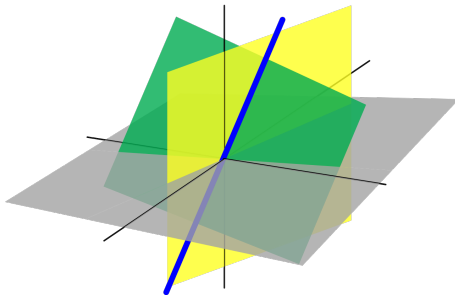


ALGÈBRE LINÉAIRE

COURS DU 12 DÉCEMBRE

Jérôme Scherer



7.1.3 THÉORÈME SPECTRAL

THÉORÈME SPECTRAL

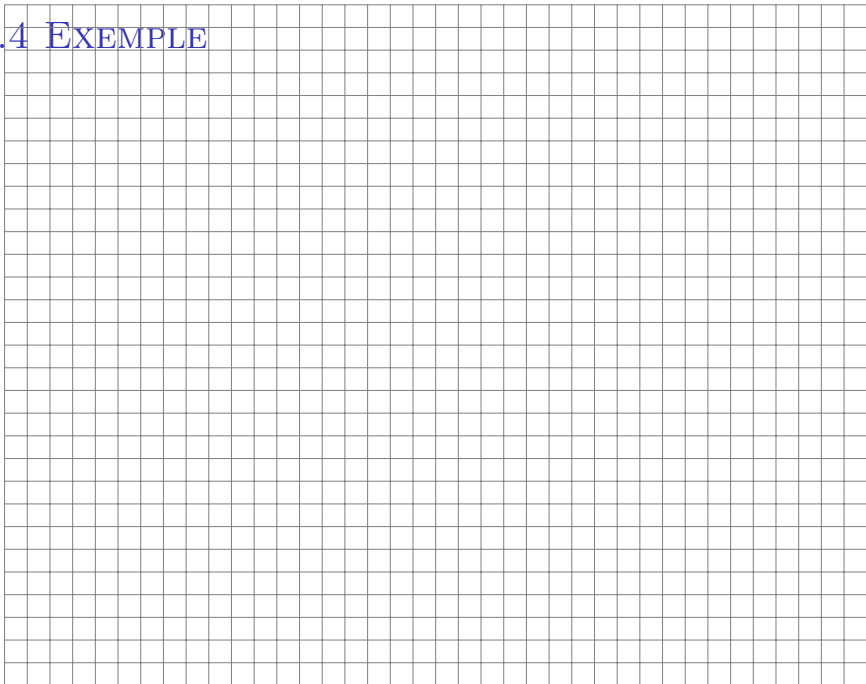
Soit A une matrice symétrique. Alors

- 1 A admet n valeurs propres réelles (avec multiplicité).
- 2 Pour toute valeur propre λ on a $\text{mult}(\lambda) = \dim E_\lambda$.
- 3 Si $\lambda \neq \mu$, alors $E_\lambda \perp E_\mu$.
- 4 A est orthodagonalisable.

ATTENTION !

Si λ est une valeur propre de multiplicité ≥ 2 , alors la base de vecteurs propres de E_λ fournie par la méthode de Gauss n'est pas orthogonale en général, il faut **Gram-Schmidter** pour obtenir une base orthonormée de vecteurs propres.

7.1.4 EXAMPLE



7.1.4 EXAMPLE, FIN



7.1.5 MÉTHODE.

- ❶ Vérifier que A est symétrique.
- ❷ Calculer $c_A(t)$ et en extraire les racines (valeurs propres).
- ❸ Calculer les espaces propres. Pour chacun, le procédé de Gram-Schmidt donne une base orthonormée.
- ❹ En rassemblant les bases des espaces propres on obtient une base orthonormée $\mathcal{U}$ de $\mathbb{R}^n$.
- ❺ La matrice P dont les colonnes sont les vecteurs $\vec{u}_i$ de $\mathcal{U}$ est orthogonale et $P^T A P$ est diagonale.

AVANTAGE

La matrice de changement de base inverse est P^T .

