Théorème.

> Soit $(G, \star)$ un groupe fini. Alors tous ses éléments sont d'ordre fini.
> Plus précisément, pour tout $a \in G$:
> $$\text{ordre}(a) \mid \text{Card}(G)$$
> c'est-à-dire que $a^{\text{Card}(G)} = e$.

Corollaire. Tout groupe fini dont le cardinal est premier est cyclique, et engendré par chacun de ses éléments différent du neutre.

$n = \text{Card}(G)$ Cas où $\star$ commutative

$a \in G$, mq a d'ordre fini et ordre$(a) \mid n$

(On va mq $a^n = e$)

On énumère les éléments de $G = \{g_1, g_2, \dots, g_n\}$

$$g_1 \star \dots \star g_n = g_2 \star g_n \star g_1 \star \dots \quad \star \text{ commutative}$$

$$= g_{\sigma(1)} \star g_{\sigma(2)} \star \dots \star g_{\sigma(n)} \quad \text{où } \sigma \in \mathfrak{S}_n$$

$$\phi : \begin{array}{l} G \longrightarrow G \\ x \longmapsto a \star x \end{array} \quad \text{est bijective : } \phi^{-1} : x \mapsto a^{-1} \star x$$

donc ϕ correspond à une permutation "mélange les élts de G"

Donc $g_1 \star \dots \star g_n = \phi(g_1) \star \dots \star \phi(g_n)$

$$= (a \star g_1) \star \dots \star (a \star g_n)$$

$$= a^n \star (g_1 \star \dots \star g_n)$$

$\times (g_1 \dots g_n)^{-1}$

donc $e = a^n$

donc a est d'ordre fini, et $a^n = e$ donc ordre$(a) \mid n$.

Pour lu : un ex à rédiger

Pour ma : 22.1, 21.23, 21.34

Compléments sur les matrices

Je me souviens

1. Qu'est-ce qu'une **matrice** ?
2. À quoi ça sert ?
3. Qu'est-ce que la matrice d'un vecteur ? d'une famille de vecteurs ? d'une application linéaire ?

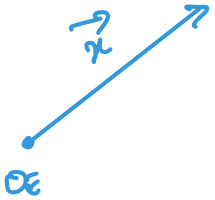
(1) Tableau de scalaires

E ev — $\mathbb{R}^3$, $\mathbb{R}^{\mathbb{N}}$, $\mathbb{K}_n[X]$, $\mathcal{C}^0(\mathbb{R},\mathbb{R})$

(3)

- Soit E ev, $\mathcal{B} = (e_1 \dots e_n)$ base de E

$\vec{x} \in E$



$$X = \mathrm{Mat}_{\mathcal{B}}(\vec{x}) = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad \text{où} \quad \vec{x} = \sum_{i=1}^{n} a_i \vec{e_i}$$

les coord de x dans $\mathcal{B}$

$$\begin{array}{ccc} E & \overset{\mathcal{B}}{\longleftrightarrow} & \mathcal{M}_{n1}(\mathbb{K}) \\ \vec{x} & & X \end{array}$$

- Soit E ev $\mathcal{B} = (e_1 \dots e_n)$ base de E

$x_1, \dots, x_p \in E$

$$\mathrm{Mat}_{\mathcal{B}}(x_1, \dots, x_p) = \begin{array}{c|c} \begin{array}{cccc} x_1 & x_2 & \dots & x_p \end{array} & \\ \begin{pmatrix} & & & \\ & & & \\ & & & \\ & & & \end{pmatrix} & \begin{array}{c} e_1 \\ e_2 \\ \vdots \\ e_n \end{array} \end{array}$$

en colonne les coord de $x_1, \dots x_p$

$$= \left(X_1 \,\middle|\, X_2 \, \dots \,\middle|\, X_p \right)$$

où $\quad X_k = \mathrm{Mat}_{\mathcal{B}}(x_k)$

- Soit $u = \mathcal{L}(E, F)$ $\qquad u : E \longrightarrow F$

$\mathcal{B} = (e_1 \dots e_p)$ base de E

$\mathcal{C} = (f_1 \dots f_n)$ base de F

$$\mathrm{Mat}(u, \mathcal{B}, \mathcal{C}) = \begin{array}{c|c} \begin{array}{ccc} u(e_1) & \dots & u(e_p) \end{array} & \\ \begin{pmatrix} & & \\ & & \\ & & \\ & & \end{pmatrix} & \begin{array}{c} f_1 \\ \vdots \\ \\ f_n \end{array} \end{array}$$

