lambda = \det B$, donc

$$\det\left(\begin{array}{c|c} C_1 \ldots C_k & C \\ \hline 0 & B \end{array}\right) = \det B \cdot \det(C_1 \ldots C_k) \quad \square$$

⚠ On a en général pas de formule du type

$$\det\left(\begin{array}{c|c} A & C \\ \hline B & D\end{array}\right) = \det A \cdot \det B - \det B \cdot \det C.$$

Corollaire : Si $M = \begin{pmatrix} \boxed{A_1} & & * \\ & \boxed{A_2} & \\ 0 & & \boxed{A_p}\end{pmatrix}$ est triangulaire (supérieure) par bloc avec les blocs diagonaux carrés, on a

$\det M = \det A_1 \cdots \det A_p$. démo : récurrence □.

Chapitre 3 : Éléments d'arithmétique des polynômes et de réduction des endomorphismes.

I. Polynômes

Définition : Soit $\mathbb{K}$ un corps. On dit qu'une application $f : \mathbb{K} \to \mathbb{K}$ est polynomiale s'il existe $n \in \mathbb{N}$, $a_0, \dots, a_n \in \mathbb{K}$ tels que $\forall x \in \mathbb{K}$,

$$f(x) = a_0 + \dots + a_n x^n = a_n x^n + \dots + a_0$$

Une fonction polynomiale est associée à au moins une suite d'éléments $a_0, \dots, a_n$

i.e. une suite infinie dans $\mathbb{K}$ nulle à partir d'un certain rang.

Exemple $f : \begin{array}{l}\mathbb{C} \to \mathbb{C} \\ x \mapsto x^2+2\end{array}$ est associée à la suite $(\underset{a_0}{2}, \underset{a_1}{0}, \underset{a_2}{1}, \underset{a_3}{0} \dots \underset{a_n}{0})$

Définition : On appelle polynôme à coefficients dans $\mathbb{K}$ toute suite de $\mathbb{K}$ nulle à partir d'un certain rang.

Le polynôme $(a_0, \dots, a_n, 0, \dots)$ est noté $a_0 + a_1 X + \dots + a_n X^n$.

a_i s'appelle le coefficient de degré i du polynôme.

Définition : On appelle degré d'un polynôme le plus petit i tel que $a_j = 0$ pour tout $j > i$.

C'est le plus grand i tel que $a_i \neq 0$. On note $\deg(P)$ le degré de P.

Exemple : $(2, 0, 1, 0, \dots, 0, \dots)$ est noté $2 + X^2$. Son degré est 2.

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. On va ~~vérifier~~ définir des lois + et × dans $\mathbb{K}[X]$ (somme et produit usuels des fonctions polynômiales)

$\boxed{\text{Loi } +}$ Si $P = (a_0, \dots, a_n \dots)$ et $Q = (b_0, \dots, b_n \dots)$ sont des éléments de $\mathbb{K}[X]$, alors $(a_0+b_0, \dots, a_n+b_n \dots)$ est un élément de $\mathbb{K}[X]$.

En effet, si $\deg(P) = n$, $\deg(Q) = m$ alors $\forall i > \max(n, m)$, $a_i + b_i = 0$.

On définit $P+Q$ par cet élément. On vient de montrer

Fait : $\forall P, Q \in \mathbb{K}[X]$, $\deg(P+Q) \leq \max(\deg P, \deg Q)$

Exemples 1) $P = (1, 1, 0, -1, 0, \dots) = -X^3 + X + 1$ $\quad Q = (2, 0, -3, 0 \dots 0 \dots) = -3X^2 + 2$

Alors $P+Q = (3, 1, -3, -1, 0, \dots) = -X^3 - 3X^2 + X + 3$ et $\deg(P+Q) = 3 = \deg(P) = \max(\deg P, \deg Q)$

2) $P = (1, 1, 0, -1, 0 \dots)$ $\quad Q = (-2, 0, 1, 1, 0 \dots)$

$P+Q = (-1, 1, 1, 0 \dots)$ et $\deg(P+Q) < \max(\deg P, \deg Q)$

Remarque : cette addition est l'opération qui réalise $aX^k + bX^k = (a+b)X^k$ pour tous $a, b \in \mathbb{K}$, $k \in \mathbb{N}$.

$(\mathbb{K}[X], +)$ est un groupe abélien (le neutre est la suite nulle, etc…)

$\boxed{\text{Loi} \times}$ Si $P=(a_0,\dots,a_n,\dots)$ $Q=(b_0,\dots,b_n,\dots)$ $\in \mathbb{K}[X]$ alors la suite

$(c_0,\dots,c_n,\dots)$ définie par $c_n=\sum_{k=0}^{n} a_k b_{n-k}$ pour tout $n\in\mathbb{N}$ est un élément

de $\mathbb{K}[X]$, noté $P\times Q$ (ou $P\cdot Q$).

(Le produit est l'opérateur qui réalise $aX^k * bX^{n-k} = abX^n$)

Précisement:

Fait: Si $d^\circ P=n$, $d^\circ Q=m$, alors $d^\circ(P\times Q)=n+m$.

Preuve: On suppose $d^\circ P=n$, $d^\circ Q=m$.

Soit p tq $p>n+m$, alors tous les termes de la somme $\sum_{k=0}^{p} a_k b_{p-k}$ sont nuls car

soit $a_k=0$ (si $k>n$)

soit $b_{p-k}=0$ (si $k\le n$, donc $p-k>n+m-k>m$)

Cela montre $d^\circ PQ\le n+m$.

D'autre part: $C_{n+m}=\sum_{k=0}^{n+m} a_k b_{n+m-k} = a_0b_{n+m}+a_1b_{n+m-1}+\dots+a_nb_m+a_{n+1}b_{m-1}+\dots+a_{n+m}$

$= a_nb_m\neq 0$ car $a_n\neq0$, $b_m\neq 0$

Ceci montre $d^\circ(PQ)\ge n+m$, d'où l'égalité. $\boxtimes$

Un polynome se note $(1,-1,0,2,0,0,\dots)\in\mathbb{R}[X]$

$\hookrightarrow = 1-X+2X^3$

$(\mathbb{K}[X],+,\times)$ est un anneau commutatif.

$a_kX^k * b_lX^l = a_kb_lX^{k+l}$

$c_n=\sum_{k=0}^{n} a_k b_{n-k}$

Si $P(X)=a_nX^n+\dots+a_0$ avec $a_n\neq0$, alors $d^\circ P=n$.

Convention: $d^\circ 0=-\infty$

$\uparrow$ polynome nul

Fait $\cdot$ $d^\circ(P+Q)\le \max(d^\circ P, d^\circ Q)$

$\cdot$ $d^\circ(P\cdot Q)=d^\circ P+d^\circ Q$

idée de preuve: On vérifie ces propriétés si $P=0$ ou $Q=0$, avec la convention

si $n\in\mathbb{N}$, $-\infty+n=-\infty$ $\square$

Corollaire: $\forall P,Q\in\mathbb{K}[X]$, $PQ=0 \iff P=0$ ou $Q=0$.

démo: Si $P=0$ ou $Q=0$ alors $P\cdot Q=0$. (appliquer la formule du produit) $\boxtimes$

Réciproquement[(1)], supposons $P\neq0$ et $Q\neq0$.

Alors $d^\circ P\ge0$ et $d^\circ Q\ge0$. Donc $d^\circ(PQ)=d^\circ P+d^\circ Q\ge0$.

Ceci montre (c'est équivalent à) $PQ\neq0$. $\square$.

‼ les polynômes ne sont pas des applications

Fait: Soit $P\in\mathbb{K}[X]$. $P\neq0 \iff d^\circ P\ge0$

Autre façon de faire (1): si $P\neq0$, $Q\neq0$, $\exists n,m$, $\exists a_n\neq0$, $\exists b_m\neq0$ tq

$P(X)=a_nX^n+\dots+a_0$, $Q(X)=b_mX^m+\dots+b_0$

liée à la preuve pour $d^\circ(PQ)=d^\circ P+d^\circ Q$

Alors $P(X)Q(X)=a_nb_mX^{n+m}+R(X)$ avec $d^\circ R<n+m$. Comme $a_nb_m\neq0$, $P(X)Q(X)\neq 0$

On dit que l'anneau $\mathbb{K}[X]$ (qui vérifie le corollaire) est <u>intègre</u>.

Exemple d'anneau commutatif non intègre : $\mathbb{Z}/6\mathbb{Z}$

Exemple d'anneau non commutatif non intègre : $M_n(\mathbb{K})$, $n \geq 2$.

$$\underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_{\neq 0} \underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_{\neq 0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

<u>Corollaire</u> : Soit $P, Q, R \in \mathbb{K}[X]$ tels que $P \cdot R = Q \cdot R$ et $R \neq 0$. Alors $P = Q$.

On peut "simplifier" une equation par un terme non nul.

⚠ Pour la preuve, on ne peut pas multiplier par l' "inverse" de R, car en général R n'a pas d'inverse dans $\mathbb{K}[X]$.

<u>Preuve</u> : Comme $PR = QR$, on a $PR - QR = 0$ donc $(P-Q)R = 0$ (distributivité de $\times$ sur $+$)

D'après le corollaire précédent, cela implique $P - Q = 0$ ou $R = 0$.

