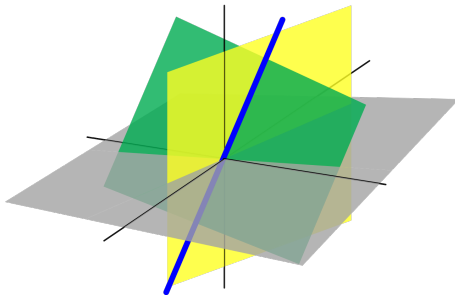


ALGÈBRE LINÉAIRE

COURS DU 17 DÉCEMBRE

Jérôme Scherer



A.14 CONSTRUCTION DE CORPS FINIS

La méthode générale de construction des corps finis fonctionne comme suit. 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 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.16' QUELQUES FAITS SANS PREUVE

THÉORÈME

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

La construction explicite est la suivante : on choisit un polynôme (unitaire) irréductible de degré n dans $\mathbb{F}_p[t]$ et on pose $\mathbb{F}_{p^n} = \mathbb{F}_p[t]/(p(t))$.

NOTATION

On note α l'élément représenté par t . Les éléments de $\mathbb{F}_{p^n}$ sont les restes de la division par $p(t)$, ce sont donc des expressions de la forme $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$. Ainsi $\{1, \alpha, \dots, \alpha^{n-1}\}$ est une base de $\mathbb{F}_{p^n}$ comme $\mathbb{F}_p$ -espace vectoriel.

A.17 DEUX CORPS À HUIT ÉLÉMENTS ?

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

- 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.19 RÉSUMÉ

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 $\mathbb{F}'_8$.

- 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 !

A.20 UN SEUL CORPS À HUIT ÉLÉMENTS

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 ?

Nous avons calculé les puissances de α comme combinaisons linéaires de 1 , α et α^2 , puis nous nous occupons de celles de β pour comparer la structure multiplicative de ces deux corps.

$$\textcircled{1} \quad \alpha^0 = 1;$$

$$\textcircled{2} \quad \alpha^1 = \alpha;$$

$$\textcircled{3} \quad \alpha^2 = \alpha^2;$$

$$\textcircled{4} \quad \alpha^3 = \alpha + 1;$$

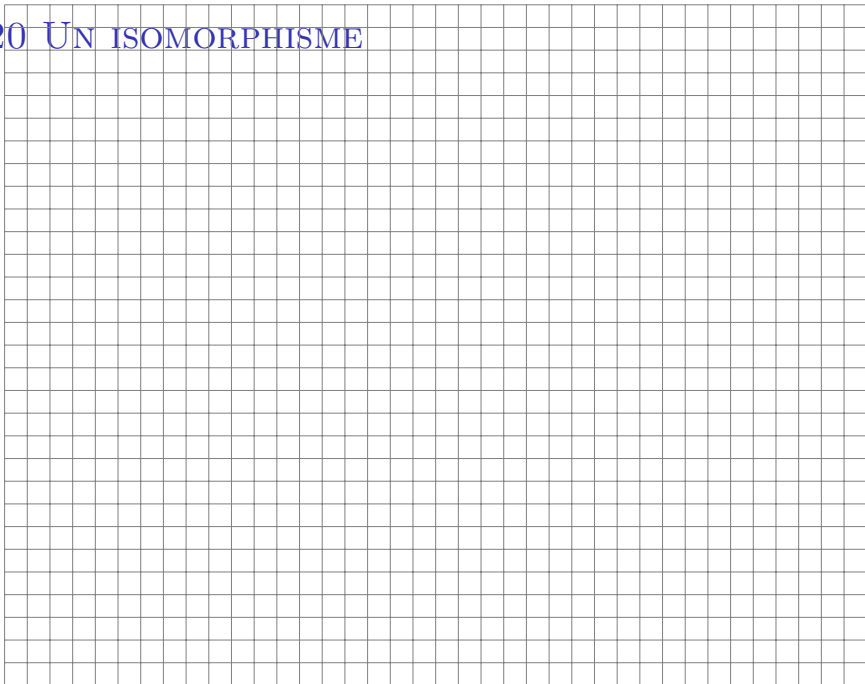
$$\textcircled{5} \quad \alpha^4 = (\alpha + 1)\alpha = \alpha^2 + \alpha;$$

$$\textcircled{6} \quad \alpha^5 = \alpha^2 + \alpha + 1$$

$$\textcircled{7} \quad \alpha^6 = \alpha^2 + 1$$

$$\textcircled{8} \quad \alpha^7 = 1$$

A.20 UN ISOMORPHISME



A.20 UN ISOMORPHISME, SUITE



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 $\mathcal{B}$.