$$= \mathrm{Mat}_{\mathcal{C}}\left(u(e_1) \dots \; u(e_p)\right)$$

4. Y a-t-il un isomorphisme entre les applications linéaires et les matrices ?

Si notations $\mathcal{B}, \mathcal{C}$ fixées

$$\phi : \mathcal{L}(E,F) \longrightarrow \mathcal{M}_{n,p}(\mathbb{K})$$
$$u \longmapsto \mathrm{Mat}(u, \mathcal{B}, \mathcal{C})$$

isomorphisme d'ev

5. Qu'est-ce que l'application linéaire canoniquement associée à une matrice ?

6. Que sont l'image et le noyau d'une matrice ?

3 types d'exercices :

- Soit $E = \mathbb{R}^3$ muni de sa base canonique

  $u \in \mathcal{L}(\mathbb{R}^3)$ tq - - -

  ev $\hookrightarrow$ matrice $\mathbb{R}^3$

  $A = \mathrm{Mat}(u, \mathrm{can})$

- Soit E ev de dim 3 — $\mathbb{R}^3$, $\mathbb{R}_2[X]$, $\mathrm{Vect}(\cos, \sin, \sqrt{\ })$

  $\mathcal{B} = (e_1, e_2, e_3)$ base

  $u \in \mathcal{L}(E)$ tq

  ev $\hookrightarrow$ matrice abstrait

  $\mathrm{Mat}(u, \mathcal{B}) = \begin{pmatrix} \cdot & - & - \\ \cdot & - & - \\ \cdot & - & - \end{pmatrix}$

- Soit $A = \begin{pmatrix} - & - & \cdot \\ \vdots & - & \vdots \\ - & - & - \end{pmatrix}$

matrice

$\leftrightarrow$ ev

puis questions - - -

Soit u canoniquement associée à A.

$$u : \mathcal{M}_{n1}(\mathbb{K}) \longrightarrow \mathcal{M}_{n1}(\mathbb{K})$$
$$X \longmapsto AX$$

- <u>Noyau d'une matrice</u>

$$A \in \mathcal{M}_{np}(\mathbb{K}) \longleftrightarrow \begin{array}{rcl} \mathcal{M}_{p1}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{n1}(\mathbb{K}) \\ X & \longmapsto & AX \end{array}$$

$$X \in \operatorname{Ker} A \iff AX = 0$$

De même $\quad Y \in \operatorname{Im} A \iff \exists X \in \mathcal{M}_{p1}(\mathbb{K})$ tq $Y = AX$.

base de $\mathcal{M}_{p1}(\mathbb{K})$: $E_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdots \quad E_p = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$

$$\operatorname{Im} A = \operatorname{Vect}(AE_1, \dots, AE_p)$$

$$A E_j = \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} \begin{array}{c} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \end{array} \begin{array}{l} \\ \\ \\ \leftarrow j \\ \\ \\ \\ \end{array}$$

$= C_j$ la j^e colonne de A

$\mathrm{Im}(A) = \mathrm{Vect}(C_1 \ldots C_p)$ C_j colonne de A

$= \mathrm{Vect}($les colonnes de $A)$

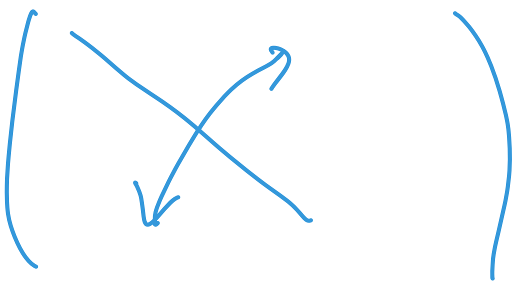
7. Qu'est-ce que le **rang** d'une matrice ?