Or $R \neq 0$, donc $P - Q = 0$, i.e. $P = Q$. $\square$

<u>Corollaire</u> : Un élément $P \in \mathbb{K}[X]$ est inversible (pour $\times$) <u>ssi</u> il est de degré 0.

Un polynome de degré ≤ 0 s'appelle un polynome "constant". Un polynome inversible est donc exactement un polynome constant non nul.

<u>démo</u> : Soit $P \in \mathbb{K}[X]$ inversible.

Alors (par définition) il existe $Q \in \mathbb{K}[X]$ t.q. $P \cdot Q = 1$.

On a $d°(P.Q) = d°P + d°Q = d°1 = 0$. Ceci impose $d°P = d°Q = 0$.

Réciproquement si $d°P = 0$, i.e. $P(X) = a_0$, $a_0 \in \mathbb{K}^*$ $(a_0 \neq 0)$ alors le polynôme

$Q(X) = \frac{1}{a_0}$ est inverse de P : $\underbrace{a_0}_{\in \mathbb{K}[X]} \cdot \underbrace{\frac{1}{a_0}}_{\in \mathbb{K}[X]} = \underbrace{1}_{\in \mathbb{K}[X]}$. $\square$

⚠ <u>Remarque</u> : Attention $\mathbb{K}$ n'est <u>pas inclus</u> dans $\mathbb{K}[X]$, mais on a une injection canonique de $\mathbb{K}$ dans $\mathbb{K}[X]$.

$$i : \mathbb{K} \longrightarrow \mathbb{K}[X]$$
$$\underset{\in \mathbb{K}}{a} \longrightarrow (a, 0, 0, \dots) = \underset{\in \mathbb{K}[X]}{a(1 + 0X + 0X^2 + \dots)}$$

<u>Exemple</u> : $i(1_{\mathbb{K}}) = 1_{\mathbb{K}[X]}$, le polynome unité par $\times$ dans $\mathbb{K}[X]$. On vérifie que i est un morphisme d'anneau donc

$i(a+b) = i(a) + i(b)$ et $i(ab) = i(a) \cdot i(b)$ (à méditer)

L'ensemble des éléments inversibles d'un anneau A se note A^*. Ici on a donc $\mathbb{K}[X]^* = i(\mathbb{K}^*)$. On vérifie que $\mathbb{Z}^* = \{+1, -1\}$

<u>Définition</u> : Soient $P, Q \in \mathbb{K}[X]$. On dit que <u>P divise Q</u> et on écrit $P | Q$, si $\exists R \in \mathbb{K}[X]$ tq $Q = P \cdot R$

<u>Exemple</u> : $X - 1 \mid X^2 - 3X + 2$ car $\underbrace{X^2 - 3X + 2}_{Q} = \underbrace{(X-1)}_{P} \underbrace{(X-2)}_{R}$

<u>Fait</u> : Soient $P_1, P_2, P_3 \in \mathbb{K}[X]$.

1) Si $P_1 | P_2$ et $P_1 | P_3$ alors $P_1 | P_2 + P_3$
2) Si $P_1 | P_2$ et $P_2 | P_3$ alors $P_1 | P_3$

démo : 1) Supposons $P_1 | P_2$ et $P_1 | P_3$. Donc $\exists R_2, R_3$ tq $\begin{cases} P_2 = P_1 R_2 \\ P_3 = P_1 R_3 \end{cases}$

Alors $P_2 + P_3 = P_1 R_2 + P_1 R_3 = P_1(R_2 + R_3)$. Ce qui montre $P_1 | P_2 + P_3$.

2) Supposons $P_1 | P_2$, $P_2 | P_3$. Donc $\exists R_2$ tq $P_2 = P_1 R_2$.

$\exists R_3$ t.q. $P_3 = P_2 R_3$. Alors $P_3 = (P_1 R_2) R_3 = P_1 (R_2 R_3)$ (associativité de $\times$). Ceci montre $P_1 | P_3$.

Remarque : La relation $|$ sur $\mathbb{K}[X]$ est réflexive ($\forall P \in \mathbb{K}[X]$, $P = P \cdot 1$ donc $P | P$)

transitive (c'est le point 2)

mais n'est pas antisymétrique. $P | 2P$ et $2P | P = \frac{1}{2}(2P)$ et $P \neq 2P$

Théorème (division euclidienne dans $\mathbb{K}[X]$)

Soient $P, Q \in \mathbb{K}[X]$. Il existe $D, R \in \mathbb{K}[X]$ tel que 1) $P = D \cdot Q + R$
$Q \neq 0$. 2) $d^\circ R < d^\circ Q$

Les polynômes D, R vérifiant 1) et 2) sont uniques.

L'exemple suivant montre l'idée de la preuve.

Division euclidienne de $2X^5 - X^3 + 2X - 1$ par $X^2 + X + 1$.

$$2X^5 - X^3 + 2X - 1 = (X^2 + X + 1)(2X^3 - 2X^2 - X + 3) - 4$$

Démo : Montrons l'unicité. Soit $P, Q \in \mathbb{K}[X]$, $D_1, D_2, R_1, R_2 \in \mathbb{K}[X]$ tels que

$$\begin{cases} P = QD_1 + R_1 & d^\circ R_1 < d^\circ Q \\ P = QD_2 + R_2 & d^\circ R_2 < d^\circ Q \end{cases}$$

On a $QD_1 + R_1 = QD_2 + R_2$ donc $QD_1 - QD_2 = R_2 - R_1$ donc $Q(D_1 - D_2) = R_2 - R_1$.

On a $d^\circ(R_2 - R_1) = d^\circ(Q(D_1 - D_2)) = d^\circ Q + d^\circ(D_1 - D_2)$.

Or $d^\circ(R_2 - R_1) \leq \max(d^\circ R_1, d^\circ R_2) < d^\circ Q$.

Comme $d^\circ Q \geq 0$, ceci impose $d^\circ(D_1 - D_2) < 0$, donc $d^\circ(D_1 - D_2) = -\infty$, i.e. $D_1 - D_2 = 0$ i.e $D_1 = D_2$. Donc $R_2 - R_1 = P \cdot 0 = 0$ i.e. $R_2 = R_1$.

Montrons l'existence. Par récurrence sur $d^\circ P$, avec Q fixé.

Soit $Q \in \mathbb{K}[X]$, $Q \neq 0$.

Si $P \in \mathbb{K}[X]$ vérifie $d^\circ P < d^\circ Q$, on a $P = 0 \cdot Q + \underbrace{P}$ avec $d^\circ R < d^\circ Q$

c'est la division euclidienne de P par Q.

Supposons que l'existence de la division euclidienne par Q soit établie pour tout polynôme de degré $\leq n$, avec $n \geq d^\circ Q - 1$. Soit $P \in \mathbb{K}[X]$ tq $d^\circ P = n+1$.

On écrit $\begin{cases} P(X) = a_{n+1} X^{n+1} + a_n X^n + \dots + a_0, & a_{n+1} \neq 0 \\ Q(X) = b_m X^m + \dots + b_0, & b_m \neq 0 \end{cases}$

On écrit

$$P(X) - \frac{a_{n+1}}{b_m} X^{n+1-m} \underbrace{(b_m X^m + \dots + b_0)}_{Q(X)} = P_1(X) \quad \text{avec} \quad d^\circ P_1(X) \leq n.$$

Par hypothèse de récurrence $\exists D_1, R_1 \in \mathbb{K}[X]$ tq $P_1 = QD_1 + R_1$.

On a donc $P(X) = \frac{a_{n+1}}{b_m} X^{n+1-m} \cdot Q(X) + D_1(X) Q(X) + R_1(X)$

$$= Q(X) \left(\frac{a_{n+1}}{b_m} X^{n+1-m} + D_1(X) \right) + R_1(X).$$

C'est une (donc l'unique) division euclidienne de P par Q. □

idée de la preuve : établir la formule pour $(P \times Q)^K$

<u>Exemple d'application</u> : a est racine de multiplicité ≥ 2 de P ssi $P(a) = P'(a) = 0$.

<u>Théorème de la factorisation en produit d'irréductibles dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.</u>

1) Tout polynôme non nul de $\mathbb{C}[X]$ s'écrit sous la forme

$$P(X) = a(X-\lambda_1)\dots(X-\lambda_n) \quad \text{avec } n = d^\circ P,\ a \in \mathbb{C}^*,\ \lambda_1, \dots, \lambda_n \in \mathbb{C}.$$

2) Tout polynôme non nul de $\mathbb{R}[X]$ s'écrit :

$$P(X) = a(X-\lambda_1)\cdots(X-\lambda_k)(X^2+a_1X+b_1)\dots(X^2+a_\ell X+b_\ell) \quad \text{avec } a \in \mathbb{R}^*,$$

$k+2\ell = d^\circ P$, $\lambda_1, \dots, \lambda_k, a_1, \dots, a_\ell, b_1, \dots, b_\ell \in \mathbb{R}$, et $X^2+a_1X+b_1, \dots, X^2+a_\ell X+b_\ell$ n'ont pas de racine dans $\mathbb{R}$.