7.1.6 MATRICE DE PROJECTION

Soit $\vec{u}$ un vecteur unitaire et $A = \vec{u} \vec{u}^T$. Alors

$$A\vec{x} = \vec{u}(\vec{u}^T \vec{x}) = (\vec{u} \cdot \vec{x}) \vec{u}$$

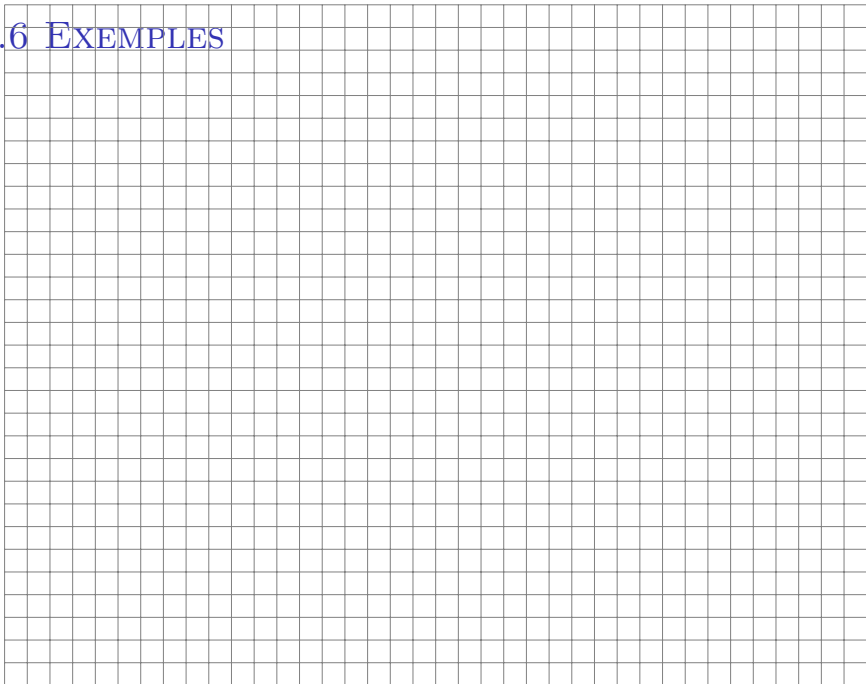
- 1 $\vec{u}$ est un vecteur propre de A pour la valeur propre 1 car $(\vec{u} \cdot \vec{u}) \vec{u} = \vec{u}$.
- 2 Posons $W = \text{Vect}(\vec{u})$. Alors $W^\perp$ est le noyau de A .
- 3 Ainsi $E_1 = W$ et $E_0 = W^\perp$.

PROPOSITION

La matrice $A = \vec{u} \vec{u}^T$ est la matrice de la projection orthogonale sur $W = \text{Vect}(\vec{u})$. On a $A\vec{x} = \text{proj}_{\vec{u}} \vec{x}$.

C'est un cas particulier que nous avons vu pour UU^T , matrice de projection orthogonale quand les colonnes de U sont orthonormées.

7.1.6 EXAMPLES



7.1.7 DÉCOMPOSITION SPECTRALE

DÉFINITION

Soit A symétrique, U orthogonale et $U^T A U = D$ diagonale.

L'ensemble des valeurs propres de A est appelé **spectre** de A .

$$\begin{aligned} A &= U D U^T = (\vec{u}_1 \ \vec{u}_2 \ \dots \ \vec{u}_n) \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda_n \end{pmatrix} \begin{pmatrix} \vec{u}_1^T \\ \vec{u}_2^T \\ \vdots \\ \vec{u}_n^T \end{pmatrix} \\ &= (\lambda_1 \vec{u}_1 \ \dots \ \lambda_n \vec{u}_n) \begin{pmatrix} \vec{u}_1^T \\ \vdots \\ \vec{u}_n^T \end{pmatrix} = \lambda_1 \vec{u}_1 \vec{u}_1^T + \dots + \lambda_n \vec{u}_n \vec{u}_n^T \end{aligned}$$

$A = \lambda_1 \vec{u}_1 \vec{u}_1^T + \dots + \lambda_n \vec{u}_n \vec{u}_n^T$

 est la **décomposition spectrale**.

7.1.7 INTERPRÉTATION DE LA DÉC. SPECTRALE

Si A est une matrice symétrique, alors

$$A = \lambda_1 \vec{u}_1 \vec{u}_1^T + \cdots + \lambda_n \vec{u}_n \vec{u}_n^T$$

est sa décomposition spectrale.

Ainsi A se décompose en une combinaison linéaire de projections orthogonales !