7.2.2 FIN DE LA PREUVE

7.2.3 ENCORE LE THÉORÈME SPECTRAL

On travaille avec

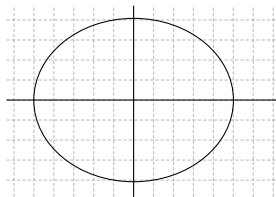
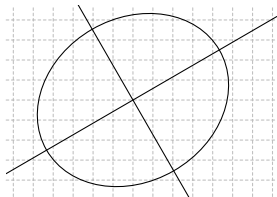
- ① un espace vectoriel V de dimension finie n et une base $\mathcal{B}$;
- ② un produit scalaire représenté par une matrice symétrique A par rapport à la base $\mathcal{B}$.

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 $\approx 8,2$.

7.4. DÉCOMPOSITION EN VALEURS SINGULIÈRES

Soit A une matrice $m \times n$ et $T : \mathbb{R}^n \rightarrow \mathbb{R}^m$ l'application linéaire associée.

Alors T transforme la sphère unité de $\mathbb{R}^n$

$$S = \{ \vec{x} \in \mathbb{R}^n \mid \|\vec{x}\| = 1 \}$$

en un ellipsoïde de $\mathbb{R}^m$.

QUESTION

Dans quelle direction l'étirement est-il **maximal** ?

On cherche donc un vecteur $\vec{v} \in S$ tel que $\|A\vec{v}\|$ est maximal :

$$\|A\vec{v}\|^2 = (A\vec{v})^T A\vec{v} = \vec{v}^T A^T A \vec{v}$$

7.4.1 ETIREMENT MAXIMAL

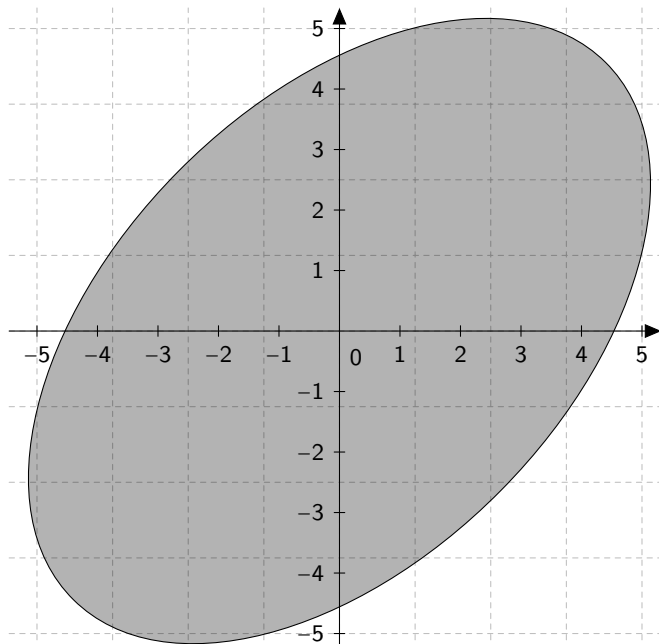
Soit $B = A^T A$. Cette matrice symétrique représente une forme bilinéaire symétrique dont on cherche le maximum, lorsqu'on l'évalue sur un vecteur de norme 1.

PROPOSITION

Le maximum (au carré) est égal à la valeur propre la plus grande de la matrice $B = A^T A$.

Exemple. Soit $A = \begin{pmatrix} 3 & 2 & 2 \\ 2 & 3 & -2 \end{pmatrix}$. L'image de la sphère unité de $\mathbb{R}^3$ est une ellipse dans $\mathbb{R}^2$.