3) Ces deux écritures sont <u>uniques</u> à permutation des termes près.

<u>démo</u> : 1) admis

2) résulte de 1 et de la propriété suivante : (exercice ☒)

<u>Lemme</u> : Soit $P \in \mathbb{R}[X] \hookrightarrow \mathbb{C}[X]$. Soit $\lambda \in \mathbb{C}$.
Si λ est racine, alors $\overline{\lambda}$ est racine de P.

<u>démo</u> : Supposons $P(\lambda) = 0$. Alors $P(\overline{\lambda}) = \overline{P(\lambda)}$ car P est à coefficients réel.

(si $a_0, \dots, a_n \in \mathbb{R}$, $a_n\overline{\lambda}^n + \dots + a_1\overline{\lambda} + a_0 = \overline{a_n\lambda^n + \dots + a_0}$ puisque $\forall i$, $a_i = \overline{a_i}$)

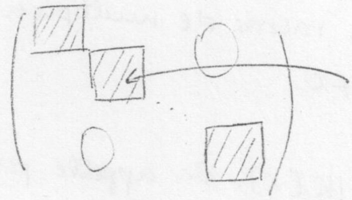
Donc $P(\overline{\lambda}) = 0$.

3) est un résultat d'arithmétique général. Exercice ☒.

II Réduction des endomorphismes. Diagonalisation.

Soit E un $\mathbb{K}$-espace vectoriel, $f : E \to E$ un endomorphisme

<u>Objectif</u> : pour "analyser" ou "comprendre" f, casser E en somme directe de sev stable par f. matriciellement : chercher $F_1, \dots, F_k$ sev de E (aussi petit que possible)

t.q. $\underset{\substack{\text{base adaptée} \\ \text{à } F_1 \oplus \dots \oplus F_k = E}}{\text{mat}} f =$  $\underset{\text{base de } F_i}{\text{mat}} f|_{F_i}$

<u>L'idéal</u> : $\dim F_i = 1$. Si (e_i) est une base d'un tel F_i, on a $f(e_i) \in F_i = \text{vect}(e_i)$ i.e $f(e_i)$ est un multiple de e_i

<u>Définition</u> : On dit que $x \in E \setminus \{0\}$ est un <u>vecteur propre</u> de f si $\exists \lambda \in \mathbb{K}$ tq $f(x) = \lambda x$.

<u>Fait</u> : $x \neq 0$ est v.p. de f <u>ssi</u> la droite $\text{vect}(x)$ est stable par f.

<u>démo</u> : déjà vu en TD.

<u>Définition</u> : On dit que $\lambda \in \mathbb{K}$ est <u>valeur propre</u> de f si $\exists x \in E \setminus \{0\}$ tq $f(x) = \lambda x$.
Dans ce cas, on dit que x est vecteur propre associé à la valeur propre λ.

<u>Exemple</u> : 0 est valeur propre de f ssi $\exists x \neq 0$ $f(x) = 0$ ssi f est non injective ssi $\det f =$
(ssi (en dimension finie) $\text{rg}(f) < \dim E$)

Définition : Soit $x \in \mathbb{K}$. Pour tout polynôme $P(X) \in \mathbb{K}[X]$,

$P(X) = a_n X^n + \dots + a_0$, on note $P(x) = a_n x^n + \dots + a_0$ (élément de $\mathbb{K}$).

Cet élément de $\mathbb{K}$ s'appelle l'évaluation de P en x.

L'application $f_x : \mathbb{K}[X] \to \mathbb{K}$, $P \mapsto P(x)$ s'appelle le morphisme d'évaluation en x.

f_x est un morphisme d'algèbre, i.e. morphisme d'anneau et d'ev, i.e. "préserve" les lois $+, \times$ et $\circ$: (exercice ☒)

$\forall x \in \mathbb{K}$

$\forall P, Q \in \mathbb{K}[X]$, $\forall \lambda \in \mathbb{K}$, $(P+Q)(x) = P(x) + Q(x)$

$(P \cdot Q)(x) = P(x) \cdot Q(x)$

$(\lambda P)(x) = \lambda P(x)$.

Définition : Soit $P \in \mathbb{K}[X]$. On dit que $a \in \mathbb{K}$ est une racine de P si $P(a) = 0$.

Théorème : Avec ces notations, a est une racine de P ssi $X - a \mid P(X)$

démo : La division euclidienne de P par $X-a$ donne

$P(X) = (X-a)Q(X) + R$ avec $d°R < 1$ donc R polynôme constant.

On évalue P en a.

Du fait que f_a est un morphisme d'algèbre, on a $P(a) = 0 \cdot Q(a) + R = R$.

Ceci montre :

a est racine de $P \underset{\text{déf}}{\iff} P(a) = 0 \iff R = 0 \iff P(X) = (X-a)Q(X) \iff X - a \mid P(X)$.

Exemple : 1 est racine de $P(X) = X^4 - 3X^3 + X + 1$ car $P(1) = 0$. On a $X^4 - 3X^3 + X + 1 = (X-1)(X^3 - 2X^2 - 2X - 1)$

Définition : Soit $a \in \mathbb{K}$, $P \in \mathbb{K}[X]$. On appelle multiplicité de a comme racine de P le plus grand entier $k \in \mathbb{N}$ tel que $(X-a)^k \mid P(X)$.

Formellement, si a n'est pas racine de P, on peut dire que la multiplicité de a comme racine de P est 0.

Proposition : Avec ces notations, a est racine de multiplicité k de P ssi

$P(X) = (X-a)^k Q(X)$ avec $Q(a) \neq 0$.

démo : exercice ☒

Définition : Soit $P(X) = a_n X^n + \dots + a_0 \in \mathbb{K}[X]$. On appelle polynôme dérivée de P le polynôme

$P'(X) = n a_n X^{n-1} + \dots + a_1$, si $n \geq 1$, 0 sinon.

Si $\mathbb{K} = \mathbb{R}$, la fonction polynomiale associée à P' est la dérivée de la fonction polynomiale associée à P. Mais cette dérivation "formelle" ou "algébrique" a un sens dans tout corps $\mathbb{K}$ (par exemple $\mathbb{K}$ fini !). Cette dérivée a les propriétés habituelles de la dérivée en analyse sur $\mathbb{R}$:

Proposition : $\forall P, Q \in \mathbb{K}[X]$, $\forall \lambda \in \mathbb{K}$, $(P+Q)' = P' + Q'$, $(\lambda P)' = \lambda P'$, $(PQ)' = P'Q + PQ'$.

démo : exérice ☒

Proposition : Soit $a \in \mathbb{K}$, $P \in \mathbb{K}[X]$. a est racine de multiplicité k de P ssi
$P(a) = 0$
$P'(a) = 0$
$\vdots$
$P^{(k-1)}(a) = 0$
$P^{(k)}(a) \neq 0$

On note $P^{(k)}$ le polynôme dérivée k^e de P défini par récurrence par $P^{(k)} = P^{(k-1)\prime}$ $(P = P^{(0)})$

démo : exercice ☒

Définition : Soit λ une valeur propre de f. On appelle espace propre de f associé à la valeur propre λ l'ensemble formé des vecteurs propres de f associée à λ et de 0. On le notera $E_\lambda(f)$ ou E_λ.

Fait : E_λ est un sev précisément $\boxed{E_\lambda = \mathrm{Ker}(f - \lambda id)}$

démo : immédiatement par définition.

idée générale : ce sont les vecteurs propres et les espaces propres qui nous intéressent pour décomposer. f, mais on cherche en général les valeurs propres pour trouver les espaces propres. C'est la conséquence de la proposition suivante.

Proposition : Soit $f : E \to E$ une endomorphisme, soit $\lambda \in \mathbb{K}$.
λ est valeur propre de f ssi $\mathrm{Ker}(f - \lambda id) \neq \{0\}$. Si $\dim E$ est finie
λ est valeur propre de f ssi $\det(f - \lambda id) = 0$.

Preuve : λ est v.p. de $f \underset{\text{déf}}{\iff} \exists x \neq 0 \;\; f(x) = \lambda x$

$$\begin{aligned}
&\iff \exists x \neq 0 \;\; f(x) - \lambda x = 0\\
&\iff \exists x \neq 0 \;\; (f - \lambda id)(x) = 0\\
&\iff \mathrm{Ker}(f - \lambda id) \neq \{0\}\\
&\left[\begin{aligned}&\iff f - \lambda id \text{ non injective}\\ &\iff f - \lambda id \;\neg\text{bijective}\end{aligned}\right]\\
&\iff \det(f - \lambda id) = 0
\end{aligned}$$

Définition : Soit $f : E \to E$ endomorphisme, $\dim E < +\infty$.
Le polynôme $\boxed{\det(X id - f)}$ s'appelle le polynôme caractéristique de f.

Exemple : Si $f : \mathbb{R}^2 \to \mathbb{R}^2$ a pour matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ dans la base de $\mathbb{R}^2$

$$\det(X id - f) = \det\left(X \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right) = \begin{vmatrix} X & 1 \\ -1 & X \end{vmatrix} = X^2 + 1$$

Si $\mathrm{mat}_{can} f = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, $\det(X id - f) = \begin{vmatrix} X-a & -c \\ -b & X-d \end{vmatrix}$

Remarque : La notation $\det(X id - f)$ peut se formaliser.
On peut définir $\det(X id - f)$ par le dét. d'une matrice à coefficient dans $\mathbb{K}[X]$, i.e. un elt de $M_n(\mathbb{K}[X])$. Le résultat est un polynôme.