7.1.7 EXEMPLE DE DÉC. SPECTRALE

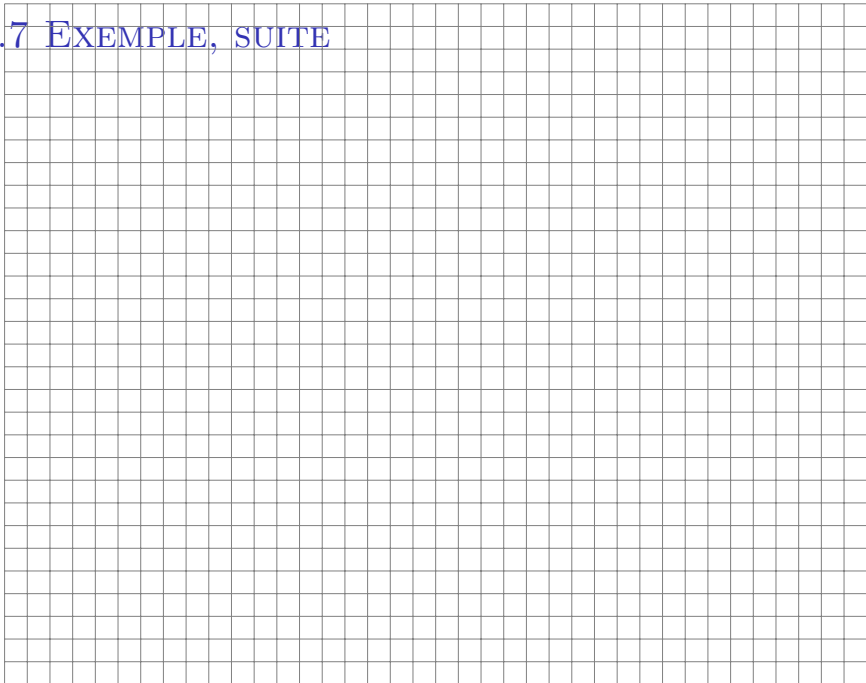
Soit $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ la matrice symétrique que nous avons orthodiagonalisée mardi. Nous avons trouvé une base orthonormée de vecteurs propres (pour les valeurs propres -1 et 3) :

$$\mathcal{U} = (\vec{u}_1, \vec{u}_2) = \left(\begin{pmatrix} -\sqrt{2}/2 \\ \sqrt{2}/2 \end{pmatrix}, \begin{pmatrix} \sqrt{2}/2 \\ \sqrt{2}/2 \end{pmatrix} \right)$$

La décomposition spectrale de A est donc

$$A = -1 \cdot \vec{u}_1 \vec{u}_1^T + 3 \cdot \vec{u}_2 \vec{u}_2^T$$

7.1.7 EXEMPLE, SUITE



A.12 LA CARACTÉRISTIQUE D'UN CORPS FINI

Soit K un corps fini (ayant un nombre fini d'éléments).

Considérons l'ensemble de tous les multiples entiers de 1_K dans K , c'est-à-dire les éléments de la forme $n \cdot 1_K = 1_K + \cdots + 1_K$.

Comme K est fini, $\{n \cdot 1_K \mid n \in \mathbb{Z}\}$ aussi est fini. Autrement dit, il existe des entiers n tels que $n \cdot 1_K = 0$ (si $m \cdot 1_K = m' \cdot 1_K$, alors $(m - m') \cdot 1_K = 0_K$).

