[MP – MATHEMATIQUES 1]

Contre-exemples

- Fonction de $\mathbb{R}$ dans $\mathbb{R}$ qui a toutes ses dérivées nulles en 0, sans être identiquement nulle.
  $t \to e^{-\frac{1}{t^2}}$
- Fonction de $\mathbb{R}$ dans $\mathbb{R}$ telle que $\forall x \in \mathbb{R}_+$, $f(nx) \to 0$ et $f(x)$ diverge en $+\infty$.
  $t \to 1$ si $\exists p \in \mathbb{N}$, $t = e^p$, et 0 sinon.
- Fonction de $\mathbb{R}_+$ dans $\mathbb{R}_+$ non bornée mais intégrable sur $\mathbb{R}_+$.
  Fonction triangles très minces.
- Fonction de $\mathbb{R}^2$ dans $\mathbb{R}$ continue selon tout vecteur en 0 mais pas continue en 0
  $(x, y) \to \text{Heaviside}(\rho - 2\pi + \theta) \in \mathcal{F}(\mathbb{R}^2, \mathbb{R})$.
- Deux fermés de E ev normé, de distance nulle et pourtant disjoints.
  $\{ (x, y) \in \mathbb{R}^2 / xy = 1 \}$ et $\{ (0, y) / y \in \mathbb{R} \} \subset \mathbb{R}^2$.
- $u \in GL(E)$, F sev. $u(F) \subset F$ et $u(F) \neq F$.
  $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$. Soit $T \in E^E$ définie par $T(f)(x) = f(x - 1)$. $T \in GL(E)$ car on connaît T^{-1}.
  $F = \{ f \in \mathbb{R}^{\mathbb{R}} / \forall x \geq 0, f(x) = 0 \}$ sev de $\mathbb{R}^{\mathbb{R}}$. $T(F) = \{ f \in \mathbb{R}^{\mathbb{R}} / \forall x \geq -1, f(x) = 0 \} \subset F$.
- Suite décroissante de fermés non vides de $\mathbb{R}$ d'intersection vide.
  $[n, +\infty[$
- Deux normes dont aucune n'est plus fine que l'autre.
  $E = \mathbb{R}[X]$. On définit N_1 et N_2 par : $N_1(P) = \sup(P[0, 1])$ et $N_2(P) = \sup(P[2, 3])$
- Une suite dont l'ensemble des valeurs d'adhérence est non borné.
  u_n = zigzag de plus en plus grands
- Deux séries de nature différente, de terme général équivalent.
  $\sum_{n=1}^{\infty} \frac{(-1)^n}{\sqrt{n}}$ converge mais pas $\sum_{n=1}^{\infty} \frac{(-1)^n}{\sqrt{n}} + \frac{1}{n}$.
- Deux séries de terme général équivalent qui ne sont pas équivalentes :
  $\frac{1}{n^2} \sim \frac{1}{n(n+1)}$ or $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \not\sim \sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1$
- Une fonction non continue mais qui possède la propriété de la valeur intermédiaire.
  Avec $f : x \to x^2 \sin\left(\frac{1}{x}\right)$, f ' vérifie ces propriétés en 0.
- Une fonction numérique qui a une tangente verticale et qui est continue à droite et à gauche.
  $x \to \sqrt{|x|}\,\frac{x}{|x|}$ prolongée en 0
- Une fonction de $\mathbb{R}^2$ dans $\mathbb{R}$ telle que les applications partielles soient continues en 0 sans qu'elle ne le soit.
  $(x, y) \to \left((x, y) \neq (0, 0) \,?\, \frac{xy}{x^2 + y^2} : 0\right)$
- Une fonction de $\mathbb{R}^2$ dans $\mathbb{R}$ telle qu'elle admette des dérivées selon tout vecteur en 0 mais ne soit pas différentiable.
  $(x, y) \to \left(y \neq 0 \,?\, \frac{x^2 + y^2}{y} : 0\right)$
- Une injection de $\mathbb{R}^2$ dans $\mathbb{R}$

$$\left(\varepsilon_a \sum_{k=-\infty}^{\infty} a_k 10^k, \varepsilon_b \sum_{k=-\infty}^{\infty} b_k 10^k\right) \in \mathbb{R}^2 \to \sum_{n=0}^{\infty} a_k 10^{2k+1} + b_k 10^{2k+2} + a_{-k-1} 10^{-2k-1} + b_{-k-1} 10^{-2k-2} + (\varepsilon_a + 1) + 2(\varepsilon_b + 1).$$

❑ Exemple de paradoxe

Soit A l'ensemble des mots de la langue française, que l'on peut trouver dans un dictionnaire de mots français donné. Par exemple, "mot" appartient a A, et "mjgiod" n'appartient pas à A. Remarquons que A est fini.

Soit $B = \bigcup_{n \in \mathbb{N}^*} A^n$

Soit C la partie de B pour laquelle chaque élément correspond a un unique entier naturel.

("un") ∈ C.

("un", "plus" ,"deux") ∈ C (c'est trois)

("un", "deux", "plus") ∉ C (pas de sens)

("nombre", "de", "lettres", "dans", "bonne") ∈ C (c'est 5)

("le", "nombre", "précédent") ∉ C (l'unicité n'est pas respectée)

("mojdi") ∉ C.

("nombre", "de", "lettres", "dans", "mojdi") ∉ C (mojdi n'est pas dans le dictionnaire)

On note f l'application qui part de C vers ℕ, qui a un uplet de mots associe le nombre en question.

f("trois") = 3

f("trois", "fois", "deux") = 6

On note C_n la partie de C pour laquelle chaque élément est un n-uplet. C_n est inclus dans A^n.
Remarquons que puisque A est fini, C_n est fini.

Soit $D = f\{C_1 \cup C_2 \cup ... \cup C_{20}\}$ Soit j = 1 + Max D.
j existe car $C_1 \cup C_2 \cup ... \cup C_{20}$ est fini.
Max D est le plus grand nombre qui puisse se caractériser en 20 mots ou moins.

Soit k = ("un", "plus", "le", "plus", "grand", "nombre", "qui", "puisse", "se", "caractériser", "en", "vingt", "mots", "ou", "moins").
Il est évident que f(k) = j, mais $k \in C_{15}$ implique que $j \in D$.
Donc Max D ≥ j. Donc j - 1 ≥ j
Contradiction.

ALGEBRE DE BASE

1 – Groupes

• Définition : Groupe → LCI associative avec existence du neutre et de symétriques. (Voir cours de MPSI)
• Sous-groupe

H ⊂ G est un sous-groupe de $(G, \times)$ si $\begin{cases} \forall (x,y) \in H^2, xy \in H \\ e \in H \\ \forall x \in H, x^{-1} \in H. \end{cases}$

• Morphisme
[...] L'application $\varphi_a : x \in G \to axa^{-1} \in G$ est appelé automorphisme intérieur. Si G abélien, $\varphi_a = Id_G$.
Les translations $x \in G \to ax \in G$ et $x \in G \to xa$ sont bijectives mais ne sont pas des morphismes de groupes.
L'application $x \in G \to x^{-1}$ est involutive mais pas toujours un morphisme.
(Th) $\text{Ker } f = \{ e_G \} \Leftrightarrow f$ injective.
• Produit de 2 groupes
Soient G et H deux groupes. On définit une LCI sur $G \times H$ par $(x, y) * (x', y') = (x * x', y * y')$.
(Th) $G \times H$ est alors un groupe pour la loi produit. Ex : $(\mathbb{R}^2, +)$
• Sous-groupe engendré par une partie
[... Définition usuelle ...] $A \neq \emptyset$.
Le sous-groupe engendré par A est $H = \{ x_1x_2...x_q, q \in \mathbb{N}^*, (x_1, ..., x_q) \in (A \cup A^{-1})^q \}$.
• L'ensemble des éléments inversibles est un groupe (Ex)
Soit $(M, *)$ un monoïde, et G l'ensemble des éléments inversibles de M. Alors G est un groupe. (demo que G est stable)
C'est utile surtout quand M est un anneau.
Ex : $\mathbb{Z}[i] = \{x + iy, (x,y) \in \mathbb{Z}^2\}$ a pour éléments inversibles $\mathbf{U}_4 = \{ 1, -1, i, -i \}$. [~d]
Ex : $\mathcal{M}_n(\mathbb{R})$ a pour éléments inversibles $GL_n(\mathbb{R})$.
• #G = #Ker f × #Im f (Ex)
f : G → H est un morphisme de groupe. Alors #G = #Ker f . #Im f. [on compte les antécédents de chacun]

2 – Groupes $\mathbb{Z}/n\mathbb{Z}$

I Construction de $\mathbb{Z}/n\mathbb{Z}$

1 – Les sous-groupes de $\mathbb{Z}$

(Th) Les sous groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$. [demo pareil que sup]

2 – Relation de congruence

$\forall n \in \mathbb{N}^*, \forall (a, b) \in \mathbb{Z}^2, a \equiv b\ [n] \Leftrightarrow n \mid b - a$.
(Th) C'est une relation d'équivalence.

3 – Groupe $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$.
$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence (ou ensemble quotient) pour la relation ≡.
(Th) $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien fini, de cardinal n. [d]

4 – Morphisme canonique de $\mathbb{Z}/n\mathbb{Z}$

Le morphisme canonique de $\mathbb{Z}/n\mathbb{Z}$ est l'application : $k \in \mathbb{Z} \to \bar{k} \in \mathbb{Z}/n\mathbb{Z}$. C'est un morphisme.

II Sous-groupe engendré par un élément

Soit G un groupe et $a \in G$.
Le sous-groupe engendré par a est $gr(a) = \{ a^k, k \in \mathbb{Z} \}$. Par convention, $a^0 = e$.