Remarque : Une autre caractérisation souvent utilisée est $\det(f - X id)$ au lieu de $\det(X id - f)$

[ex $\begin{vmatrix} X-a & -c \\ -b & X-d \end{vmatrix}$ devient $\begin{vmatrix} a-X & c \\ b & d-X \end{vmatrix}$

Une autre notation possible est
$\det(f - \lambda id)$ assimilé à la fonction polynomiale $\mathbb{K} \to \mathbb{K}$, $\lambda \to \det(f - \lambda id)$

On notera $P_f(X)$ ce polynôme. (autre notation usuelle $\chi_f(X)$)

La proposition précédente s'écrit

Fait : λ est v.p. de $f \iff \lambda$ est racine de $P_f(X)$. $\quad P_f(X) = \det(X id - f)$

λ racine de $P_f(X)$ veut dire que $\det(\lambda id - f) = 0$ donc $\exists x \neq 0$ tq $(\lambda id - f)(x) = 0$
c.à.d $f(x) = \lambda id$.

$f : E \to E$, $\dim E < +\infty$

λ est valeur propre de $f \iff \mathrm{Ker}(\lambda \, id - f) \neq \{0\} \iff P_f(\lambda) = 0$, où P_f est le polynôme caractéristique de f.

Exemples :

1) $f : \mathbb{R}^2 \to \mathbb{R}^2$ (ici $\mathbb{K} = \mathbb{R}$)
$(x,y) \to (-y,x)$ $\quad \mathrm{mat}_{can} f = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Notation : Si on munit $\mathbb{R}^2$ du produit scalaire usuel, f est la rotation d'angle $\frac{\pi}{2}$

Cette interprétation géométrique montre que f n'a pas de vecteur propre.
Donc f n'a pas de droite stable, les seuls sev stables par f sont triviaux, $\{0\}$ et $\mathbb{R}^2$.

$$P_f(X) = \underbrace{\begin{vmatrix} X-0 & 1 \\ -1 & X-0 \end{vmatrix}}_{X\,Id - \mathrm{mat}_{can} f} = X^2+1$$

P_f n'a pas de racine réelle, donc f n'a pas de valeur propre réelle (donc pas de vecteur propre)

2) Soit $f : \mathbb{C}^2 \to \mathbb{C}^2$ (ici $\mathbb{K} = \mathbb{C}$)
$(x,y) \to (-y,x)$

$\mathrm{mat}_{can} f = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $\quad P_f(X) = X^2+1$ $\quad f$ possède deux valeurs propres, i et $-i$

E_i (espace propre associé à la valeur propre i)

$$E_i = \mathrm{Ker}(i \cdot id - f) = \mathrm{Ker}(f - i \cdot id)$$

$P_f(X) = (X-i)(X+i)$

Soit $(x,y) \in \mathbb{R}^2$, $\mathbb{C}^2$?

- $(x,y) \in E_i \iff \begin{pmatrix} i & 1 \\ -1 & i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

$\left[\text{ou } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = i \begin{pmatrix} x \\ y \end{pmatrix}\right]$ $\quad \left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} - i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

$\iff \begin{cases} ix + y = 0 \\ -x + iy = 0 \end{cases}$

$\iff ix + y = 0$ $\quad$ (parce que on sait que le système est de rg 1 $\to L_2 = i L_1$)

$\iff \begin{cases} x = x \\ y = -ix \end{cases}$

$\iff (x,y) \in \mathrm{vect}(1,-i)$ $\quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -i \end{pmatrix} = \begin{pmatrix} i \\ 1 \end{pmatrix} = i \begin{pmatrix} 1 \\ -i \end{pmatrix}$

Donc $\boxed{E_i = \mathrm{vect}(1,-i)}$

E_{-i} On trouve de même $\boxed{E_{-i} = \mathrm{vect}(1,i)}$

Remarque fondamentale : E_i et E_{-i} sont en somme directe.

$\mathcal{B} = ((1,-i),(1,i))$ est une base de $\mathbb{C}^2$, base formée de vecteurs propres de f.

$$\mathrm{mat}_\beta f = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

c'est une matrice diagonale. On dit que f est diagonalisable.

Remarque : $\mathrm{tr}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = 0 + 0 = 0 \qquad \mathrm{tr}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = i - i = 0$

3) $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit $f : \mathbb{K}^2 \to \mathbb{K}^2$
$(x, y) \to (y, 0)$

$$\mathrm{mat}_{\mathrm{can}} f = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad P_f(X) = \begin{vmatrix} X & -1 \\ 0 & X \end{vmatrix} = X^2$$

0 est la seule valeur propre de f (valeur propre "double").

$E_0 = \mathrm{Ker} f$

Soit $(x, y) \in \mathbb{K}^2$.

$(x, y) \in E_0 \iff \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

$\iff y = 0$

$\iff (x, y) \in \mathrm{vect}((1, 0))$

Donc $E_0 = \mathrm{vect}((1, 0))$.

$\mathbb{K}^2$ n'a donc pas de base formée de vecteurs propres pour f. On verra que f n'est donc pas diagonalisable.

Remarque : f est nilpotente : $f^2 = 0$

4) $f : \mathbb{K}^2 \to \mathbb{K}^2$ tq. $\mathrm{mat}_{\mathrm{can}} f = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

n'est pas non plus diagonalisable.

On vérifie que $P_f(X) = (X - \lambda)^2$ (une seule valeur propre, double)

et $E_\lambda = \mathrm{vect}((1, 0))$

Conclusion : On a vu des endomorphismes
- diagonalisables
- non diagonalisables parce qu'il "manque des valeurs propres"

Dans ce cas on passe à un corps plus gros (ici de $\mathbb{R}$ à $\mathbb{C}$).
- non diagonalisables parce qu'il "manque des vecteurs propres"

Propriétés du polynôme caractéristique

Proposition : Soit $f : E \to E$ un endomorphisme, $\dim E = n$. On a :

1) $P_f(X)$ est un polynôme de degré n, unitaire (i.e. le coef de plus haut degré vaut 1) : $P_f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$

2) le terme constant de $P_f(X)$ est $a_0 = (-1)^n \det f$.

Exemple : $\mathrm{mat}_{\mathrm{can}} f = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $\det(X\,\mathrm{id} - f) = \det\begin{pmatrix} X & 1 \\ -1 & X \end{pmatrix} = X^2 + 1$

$P_f(X) = X^2 + 1$ ← degré $= 2$

unitaire ; $1 = (-1)^2\begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix}$

démo : (idée)

1) On peut le montrer :

- par récurrence en développant par rapport à la première colonne.
- par la formule des permutations

$$P_f(X) = \begin{vmatrix} X-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \ddots & & \vdots \\ \vdots & & \ddots & -a_{n-1,n} \\ -a_{n,1} & \cdots & -a_{n,n-1} & X-a_{n,n} \end{vmatrix}$$

Le développement de ce dét. par la formule des permutations fait apparaître une somme de produit de coeff. de cette matrice, i.e. de terme de la forme $X-a_{ii}$ ou $-a_{i,j}$, $i \neq j$. Parmi ces $n!$ produits, le polynôme de plus haut degré obtenu est $(X-a_{11})\dots(X-a_{n,n})$ de degré n, tous les autres termes étant de degré $\leq n-2$ (si $\sigma \neq id$, $card(supp\,\sigma) \geq 2$)

Cela montre que[(1)] $P_f(X)$ est de degré n et le terme de degré n est celui de $(X-a_{11})\dots(X-a_{nn})$, donc X^n.

Remarque : on a aussi montré que le coef. de degré $n-1$ de $P_f(X)$ est celui de $(X-a_{11})\dots(X-a_{nn})$. (on verra que c'est $tr f$).

2) le coef constant a_0 de P_f est donné par son évaluation en 0.

$$a_0 = P_f(0) = \det(0\cdot id - f) = \det(-f) = (-1)^n \det f$$

[en colonne :

$$\det(-(C_1\dots C_n)) = \det(-C_1 \dots -C_n) = (-1)^n \det(C_1 \dots C_n)$$

Remarque : la convention $\det(f - X\,id)$ donne

$$P_f(X) = (-1)^n X^n + \dots + \det f.$$

Trace d'une matrice, d'un endomorphisme

Définition : Soit $A = (a_{ij})_{1\leq i,j\leq n} \in M_n(\mathbb{K})$. On appelle trace de A le scalaire

$$tr(A) = a_{11} + \dots + a_{nn}$$

Exemple : $tr\begin{pmatrix} -1 & 0 & -1 \\ 0 & 2 & 0 \\ 1 & -1 & 0 \end{pmatrix} = -1+2+0 = 1$

Proposition : $tr : M_n(\mathbb{K}) \to \mathbb{K}$, $A \to tr(A)$ est linéaire.

démo : facile, exercice ~~à~~ rete

Proposition : Si $A, B \in M_n(\mathbb{K})$, alors $tr(AB) = tr(BA)$

démo : exercice, écrire $A = (a_{i,j})$, $B = (b_{i,j})$ et les formules ~~à~~ rete

(1) $P_0(X) = (X-a_{1,1})\dots(X-a_{n,n}) = \underline{X^n + b_{n-1}X^{n-1}} + b_{n-2}X^{n-2} + \dots + b_0$

$Q(X) = c_{n-2}X^{n-2} + \dots + c_0 \qquad (P_0+Q)(X) = \underline{X^n + b_{n-1}X^{n-1}} + (b_{n-2}+c_{n-2})X^{n-2} + \dots + (b_0$

preuve : argument déjà vu, exercice $\boxed{V}$
(ou récurrence)

Corollaire : Si P_f est scindé de degré n, de racines $\lambda_1, \dots, \lambda_n$ (comptés avec leur multiplicité) alors $\lambda_1 + \dots + \lambda_n = \operatorname{tr} f$.