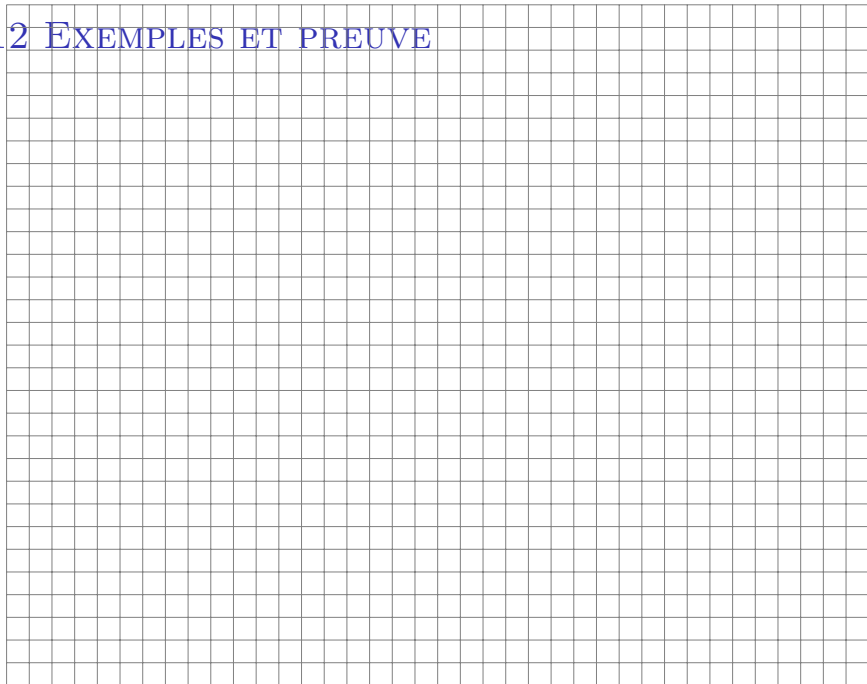
DÉFINITION

Le plus petit entier non nul n tel que $n \cdot 1_K = 0$ s'appelle la **caractéristique** de K et on le note $\text{car}K$.

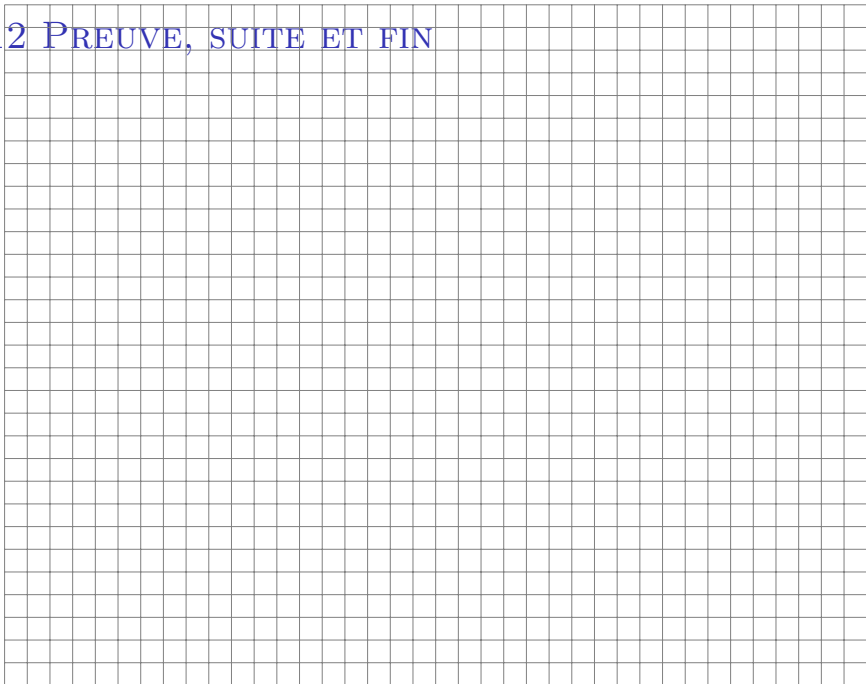
PROPOSITION

La caractéristique d'un corps fini K est un nombre premier.

A.12 EXEMPLES ET PREUVE



A.12 PREUVE, SUITE ET FIN



A.13 LA CARDINALITÉ D'UN CORPS FINI

Soit $p = \text{car}K$. Alors le corps $\mathbb{F}_p$ agit sur K par multiplication.

DÉFINITION

Soit $k \in \mathbb{F}_p$ et $x \in K$. On pose $k \cdot x = (k \cdot 1_K) \cdot x$.

Cette action est bien définie puisque $p \cdot 1_K = 0$. Les propriétés de l'action sont toutes conséquence du fait que K est un corps.