Soit $\varphi : k \in \mathbb{Z} \to a^k \in gr(a)$. C'est un morphisme de groupe surjectif.
Ker $\varphi = \{ k \in \mathbb{Z}, a^k = e \}$ est un sous-groupe de $\mathbb{Z}$. $\to \exists n \in \mathbb{N}$, Ker $\varphi = n\mathbb{Z}$.
Si n = 0, Ker $\varphi = \{0\}$
φ est alors bijective, et gr(a) est isomorphe à $(\mathbb{Z}, +)$.
Ex : $G = (\mathbb{R}^*, \times)$ et $a = 2$. $gr(2) = \{ 2^k, k \in \mathbb{Z} \}$ est un groupe isomorphe à $(\mathbb{Z}, +)$.
Si $n \geq 1$, Ker $\varphi = n\mathbb{Z}$
Soit G un groupe et $a \in G$. On suppose Ker $\varphi = n\mathbb{Z}$, $n \geq 1$.
(Th) Alors gr(a) est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
(Th) $\bar{\varphi} : \bar{k} \in \mathbb{Z}/n\mathbb{Z} \to a^k \in gr(a)$ est un isomorphisme de groupe. [justifications et demo]

Soit a élément d'un groupe G, et H le sous-groupe engendré par a.
∗ Si H est isomorphe à $\mathbb{Z}$, a est d'ordre ∞.
∗ Sinon, on appelle l'ordre de a $\text{Min}\{ k \in \mathbb{N}^*, a^k = e \}$

III Groupes cycliques

1 – Définition

Soit G un groupe. On dit que G est cyclique si G est fini et engendré par un élément.
Si G est un groupe cyclique de cardinal n, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
Ex : $\mathbb{Z}/n\mathbb{Z}$ est cyclique de cardinal n engendré par $\bar{1}$.
$\mathbf{U}_n$ est cyclique de cardinal n engendré par $e^{2i\pi/n}$.
$(\mathbb{Z}/2^n\mathbb{Z})^*$ n'est pas cyclique. [Exo 5 Feuille 1 : $a^k \equiv 1\ [2^n]$ si a impair et $k = 2^{n-2}$]

2 – Générateurs de $\mathbb{Z}/n\mathbb{Z}$

(Th) $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ $\Leftrightarrow k \wedge n = 1$. [demo $\Leftrightarrow$ rapide]
Soit $G = \{e, a, ..., a^{n-1}\}$ un groupe cyclique engendré par a. Soit $b = a^k$. L'ordre de b est alors $k \vee n$ / k. [d]

3 – Exemples

∗ Tout sous-groupe H d'un groupe cyclique G est cyclique (Ex)
Soit $\varphi : k \in \mathbb{Z} \to a^k \in G$. $\exists q \in \mathbb{N}$, $\varphi^{-1}(H) = q\mathbb{Z}$.
$H = \varphi(\varphi^{-1}(H))$ car φ surjective ; $H = \varphi(q\mathbb{Z}) = \{ a^{kq}, k \in \mathbb{Z} \} = G(a^q)$.
∗ Si f est un morphisme de groupe de G vers H et G cyclique alors Im f cyclique (Ex) [Demo simple]
∗ Soient $a \in G$ d'ordre p et $b \in H$ d'ordre q. Alors l'ordre de $(a, b) \in G \times H$ est $p \vee q$ (Ex). [Demo simple]
∗ $G \times H$ est cyclique $\Rightarrow$ G et H cycliques (Ex) [Demo]
∗ $G \times H$ est cyclique $\Rightarrow \#G \wedge \#H = 1$ (Ex) [Demo]
∗ G cyclique de cardinal p, H cyclique de cardinal q et $p \wedge q = 1 \Rightarrow G \times H$ est cyclique (Ex). [Demo rapide]

IV Exemples de groupes finis

$(\mathbf{U}_n, \times)$; $(\mathbb{Z}/n\mathbb{Z}, +)$; $(\sigma_n, \circ)$; $(\mathcal{P}_{(E)}, \Delta)$
∗ Groupe isométries du rectangle : isomorphe à $\mathbf{U}_2 \times \mathbf{U}_2$.
∗ Groupe isométries du carré. Parmi les groupes de cardinal 8, il y a :

Nom	Ordre maximal	Abélien
$\mathbf{U}_8$, $\mathbb{Z}/8\mathbb{Z}$	8	Oui
D_4 : isométries du carré	4	Non
Groupe quaternionique (Cf. TD 12/09/00)	4	Non
$\mathbf{U}_2 \times \mathbf{U}_4$	4	Oui
$\mathbf{U}_2 \times \mathbf{U}_2 \times \mathbf{U}_2$	2	Oui

3 – Action d'un groupe

I Généralités

1 – Définition

Soit G un groupe et E un ensemble. On appelle action ou opération de G sur E toute application

$$f : (g, x) \in G \times E \to g \cdot x \in E$$

telle que : $\forall x \in E, e \cdot x = x$

$\forall x \in E, \forall (g, g') \in G^2, g \cdot (g' \cdot x) = (g\,g') \cdot x$

Il revient au même de se donner un morphisme φ de G dans $\sigma(E)$: $\forall g \in G, \forall x \in E, (\varphi(g))(x) = g \cdot x$.

2 – Exemples

∗ Soit E un ensemble. $\sigma(E)$ opère sur E par : $\forall g \in \sigma(E), \forall x \in E, g \cdot x = g(x)$.

∗ Soit G un groupe. G opère sur G par translation : $\forall (g, x) \in G^2, g \cdot x = g\,x$.

∗ Soit V un **K**-ev. GL(V) opère sur l'ensemble des sev de V par : $\forall u \in GL(V), \forall W$ sev de V, $u \cdot W = u(W)$

3 – Transitivité

Une action de G sur E est dite transitive si $\forall (x, y) \in E^2, \exists g \in G, y = g \cdot x$.
Parmi les 3 exemples, seul le 3e n'est pas forcément transitif.

4 – Orbites

Soit G un groupe qui opère sur E. On définit une relation par : $\forall (x, y) \in E^2, x \,\mathfrak{R}\, y \Leftrightarrow \exists g \in G, y = g \cdot x$.
C'est une relation d'équivalence. Les classes d'équivalences sont appelées orbites.
On a $O(a) = \{ x \in E, \exists g \in G, x = g \cdot a \} = \{ g \cdot a \,/\, g \in G \} = G \cdot a$ (notation)
Rem : L'action est transitive ⇔ Il y a une seule orbite.
Chaque orbite est stable pour l'opération du groupe.

5 – Stabilisateur

Soit $x \in E$. Le stabilisateur de x est $G_x = \{ g \in G, g \cdot x = x \}$. C'est un sous-groupe. [~d]
Ex : recherche d'un stabilisateur d'un sev W d'un **K**-ev V (vis-à-vis de GL(V)).
Cardinal d'une orbite : $\#O(a) = \#G / \#G_a$. [demo avec $\varphi : g \in G \to g \cdot a \in O(a)$]

II Applications

∗ Soit G un groupe fini, et H un sous-groupe de G. H opère sur G par translation.
$O(a) = Ha$ et $H_a = \{e\}$

❍ (Th) Théorème de Lagrange : Soit G un groupe fini, et H un sous-groupe de G. Alors $\#H \mid \#G$. [d'après $*_1$]

∗ (Th) Soit G un groupe de cardinal n. Alors $\forall x \in G, x^n = e$. [demo rapide]

∗ Soit p un nombre premier et $n \in \mathbb{N}^*$. Soit G un groupe de cardinal p^n (c'est un p-groupe [def])
Alors G possède un élément d'ordre p (Ex).

Rem : Si a est d'ordre $\alpha\beta$, alors a^β est d'ordre α.

∗ Le centre de G est $Z(G) = \{ x \in G, \forall y \in G, xy = yx \}$. C'est un sous-groupe de G.
Ex : $Z(GL(V)) = \{$ homothéties $\}$; $Z(\sigma(E)) = \{Id\}$ si $\#E > 2$

∗ Soit G un groupe de cardinal p. G est cyclique ; il est engendré par n'importe quel élément de G sauf le neutre.

∗ Soit G un groupe de cardinal p^n. Alors $Z(G) \neq \{e\}$. [demo : $(g, x) \in G^2 \to g \cdot x = g\,x\,g^{-1} \in G$]

∗ Soit G un groupe de cardinal p^2. Alors G est abélien. [demo : #Z(G) est 1 ou p ou p^2 ... si p, commutant]

∗ Soit G un groupe de cardinal p^2. Alors G est isomorphe à $\mathbf{U}_{p^2}$ ou à $\mathbf{U}_p \times \mathbf{U}_p$. [demo supp non cyclique]

∗ Théorème de Cauchy (Ex). Soit G un groupe fini. Soit p premier divisant #G.
Alors G possède un élément d'ordre p. [DEMO : $E = \{ (x_1, ..., x_p) \in G^p, x_1 ... x_p = e \}$; #E ; scroll φ...]

∗ Nombre d'isométries du cube. [...] Il y en a 48.

∗ Théorème de Cayley (Ex) : Soit G un groupe fini. Alors G est isomorphe à un sous-groupe de $(\sigma_{\#G}, \circ)$. [d]

∗ Les seuls sous-groupes finis de $(\mathbb{C}^*, \times)$ sont les $\mathbf{U}_n$, $n \in \mathbb{N}^*$. [d]

ARITHMETIQUE

4 – Anneaux commutatifs

I Généralités

1 – Définition

A anneau.
$B \subset A$ est un sous-anneau de A si $\begin{cases} B \text{ sous-groupe de } (A, +) \\ B \text{ stable pour } \times \\ 1 \in B \end{cases}$

2 – Morphisme

Soient A et B des anneaux.
$f : A \to B$ est un morphisme d'anneaux si f est un morphisme de groupe additif,
f est un morphisme de $\times$
et $f(1) = 1$.