Application : Si on connaît $n-1$ racines $\lambda_1 \dots \lambda_{n-1}$ de P_f, alors on connaît la dernière racine : $\lambda_n = \operatorname{tr} f - (\lambda_1 + \dots + \lambda_{n-1})$

Éléments propres d'une matrice

La théorie qu'on vient de voir sur les endomorphismes s'applique aux matrices.
Soit $A \in M_n(\mathbb{K})$.
On appelle "éléments propres" de A, i.e. valeurs propres, vecteurs propres, espaces propres de A, les éléments propres de l'endomorphisme $\phi_A : \mathbb{K}^{n,1} \to \mathbb{K}^{n,1}$
$X \mapsto \phi_A(X) = A \cdot X$

Exemple : $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ est valeur propre de $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, associée à la valeur propre 2.

$\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ est valeur propre de $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, associée à la valeur propre 0.

Remarque : $\operatorname{mat}_{can} \phi_A = A$ car $A \cdot e_i$ donne la $i$ème colonne de A

III. Diagonalisation

Théorème : Soit $f : E \to E$ un endomorphisme
Si $\lambda_1 \dots \lambda_k$ sont des valeurs propres de f 2 à 2 distincts, alors les espaces propres associées $E_{\lambda_1}, \dots, E_{\lambda_k}$ sont en somme directe.

On verra une preuve de ce théorème utilisant des propriétés arithmétiques de $\mathbb{K}[X]$
voici une autre idée de preuve.

idée de preuve : Soit $x_1 \in E_{\lambda_1} \dots x_k \in E_{\lambda_k}$ tels que $x_1 + \dots + x_k = 0$. Pour montrer que la somme des E_{λ_i} est directe, il faut montrer que $x_1 = \dots = x_k = 0$ (exercice $\boxed{VI}$).

On a : $f(x_1 + \dots + x_k) = 0$, i.e., $f(x_1) + \dots + f(x_k) = 0$, donc $\lambda_1 x_1 + \dots + \lambda_k x_k = 0$

On itère :
$$f^2(x_1 + \dots + x_k) = 0$$
Or $f^2(x_i) = f(f(x_i)) = f(\lambda_i x_i) = \lambda_i f(x_i) = \lambda_i^2 x_i$.

Donc $\lambda_1^2 x_1 + \dots + \lambda_k^2 x_k = 0$.
Et de même jusqu'à $\lambda_1^{k-1} x_1 + \dots + \lambda_k^{k-1} x_k = 0$.

Ainsi
$$\begin{cases} x_1 + \dots + x_k = 0 \\ \lambda_1 x_1 + \dots + \lambda_k x_k = 0 \\ \vdots \\ \lambda_1^{k-1} x_1 + \dots + \lambda_k^{k-1} x_k = 0 \end{cases}$$

Or
$$\begin{vmatrix} 1 & \cdots & 1 \\ \lambda_1 & \cdots & \lambda_k \\ \vdots & & \vdots \\ \lambda_1^{k-1} & \cdots & \lambda_k^{k-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (\lambda_j - \lambda_i) \neq 0$$
on peut la triangulariser

En raisonnant par coordonnées en dimension finie cela conclut (toutes coordonnées des x_i sont nulles). On peut généraliser la preuve à dim E qcq (raisonner sur $\operatorname{vect}(x_1 \dots x_k)$)

? Comment ça ?

$\boxed{VII}$

marche aussi pour des matrices rectangulaires $(n,m)\times(m,n)$

Corollaire: Si $A \in M_n(\mathbb{K})$, $P \in GL_n(\mathbb{K})$ alors $tr(P^{-1}AP) = tr A$

"Deux matrices semblables ont même trace".

démo: D'après la proposition précédente, on a $tr(P^{-1}AP) = tr(AP.P^{-1}) = tr(A)$

Corollaire: Si $f : E \to E$, $\dim E < +\infty$,
$tr(mat_B f)$ ne dépend pas du choix d'une base B de E. On l'appelle trace de f, notée $tr(f)$.

Proposition: Le terme de degré $n-1$ de $P_f(X)$ est $-tr(f)$

démo: La preuve précédente nous a dit que le coef. de degré $n-1$ de $P_f(X)$ est le même que celui de

$$(X-a_{11})\dots(X-a_{nn}).$$

En développant ce produit, on trouve exactement n termes de degré $n-1$:

$$(-a_{11})\underbrace{X\dots X}_{n-1 \text{ fois}} + \dots + \underbrace{X\dots X}_{n \text{ fois}}(-a_{nn})$$

$$= (-a_{11} \cdots -a_{nn})X^{n-1} = -trf \cdot X^{n-1}$$

Exemple: Si $mat_B f = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$

$$P_f(X) = X^2 - \underbrace{(a+d)}_{=}X + (ad-bc)$$
$$\quad\quad -trf \quad\quad (-1)^2 \det f$$

$$P_f(X) = X^n - trf\, X^{n-1} + a_{n-2}X^{n-2} + \dots + a_1 X + (-1)^n \det f$$

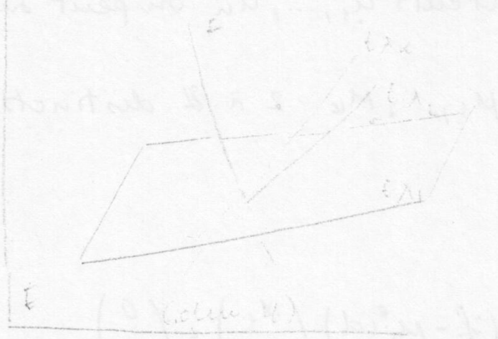
Définition: On dit qu'un polynôme $P \in \mathbb{K}[X]$ est <u>scindé</u> ssi P est facteur de polynôme de degré 1 et d'une constante. $P(X) = c(X-\lambda_1)\dots(X-\lambda_n)$

Exemples:
- X^2-1 est scindé dans $\mathbb{R}[X]$: $X^2-1 = (X-1)(X+1)$
- X^2+1 n'est pas scindé dans $\mathbb{R}[X]$: ce polynôme est irréductible, sans racine réel.
- X^2+1 est scindé dans $\mathbb{C}[X]$: $X^2+1 = (X+i)(X-i)$
- X^3-1 n'est pas scindé dans $\mathbb{R}[X]$. Sa décomposition en produit d'irréductible est $X^3-1 = (X-1)(X^2+X+1)$
- X^3-1 est scindé dans $\mathbb{C}[X]$: $X^3-1 = (X-1)(X-j)(X-j^2)$
- Tout polynôme de $\mathbb{C}[X]$ est scindé, d'après sa décomposition en produit d'irréductibles vue au paragraphe précédent.

Tout pol. complexe est scindé

Proposition: Si $P(X) = (X-\lambda_1)\dots(X-\lambda_n)$ alors le coefficient de degré $n-1$ de P est $-(\lambda_1 + \dots + \lambda_n)$. c'est $(-trf)$

Représentation géométrique associée à cette somme éventuellement



$E = E_{\lambda_1} \oplus \dots \oplus E_{\lambda_n} \oplus F$ ⟵ supplémentaire éventuel

les espaces prop. de f (stables par f)

<u>Définition</u>:

1) Soit $f : E \to E$ un endomorphisme, $\dim E = n$. On dit que f est <u>diagonalisable</u> <u>ssi</u> il existe une base $\mathcal{B}$ de E telle que $\mathrm{mat}_{\mathcal{B}} f$ est diagonale.

2) Soit $A \in M_n(\mathbb{K})$. On dit que A est <u>diagonalisable</u> si elle est semblable à une matrice diagonale, i.e. si $\exists P \in GL_n(\mathbb{K})$ tq $P^{-1}AP$ est diagonale.

<u>Objectif</u>: trouver des critères de "diagonalisabilité"

<u>Fait</u> (exercice) ☒. A est diagonalisable $\Leftrightarrow$ Φ_A est diagonalisable?

<u>Proposition</u>: Soit $f : E \to E$. On a l'équivalence des propriétés suivantes:

1) f est diagonalisable
2) E possède une base formée de vecteurs propres de f.
3) E est la somme directe des espaces propres de f

<u>Preuve</u>: <u>1) ⇒ 2)</u> Supposons f diagonalisable, soit $B = (u_1, \dots, u_n)$ une base de E t.q

$\mathrm{mat}_B f = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$, diagonale.