7.4.2 L'IMAGE DE LA SPHÈRE UNITÉ



7.4.3 CALCUL

$$B = A^T A = \begin{pmatrix} 3 & 2 \\ 2 & 3 \\ 2 & -2 \end{pmatrix} \begin{pmatrix} 3 & 2 & 2 \\ 2 & 3 & -2 \end{pmatrix} = \begin{pmatrix} 13 & 12 & 2 \\ 12 & 13 & -2 \\ 2 & -2 & 8 \end{pmatrix}$$

$$c_B(t) = -t(t-25)(t-9)$$

L'étirement maximal est de 5. Mais dans quelle direction ?

$$E_{25} = \text{Vect} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \text{Vect} \begin{pmatrix} \sqrt{2}/2 \\ \sqrt{2}/2 \\ 0 \end{pmatrix}$$

7.4.3 CALCUL, SUITE

$$\begin{pmatrix} 3 & 2 & 2 \\ 2 & 3 & -2 \end{pmatrix} \begin{pmatrix} \sqrt{2}/2 \\ \sqrt{2}/2 \\ 0 \end{pmatrix} = \begin{pmatrix} 5\sqrt{2}/2 \\ 5\sqrt{2}/2 \end{pmatrix}$$

Ce vecteur est l'image par T d'un vecteur unitaire (de la sphère unité). Il est de longueur maximale (5) et correspond au grand axe de l'ellipse que nous avons vue tout-à-l'heure.

LEMME

Soit A une matrice $m \times n$ et $B = A^T A$. Les valeurs propres de B sont positives.

7.4.3 PREUVE



7.4.4 VALEURS SINGULIÈRES

On ordonne les valeurs propres de $B = A^T A$ de sorte que

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0$$

DÉFINITION

Les **valeurs singulières** de A sont les $\sigma_i = \sqrt{\lambda_i}$.

Remarque. On a $\sigma_i = \|Av_i\|$ où v_i est un vecteur propre unitaire de B pour la valeur propre λ_i .

7.4.4 EXEMPLE, SUITE

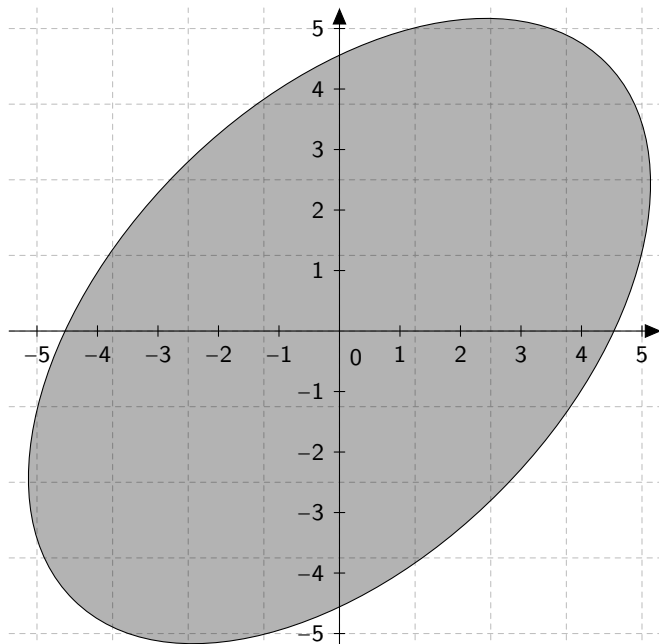
Soit $A = \begin{pmatrix} 3 & 2 & 2 \\ 2 & 3 & -2 \end{pmatrix}$. Alors

❶ $\sigma_1 = 5, \sigma_2 = 3, \sigma_3 = 0.$

❷ $E_9 = \text{Vect} \left\{ \begin{pmatrix} \sqrt{2}/6 \\ -\sqrt{2}/6 \\ 2\sqrt{2}/3 \end{pmatrix} \right\} = \text{Vect} \{ \vec{v}_2 \}$

❸ $A\vec{v}_2 = \begin{pmatrix} 3\sqrt{2}/2 \\ -3\sqrt{2}/2 \end{pmatrix}$

7.4.4 GRAND AXE ET PETIT AXE



7.4.5 L'IMAGE DE A

Soit A une matrice de taille $m \times n$, $(v_1, \dots, v_n)$ une base orthonormée de vecteurs propres unitaires de $B = A^T A$ pour les valeurs propres $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n \geq 0$.

THÉORÈME

Si A admet exactement r valeurs singulières non nulles, alors $(Av_1, \dots, Av_r)$ est une base orthogonale de l'image de A .

Preuve. $(Av_i) \cdot (Av_j) = v_i^T A^T A v_j = v_i^T \lambda_j v_j = 0$ pour $i \neq j$.