3 – Idéal

Soit A un anneau commutatif.
$I \subset A$ est un idéal si I est un SG de (A, +)
$\forall (x, y) \in A \times I, xy \in I$.

Ex : Soit $a \in A$. L'idéal principal engendré par a est $(a) = aA = \{ ax, x \in A \}$. [def]
Ex : tous les idéaux de $\mathbb{Z}$ sont $n\mathbb{Z}$, $n \in \mathbb{N}$.
Rem : un idéal n'est pas forcémént un sous-anneau (ne contient pas forcément 1)

(Th) Le noyau d'un morphisme d'anneaux est toujours un idéal.

4 – Ensembles nilpotents (Ex)

Soit A un anneau commutatif. Soit $N = \{ x \in A, \exists n \in \mathbb{N}^*, x^n = 0 \}$. Alors N est un idéal.[d]
Si A n'est pas commutatif : Contrexemple avec $\mathcal{M}_2(\mathbb{R})$.

5 – Les inversibles d'un anneau constituent un groupe multiplicatif

II Anneaux intègres

1 – Définition

Soit A un anneau.
A est dit intègre si : $\begin{cases} A \text{ est commutatif} \\ A \neq \{0\} \\ \forall (x, y) \in A^2, xy = 0 \Rightarrow x = 0 \text{ ou } y = 0. \end{cases}$

Ex : tous les corps ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$) et tous les sous-anneaux de corps ($\mathbb{Z}$) sont intègres.

2 – Divisibilité

Soit A un anneau intègre. On dit que $x|y$ si $\exists z \in A, xz = y$.
(Th) $x|y \Leftrightarrow (y) \subset (x)$ [demo rapide]

3 – Propriété sur les éléments inversibles (Ex)

Soit A un anneau intègre. On note A^* le groupe des éléments inversibles de A (ex : $\mathbb{R}^*$, $\mathbb{C}^*$ mais pas $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$)
Soit $(x, y) \in A^2$. On a : $(x) = (y) \Leftrightarrow \exists u \in A^*, y = ux$. [demo]

5 – Arithmétique dans $\mathbb{Z}$

(Def) Soit A un anneau. A est dit principal si A est intègre et tout idéal de A est principal (de la forme (a) = aA).

$\mathbb{Z}$ est principal.

I PGCD et PPCM

1 – PGCD

Soit $(a, b) \in \mathbb{Z}^2$. Soit $I = (a) + (b)$ est un idéal (somme de 2 idéaux). $\exists\, d \in \mathbb{N}$, $I = (d)$.
Les diviseurs communs à a et b sont les diviseurs de d.
On note $d = \text{PGCD}(a, b) = a \wedge b$.
Rem : $a \wedge 0 = a$.

2 – Nombres premiers entre eux

(a, b) sont dits premiers entre eux si $a \wedge b = 1$.
(Th) Théorème de Bezout : $a \wedge b = 1 \Leftrightarrow \exists\, (u, v) \in \mathbb{Z}^2$, $au + bv = 1$. [d]

3 – Théorème de Gauss

(Th) Soient $a, b, c \in \mathbb{Z}$. $a \wedge b = 1$ et $a \mid bc \Rightarrow a \mid c$. [d]

4 – PPCM

Soient $a, b \in \mathbb{Z}$. Les multiples communs sont $(a) \cap (b)$. C'est un idéal (intersection de 2 idéaux).
$\exists\, m \in \mathbb{N}$, $(a) \cap (b) = (m)$.
Les multiples communs à a et b sont les multiples de m.
On note $m = \text{PPCM}(a, b) = a \vee b$.

II Anneau $\mathbb{Z}/n\mathbb{Z}$

1 – Structure d'anneau

Soit $n \in \mathbb{N}^*$. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique. On définit une multiplication. On vérifie qu'elle est cohérente.
(Th) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.
(Th) Le morphisme $\varphi : k \in \mathbb{Z} \to \bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est alors un morphisme d'anneau.

2 – Inversibles de $\mathbb{Z}/n\mathbb{Z}$

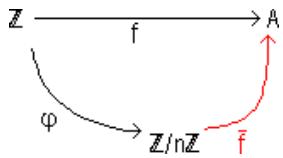
(Th) Soit $k \in \mathbb{Z}$. Alors $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow k \wedge n = 1$. [demo rapide $\Leftrightarrow$]
Ex : $(\mathbb{Z}/10\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ est isomorphe à $\mathbf{U}_4$.
Soit $n \in \mathbb{N}^*$. Alors $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ n est premier. [d]
$\forall$ p premier, $\mathbb{Z}/p\mathbb{Z}$ est donc un corps noté $\mathbf{F}_p$.

3 – Théorème chinois

(Th) Soient $(p, q) \in \mathbb{N}^{*2}$, $p \wedge q = 1$.
Alors $\mathbb{Z}/pq\mathbb{Z}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ (en tant qu'anneaux). [demo simple]
Ex : résoudre $x \equiv 3[5]$ et $x \equiv 2[6]$.

III Un théorème de factorisation

(Th) Soit A un anneau, et $f : \mathbb{Z} \to A$ un morphisme d'anneaux.
Soit $n \in \mathbb{N}$ et $\varphi : k \in \mathbb{Z} \to \bar{k} \in \mathbb{Z}/n\mathbb{Z}$.
Si $n\mathbb{Z} \subset \text{Ker } f$, alors il existe un morphisme d'anneaux $\bar{f}$ tel que $f = \bar{f} \circ \varphi$.
[demo simple – Application : démontrer le théorème chinois]



IV Indicateur d'Euler (Ex)

Soit $n \geq 1$. On note $\varphi(n)$ le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. C'est aussi le nombre de générateurs de $\mathbf{U}_n$.
$\varphi(n) = \#\{ i \in \mathbb{N}_{n-1} / i \wedge n = 1 \}$

∗ Soit p premier et $\alpha \in \mathbb{N}^*$. Alors, $\varphi(p^\alpha) = p^\alpha\left(1 - \frac{1}{p}\right)$.

∗ Soit $(n, m) \in \mathbb{N}^{*2}$, $n \wedge m = 1$. Alors $\varphi(nm) = \varphi(n)\,\varphi(m)$. [th Chinois]

∗ $\forall\, n \in \mathbb{N}^*$, $\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right)$

∗ $\forall\, n \in \mathbb{N}^*$, $n = \sum_{d \mid n} \varphi(d)$ [application]

∗ Soit **K** un corps commutatif. Soit G un sous-groupe fini de $(\mathbf{K}^*, \times)$. Alors G est cyclique.
DEMO :
On appelle $\psi(d)$ le nombre d'éléments de G d'ordre d. Soit $n = \#G$.
On a : $n = \sum \psi(d) = \sum \varphi(d)$. On montre également que $\forall\, d \in \mathcal{D}_n$, $\varphi(d) \geq \psi(d)$.
[si $\psi(d) \geq 1$, $\varphi(d) = \psi(d)$ grâce au polynôme $X^d - 1$]
Donc $\forall\, d \in \mathcal{D}_n$, $\psi(d) = \varphi(d)$, d'où $\psi(n) = \varphi(n) \neq 0$. G est bien cyclique.
[Autre démo : Exo 7 feuille 1, ppcm des ordres = cardinal de $\mathbf{K}^*$ (dfp poly)]

6 – (Ex) Nombres premiers

∗ Soit p premier. Soit $a \in \mathbb{Z}$, $a \wedge p = 1$. Alors $a^{p-1} \equiv 1$ [p].
∗ Soit p premier. Soit $k \in \mathbb{N}_{p-1}$. Alors $p \mid C_p^k$.
∗ Petit théorème de Fermat. Soit p premier. Soit $a \in \mathbb{Z}$. Alors $a^p \equiv a$ [p]. [2 démos]
∗ Il y a une infinité de nombres premiers.
∗ Il y a une infinité de nombres premiers tels que $p \equiv -1$ [4]

∗ Soit p premier. Soit $n \in \mathbb{N}^*$. Alors $v_p(n!) = \sum_{k=1}^{\infty} E\left(\frac{n}{p^k}\right)$ où $v_p(a) = \text{Max}\{\, x \in \mathbb{N},\, p^x \mid a \,\}$.

∗ Théorème de Wilson. Soit $p \geq 2$. On a : p premier $\Leftrightarrow p \mid 1 + (p-1)!$ [demo]
Une autre démonstration utilise le polynôme $(X - \bar{1})(X - \bar{2})\ldots(X - \bar{p} + \bar{1}) = X^{p-1} - \bar{1}$ (même d°, racines, unitaire).

7 – (Ex) Fonction de Mobius

Soit μ la fonction de mobius de $\mathbb{N}^*$ vers $\{ 0, 1, -1 \}$ telle que

$\mu(1) = 1$
$\mu(p_1 \ldots p_r) = (-1)^r$ si $p_1, \ldots, p_r$ sont des premiers distincts 2 à 2
$\mu(n) = 0$ sinon

∗ $a \wedge b = 1 \Rightarrow \mu(ab) = \mu(a)\,\mu(b)$. [plusieurs cas]

∗ $\forall\, n \geq 2$, $\sum_{d \mid n} \mu(d) = 0$ [ramène au cas où $n = p_1 p_2 \ldots p_r$]

∗ Formule d'inversion. Soit $(a_n) \in \mathbb{C}^{\mathbb{N}}$. On définit (b_n) par $\forall\, n \in \mathbb{N}^*$, $b_n = \sum_{d \mid n} a_d$.