8. Qu'est-ce que la **transposée** d'une matrice ?

9. Qu'est-ce que la **trace** d'une matrice ?

$$\mathrm{rg}(A) = \dim(\mathrm{Im}\, A)$$
$$= \dim \mathrm{Vect}(C_1 \dots C_p)$$
$$= \mathrm{rg}(\text{famille des colonnes})$$

$$A \in \mathcal{M}_{np}(\mathbb{K})$$
$$A^T = (a'_{ij}) \in \mathcal{M}_{pn}(\mathbb{K})$$
$$\forall i,j \quad a'_{ij} = a_{ji}$$



Trace: $\mathrm{tr}(A)$ $\qquad A \in \mathcal{M}_n(\mathbb{K})$

$= $ somme des coeff diagonaux.

- $$\mathrm{tr} : \overset{+,\ \cdot,\ \times}{\mathcal{M}_n(\mathbb{K})} \longrightarrow \mathbb{K}$$
$$A \longmapsto \mathrm{tr}(A)$$

$$\mathrm{tr}(\lambda A + \mu B) = \lambda\, \mathrm{tr}(A) + \mu\, \mathrm{tr}(B)$$

tr linéaire, c'est <u>une forme linéaire</u>

- $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ ⚠ $AB \neq BA$

↳ à savoir démontrer.

<u>M1</u> : Soit $A = (a_{ij})_{1 \leq i,j \leq n}$

$B = (b_{ij})$

$AB = (c_{ij})$

$BA = (d_{ij})$

<u>M2</u> : On note $[M]_{ij}$ le coeff ij de M.

$$[AB]_{ij} = \sum_{k=1}^{n} [A]_{ik} [B]_{kj}$$

donc $$\mathrm{tr}(AB) = \sum_{i=1}^{n} [AB]_{ii}$$

$$= \sum_{i=1}^{n} \sum_{k=1}^{n} [A]_{ik} [B]_{ki}$$

$$= \sum_{k=1}^{m} \sum_{i=1}^{m} [B]_{ki} [A]_{ik}$$

$$= \sum_{k=1}^{n} [BA]_{kk}$$

$$= tr(BA)$$

<u>Rmq</u> :

$$tr(ABC) \neq tr(BAC)$$

$$tr(ABC) = tr((A)(BC))$$

$$= tr((BC)(A))$$

1 Matrice comme tableau de scalaires

1.1 Structure d'espace vectoriel de $\mathcal{M}_{np}(\mathbb{K})$

Proposition. Soit n, p, q des entiers. L'application $\begin{array}{ccc} \mathcal{M}_{np}(\mathbb{K}) \times \mathcal{M}_{pq}(\mathbb{K}) & \to & \mathcal{M}_{nq}(\mathbb{K}) \\ (A, B) & \mapsto & A \times B \end{array}$ est bilinéaire.

En passant.

$$\boxed{AB = 0 \iff \operatorname{Im} B \subset \operatorname{Ker} A}$$

Proposition. $(\mathcal{M}_{np}(\mathbb{K}, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel. Il est de dimension finie np.

Définition. La **base canonique** de $\mathcal{M}_{np}(\mathbb{K})$ est $(E_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ où les coefficients de E_{ij} sont tous nuls, sauf celui de la i-ème colonne, j-ème ligne qui vaut 1.

Remarque. *Ainsi, pour $A = (a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$, on a :*

$$A = \sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}} a_{ij} E_{ij}$$

Proposition. Si les dimensions des matrices sont compatibles, par exemples pour des matrices carrées, on a :

$$E_{ij} \times E_{k\ell} = \delta_{jk} E_{i\ell}$$

Proposition. $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$ est une algèbre, non commutative et non intègre.

Proposition. $(\mathrm{GL}_n(\mathbb{K}), \times)$ est un groupe, non commutatif.

Remarque. *Il est remarquable que, pour une matrice carrée, l'existence d'un inverse à droite ou à gauche soit équivalent à l'existence d'un inverse.*

$(\mathcal{M}_n(\mathbb{K}), +, \times)$ est anneau, non commutatif
non intègre

$(\mathcal{M}_n(\mathbb{K}), +, \cdot)$ est un ev

et $\times$ et $\cdot$ se comportent bien entre elles :

$$\lambda.(A \times B) = (\lambda.A) \times B$$
$$= A \times (\lambda.B)$$

c'est une algèbre.

$(GL_n(\mathbb{K}), \times)$ groupe