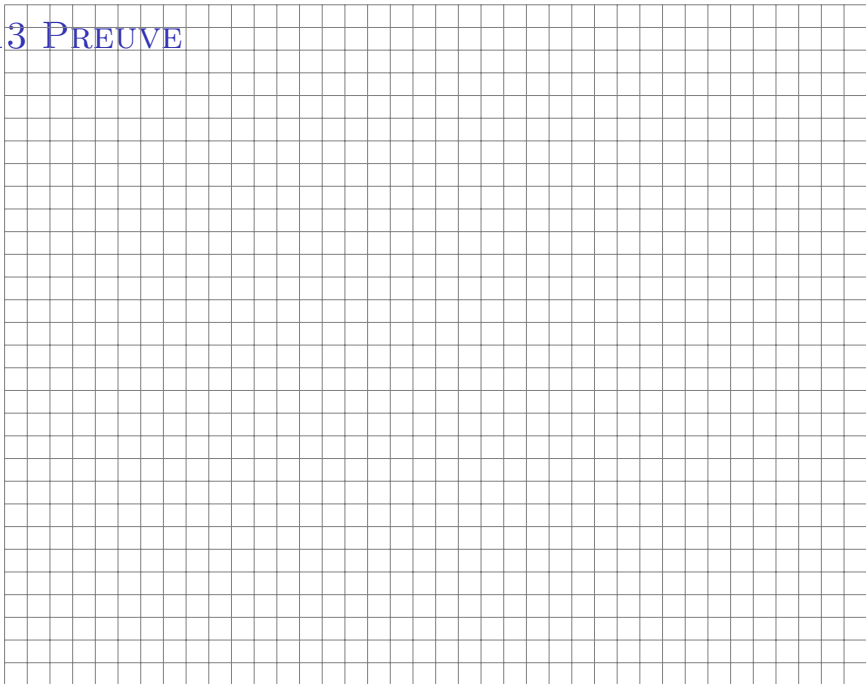
PROPOSITION

Soit K un corps fini et $p = \text{car}K$. Alors K est un $\mathbb{F}_p$ -espace vectoriel.

THÉORÈME

Soit K un corps fini et $p = \text{car}K$. Alors il existe n tel que K a p^n éléments. On appelle ce nombre la **cardinalité** de K .

A.13 PREUVE



A.14 CONSTRUCTION DE CORPS FINIS

La construction de $\mathbb{F}_4$ n'est pas un cas isolé, la méthode générale fonctionne de la même manière. Soit p un nombre premier.

- 1 Trouver un polynôme $p(t)$ unitaire irréductible de degré n dans $\mathbb{F}_p[t]$.
- 2 Considérer l'ensemble K de tous les restes de division par $p(t)$. Il y en a p^n .
- 3 Définir la somme dans K comme dans $\mathbb{F}_p[t]$.
- 4 Définir le produit dans K par celui de $\mathbb{F}_p[t]$, **modulo** $p(t)$.
- 5 Alors K est un corps de cardinalité p^n .

A.15 EXEMPLE : LE CORPS $\mathbb{F}_{49}$

Nous cherchons un polynôme irréductible de degré 2.

PROPOSITION

Soit K un corps et $p(t) = t^2 - a$. Si a n'est pas un carré, alors $p(t)$ est irréductible.

Preuve. En effet $p(t)$ est irréductible si et seulement si il n'a pas de racine (car il est de degré 2), si et seulement si $p(x) \neq 0$ pour tout $x \in K$.

Or, $p(x) = x^2 - a = 0$ si et seulement si $a = x^2$ est un carré. $\square$.