Alors $\forall\, n \in \mathbb{N}^*$, $a_n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) b_d$ [demo permutation $\Sigma\Sigma$]

Rem : cette formule est valable dans n'importe quel groupe abélien. $(\mathbb{C}(X) \setminus \{0\}, \times)$ par exemple.

8 – Idéaux de K[X]

Soit **K** un sous-corps de $\mathbb{C}$.

I Structure des idéaux

1 – Division euclidienne

(Th) Soient $A \in \mathbf{K}[X]$ et $B \in \mathbf{K}[X] \setminus \{0\}$. Alors $\exists ! (Q, R) \in \mathbf{K}[X]^2$, $A = BQ + R$ et $d°R < d°B$.
[demo : $\mathbf{K}_n[X] = \mathbf{K}_{q-1}[X] \oplus B\, \mathbf{K}_{n-q}[X]$ avec app. linéaire]

2 – Algorithme de la division euclidienne

$A = a_0 + ... + a_n X^n$. $B = b_0 + ... + b_q X^q$. $b_q \neq 0$.
$A = B . (a_n/b_q) X^{n-q} + A_1$ où $d°A_1 < d°A$
On peut démontrer comme ça l'existence de (Q, R) par récurrence sur d°A.
Ex : Soient A et $B \in \mathbb{Z}[X]$; B est unitaire. Alors $(Q, R) \in \mathbb{Z}[X]^2$. [important]

3 – K[X] est principal

(Th) **K**[X] est principal
Soit I un idéal de **K**[X].
Si $I \neq \{0\}$, on appelle P un polynôme de degré minimum de I. On a $I = (P)$. [demo comme groupes + de $\mathbb{Z}$]

4 – Z[i] est un anneau principal (Ex)

$\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. Il est intègre.
Pseudodivision euclidienne dans $\mathbb{Z}[i]$:
$\forall (z_1, z_2) \in \mathbb{Z}[i] \times \mathbb{Z}[i] \setminus \{0\}, \exists (q, r) \in \mathbb{Z}[i]^2, z_1 = z_2 q + r$ et $|r| < |z_2|$. [demo – pas unicité]

II Arithmétique dans K[X]

Inversibles de $\mathbb{Z}$: $\{1, -1\}$. Inversibles de **K**[X] : **K** \ {0}.

1 – PGCD

Soient A et $B \in \mathbf{K}[X]$.
$I = (A) + (B)$ est un idéal principal. Son générateur unitaire est le PGCD de A et de B.
L'application $(A, B) \to A \wedge B$ est une LCI associative et commutative.
Neutre : 0

2 – Théorème de Bezout

3 – Théorème de Gauss

4 – PPCM

$I = (A) \cap (B)$ est un idéal principal. Son générateur unitaire est le PPCM de A et de B.
L'application $(A, B) \to A \vee B$ est une LCI associative et commutative.
Neutre : 1

III Etude de K[a]

Soit **K** un corps commutatif, et E une **K** – algèbre (unitaire).
Ex : **K**[X], **K**, $\mathcal{M}_n(\mathbf{K})$, $(\mathcal{L}(V), +, \circ)$ sont des **K** – algèbres (V est un **K** – ev). $\mathbb{C}$ est une $\mathbb{C}$ – algèbre et une $\mathbb{R}$ – algèbre.
Soit $a \in E$, et $\varphi : P \in \mathbf{K}[X] \to P(a) \in E$.
Im φ est une sous-algèbre de E, notée **K**[a]. C'est la sous-algèbre de E engendrée par a.
Ker φ est un idéal appelé idéal des polynômes annulateurs de a.

1 – Cas où Ker φ = {0} : a transcendant

a est alors dit transcendant sur **K**.

φ induit un isomorphisme d'algèbre de $\mathbf{K}[X]$ sur $\mathbf{K}[a]$.
Ex : Dans $E = \mathbf{K}[X]$, X est transcendant.

2 – Cas où Ker $\varphi \neq \{0\}$: a algébrique

a est alors dit algébrique sur $\mathbf{K}$.
Ker φ possède un unique générateur unitaire, appelé polynôme minimal de a, noté π_a.
Ex : $\pi_i = X^2 + 1$ $\pi_{\sqrt{2}} = X^2 - 2$ $\pi_{\sqrt{2}+\sqrt{3}} = (X^2 - 1)^2 - 8X^2$ $\pi_j = X^2 + X + 1$
❍ (Th) E intègre et a algébrique $\Rightarrow \pi_a$ irréductible dans $\mathbf{K}[X]$. [demo]
Ex : dans $\mathcal{L}(V)$ non intègre, $\pi_p = X(X-1)$ si p est un projecteur.

3 – a algébrique $\Leftrightarrow$ K[a] est de dimension finie

(Th) a est algébrique $\Leftrightarrow \mathbf{K}[a]$ est de dimension finie. [demo $\Leftrightarrow$]

4 – Propriétés de K[a] quand a est algébrique

(Th) $\dim_{\mathbf{K}} \mathbf{K}[a] = d^\circ\pi_a$ [demo]
(Th) $\forall P \in \mathbf{K}[X]$, P(a) inversible dans $E \Leftrightarrow P \wedge \pi_a = 1$, et dans ce cas, $P(a)^{-1} \in \mathbf{K}[a]$. [demo]
(Th) E intègre $\Rightarrow \mathbf{K}[a]$ est un corps [2 demos]
Rem : Toute $\mathbf{K}$ – algèbre intègre (unitaire) de dimension finie est un corps. [demo]

IV Rappels : relations coefficients/racines

$P \in \mathbf{K}[X]$
$P = a_0 + a_1X + ... + a_nX^n = a_n(X - \alpha_1)(X - \alpha_2)...(X - \alpha_n)$
Alors $\forall k \in \{0, ..., n-1\}$, $\sum x_1x_2...x_{n-k} = (-1)^{n-k}\frac{a_k}{a_n}$.

9 – (Ex) Algébriques

On se place dans le corps des complexes, $\mathbb{Q}$ – algèbre.
α est algébrique si $\exists P \in \mathbb{Q}[X] \setminus \{0\}$, $P(\alpha) = 0$.
$\mathbf{A}$ désigne l'ensemble des nombres algébriques.
Rem : Dans ce cas, $\exists P \in \mathbb{Z}[X] \setminus \{0\}$, $P(\alpha) = 0$.
∗ Soit $\alpha \in \mathbf{A} \setminus \mathbb{Q}$. Alors π_α est irréductible dans $\mathbb{Q}[X]$, et à racines simples dans $\mathbb{C}$. [demo avec une racine de π_a]
∗ Lemme : soient $K \subset L$ deux corps, et $E \neq \{0\}$ un L – espace vectoriel.
Alors $\dim_K E = \dim_L E \cdot \dim_K L$. [demo bases]
∗ $\mathbf{A}$ est un sous-corps de $\mathbb{C}$.
DEMO kaf
$\forall (a, b) \in \mathbf{A}^2$, on pose $\mathbf{K} = \mathbb{Q}[a]$. $\mathbf{K}[b]$ est un corps de dimension finie sur $\mathbf{K}$, contenant a et b.
$\mathbf{K}[b]$ est de dimension finie sur $\mathbb{Q}$ (Cf. Lemme précédent).
Utilisation du lemme :
Lemme : Soit L un $\mathbf{K}$ – espace vectoriel de dimension finie. $c \in L \Rightarrow$ c algébrique sur $\mathbf{K}$. [demo]
∗ Exemple : $\pi_{i+\sqrt{2}} = X^4 - 2X^2 + 9$
∗ $\mathbf{A}$ est algébriquement clos. [demo : construction de corps emboités]

10 – Corps commutatifs

I Généralités

1 – Caractéristique

Soit $(\mathbf{K}, +, \times)$ un corps commutatif.
Si 1 (le neutre pour $\times$) est d'ordre fini p (dans $\mathbf{K}$, +) alors on pose car $\mathbf{K} = p$.
S'il est d'ordre infini, on pose car $\mathbf{K} = 0$.
Rem : car $\mathbf{K} = 0 \Rightarrow \mathbf{K}$ infini. $\mathbf{K}$ fini $\Rightarrow$ car $\mathbf{K} \neq 0$
(Th) $\mathbf{K}$ corps de caractéristique $p \neq 0$ alors p est premier. [demo absurde p = rs]

2 – Applications (Ex)

car $\mathbf{K} = 0 \Rightarrow \mathbf{K}$ contient un sous corps isomorphe à $\mathbb{Q}$ [DIY]
car $\mathbf{K} = p \Rightarrow \mathbf{K}$ contient un sous corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$ [demo : utilisation de gr(1)]
Et alors $\exists\, n \in \mathbb{N}^*$, $\#\mathbf{K} = p^n$. [demo alg. linéaire]
☠ (Ex) Tout anneau intègre fini est un corps. [demo translation injective]
☠ (Ex) Toute algèbre intègre de dimension finie est un corps. [demo]

II Polynômes primitifs (Ex)

1 – Définition

$\forall\, P \in \mathbb{Z}[X]$, P est dit primitif si ses coefficients sont premiers entre eux dans leur ensemble.
Soit $(P, Q) \in \mathbb{Z}[X]^2$. P et Q primitifs $\Rightarrow$ PQ primitfs
[2 demos : Absurde et $\mathbb{Z}/p\mathbb{Z}$; Direct avec une idée donnée par $\mathbb{Z}/p\mathbb{Z}$]

2 – Contenu

Soit $p \in \mathbb{Z}[X]$. Le contenu de P, noté c(P), est le PCGD de ses coefficients.
c est un morphisme de $(\mathbb{Z}[X], \times)$ dans $(\mathbb{N}, \times)$. [demo]
Rem : $\forall\, \lambda \in \mathbb{Z}$, $\forall\, R \in \mathbb{Z}[X]$, $c(\lambda R) = |\lambda|\, c(R)$.

