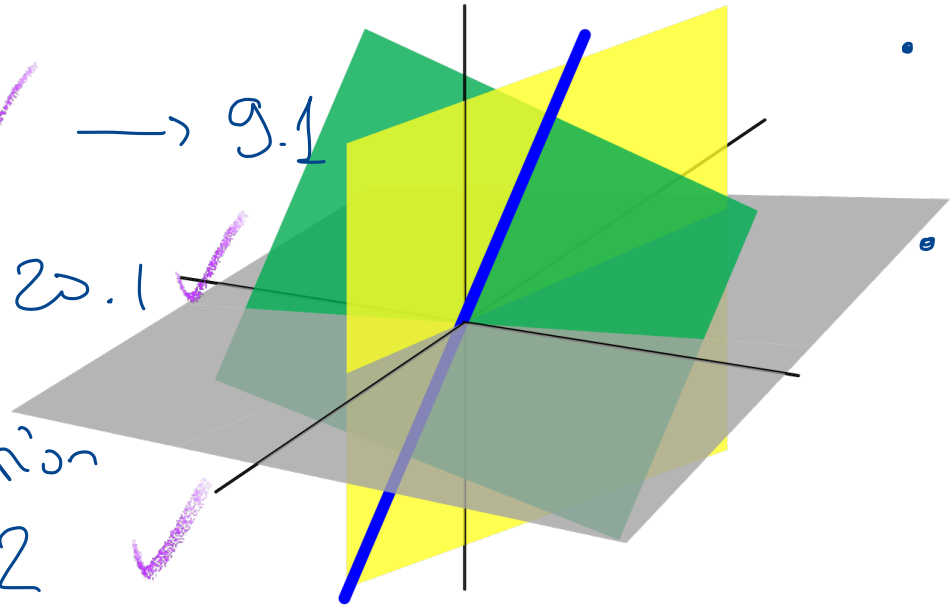
Algèbre Linéaire

Cours du 17 décembre

Jérôme Scherer



1. Evaluation ✓
2. Vendredi CM 1121 ✓
3. Forum ✓ → 17.1.
4. R a Q ✓ → 9.1
5. Examen 20.1 ✓
6. Consultation 13.2 ✓

Pas à l'examen

- évolution de population
- LU
- produit scalaire exotique
- Cramer

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 $\mathbb{F}_p$:

$$\ldots, 2-2p, 2-p, 2, 2+p, 2+2p, \ldots$$

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

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

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 $f : \mathbb{F}_p[t]/(p(t)) \to \mathbb{F}_p[t]/(q(t))$.

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 expression de la forme $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$. Ainsi $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 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 :

1. t^3, t^3+t, t^3+t^2 et t^3+t^2+t s'annulent en 0 : éliminés !
2. 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 $\mathbb{F}'_8$.

A.18 Remarques

$\mathbb{F}_8$ = restes de la division dans $\mathbb{F}_2[t]$ par $p(t)$

$= \{ a + bt + ct^2 \mid a, b, c \in \mathbb{F}_2 \}$

Avec la notation $\alpha = [t]$, $(1, \alpha, \alpha^2)$ est une base du $\mathbb{F}_2$ - espace vectoriel $\mathbb{F}_8$.

Calculons les puissances de α : $[t^3] = [t+1]$

$\alpha^0 = 1$, $\alpha^1 = \alpha$, $\alpha^2 = \alpha^2$, $\alpha^3 = \alpha + 1$ parce que $\alpha^3 + \alpha + 1 = [t]^3 + [t] + [1] = [\underbrace{t^3 + t + 1}_{p(t)}] = 0$ def de $+$ et $\cdot$

$\alpha^4 = \alpha^3 \cdot \alpha = (\alpha+1)\alpha = \alpha + \alpha^2$

$\alpha^5 = \alpha^4 \cdot \alpha = (\alpha + \alpha^2)\alpha = \alpha^2 + \alpha^3 = \alpha^2 + \alpha + 1$

$\alpha^6 = (\alpha^2 + \alpha + 1)\alpha = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha$

$= \alpha^2 + 1$

$\alpha^7 = (\alpha^2 + 1)\alpha = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1$.

tous les éléments non-nuls de $\mathbb{F}_8$

$\mathbb{F}_8^\times$: $1, \beta, \beta^2, \beta^2+1, \beta^2+\beta+1, \beta+1, \beta^2+\beta, 1 = \beta^7, \beta^8 = \beta$!