Alors [par déf. de la matrice] $\forall i = 1 \dots n$, $f(u_i) = \lambda_i u_i$ i.e. u_i est vecteur propre de f.

<u>2) ⇒ 1)</u> Soit $B = (u_1 \dots u_n)$ une base de vecteurs propres de f, donc $f(u_i) = \lambda_i u_i$ pour λ_i valeur propre associée à u_i. Ainsi $\mathrm{mat}_B f = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ et f est diagonalisable.

<u>3) ⇒ 2)</u>: Notons $\mu_1, \dots, \mu_k$ les valeurs de f, 2 à 2 distincts. ($k \leq n = \dim E$). Supposons $E = E_{\mu_1} \oplus \dots \oplus E_{\mu_k}$. Prenons une base de E adaptée à cette somme directe. Cette base est formée de vecteurs propres, CQFD. la réunion de bases est base de la réunion car somme directe

<u>1) ⇒ 3)</u> Supposons f diagonalisable, avec

$$\mathrm{mat}_B f = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \quad B = (u_1, \dots, u_n).$$

On a $P_f(X) = \begin{vmatrix} X - \lambda_1 & & 0 \\ & \ddots & \\ 0 & & X - \lambda_n \end{vmatrix} = (X - \lambda_1) \dots (X - \lambda_n)$.

$P_f(X)$ est scindé, de racines les termes diagonaux $\lambda_1, \dots, \lambda_n$, qui sont donc les valeurs propres de f. Quitte à réordonner les vecteurs $u_1, \dots, u_n$ on peut supposer

$$\mathrm{mat}_B f = \begin{pmatrix} \overbrace{\boxed{\begin{matrix}\mu_1 & \cdots & 0\\ 0 & & \mu_1\end{matrix}}}^{n_1} & & \\ & \boxed{\begin{matrix}\mu_2 & & \\ & \ddots & \\ & & \mu_2\end{matrix}} & \overbrace{\quad 0 \quad}^{n_k} \\ 0 & & \boxed{\begin{matrix}\mu_k & \\ & \mu_k\end{matrix}} \end{pmatrix}$$

avec $\mu_1, \dots, \mu_k$ 2 à 2 distincts.

On a alors : $x_1u_1 + \dots + x_nu_n \in E_{\mu_i} \iff \mathrm{mat}_B(f - \mu_i\, id)\begin{pmatrix}x_1\\ \vdots \\ x_n\end{pmatrix} = \begin{pmatrix}0\\ \vdots \\ 0\end{pmatrix}$

$$\iff \begin{array}{l} \\ \\ n_1+\dots+n_{i-1}+1 \\ n_1+\dots+n_i \\ \\ \\ \end{array} \begin{pmatrix} \boxed{\begin{matrix}\mu_1-\mu_i & \\ & \mu_1-\mu_i\end{matrix}} & & 0 \\ & \boxed{\begin{matrix}0 & \cdots & \\ & & 0\end{matrix}} & \\ 0 & & \boxed{\begin{matrix}\mu_k-\mu_i & \\ & \ddots \\ & & \mu_k-\mu_i\end{matrix}} \end{pmatrix} \begin{pmatrix}x_1\\ \vdots \\ \vdots \\ x_n\end{pmatrix} = \begin{pmatrix}0\\ \vdots \\ \vdots \\ 0\end{pmatrix}$$

$\iff$ toutes les coordonnées $x_1 \dots x_n$ sont nulles, sauf éventuellement celles associées au bloc $\boxed{\begin{matrix}\mu_i & \\ & \ddots & \\ & & \mu_i\end{matrix}}$ de $\mathrm{mat}_B f$ i.e. $x_{n_1+\dots+n_{i-1}+1}, \dots, x_{n_1+\dots+n_i}$

Autrement dit $E_{\mu_i} = \mathrm{vect}(u_{n_1+\dots+n_{i-1}+1}, \dots, u_{n_1+\dots+n_i})$.

Ceci montre $E = E_{\mu_1} \oplus \dots \oplus E_{\mu_k}$ [puisque la réunion des bases de E_{μ_i} donne la base B de E.]

Exemple : Soit $f : E \to E$ t.q. $\dim E = 4$ $\quad \mathrm{mat}_B f = \begin{pmatrix} 1 & & & 0 \\ & -1 & & \\ & & -1 & \\ 0 & & & 2\end{pmatrix}$ où $B = (u_1, u_2, u_3, u_4)$

On voit immédiatement que :

les valeurs propres de f sont 1 (simple)
-1 (double)
2 (simple)

et $E_1 = \mathrm{vect}(u_1)$
$E_{-1} = \mathrm{vect}(u_2, u_3)$
$E_2 = \mathrm{vect}(u_4)$.

Définition : Soit $f : E \to E$ endomorphisme, $\dim E = n$. Soit λ une valeur propre de f. On appelle

- multiplicité algébrique de la valeur propre λ la multiplicité m_λ de λ comme racine du polynôme caractéristique
- multiplicité géométrique de la valeur propre λ la dimension g_λ de l'espace propre E_λ associée.

Exemples : 1) $f : \mathbb{C}^2 \to \mathbb{C}^2$
$(x, y) \to (-y, x)$

$P_f(X) = (X-i)(X+i)$. $i, -i$ sont valeurs propres de multiplicité algébrique $m_i = m_{-i} = 1$ et de multiplicité géométrique $g_i = g_{-i} = 1$ (vu préc.)

2) $f : \mathbb{R}^2 \to \mathbb{R}^2$

$(x,y) \to (x+y, y)$

Alors $P_f(X) = (X-1)^2$. 1 est valeur propre de multiplicité algébrique $m_1 = 2$ (valeur propre "double") et de multiplicité géométrique $g_1 = 1$ (vu préc.)

On a $g_1 < m_1$. On verra que ça signifie que f n'est pas diagonalisable.

Théorème : Soit $f : E \to E$ $\dim E = n$.

Soient $\mu_1 \dots \mu_k$ les valeurs propres de f, 2 à 2 distinctes. On a :

1) $m_{\mu_1} + \dots + m_{\mu_k} \leq n$ avec égalité ssi P_f est scindé.

2) $g_{\mu_1} + \dots + g_{\mu_k} \leq n$

3) $\forall i = 1 \dots k$ $1 \leq g_{\mu_i} \leq m_{\mu_i}$

4) les propositions suivants sont équivalentes :

a) f est diagonalisable

b) $g_{\mu_1} + \dots + g_{\mu_k} = n$

c) P_f est scindé et $\forall i = 1 \dots k$, $g_{\mu_k} = m_{\mu_k}$.

Théorème $f : E \to E$ $\lambda_1, \dots, \lambda_k$ v.p. de f 2 à 2 $\neq$.

1) $m_{\lambda_1} + \dots + m_{\lambda_k} \leq n$ ($= \dim E$) avec égalité ssi P_f scindé

2) $g_{\lambda_1} + \dots + g_{\lambda_k} \leq n$

3) $\forall i$ $1 \leq g_{\lambda_i} \leq m_{\lambda_i}$

4) f diagonalisable $\Leftrightarrow g_{\lambda_1} + \dots + g_{\lambda_k} = n$

$\Leftrightarrow \forall i$ $g_{\lambda_i} = m_i$ et P_f est scindé

démo : 1) Comme λ_i est racine de P_f de multiplicité m_{λ_i}, on a $(X-\lambda_i)^{m_{\lambda_i}} | P_f$

On admet ici (voir prochain chapitre) qu'alors

$$(X-\lambda_1)^{m_{\lambda_1}} \dots (X-\lambda_k)^{m_{\lambda_k}} \mid P_f(X), \text{ i.e. } P_f(X) = (X-\lambda_1)^{m_{\lambda_1}} \dots (X-\lambda_k)^{m_{\lambda_k}} Q(X),$$

avec $Q(X) \in \mathbb{K}[X]$. On a alors

$$n = d^\circ P_f \; [= d^\circ (X-\lambda_1)^{m_{\lambda_1}} + \dots + d^\circ (X-\lambda_k)^{m_k} + d^\circ Q] = m_{\lambda_1} + \dots + m_{\lambda_k} + d^\circ Q.$$

Cela montre $m_{\lambda_1} + \dots + m_{\lambda_k} \leq n$.

Il y a égalité ssi $d^\circ Q = 0$, i.e. Q constant (non nul), donc $Q = 1$ puisque $P_f(X)$ est unitaire. Si $m_{\lambda_1} + \dots + m_{\lambda_k} = n$, alors $P_f(X) = (X-\lambda_1)^{m_{\lambda_1}} \dots (X-\lambda_k)^{m_{\lambda_k}}$ est scindé.

Réciproquement, supposons que $P_f(X)$ est scindé. Cela entraîne (par unicité de la factorisation, voir prochain chapitre, admis ici) que Q est scindé, de la forme $Q(X) = (X-\alpha_1) \dots (X-\alpha_l)$. Ainsi $P_f(X) = (X-\lambda_1)^{m_1} \dots (X-\lambda_k)^{m_k} (X-\alpha_1) \dots (X-\alpha_l)$.