3 – Exercice sur $\mathbb{Z}[X]$

$\forall\, P \in \mathbb{Z}[X]$, $\forall\, (Q, R) \in \mathbb{Q}[X]^2$ unitaires, $P = QR \Rightarrow Q$ et $R \in \mathbb{Z}[X]$. [demo avec le contenu]

11 – (Ex) Polynômes cyclotomiques

I Définition

Soit $n \in \mathbb{N}^*$. On note $\mathcal{P}_n$ l'ensemble des racines primitives de l'unité (générateurs de $\mathbf{U}_n$).
$\mathcal{P}_n = \{\, \omega^k \,/\, k \wedge n = 1 \,\} \subset \mathbf{U}_n$ où $\omega = e^{2i\pi/n}$.
On pose $\phi_n = \prod (X - \alpha)$ où α décrit $\mathcal{P}_n$.
$\phi_1 = X - 1$ $\phi_2 = X + 1$ $\phi_3 = X^2 + X + 1$ $\phi_4 = X^2 + 1$ $\phi_5 = X^4 + X^3 + X^2 + X + 1$
Rem : $\phi_n \mid X^n - 1$

II Exemples

$\forall\, n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d|n} \phi_d$. [Demo avec $f : \alpha \in \mathbf{U}_n \to$ ordre de $\alpha \in \mathcal{D}_n$.]
$\forall\, n \in \mathbb{N}^*$, $\phi_n \in \mathbb{Z}[X]$ [Demo recurrence sur n et D.E. $\mathbb{Z}[X]$]
$\forall\, n \in \mathbb{N}^*$, $\phi_n = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$ [Demo avant]
$\forall\, n \in \mathbb{N}^*$, ϕ_n est irréductible dans $\mathbb{Q}[X]$. [Dur]
Conséquences : $\forall\, n \in \mathbb{N}^*$, $\forall\, \omega \in \mathcal{P}_n$, $\phi_n = \pi_\omega$
$\dim_{\mathbb{Q}} \mathbb{Q}[\omega] = d^\circ \phi_n = \varphi(n)$

ESPACES VECTORIELS

12 – Espace vectoriel sur un corps commutatif

I Famille de vecteurs

[...]
Notation : $A^{(B)}$ désigne une famille d'éléments presque tous nuls de A indexée par B.
Soit E un $\mathbf{K}$ – espace vectoriel.
Soit $(e_i)_{i \in I}$ une base de E. $\forall x \in E, \exists ! (\lambda_i) \in \mathbf{K}^{(I)}, x = \Sigma \lambda_i e_i$. On note $e_i^* : x \in E \to \lambda_i$. [un peu simple]
Ex : dans la base canonique de $\mathbf{K}[X]$, la famille des coordonnées de P est P.
Ex : Soit E l'espace vectoriel des fonctions polynomiales sur $\mathbf{K}^n$, c'est-à-dire :
$\forall \alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$ (α est un multi indice), on note $f_\alpha : (x_1, ..., x_n) \in \mathbf{K}^n \to \Pi x_i^{\alpha_i}$.
$E = \text{Vect}\{ f_\alpha , \alpha \in \mathbb{N}^n \} \subset \mathcal{F}(\mathbf{K}^n, \mathbf{K})$.
Alors, les (f_α) forment une base de E. [demo libre par récurrence en fixant n – 1 paramètres]
(Th) Soit $(e_i)_{i \in I}$ une base de E. Soit $(f_i)_{i \in I} \in F^I$. Alors $\exists ! u \in \mathcal{L}(E, F), \forall i \in I, u(e_i) = f_i$.
[... exemple insultant ...]

II Somme de sous-espaces vectoriels

1 – Définition

Soient $F_1, ..., F_p$ des sous-espaces vectoriels de E ($p \geq 2$). Soit $u : (x_1, ..., x_p) \in \Pi F_i \to \Sigma x_i \in E$.
u est linéaire. Im u est notée $F_1 + ... + F_2$.
Rem : c'est en fait le sev engendré par leur réunion.
La somme est dite directe si Ker u = {0}.

(Th) $F_1, .., F_p$ sont en somme directe $\Leftrightarrow$
$$\begin{cases} F_1 \cap F_2 = \{0\} \\ (F_1 + F_2) \cap F_3 = \{0\} \\ (F_1 + F_2 + F_3) \cap F_4 = \{0\} \\ ... \\ (F_1 + ... + F_{p-1}) \cap F_p = \{0\} \end{cases}$$ [demo $\Leftrightarrow$]

On dit que $F_1, ..., F_p$ sont supplémentaires si leur somme est directe et est égale à E.
u est alors un isomorphisme de ΠF_i vers E.
(Ex) Soit $\mathbf{K}$ corps infini et E $\mathbf{K}$ ev union des sev $F_1, ..., F_n$. Alors $\exists i \in \mathbb{N}_n, F_i = E$. [exo 9 feuille 3]

2 – Dimension finie

Soit E de dimension finie.
∗ (Th) Soient $F_1, ..., F_p$ en somme directe. Alors $\dim (F_1 \oplus ... \oplus F_p) = \Sigma \dim F_i$. [demo découle du lemme]
Lemme : Si F et G sont des $\mathbf{K}$ – espaces vectoriels de dimension finie, $\dim F \times G = \dim F + \dim G$. [demo base]
Rem : Si $F_1, ..., F_p$ sont en somme directe, $E = F_1 \oplus ... \oplus F_p \Leftrightarrow \Sigma \dim F_i = \dim E$.
∗ Si $E = F_1 \oplus ... \oplus F_p$, l'application $u : (x_1, ..., x_p) \in \Pi E_i \to \Sigma x_i \in E$ est un isomorphisme.
On note $p_i : x \in E \to x_i \in E$. C'est un projecteur. $p_i = f_i \circ u^{-1}$ où f_i extrait le $i^{ème}$ élément de ΠF_i.
∗ (Th) Si $E = F_1 \oplus ... \oplus F_p$, soient $u_1 \in \mathcal{L}(F_1, V), ..., u_p \in \mathcal{L}(F_p, V)$. Alors $\exists ! u \in \mathcal{L}(E, V), \forall i \in \mathbb{N}_p, u|_{F_i} = u_i$.
∗ $n \in \mathbb{N}$. $P \in \mathbf{K}[X]$ de degré n+1. Alors $\mathbf{K}[X] = P\,\mathbf{K}[X] \oplus \mathbf{K}_n[X]$.
∗ Définition de la base adaptée de E à un sev F de E...
∗ Définition de la base adaptée de E à des sevs supplémentaires de E...

13 – Rang d'une application linéaire

I Isomorphisme induit

∗ (Th) Soit $u \in \mathcal{L}(E, F)$. On suppose que E ' est un supplémentaire de Ker u.
Soit $u' : x \in E' \to u(x) \in$ Im u. C'est un isomorphisme. [d]
∗ (Th) Théorème du rang : $\dim E = \dim \text{Ker } u + \dim \text{Im } u$.
∗ (Th) Si $\dim E = \dim F$, et $u \in \mathcal{L}(E, F)$, alors u injective $\Leftrightarrow$ u surjective $\Leftrightarrow$ u bijective.

II Applications

∗ (Ex) E de dimension finie. $f, g \in \mathcal{L}(E)$. Alors $\dim \operatorname{Ker} g \circ f \leq \dim \operatorname{Ker} f + \dim \operatorname{Ker} g$. [demo : $x \in \operatorname{Ker} g \circ f \to f(x)$]

∗ (Ex) E de dimension finie. $u \in \mathcal{L}(E)$. On note $a_k = \dim \operatorname{Ker} u^k$.

(a_k) est croissante, stationnaire, et $(a_{k+1} - a_k)$ est décroissante. [demos]

∗ E de dimension finie. $(u, v) \in \mathcal{L}(E)$. Alors :

$\operatorname{rg}(u \circ v) \leq \operatorname{rg}(u)$ $\operatorname{rg}(u \circ v) \leq \operatorname{rg}(v)$

$\operatorname{rg}(u + v) \leq \operatorname{rg}(u) + \operatorname{rg}(v)$ $|\operatorname{rg}(u) - \operatorname{rg}(v)| \leq \operatorname{rg}(u - v)$. [d]

Rem : $\dim (A + B) \leq \dim A + \dim B$.

∗ Etude de $\Delta : P \in \mathbb{C}[X] \to P(X + 1) - P \in \mathbb{C}[X] \in \mathcal{L}(\mathbb{C}[X])$

$\forall P \in \mathbb{C}[X] \setminus \mathbb{C}, d^\circ \Delta P = d^\circ P - 1$ $\Rightarrow \operatorname{Ker} \Delta = \mathbb{C}$.

$\Delta_n : P \in \mathbb{C}_n[X] \to \Delta P \in \mathbb{C}_{n-1}[X]$ est surjective. $\Rightarrow \Delta$ surjective

Matrice de Δ_n dans la base canonique... [demos]

∗ Soit E un $\mathbf{K}$ – ev de dimension finie, et F et G deux sevs de E. Alors $\dim (F+G) = \dim F + \dim G - \dim (F \cap G)$. [2d]

III Interpolation de Lagrange

Soit $n \geq 1$. Soit $\mathbf{K} = \mathbb{R}$ ou $\mathbb{C}$. Soient $a_0, ..., a_n \in \mathbf{K}$ distinctes et $y_0, ..., y_n \in \mathbf{K}$.

Alors $\exists ! P \in \mathbf{K}_n[X], \forall i \in \{0, ..., n\}, P(a_i) = y_i$.