En particulier $\|Av_i\|^2 = \lambda_i \|v_i\|^2 > 0$ et les vecteurs $Av_1, \dots, Av_r$ sont orthogonaux, donc linéairement indépendants.

Ils engendrent $\text{Im}A$ car $Av_{r+1} = \dots = Av_n = 0$.

□

7.4.6 DÉCOMPOSITION EN VALEURS SINGULIÈRES

Une **décomposition de A en valeurs singulières** (SVD) est une factorisation $A = U\Sigma V^T$ telle que

❶ U est orthogonale $m \times m$;

❷ V est orthogonale $n \times n$;

❸ $\Sigma = \begin{pmatrix} \sigma_1 & 0 & 0 & \dots & 0 \\ 0 & \ddots & 0 & \dots & 0 \\ 0 & 0 & \sigma_r & 0 & 0 \\ 0 & \dots & 0 & \dots & 0 \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix}$ est de taille $m \times n$.

Les lignes de U et de V sont appelés les **vecteurs singuliers** à gauche et à droite de A .

7.4.6 EXISTENCE DE LA SVD

- ❶ On choisit $V = (\vec{v}_1 \cdots \vec{v}_n)$ où les $\vec{v}_i$ forment une base orthonormée de vecteurs propres de $B = A^T A$, classés dans l'ordre décroissant des valeurs propres λ_i .
- ❷ On pose $\vec{u}_i = \frac{A\vec{v}_i}{\|A\vec{v}_i\|} = \frac{1}{\sigma_i} A\vec{v}_i$ pour $1 \leq i \leq r$.
- ❸ On complète en une base orthonormée $(\vec{u}_1, \dots, \vec{u}_r, \vec{u}_{r+1}, \dots, \vec{u}_m)$ de $\mathbb{R}^m$ et on pose $U = (\vec{u}_1 \cdots \vec{u}_m)$.
- ❹ On calcule $U\Sigma = (\sigma_1 \vec{u}_1, \dots, \sigma_r \vec{u}_r, \vec{0}, \dots, \vec{0}) = A(\vec{v}_1 \cdots \vec{v}_n) = AV$.
- ❺ $U\Sigma V^T = AVV^T = A$.

7.4.6 EXEMPLE, FIN

Si $A = \begin{pmatrix} 3 & 2 & 2 \\ 2 & 3 & -2 \end{pmatrix}$ et $B = A^T A$. Alors $E_0 = \text{Vect} \left\{ \begin{pmatrix} 2/3 \\ -2/3 \\ -1/3 \end{pmatrix} \right\}$.

$$\text{Donc } V = \begin{pmatrix} \sqrt{2}/2 & \sqrt{2}/6 & 2/3 \\ \sqrt{2}/2 & -\sqrt{2}/6 & -2/3 \\ 0 & 2\sqrt{2}/3 & -1/3 \end{pmatrix}$$

$$\text{On connaît déjà } U = \begin{pmatrix} \sqrt{2}/2 & \sqrt{2}/2 \\ \sqrt{2}/2 & -\sqrt{2}/2 \end{pmatrix}$$

$$\text{et enfin } \Sigma = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}.$$

7.4.7 COMMENTAIRES

- ❶ Fonctionne pour des matrices non diagonalisables, même rectangulaires !
- ❷ Utile pour des applications numériques. Les matrices U et V étant orthogonales, l'estimation de l'erreur ou de l'imprécision est dans Σ uniquement.
- ❸ Utile en statistiques (PCA).
- ❹ Utile pour la compression de données

7.4.7 COMPRESSION DES DONNÉES

Exemple trouvé chez [http ://andrew.gibiansky.com/blog/](http://andrew.gibiansky.com/blog/)

Une photo (d'un tigre) est codée par une matrice A de rang 500.

Chacune des images suivantes est produite en remplaçant la matrice

$$A = U\Sigma V^T$$

par la meilleure approximation possible de rang m , c'est-à-dire

$$U\Sigma_m V^T$$

où Σ_m est la matrice Σ_m est obtenue en ne gardant que les m premières valeurs singulières (les plus grandes) :

7.4.7 COMPRESSION DES DONNÉES

Full-Rank Tiger



Rank 200 Tiger



Rank 100 Tiger



Rank 50 Tiger



Rank 30 Tiger



Rank 20 Tiger



Rank 10 Tiger



Rank 3 Tiger