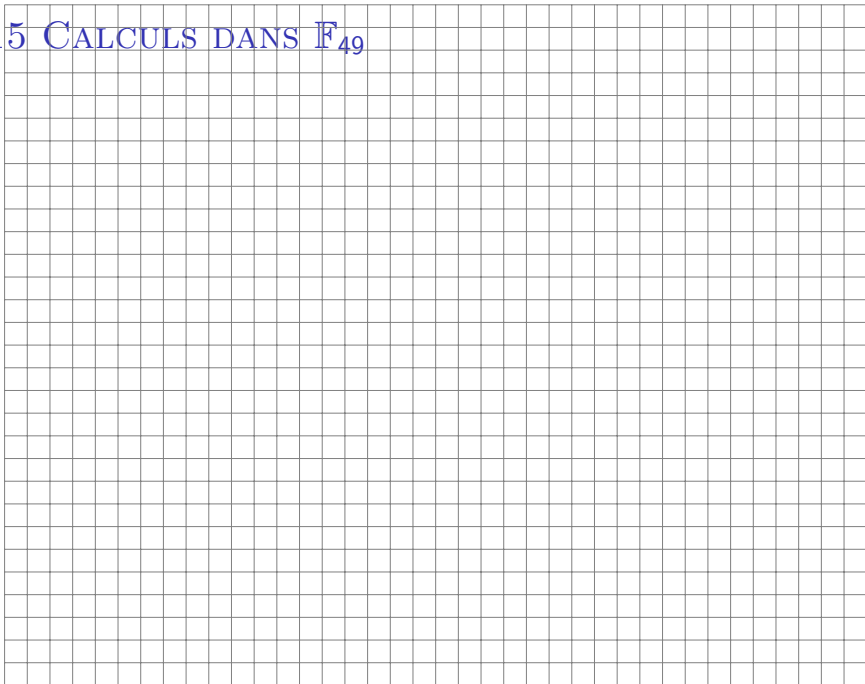
REMARQUE

Pour trouver un polynôme irréductible de degré 2 à coefficients dans $\mathbb{F}_7$, nous cherchons à comprendre quels éléments sont des carrés.

A.15 LES CARRÉS DE $\mathbb{F}_7$



A.15 CALCULS DANS $\mathbb{F}_{49}$



A.15 LA NOTION DE CLASSE

Nous avons construits $\mathbb{F}_p$ comme le corps des restes de la division euclidienne des entiers $\mathbb{Z}$ par p , un nombre premier. Chaque entier dont le reste de la division vaut 2 représente alors dans $\mathbb{Z}$ le même élément dans $\mathbb{F}_p$:

$$\dots, 2 - 2p, 2 - p, 2, 2 + p, 2 + 2p, \dots$$

On dit que le reste 2 est la **classe** de tous ces nombres, on écrit souvent $[2] \in \mathbb{F}_p$ pour distinguer cet élément du nombre entier 2.

Dans $\mathbb{F}_{49}$, l'élément α est la classe $[t]$. C'est un élément qui est représenté dans $\mathbb{F}_7[t]$ par tous les polynômes dont le reste de la division par $t^2 - 3$ vaut t , par exemple

$$t^2 + t + 3, t^3 + 5t, \dots$$

A.16 QUELQUES FAITS SANS PREUVE

PROPOSITION

Soit p un nombre premier et $n \geq 1$ un entier. Il existe toujours un polynôme irréductible de degré n dans $\mathbb{F}_p[t]$.

THÉORÈME

Soit p un nombre premier et $n \geq 1$ un entier. Il existe toujours un corps fini de cardinalité p^n .

REMARQUE

En fait un tel corps est unique à isomorphisme près, ce qui signifie que deux choix différents de polynômes $p(t)$ et $q(t)$ donnent des corps $\mathbb{F}_p[t]/(p(t))$ et $\mathbb{F}_p[t]/(q(t))$ qui sont isomorphes.

Il existe donc un isomorphisme $f: \mathbb{F}_p[t]/(p(t)) \rightarrow \mathbb{F}_p[t]/(q(t))$.

A.17 DEUX CORPS À HUIT ÉLÉMENTS ?

On cherche dans $\mathbb{F}_2[t]$ un polynôme de degré 3 irréductible. Il y en a huit.

- ❶ t^3 , $t^3 + t$, $t^3 + t^2$ et $t^3 + t^2 + t$ s'annulent en 0 : éliminés !
- ❷ $t^3 + 1$, $t^3 + t^2 + t + 1$ s'annulent en 1 : éliminés !

PROPOSITION

Les polynômes $p(t) = t^3 + t + 1$ et $q(t) = t^3 + t^2 + 1$ sont les seuls polynômes de degré 3 irréductibles de $\mathbb{F}_2[t]$.

On peut donc construire $\mathbb{F}_8 = \mathbb{F}_2[t]/(p(t))$ et $\mathbb{F}'_8 = \mathbb{F}_2[t]/(q(t))$.

Appelons α la classe de t dans $\mathbb{F}_8$ et β celle de t dans $\mathbb{F}'_8$.

8 REMARQUES

A.18 UN SEUL CORPS À HUIT ÉLÉMENTS

- ❶ Dans $\mathbb{F}_8$, on a $t^3 + t + 1 = 0$, autrement dit $\alpha^3 = \alpha + 1$.
- ❷ Dans $\mathbb{F}'_8$, on a $t^3 + t^2 + 1 = 0$, autrement dit $\beta^3 = \beta^2 + 1$.

REMARQUE

Les éléments α et β se comportent différemment sous la multiplication !