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 $\mathbb{F}'_8$.

1. Dans $\mathbb{F}_8$, on a $t^3 + t + 1 = 0$, autrement dit $\alpha^3 = \alpha + 1$.
2. 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 $f : \mathbb{F}_8 \to \mathbb{F}'_8$, 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.

1. $\alpha^0 = 1$;
2. $\alpha^1 = \alpha$;
3. $\alpha^2 = \alpha^2$;
4. $\alpha^3 = \alpha + 1$;
5. $\alpha^4 = (\alpha + 1)\alpha = \alpha^2 + \alpha$;
6. $\alpha^5 = \alpha^2 + \alpha + 1$
7. $\alpha^6 = \alpha^2 + 1$
8. $\alpha^7 = 1$

A.20 Un isomorphisme

Idée : $f(\alpha) = \beta$

compatible avec $q(t) = t^3 + t^2 + 1$

$$f(\alpha) + f(1) = f(\alpha + 1) = f(\alpha^3) = f(\alpha)^3 = \beta^3 = \beta^2 + 1$$

$\beta + 1$

compatibilité avec $+$

Observation : Si $f(\alpha) = x$, alors

$$x + 1 = x^3$$

Conclusion : On cherche $x \in \mathbb{F}_8^\times$ tq $x^3 = x + 1$.

Essai : $x = \beta^2$. On veut $(\beta^2)^3 = \beta^2 + 1$

Calcul : $(\beta^2)^3 = \beta^6 = \beta^2 + \beta$

Essai : $x = \beta^3$. Ici $(\beta^3)^3 = \beta^9 = \beta^2 = \beta^3 + 1$.

$\beta^7 = 1$ ✓

A.20 Un isomorphisme, suite

On construit $f : \mathbb{F}_8 \longrightarrow \mathbb{F}_8'$ est un isomorphisme de corps :

0	$\longmapsto$	0	injectif ①
1	$\longmapsto$	1	surjectif ②
α	$\longmapsto$	$\beta^3 = \beta^2 + 1$	
α^2	$\longmapsto$	$(\beta^2+1)^2 = \beta^4 + 1 = \beta^2 + \beta$	
$\vdots$			

① $\ker f = 0$

② $\forall y \in \mathbb{F}_8'$, $\exists u \in \mathbb{F}_8$ tq $f(u) = y$

$+$

$$f(\alpha^2+\alpha+1) = f(\alpha^2) + f(\alpha) + f(1)$$

$\odot$

$$= f(\alpha)^2 + f(\alpha) + f(1)$$

$$= (\beta^3)^2 + \beta^3 + 1$$

$$= \beta^2 + \beta + \beta + 1 + 1 = \beta^2$$

7.2.0 Rappel : Terminologie

1. **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.

2. **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.

3. **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 $\mathcal{C} = (e_1, \ldots, e_n)$, alors

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

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

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

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

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

7.2.2 Fin de la preuve

$$(\vec{x})_{\mathcal{B}}^T \, B \, (\vec{x}')_{\mathcal{B}} = (P^T \vec{x})^T \, B \, (P^T \vec{x}')$$

$$= \vec{x}^T \underbrace{(P^T)^T}_{P} B P^T \vec{x}'$$

$$= \vec{x}^T \underbrace{P B P^T}_{A} \vec{x}' = \langle \vec{x}, \vec{x}' \rangle \quad \square$$