[demo : étude de $u : P \in \mathbf{K}_n[X] \to (P(a_0), ..., P(a_n)) \in \mathbf{K}^{n+1}$]

Détermination du polynôme interpolateur (à partir des éléments de la base canonique de $\mathbf{K}[X]$).

Rem : soit $\varphi : \mathbf{K}[X] \to \mathcal{F}(\mathbf{K}, \mathbf{K})$.

$\mathbf{K}$ infini $\Rightarrow \varphi$ injective mais pas surjective. [car $\varphi^{-1}\{\sin\} = \varnothing$]

$\mathbf{K}$ fini $\Rightarrow \varphi$ surjective mais non injective. [car ~ ; car $\mathbf{K}[X]$, lui, est infini]

14 – Hyperplans

I Généralités

♦ Soit E un $\mathbf{K}$ espace vectoriel. On note $E^* = \mathcal{L}(E, \mathbf{K})$ l'ensemble des formes linéaires sur E.

La forme bilinéaire canonique est l'application : $(x, \varphi) \in E \times E^* \to \varphi(x) \in \mathbf{K}$.

♦ (Th) Deux supplémentaires d'un même sev sont isomorphes (même en dim ∞) [projection]

♦ Soit F un sev de E. On dit que F est de codimension finie si F possède un suppléméntaire G de dimension finie. Dans ce cas, on écrit : codim F = dim G.

Cas particulier : Si E est de dimension finie, alors $\forall$ F sev $\subset$ E, codim F + dim F = dim E.

♦ On appelle hyperplan de E tout sev H de codimension 1.

Ex : codim $\{ P \in \mathbb{C}[X] / P(1) = P(2) = 0 \} = 2$.

Ex : L'ensemble des fonctions paires (sev de $\mathbb{R}^{\mathbb{R}}$) est de dimension et de codimension infinies.

♦ (Th) Soit $u \in \mathcal{L}(E, F)$. u est de rang fini $\Rightarrow$ Ker u est de codim finie dans E. [demo ∞]

II Formes linéaires et hyperplans

♦ (Th) Soit $H \subset E$. H est un hyperplan de $E \Leftrightarrow \exists \varphi \in E^* \setminus \{0\}, H = \operatorname{Ker} \varphi$. [demos]

♦ (Th) Equations d'un hyperplan : Soient $\varphi, \psi \in E^* \setminus \{0\}$. $\operatorname{Ker} \varphi = \operatorname{Ker} \psi \Leftrightarrow (\varphi, \psi)$ est liée [demo]

♦ (Th) dim E = n. Soit F un sev de E. F est un hyperplan de $E \Leftrightarrow \dim F = n - 1$.

♦ Hyperplan de $\mathbf{K}^n$. Soit $\varphi \in \mathbf{K}^{n\,*}$. On note $(e_1, ..., e_n)$ la base canonique de E. Soit $x = (x_1, ..., x_n) \in E$.

Alors $x = \Sigma\, x_i\, e_i$. $\varphi(x) = \Sigma\, \lambda_i\, x_i$ où $\forall i \in \mathbb{N}_n, \lambda_i = \varphi(e_i)$.

Ex : équation de plan vectoriel dans $\mathbb{R}^3$. $ax + by + cz = 0$ où $(a, b, c) \neq (0, 0, 0)$.

15 – Dualité en dimension finie

I Bases duales

1 – Théorème

(Th) Soit E un $\mathbf{K}$ – ev de dimension finie. $\forall x \in E \setminus \{0\}, \exists \varphi \in E^*, \varphi(x) = 1$. [demo]

(Th) Soit $B = (e_1, ..., e_n)$ base de E. On note e_j^* la forme linéaire $x = \Sigma\, x_k\, e_k \in E \to x_j \in \mathbf{K}$.

Alors (e_i^*) est une base de $E^* = \mathcal{L}(E, \mathbf{K})$ [demo]

Notation : symbole de Kronecker ; $\forall (i, j) \in \mathbb{N}_n^2$, $e_i^*(e_j) = \delta_{ij}$.

2 – Exercices

∗ $E = \mathbb{R}[X]$. $B = (e_i)$: base canonique de E. (e_i^*) est-elle une base de $\mathbb{R}[X]^*$? Et bien non. Mais elle est libre.

∗ Soit (e_1, e_2) base de E. $f_1 = e_1$ et $f_2 = e_1 + e_2$. Alors, $f_1^* = e_1^* - e_2^*$ et $f_2 = e_2^*$.

II Etude d'une application linéaire

Soient $(e_1, ..., e_p) \in E^p$.

Soit $u : \varphi \in E^* \to (\varphi(e_1), ..., \varphi(e_p)) \in \mathbf{K}^p$.

♦ (Th) $(e_1, ..., e_p)$ est une base de $E \Rightarrow$ u isomorphisme. [demo]

♦ (Th) $(e_1, ..., e_p)$ est libre $\Leftrightarrow$ u surjective. [2 demos]

(Th) Et dans ce cas : ∗ codim Ker u = p

∗ $\{ x \in E / \forall \varphi \in E^*, \varphi(x) = 0 \} = \cap \text{Ker } \varphi = \text{Vect } \{ e_i, i \in \mathbb{N}_p \}$

♦ Famille d'équations d'un sev : Soit F un sev de E. $(e_1, ..., e_p)$ base de F. $\text{Ker } u = \{ \varphi \in E^*, \varphi(F) = \{0\} \}$.

Soit $q = \dim E - p = \dim \text{Ker } u$. Soit $(\varphi_1, ..., \varphi_q)$ base de Ker u. $(\varphi_1, ..., \varphi_q)$ est appelée famille d'équations de F.

$\forall x \in E, x \in F \Leftrightarrow \forall i \in \mathbb{N}_q, \varphi_i(x) = 0$.

Rem : $\dim F = n - q$.

III Intersection d'hyperplans

Soient $\varphi_1, ..., \varphi_q \in E^* \setminus \{0\}$ et $\forall j \in \mathbb{N}_q$, $H_j = \text{Ker } \varphi_j$.

Soit $v : x \in E \to (\varphi_1(x), ..., \varphi_2(x)) \in \mathbf{K}^p$.

♦ (Th) $(\varphi_1, ..., \varphi_q)$ base de $E^* \Rightarrow$ v isomorphisme [demo]

$\Rightarrow$ Soit $C = (\varphi_1, ..., \varphi_q)$ base de E^*. Alors $\exists !$ B base de E dont C est la duale.

♦ (Th) $(\varphi_1, ..., \varphi_q)$ libre $\Leftrightarrow$ v surjective [2 demos]

(Th) Et dans ce cas : ∗ codim Ker v = q

∗ $\{ \varphi \in E^* / \varphi(\text{Ker } v) = \{0\} \} = \text{Vect } \{ \varphi_i, i \in \mathbb{N}_q \}$ [demo]

Application : l'équation de tout plan qui passe par l'intersection de 2 plans A et B est combinaison linéaire des équations de A et de B.

♦ $(\varphi_1, ..., \varphi_q)$ non nécessairement libre. Alors, $\text{Ker } v = \dim E - rg(\varphi_1, ..., \varphi_q)$.

MATRICES

16 – Trace

I Trace d'une matrice carrée

♦ Soit (E_{ij}) la base canonique de E. On définit $Tr = \Sigma E_{ii}^*$.
♦ (Th) $\forall (A, B) \in \mathcal{M}_n(\mathbf{K})^2$, $Tr(AB) = Tr(BA)$. [d]
♦ (Th) $\forall A \in \mathcal{M}_n(\mathbf{K})$, $\forall P \in GL_n(\mathbf{K})$, $Tr\ A = Tr\ (P^{-1} A P)$.
♦ Soit $M \in \mathcal{M}_n(\mathbf{K})$ telle que $\forall X \in \mathcal{M}_n(\mathbf{K})$, $Tr(MX) = 0$. Alors $M = 0$. (Ex)
Rem : $Tr(M E_{i\,j}) = m_{j\,i}$
♦ $\forall M \in E$, Soit $T_M : X \in \mathcal{M}_n(\mathbf{K}) \to Tr(MX) \in \mathbf{K} \in \mathcal{M}_n(\mathbf{K})^*$.
Alors $\forall \varphi \in \mathcal{M}_n(\mathbf{K})^*$, $\exists !\ M \in \mathcal{M}_n(\mathbf{K})$, $\varphi = T_M$. (Ex) [d $M \to T_M$]
♦ $F = \{ M \in \mathcal{M}_n(\mathbf{K}) / Tr\ M = 0 \}$ = Ker Tr est un hyperplan. $\dim F = n^2 - 1$. Base : $(E_{ij})_{i \neq j} \cup (E_{ii} - E_{nn})_{i \in \mathbb{N}n-1}$. (Ex)

II Trace d'un endomorphisme

E est supposé de dimension finie.
♦ Soit $u \in \mathcal{L}(E)$. Soit B base de E, et M = Mat(u,B). Alors Tr(M) ne dépend pas de B. Par définition, Tr(u) = Tr(M). [demo]
(Th) $\forall (u, v) \in \mathcal{L}(E)^2$, $Tr(u \circ v) = Tr(v \circ u)$.
♦ Cas d'un projecteur : $Tr(p) = rg(p) \,.\, 1_{\mathbf{K}}$.
☠ $\mathbf{K} \subset \mathbb{C}$. Soient p, q projecteurs. Alors p + q projecteur $\Leftrightarrow p \circ q = q \circ p = 0$. (Ex)
Et dans ce cas, $E = Im\ p \oplus (Im\ q \oplus (Ker\ q \cap Ker\ p))$.
♦ $\mathbf{K} \subset \mathbb{C}$. $p_1, ..., p_k$ projecteurs. Alors $\Sigma\ p_i$ projecteur $\Leftrightarrow \forall (i, j) \in \mathbb{N}_k^2$, $i \neq j \Rightarrow p_i \circ p_j = 0$. (Ex)