Calculons les puissances de α et celles de β pour comparer la structure multiplicative de ces deux corps. Pour construire un isomorphisme $f: \mathbb{F}_8 \rightarrow \mathbb{F}'_8$, nous devons envoyer zéro sur zéro, et un sur un, mais où donc envoyer α ?

7.2.0 RAPPEL : TERMINOLOGIE

- ❶ **Equivalence.** $A \sim B$ si on peut passer de A à B par des opérations élémentaires sur les lignes. Utilité : Résolution de systèmes, calcul du rang.
- ❷ **Similitude.** $A \approx B$ si on peut passer de A à B par un changement de base $A = SBS^{-1}$. Utilité : Représentation d'une application linéaire, diagonalisation.
- ❸ **Congruence.** $A \approx\approx B$ si on peut passer de A à B par un changement de base orthonormée $A = PBP^T$. Utilité : Représentation d'un produit scalaire, pour les matrices symétriques uniquement !

7.2.1 MATRICES CONGRUENTES

Si A est la matrice d'un produit scalaire de V , exprimé dans la base orthonormée $\mathcal{C} = (e_1, \dots, e_n)$, alors

$$\langle u, v \rangle = (u)_{\mathcal{C}}^T A (v)_{\mathcal{C}}$$

On calcule par exemple $\vec{e}_i^T A \vec{e}_j = \vec{e}_i^T \vec{a}_j = a_{ij}$

et comme $\langle e_i, e_j \rangle = a_{ij}$ doit coïncider avec $\langle e_j, e_i \rangle = a_{ji}$, la matrice A est **symétrique**.

PROPOSITION

Deux matrices symétriques A et B représentent le même produit scalaire si elles sont congruentes.

7.2.2 PREUVE

Soit P une matrice orthogonale. On considère P comme une matrice de changement de base $(Id)_{\mathcal{B}}^{\mathcal{C}^{an}}$ dont les colonnes sont les vecteurs d'une base orthonormée exprimés en coordonnées dans la base canonique.

On pose $\boxed{\vec{y} = P^{-1}\vec{x} = P^T\vec{x} = (Id)_{\mathcal{C}^{an}}^{\mathcal{B}}\vec{x}}$

Si $\vec{x}$ est un vecteur de $\mathbb{R}^n$ exprimé en coordonnées dans la base canonique, $\vec{y}$ est $(\vec{x})_{\mathcal{B}}$, ce même vecteur exprimé dans la nouvelle base.

Nous avons $\langle \vec{x}, \vec{x}' \rangle = \vec{x}^T A \vec{x}'$ et nous devons démontrer que la matrice congruente $B = P^T A P$ représente le même produit scalaire, mais pour des vecteurs exprimés dans la base orthonormée $\mathcal{B}$.

7.2.3 ENCORE LE THÉORÈME SPECTRAL

On travaille avec

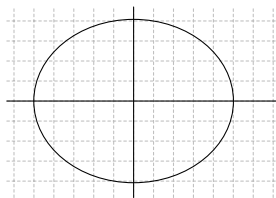
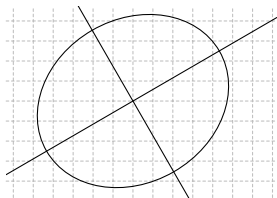
- ① un espace vectoriel V de dimension finie n et une base $\mathcal{B}$;
- ② un produit scalaire représenté par une matrice symétrique A par rapport à la base $\mathcal{B}$.

THÉORÈME SPECTRAL

Il existe un changement de base orthonormée qui permet de représenter ce produit scalaire par une matrice diagonale.

7.2.4 EXEMPLE : ELLIPSE

Que représente l'équation $\frac{9}{2}x_1^2 - \sqrt{3}x_1x_2 + \frac{11}{2}x_2^2 = 100$? C'est une courbe de niveau de la fonction de deux variables $Q(x_1, x_2)$.



Via une rotation de 30° on amène les axes de l'ellipse en position standard, $4y_1^2 + 6y_2^2 = 100$.

On peut calculer la longueur des axes de l'ellipse : Si $y_2 = 0$, alors $4y_1^2 = 100$, i.e. $y_1 = \pm 5$. Le **grand axe** mesure 10.

Si $y_1 = 0$, $y_2 = \pm\sqrt{50/3}$, la longueur du **petit axe** vaut $\approx 8,2$.