7.2.3 Encore le Théorème spectral

On travaille avec

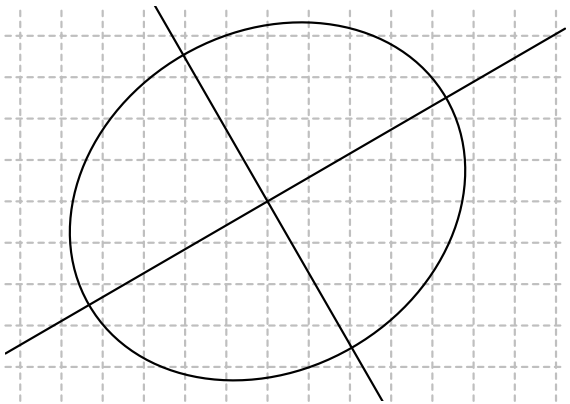
1. un espace vectoriel V de dimension finie n et une base $\mathcal{B}$;
2. un produit scalaire représenté par une matrice symétrique A par rapport à la base $\mathcal{B}$.

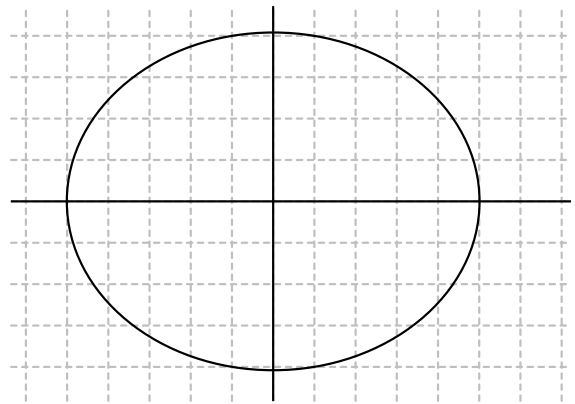
Théorème spectral

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^o 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 $T : \mathbb{R}^n \to \mathbb{R}^m$ 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

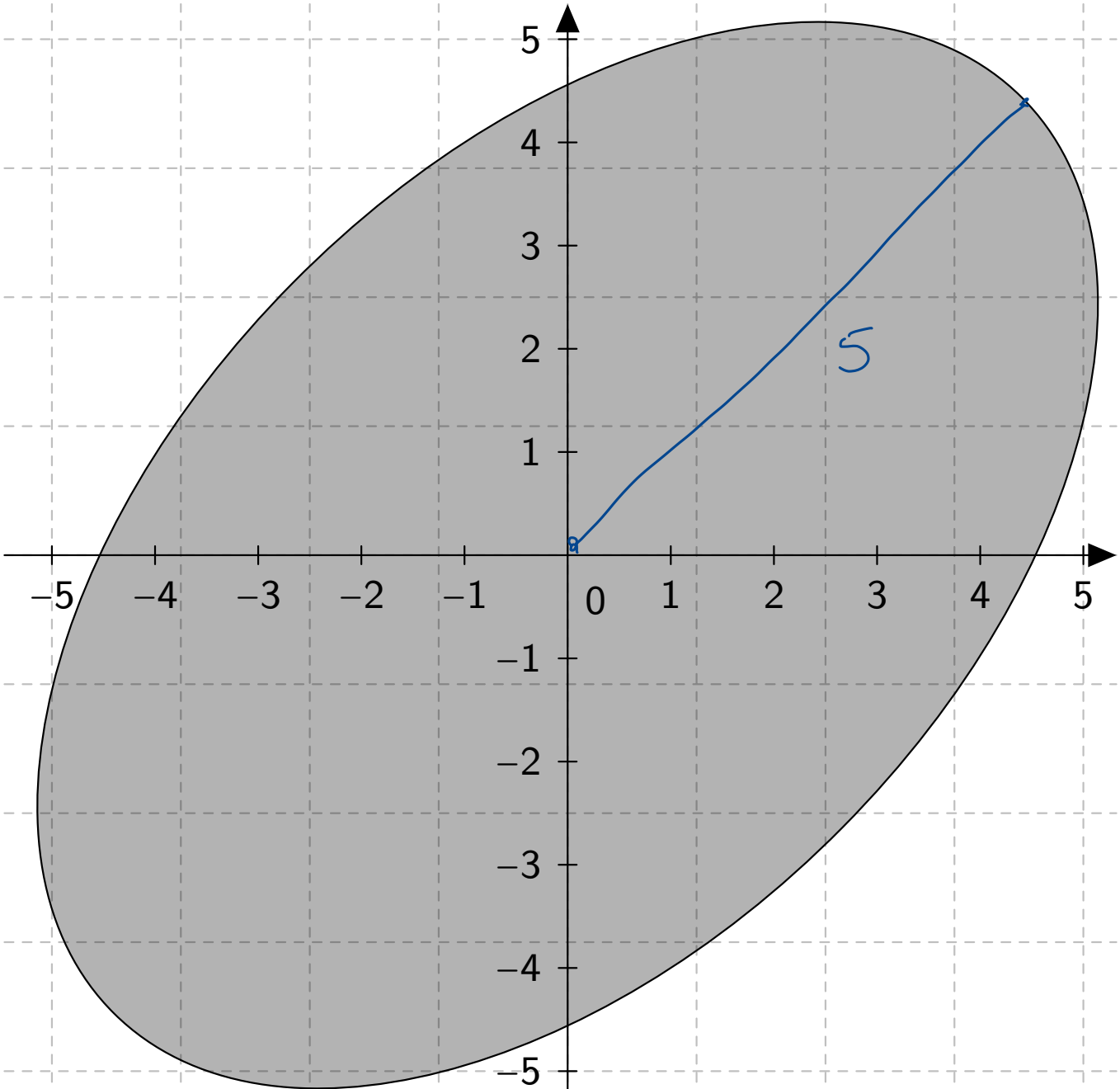
Soit $B = A^T A$. Cette matrice symétrique représente une forme bilinéaire symétrique dont on cherche le maximum, lorsqu'on l'évalue sur un vecteur de norme 1.