17 – Matrices équivalentes

♦ Soient $A, B \in \mathcal{M}_{p,q}(\mathbf{K})$. A et B sont équivalentes si $\exists P \in GL_p(\mathbf{K})$, $\exists Q \in GL_q(\mathbf{K})$, A = PBQ. On note $A \sim B$.
(Th) Il s'agit d'une relation d'équivalence sur $\mathcal{M}_{p,q}(\mathbf{K})$.
♦ Soit $M \in \mathcal{M}_{p,q}(\mathbf{K})$. Soient $C_1, ..., C_q \in \mathcal{M}_{p,1}(\mathbf{K})$ les vecteurs colonnes de M.
On définit $rg(M) = rg(C_1, ..., C_q) = \dim Vect \{ C_i, i \in \mathbb{N}_q \}$.
Rem : $rg(M) \leq Min(p, q)$
♦ (Th) Soit $u \in \mathcal{L}(E_1, E_2)$. B_1 base de E_1 et B_2 base de E_2. Alors $rg(u) = rg(Mat(u, B_1, B_2))$. [demo]
$A \sim B \Rightarrow rg\ A = rg\ B$.
(Rappels sur les matrices de changement de base)
❍ (Th) Soient $(p, q) \in \mathbb{N}^{*2}$. On note $J_r = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \in \mathcal{M}_{p,q}(\mathbf{K})$. Soit $M \in \mathcal{M}_{p,q}(\mathbf{K})$. $rg(M) = r \Rightarrow M \sim J_r$.
♦ (Th) $\forall (A, B) \in \mathcal{M}_{p,q}(\mathbf{K})$, $A \sim B \Leftrightarrow rg\ A = rg\ B$.
Le nombre de classes d'équivalence est $Min(p, q) + 1$.
♦ (Th) $\forall M \in \mathcal{M}_{p,q}(\mathbf{K})$, $rg(M) = rg({}^tM)$. [demo avec J_r]

18 – Opérations élémentaires sur les matrices

I Base canonique de $\mathcal{M}_n(K)$

Rem : $E_{i\,j}\, E_{k\,l} = \delta_{j\,k}\, E_{i\,l}$.
Transvection : $T_{i\,j}(\lambda) = I_n + \lambda E_{i\,j}$. $(i \neq j)$
Permutation : $P_{i\,j} = I_n - E_{i\,i} - E_{j\,j} + E_{i\,j} + E_{j\,i}$. $(i \neq j)$
Dilatation : $D_i(\lambda) = I_n + (1 - \lambda) E_{i\,i}$.

II Résolution de AX = B par pivot partiel

$A \in GL_n(\mathbf{K})$, $B \in \mathcal{M}_{n,1}(\mathbf{K})$. On cherche X dans $\mathcal{M}_{n,1}(\mathbf{K})$ tel que AX = B.
On triangulise le tout. On remonte. Le nombre d'opérations $\sim n^3/3$.

III Autres applications

♦ Calcul de A^{-1} : $AX = B_j$ où $B_j = {}^t[\,0 \ldots 0\ 1\ 0 \ldots 0\,]$. Nombre d'opérations = $O(n^3)$.
Les solutions X seront les vecteurs colonnes de A^{-1}.

♦ Calcul de dét A : produit des éléments diagonaux pour la matrice triangulisée.
Mais numériquement, si A n'est pas inversible, dét $A = 10^{-15}$.

IV (Ex) $Sl_n(\mathbb{R})$ engendré par les transvections

$SL_n(\mathbb{R}) = \{ M \in \mathcal{M}_n(\mathbb{R}) / \text{dét } M = 1 \}$ est un sous-groupe de $GL_n(\mathbb{R})$.

Il est engendré par $\{ T_{i\,j}(\lambda) / i \neq j \text{ et } \lambda \in \mathbb{R}^* \}$

Démo : par des $T_{i\,j}$, on rend la matrice égale à l'identité : $(\Pi\, T_{i\,j}(\lambda))\ M = I_n$. Les inverses des $T_{i\,j}(\lambda)$ sont des $T_{i\,j}(-\lambda)$ donc M peut s'écrire en fonction des $T_{i\,j}$.

V (Ex) Décomposition LR

♦ Soit $M \in GL_n(\mathbb{R})$.

$\exists$ L triangulaire inférieure, $\exists$ R triangulaire supérieure tels que $M = LR \Leftrightarrow \forall\, k \in \mathbb{N}_n$, dét $M_k \neq 0$.

où M_k (mineurs principaux) est la matrice de $\mathcal{M}_k(\mathbb{R})$ extraite de M qui comporte le carré $k \times k$ du haut à gauche.

[demo $\Rightarrow$ produit par blocs ; $\Leftarrow$ récurrence sur n]
Rem : L'unicité est assurée si on impose à L de ne comporter que des 1 sur la diagonale.
Autre démonstration "constructive" de $\Leftarrow$: on multiplie M à gauche par des $T_{i\,j}(\lambda)$ pour obtenir une matrice triangulaire supérieure. On fait en sorte que les $T_{i\,j}$ soient tous triangulaires inférieurs.

♦ Application : Pour résoudre MX = B, et M = LR on résoud d'abord RY = B puis RX = Y.
Nombre d'opérations = $O(n^2)$.

FORMES QUADRATIQUES

19 – Formes bilinéaires symétriques sur un $\mathbb{R}$ ev

I Généralités

Soit E un $\mathbb{R}$ – ev. Soit $B : E \times E \to \mathbb{R}$.

On dit que B est bilinéaire si $\forall x \in E$, $y \to B(x, y)$ et $y \to B(y, x)$ sont des formes linéaires.

On dit que B est symétrique si $\forall (x, y) \in E^2$, $B(x, y) = B(y, x)$.

Ex : $\mathbb{R}^n$. Produit scalaire canonique

Ex : $(X, Y) \in \mathcal{M}_n(\mathbb{R})^2 \to Tr(XY)$ est une forme bilinéaire symétrique (pas définie positive).

Ex : (f, g) $C^0([a, b], \mathbb{R})^2 \to \int_a^b fgw$ où $w \in C^0([a, b], \mathbb{R}_+^*)$ aussi.

Ex : $(x, y) \in E \to \varphi(x)\psi(y)$ où $(\varphi, \psi) \in E^{*2}$ est une forme bilinéaire.

II Formes quadratiques

(Def) Soit $B : E \to \mathbb{R}^2$ une FBS sur E. $q : x \in E \to B(x, x) \in \mathbb{R}$ est appelée forme quadratique associée à B.

L'ensemble $\mathcal{B}(E)$ des formes bilinéaires symétriques sur E est un **K**–ev.

L'ensemble $\mathcal{Q}(E)$ des formes quadratiques sur E est aussi un **K**–ev.

L'application $\varphi : B \in \mathcal{B}(E) \to q \in \mathcal{Q}(E)$ appartient à $\mathcal{L}(\mathcal{B}(E), \mathcal{Q}(E))$

Formules de polarisation : Soit $B \in \mathcal{B}(E)$ et q la forme quadratique associée.

- $\forall (x, y) \in E^2$, $B(x, y) = \frac{1}{4} (q(x + y) - q(x - y))$
- $\forall (x, y) \in E^2$, $B(x, y) = \frac{1}{2} (q(x + y) - q(x) - q(y))$ [demos developpement]

(Th) φ est donc un isomorphisme.

III Formes quadratiques positives

$q \in \mathcal{Q}(E)$ est dite positive si $\forall x \in E$, $q(x) \geq 0$. Rem : $(\forall (x, y) \in Z^2, B(x, y) \geq 0) \Rightarrow B = 0$.

Ex : $B(x, y) = \Sigma \alpha_i x_i y_i \in \mathcal{B}(\mathbb{R}^n)$ est positive $\Leftrightarrow \forall i \in \mathbb{N}_n$, $\alpha_i \geq 0$.

Ex : $B(f, g) = \int_a^b f g w \in \mathcal{B}(C^0([a, b], \mathbb{R})$ est positive $\Leftrightarrow$ w positive.

Ex : $B(X, Y) = Tr(XY) \in \mathcal{B}(\mathcal{M}_n(\mathbb{R}))$ n'est pas forcément positive (Contrexemple dans $\mathbb{R}^2$).

(Th) Théorème de Cauchy Schwarz : Soit $B \in \mathcal{B}(E)$, B positive. Alors $\forall (x, y) \in E^2$, $|B(x, y)|^2 \leq B(x, x)\, B(y, y)$.

[demo avec $f : t \to q(x + ty) \geq 0$]

IV Formes bilinéaires symétriques définies positives

Soit $B \in \mathcal{B}(\mathbb{R}^n)$. On dit que B est définie positive si $\forall x \in E \setminus \{0\}$, $q(x) > 0$.

Ex : $B(f, g) = \int_a^b fgw \in \mathcal{B}(C^0([a, b], \mathbb{R})$ est définie positive $\Leftrightarrow \{ x \in [a, b] / w(x) > 0 \}$ est dense dans [a, b].

$w(x) = x\,|\sin(1/x)|$ convient.

(Th) Soit B une FBSDP sur E. Alors $\forall (x, y) \in E^2$, $|B(x, y)|^2 \leq q(x)\, q(y)$, et $|B(x, y)|^2 = q(x)\, q(y) \Leftrightarrow (x, y)$ liée.