Si $l \geq 1$, $\alpha_1 \dots \alpha_l$ sont des valeurs propres de f, cela contredit que les racines $\lambda_1 \dots \lambda_k$ sont de multiplicité $m_1, \dots, m_k$. Cela impose $l = 0$ i.e. $Q = 1$.

2) Soient E_{λ_i} l'espace propre associé à la valeur propre λ_i, avec $g_{\lambda_i} = \dim E_{\lambda_i}$.

On a vu que $E_{\lambda_1}, \dots, E_{\lambda_k}$ sont en somme directe. Soit F un supplémentaire de $E_{\lambda_1} \oplus \dots \oplus E_{\lambda_k}$ dans E :

$E = E_{\lambda_1} \oplus \dots \oplus E_{\lambda_k} \oplus F$.

Cela donne

$$n = \dim E = \dim E_{\lambda_1} + \dots + \dim E_{\lambda_k} + \dim F = g_{\lambda_1} + \dots + g_{\lambda_k} + \dim F$$

Cela montre $g_{\lambda_1} + \dots + g_{\lambda_k} \leq n$ avec l'égalité ssi $E = E_{\lambda_1} \oplus \dots \oplus E_{\lambda_k}$, i.e. ssi f est diagonalisable (première partie du point 4)

3) (***) comme λ_i est valeur propre de f, $E_{\lambda_i} \neq \{0\}$, donc $g_{\lambda_i} = \dim E_{\lambda_i} \geq 1$.

Prenons B_{λ_i} une base de E_{λ_i}, $i = 1 \dots k$.

Prenons F un supplémentaire de $E_{\lambda_1} \oplus \dots \oplus E_{\lambda_k}$ dans E et B_F une base de F.

Alors

$$\operatorname{mat}_B f = \begin{array}{c} \left(\begin{array}{cc|c|cc|c} \lambda_1 & 0 & & & & \\ 0 & \lambda_1 & & & & \\ \hline & & \ddots & & & C \\ \hline & & & \lambda_k & 0 & \\ & & & 0 & \lambda_k & \\ \hline & & & & & B \end{array}\right) \begin{array}{l} E_{\lambda_1} \\ \\ \\ E_{\lambda_k} \\ \\ F \end{array} \\ \underbrace{\qquad}_{g_{\lambda_1}} \ \cdots \ \underbrace{\qquad}_{g_{\lambda_k}} \ \underbrace{\quad}_{\dim F = l} \end{array}$$

On a alors

$$P_f(X) = \left|\begin{array}{cc|c|cc|c} X-\lambda_1 & 0 & & & & \\ 0 & X-\lambda_1 & & 0 & & \\ \hline & & \ddots & & & -C \\ \hline & 0 & & X-\lambda_k & 0 & \\ & & & 0 & X-\lambda_k & \\ \hline & 0 & & 0 & & XI_l - B \end{array}\right|$$

Cette matrice est triangulaire supérieure par bloc, cela donne :

$$P_f(X) = \begin{vmatrix} X-\lambda_1 & & 0 \\ & \ddots & \\ 0 & & X-\lambda_1 \end{vmatrix} \cdots \begin{vmatrix} X-\lambda_k & & 0 \\ & \ddots & \\ 0 & & X-\lambda_k \end{vmatrix} \det(XI_l - B)$$

$$= (X-\lambda_1)^{g_{\lambda_1}} \cdots (X-\lambda_k)^{g_{\lambda_k}} \cdot Q(X) \qquad \text{avec } Q(X) = \det(XI_l - B)$$

Cela montre que les racines λ_i de P_f sont de multiplicité $\geq g_{\lambda_i}$ i.e. $m_{\lambda_i} \geq g_{\lambda_i}$

<u>Remarque</u> : en général (par ex. sur $\mathbb{C}$) on ne pourra pas trouver de supplémentaire F stable par f, donc on aura $C \neq 0$ si $F \neq \{0\}$.

4) On a vu que f est diagonalisable <u>ssi</u> $g_{\lambda_1} + \dots + g_{\lambda_k} = n$.

Or $\underset{(\text{point } 3)}{g_{\lambda_1} + \dots + g_{\lambda_k} \leq m_{\lambda_1} + \dots + m_{\lambda_k}} \underset{(\text{point } 1)}{\leq n}$.

Donc $g_{\lambda_1} + \dots + g_{\lambda_k} = n \iff \left| \begin{array}{l} g_{\lambda_1} + \dots + g_{\lambda_k} = m_{\lambda_1} + \dots + m_{\lambda_k} \\ m_{\lambda_1} + \dots + m_{\lambda_k} = n \end{array} \right. \iff \left| \begin{array}{l} \forall i = 1 \dots k \ \ g_{\lambda_i} = m_{\lambda_i} \\ P_f \text{ est scindé (d'ap} \end{array} \right.$

<u>Exemples</u> : 1) $f : \mathbb{R}^2 \to \mathbb{R}^2$ t.q. $\operatorname{mat}_{\text{can}} f = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ n'est pas diagonalisable car

$P_f(X) = X^2 + 1$ n'est pas scindé (sur $\mathbb{K} = \mathbb{R}$)

2) $f : \mathbb{R}^2 \to \mathbb{R}^2$ t.q. $\mathrm{mat}_{can} f = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ n'est pas diagonalisable car 2 est valeur propre de f de multiplicité algébrique 2, $P_f(X) = (X-2)^2$ et de multiplicité géometrique 1. $E_2 = \mathrm{vect}((1,0))$: $1 = g_2 < m_2 = 2$.

3) $f : \mathbb{C}^2 \to \mathbb{C}^2$ t.q. $\mathrm{mat}_{can} f = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est diagonalisable car $P_f(X) = (X-i)(X+i)$,

$1 = g_i = m_i = 1 \qquad 1 = g_{-i} = m_{-i} = 1.$

Remarque : si λ est valeur propre simple de f, i.e. de multiplicité algébrique 1, alors $1 = g_\lambda = m_\lambda = 1$.

Les valeurs propres simples ne posent pas de problème à la diagonalisation.

Exemple : si $f : \mathbb{R}^7 \to \mathbb{R}^7$ a pour valeur propre

0 mult. $m_0 = 1$
-1 " $m_{-1} = 1$
2 " $m_2 = 3$
4 " $m_4 = 2$

alors

1) P_f est scindé $P_f(X) = X(X+1)(X-2)^3(X-4)^2$
2) E_0, E_{-1} sont des droites
3) f est diagonalisable ssi $\left| \begin{array}{l} \dim E_2 = 3 \\ \dim E_4 = 2 \end{array} \right.$

Corollaire : Soit $f : E \to E$. Si P_f est scindé et n'a que des racines simples, alors f est diagonalisable.

démo : le point 4 du théorème est rempli.

Exemple : $f : \mathbb{R}^5 \to \mathbb{R}^5$ t.q. $\mathrm{mat}_{can} f = \begin{pmatrix} 1 & -1 & 2 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 4 \end{pmatrix}$ est diagonalisable

$\mathbb{R}^5 = \underbrace{E_1 \oplus E_0 \oplus E_{-1} \oplus E_2 \oplus E_4}_{\text{droites vectorielles}}$

$\exists P \in GL_5(\mathbb{R})$ t.q. $P^{-1} \mathrm{mat}_{can} f \cdot P = \begin{pmatrix} 1 & & & & \\ & 0 & & & \\ & & -1 & & \\ & & & 2 & \\ & & & & 4 \end{pmatrix}$

en effet $P_f(X) = \begin{vmatrix} X-1 & & & * & \\ & X & & & \\ & & X+1 & & \\ & 0 & & X-2 & \\ & & & & X-4 \end{vmatrix} = (X-1)X(X+1)(X-2)(X-4)$

Arithmétique approfondie et applications à la réduction des endomorphismes.

I. Arithmétique dans les anneaux principaux.

Soit $(A, +, \times)$ un anneau commutatif
- $(A, +)$ groupe commutatif
- $\times$ possède un neutre
- $\times$ associative
- $\times$ est distributive par rapport à $+$ $\quad \forall a,b,c \in A \quad a\times(b+c) = a\times b + a\times c$.

A est commutatif si $\times$ est commutative

Exemple : $(\mathbb{Z}, +, \times)$ est un anneau commutatif
$(\mathbb{K}[X], +, \times)$ " " " (si $\mathbb{K}$ est un corps)
$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ " " "

$(M_n(\mathbb{K}), +, \times)$ est un anneau non commutatif.

On s'intéressera à l'arithmetique dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$, donc on pourra faire $A = \mathbb{Z}$ ou $A = \mathbb{K}[X]$ dans les définitions suivantes:

<u>Définition</u>: 1) Un élément $a \in A$ est dit <u>inversible</u> s'il existe $b \in A$ t.q.

$$ab = ba = 1$$

2) a est un diviseur de 0 si $a \neq 0$ et s'il existe $b \in A \setminus \{0\}$ t.q. $ab = 0$.

3) si $a, b \in A$, on dit que $a | b$ s'il existe $c \in A$ t.q. $b = ac$.

On note A^* ou $A^\times$ ou $U(A)$ l'ensemble des éléments inversibles de A.

<u>Proposition</u>: $(U(A), \times)$ est un groupe.

<u>démo</u>: exercice.