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 ?

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

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

Soit $\lambda \in \mathbb{R}$ valeur propre de $A^T A$. Soit $\vec{v} \in \mathbb{R}^n$ vecteur propre ($\neq \vec{0}$).

$$\underbrace{\|A\vec{v}\|^2}_{\geq 0} = A\vec{v} \cdot A\vec{v} = (A\vec{v})^T A\vec{v}$$

$$= \vec{v}^T \underbrace{A^T A}_{B} \vec{v}$$

$$= \vec{v}^T \cdot \lambda \vec{v}$$

comp. avec achim $= \lambda \underbrace{\vec{v}^T \vec{v}}_{\|\vec{v}\|^2}$

≥ 0

$$\Rightarrow \lambda \geq 0$$

$\square$

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 $\sigma_i = \sqrt{\lambda_i}$.

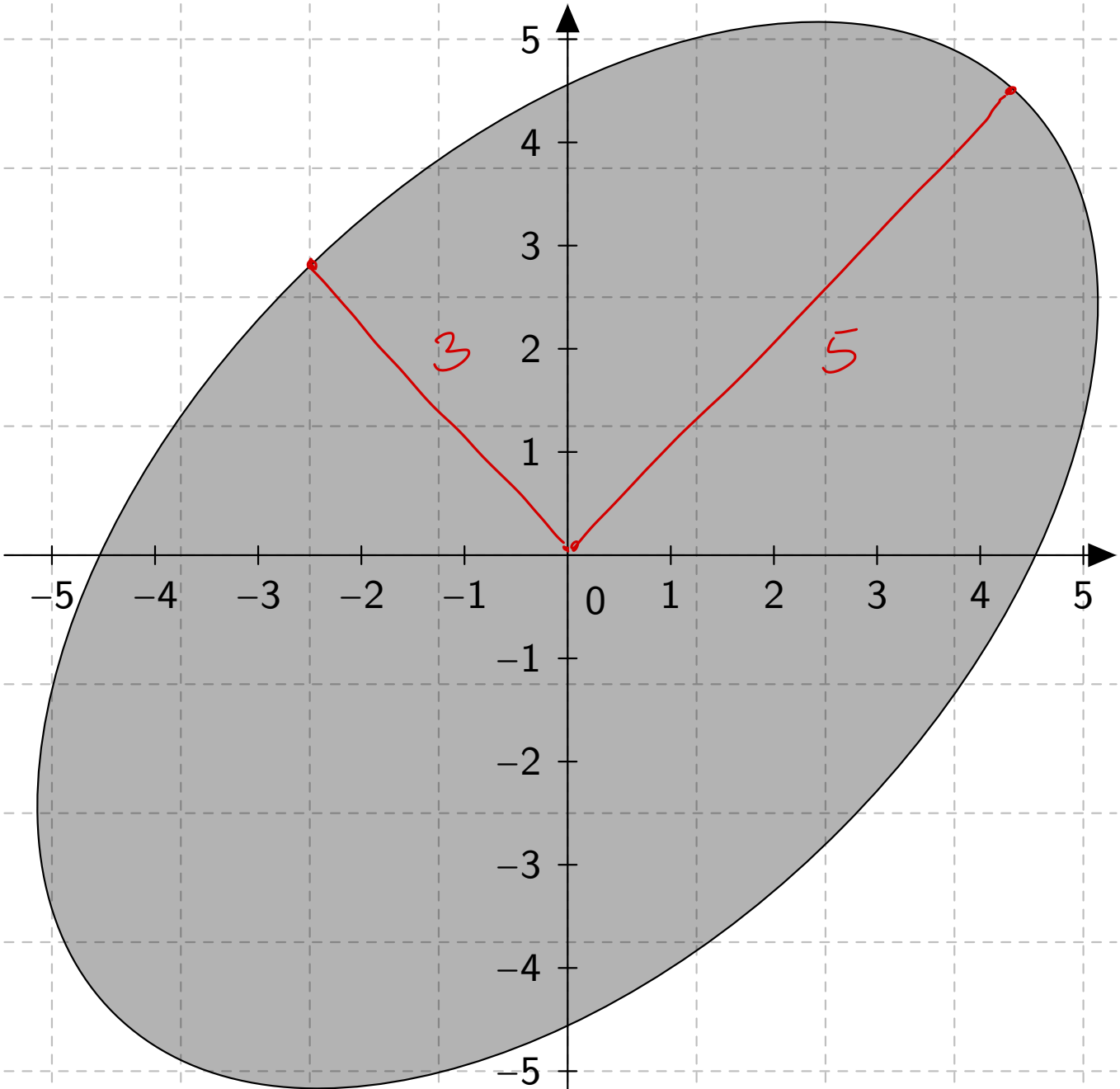
Remarque. On a $\sigma_i = \|Av_i\|$ où v_i est un vecteur propre unitaire de B pour la valeur propre λ_i.

7.4.4 Exemple, suite

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

1. $\sigma_1 = 5,\ \sigma_2 = 3,\ \sigma_3 = 0.$
2. $E_9 = \mathrm{Vect}\left\{\begin{pmatrix} \sqrt{2}/6 \\ -\sqrt{2}/6 \\ 2\sqrt{2}/3 \end{pmatrix}\right\} = \mathrm{Vect}\{\vec{v}_2\}$
3. $A\vec{v}_2 = \begin{pmatrix} 3\sqrt{2}/2 \\ -3\sqrt{2}/2 \end{pmatrix}$

7.4.4 Grand axe et petit axe



7.4.5 L'image de A

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

Théorème

Si A admet exactement r valeurs singulières non nulles, alors $(Av_1, \ldots, Av_r)$ 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 $Av_1, \ldots, Av_r$ sont orthogonaux, donc linéairement indépendants.

Ils engendrent $\mathrm{Im}A$ car $Av_{r+1} = \cdots = Av_n = 0$. □

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

1. U est orthogonale $m \times m$;
2. V est orthogonale $n \times n$;
3. $\Sigma = \begin{pmatrix} \sigma_1 & 0 & 0 & \dots & 0 \\ 0 & \ddots & 0 & \dots & 0 \\ 0 & 0 & \sigma_r & 0 & 0 \\ 0 & \dots & 0 & \dots & 0 \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix}$ 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.