[demo avec le même f]

20 – FBS sur un $\mathbb{R}$ ev de dimension finie

I Matrice d'une FBS

♦ Soit $B = (e_1, ..., e_n)$ une base de E, et $\varphi \in \mathcal{B}(E)$. On note $a_{ij} = \varphi(e_i, e_j)$.
On définit $Mat(\varphi, B)$ comme $[a_{ij}]$.
(Th) $\forall (x, y) \in E^2$, soient X et $Y \in \mathcal{M}_{n,1}(\mathbb{R})$ leurs coordonnées dans B. Alors $\varphi(x, y) = {}^tX\, M\, Y$. [demo]

Rem : Soit $B = (e_1, ..., e_n)$ base de E. L'application $q \in \mathcal{Q}(E) \to Mat(q, B) \in \mathcal{S}_n(\mathbb{R})$ est un isomorphisme. [d]

Corollaire : $\dim \mathcal{Q}(E) = \dim \mathcal{B}(E) = n(n+1)/2$.

♦ Soient B, B' bases de E. $\varphi \in \mathcal{B}(E)$. Soient $M = Mat(\varphi, B)$ et $M' = Mat(\varphi, B')$.
Soit P la matrice de passage de B à B' : $P = Mat(Id, B', B)$. Alors $M' = {}^tP\, M\, P$. [demo avec lemme]
Lemme : $(\forall (U, V) \in \mathcal{M}_{n,1}(\mathbb{R})^2, {}^tU\, M\, V = 0) \Rightarrow M = 0$. [demo avec vecteurs de la base canonique]
On définit 3 relations d'équivalence (à ne pas confondre) :

$\forall (M, M') \in \mathcal{S}_n(\mathbb{R})^2$, M et M' sont dites <u>congruentes</u> ssi $\exists P \in GL_n(\mathbb{R}), M' = {}^tP\, M\, P$.
$\forall (M, M') \in \mathcal{M}_n(\mathbb{R})^2$, M et M' sont dites <u>semblables</u> ssi $\exists P \in GL_n(\mathbb{R}), M' = P^{-1}\, M\, P$.
$\forall (M, M') \in \mathcal{M}_n(\mathbb{R})^2$, M et M' sont dites <u>équivalentes</u> ssi $\exists (P, Q) \in GL_n(\mathbb{R}), M' = P\, M\, Q \Leftrightarrow rg\, M = rg\, M'$. (Rappel)

II Rang

♦ Soit B une base de E. Soit $q \in \mathcal{Q}(E)$. On définit $rg\, q = rg\, Mat(q, B)$. [indép de B]
♦ <u>Application linéaire associée à une forme quadratique</u> : Soit $\varphi \in \mathcal{B}(E)$.
Soit $u : x \in E \to \varphi_x \in E^*$ où $\varphi_x : y \in E \to \varphi(x, y) \in \mathbb{R}$. $u \in \mathcal{L}(E, E^*)$.
Soit B une base de E et B^* sa duale. Alors : $Mat(u, B, B^*) = Mat(\varphi, B)$.
Rem : $rg\, \varphi = rg\, u$. (autre manière de définir $rg\, \varphi$)
<u>Par définition</u>, on pose $Ker\, q = Ker\, u = \{ x \in E / \forall y \in E, \varphi(x, y) = 0 \}$ [attention]
On appelle l'ensemble des vecteurs <u>isotropes</u> de q $\{ x \in E / q(x) = 0 \}$.
Warning, $Ker\, q \neq \{ x \in E / q(x) = 0 \}$ en général.
♦ Soit $q \in \mathcal{Q}(E)$. On dit que q est <u>dégénérée</u> si $Ker\, q \neq \{0\}$.
Rem : q non dégénérée $\Leftrightarrow Ker\, q = \{0\} \Leftrightarrow$ u isomorphisme $\Leftrightarrow Mat(q, B) \in GL_n(\mathbb{R})$ où B est une base de E.

III Exemples

♦ Dans $\mathbb{R}^2$, $q(x_1, x_2) = x_1^2 - x_2^2$. Alors $\varphi((x_1, x_2), (y_1, y_2)) = x_1x_2 - y_1y_2$. $Ker\, q = \{0\}$. Isotropes = 2 droites.
♦ Dans $\mathbb{R}^2$, $q(x_1, x_2) = x_1^2$. $Ker\, q = \mathbb{R}\,(0,1)$ = vecteurs isotropes.
♦ Dans $\mathcal{M}_n(\mathbb{R})$, $q(M) = Tr(M^2)$. $\varphi(M, N) = Tr(MN)$. $Ker\, q = \{0\}$. $\varphi(E_{ij}, E_{kl}) = 1 \Leftrightarrow j = k$ et $i = l$.
$Mat(q, canon)$ est une matrice de permutation. On peut l'écrire en rangeant les E_{ij} suivant : (E_{ii}) ; $(E_{ij}\, E_{ji})$...
♦ Dans $\mathcal{M}_2(\mathbb{R})$, $q(M) = dét(M)$. $Ker\, q = \{0\}$.

IV Formes quadratiques positives

♦ (Th) Soit $q \in \mathcal{Q}(E)$, $q \geq 0$. Alors $\forall x \in E, q(x) = 0 \Leftrightarrow x \in Ker\, q$. [demo rapide]
L'ensemble des vecteurs isotropes est $Ker\, q$.
♦ (Th) Soit $q \in \mathcal{Q}(E)$. q est positive et non dégénérée $\Leftrightarrow$ q est définie positive.
♦ Soit E un espace vectoriel euclidien. Soit $p \in \mathcal{L}(E)$ un projecteur tel que $\forall x \in E, \|p(x)\| \leq \|x\|$.
Montrer $Ker\, p \perp Im\, p$ (Ex) [on utilise $q(x) = \|x\|^2 - \|p(x)\|^2$]

21 – Méthode de Gauss

Soit E un $\mathbb{R}$ – espace vectoriel de dimension finie.

♦ (Th) Soit $q \in \mathcal{Q}(E)$ et φ sa forme polaire. Alors E possède une base orthogonale $B = (e_1, ..., e_n)$ pour q :

$\forall (i, j) \in \mathbb{N}_n^2, i \neq j \Rightarrow \varphi(e_i, e_j) = 0.$ [demo par récurrence sur n = dimE]

♦ Soit $q \in \mathcal{Q}(E)$. Soit $B = (e_1, ..., e_n)$ une base q – orthogonale. $Mat(q, B) = diag(\alpha_1, ..., \alpha_n)$ où $\forall i \in \mathbb{N}_n, \alpha_i = q(e_i)$.

Soit $r = rg(q) = \#\{ i \in \mathbb{N}_n / \alpha_i \neq 0 \}$. On suppose $a_1, ..., a_r$ non nuls et $a_{r+1}, ..., a_n$ nuls ($e_{r+1}, ..., e_n$ sont isotropes).

Alors $q = \Sigma \alpha_i e_i^{*2}$.

Réciproque : supposons $\alpha_1, ..., \alpha_r$ réels non nuls et $\varphi_1, ..., \varphi_r$ des formes linéaires indépendantes.

Soit $q = \Sigma \alpha_i \varphi_i^2$. C'est une forme quadratique. On peut trouver une base $B = (e_1, ..., e_n)$ telle que $q = \Sigma \alpha_i e_i^{*2}$.

♦ Algorithme de Gauss : Soit $B = (e_1, ..., e_n)$ une base de E. Soit $q \in \mathcal{Q}(E)$. Soit $M = [a_{ij}] = Mat(q, B)$.

Soit $x \in E$. On note $x_i = e_i^*(x)$. $q(x) = {}^tX M X = \Sigma a_{ij} x_i x_j$

• 1e cas : $\exists i \in \mathbb{N}_n, a_{ii} \neq 0$. Si par exemple $a_{11} \neq 0$, on écrit

$$q(x) = a_{11}\left(x_1 + \frac{a_{12}}{a_{11}} x_2 + ... + \frac{a_{1n}}{a_{11}} x_n\right)^2 + q_1(x_2, ..., x_n).$$

On recommence avec q_1.

• 2e cas : $\forall i \in \mathbb{N}_n, a_{ii} = 0$. Si par exemple $a_{12} \neq 0$, on écrit

$$q(x) = a_{12}\left(x_1 + \frac{a_{23}}{a_{12}} x_3 + ... + \frac{a_{2n}}{a_{12}} x_n\right)\left(x_2 + \frac{a_{13}}{a_{12}} x_3 + ... + \frac{a_{1n}}{a_{12}} x_n\right) + q_1(x_3, ..., x_n) = a_{12}\,\varphi_1\,\varphi_2 + q_1(x_3, ..., x_n)$$

$$q(x) = \frac{a_{12}}{4}(\varphi_1 + \varphi_2)^2 - \frac{a_{12}}{4}(\varphi_1 - \varphi_2)^2 + q_1(x_3, ..., x_n).$$

On recommence avec q_1.

A la fin, on obtient l'écriture de q sous la forme $\sum \alpha_i \varphi_i^2$, où (φ_i) est une famille libre dans E^*

[~d récurrence sur le nombre de variables, avec des matrices]

Ex : $$x_1 x_2 = \frac{1}{4}(x_1 + x_2)^2 - \frac{1}{4}(x_1 - x_2)^2$$

$$x_1 x_2 + x_1 x_3 + x_2 x_3 = \frac{1}{4}(x_1 + x_2 + 2x_3)^2 - \frac{1}{4}(x_1 - x_2)^2 - x_3^2$$

$$x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4 = \frac{1}{4}(x_1 + x_2 + 2x_3 + 2x_4)^2 - \frac{1}{4}(x_1 - x_2)^2 - \left(x_3 + \frac{1}{2} x_4\right)^2 - \frac{3}{4} x_4^2$$

⌦ Il faut bien connaître la méthode de Gauss. (Centrale2000)