<u>Exemple</u>: 1) $U(\mathbb{Z}) = \{+1, -1\}$ (exercice)

2) On a vu que $U(\mathbb{K}[X]) = \{P \in \mathbb{K}[X] \,/\, d°P = 0\} = \{$pol. constants non nuls$\}$

3) $\mathbb{Z}$ n'a pas diviseur de 0 (non nul). On a vu que $\mathbb{K}[X]$ non plus.

<u>Définition</u>: On dit qu'un anneau est <u>intègre</u> s'il n'a pas de diviseur de 0,

i.e. si $\forall a, b \in A$, $ab = 0 \Rightarrow (a = 0$ ou $b = 0)$

i.e. si $\forall a, b \in A$, $(a \neq 0$ et $b \neq 0) \Rightarrow ab \neq 0$.

<u>Exemple</u>: $(\mathbb{Z}/6\mathbb{Z}, +, \times)$ n'est pas intègre: $\bar{2} \cdot \bar{3} = \bar{0}$.

<u>Proposition</u>: Si A est intègre, alors $\forall a, b, c \in A$, $\begin{pmatrix} ac = bc \\ \text{et} \\ c \neq 0 \end{pmatrix} \Rightarrow a = b$

<u>démo</u>: déjà vu.

<u>Proposition</u>: Soit A un anneau commutatif intègre. Soit $a, b \in A \setminus \{0\}$. On a l'équivalence

1) des propositions suivants $a | b$ et $b | a$.

2) $\exists \lambda \in U(A)$ t.q. $b = \lambda a$

3) a et b ont même diviseurs. Deux tels élements sont dits <u>associés</u>.

<u>démo</u>: 2) $\Rightarrow$ 1) et 2) $\Rightarrow$ 3) sont faciles, exercice.

1) $\Rightarrow$ 2) supposons $a | b$ et $b | a$. Donc $\exists c, d$ t.q. $\left| \begin{array}{l} b = ac \\ a = db \end{array} \right.$. Donc $a = acd$.

Or $a = acd$. Or $a \neq 0$ donc d'après la proposition précédente, $1 = cd$.

ceci montre $c \in U(A)$, $d \in U(A)$.

3) $\Rightarrow$ 1) Supposons que a et b ont même diviseurs.

Comme $a | a$, cela implique $a | b$. De même $b | b$ donc $b | a$.

<u>Exemple</u>: 1) 6 et -6 sont associés dans $\mathbb{Z}$

2) $X - 1$, $2X - 2$, $\frac{1}{\pi}(X - 1)$ sont associés dans $\mathbb{R}[X]$.

Morphisme de groupes

Un morphisme de groupes ou homomorphisme de groupes est un application entre deux groupes qui respecte la structure de groupe.
Plus précisement, si $(G,*)$ et $(G',*)$ sont deux groupes, une application $f : G \to G'$ est un morphisme de groupes lorsque

$$\forall x,y \in G \quad f(x*y) = f(x)*f(y)$$

On en déduit alors que
- $f(e)=e'$ (où e et e' désignent les neutres respectifs de G et G')
- $\forall x \in G \quad f(x^{-1}) = [f(x)]^{-1}$.

Exemple : $\begin{array}{l}\mathbb{C} \to \mathbb{C}^* \\ z \mapsto e^z\end{array}$ vérifie $e^{z+z'} = e^z \times e^{z'}$

C'est donc un morphisme de groupes de $(\mathbb{C},+)$ dans $(\mathbb{C}^*,\times)$ et – par restriction – de $(\mathbb{R},+)$ dans $(\mathbb{R}^*_+,\times)$.

Isomorphisme de groupes

Un isomorphisme de groupes est un morphisme de groupes qui est bijectif.
Lorsqu'il existe un isomorphisme du groupe G vers le groupe G', sa bijection réciproque est un isomorphisme du groupe G' vers le groupe G; on dit alors que les deux groupes sont isomorphes, ce que l'on note $G \simeq G'$.

Automorphismes de groupe

Un automorphisme de groupe est un morphisme qui est à la fois un isomorphisme de groupes et un endomorphisme de groupe.
L'ensemble des automorphismes du groupe G est généralement noté $Aut(G)$
C'est un sous-groupe du groupe des bijections de G dans G (muni de la loi de composition).

Si $\left| \begin{array}{l} rg(e_1,e_2)=2 \\ rg(e_1,e_2,e_3)=2 \end{array} \right.$ alors $e_3 \in vect(e_1,e_2)$

Sous-espace stricte

$A \subsetneq E \iff E \setminus A \neq \emptyset$

F sev stricte de $E \Rightarrow$ il existe un vecteur dans $E \setminus F$ (non nul)

E espace vectoriel
si $F \subset G$ et $\dim F = \dim G$ alors $F = G$.

$\forall\ w = f(v) \in f(A)$
$w = f(a_1 x_1 + \dots + a_n x_n) = a_1 f(x_1) + \dots + a_n f(x_n)$
or $\forall x_i \in X \ f(x_i) \in A$ donc $\underline{w \in A}$

Fait : Si $A = vect(X)$, $X \subset E$, alors A est stable par f (i.e. $f(A) \subset A$) <u>ssi</u>
$f(X) \subset A$ i.e $\forall x \in X,\ f(x) \in A$.

Demo : $(\Rightarrow)$ trivial $f(X) \subset f(A) \subset A$ (par déf, $f(A) \subset A$ dit que $\forall v \in A,\ f(v) \in A$ donc nécessairement, $\forall x \in X \subset A,\ f(x) \in A$)
$(\Leftarrow)$ car tout vecteur de A est CL de vecteurs de X et f est linéaire

Remarque

Si τ est une transposition alors $\tau^2 = Id$ et $\tau^{-1} = \tau$.

Plus généralement :

Proposition :

Si c est un cycle de longueur p alors $c^p = Id$ et $c^{-1} = c^{p-1}$

Preuve :

Soit $c = (a_1\ a_2\ \dots\ a_p)$ un p cycle (avec des $a_1, \dots, a_p$ deux à deux distincts). $c^0(a_1) = a_1$, $c(a_1) = a_2$, $c^2(a_1) = a_3, \dots, c^{p-1}(a_1) = a_p$ donc pour tout $1 \leq k \leq p-1$, $c^k(a_1) = a_{k+1}$ et par suite $c^p(a_1) = c(a_p) = a_1$.

Pour $2 \leq k \leq p$, $c^p(a_k) = c^p(c^{k-1}(a_1)) = c^{p+k-1}(a_1) = c^{k-1}(c^p(a_1)) = c^{k-1}(a_1) = a_k$

Enfin pour $x \in \mathbb{N}_n \setminus \{a_1, \dots, a_p\}$, $c(x) = x$ donc $c^p(x) = x$.

Finalement $c^p = Id$.

+ Cours : Une somme des sous-espaces stables est stable.

Fait : Si $f(x) = \lambda \cdot x$, $\lambda \in \mathbb{K}$, $vect(x)$ est stable par f.

+ Cours : On dit que f est une projection (linéaire) ou un projecteur (linéaire) s'il existe F, G supplémentaires dans E tq. $f = p_{F,G}$

, Pour vérifier que des vecteurs colonnes sont liées, leur déterminant doit être zéro.

Fait : $\forall \sigma \in S_n$, $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$

$\varepsilon(\sigma^{-1}) \cdot \varepsilon(\sigma) = \varepsilon(id) = 1$ donc $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)^{-1} = \varepsilon(\sigma)$ $\left(\frac{1}{-1} = -1,\ \frac{1}{1} = 1\right)$

$f : E \times F \to G$
$(u, v) \to f(u, v)$ est linéaire "en u" ou "par rapport à la 1ère composante"
si $\forall \lambda, \lambda' \in \mathbb{K}$, $\forall u, u' \in E$, $f(\lambda u + \lambda' u', v) = \lambda f(u, v) + \lambda' f(u', v)$.

Ex : $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(x, x') \to xx'$

$f : \mathbb{R}^2 \to \mathbb{R}^2 \to \mathbb{R}$, $((x,y),(x',y')) \to (x+y)(x'+y')$

$f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$, $((x,y),(x',y')) \to xx' + yy'$.

‼ On peut pas faire 2 opérations à la fois :

$$\det(C_1\ C_2\ C_3) = \det(C_1 + 2C_2 - C_3\quad C_2 - C_3\quad C_3)$$
$$= \det(C_1 + 2C_2 - C_3\quad C_2\quad C_3)$$

J'ai le droit de faire ça mais je peux pas faire $C_2 + C_1$ car C_1 est modifié.

$$\det(C_1\ C_2\ C_3) \neq \det(C_1 + C_2\quad C_2 + C_1\quad C_3)$$

On doit faire les opérations une par une pas à la fois.

. On change pas le déterminant si on additionne aux colonnes une C.L. des colonnes précédentes (colonnes suivantes).

$$\det\begin{pmatrix} \boxed{D_1} & & * \\ & \boxed{D_2} & \\ 0 & & \boxed{D_n} \end{pmatrix} = \det D_1 \cdot \det D_2 \cdots \det D_n$$ (matrice triangulaire par bloc)

. rang d'une matrice = dim ev engendré par les lignes = dim ev engendré par les colonnes.