



Chapitre 11 Fonctions convexes

■ Définitions, propriétés

► Définition :

Une fonction est convexe sur un intervalle \mathbb{R} non vide et non réduit à un point si :

$$\forall (x, y) \in I^2, \quad \forall \lambda \in [0, 1], \quad f(\lambda x + (1-\lambda)y) \leq \lambda f(x) + (1-\lambda)f(y)$$

► Propriété (inégalité de Jensen) :

Soit I un intervalle de \mathbb{R} et $f : I \rightarrow \mathbb{R}$. f est convexe sur I si et seulement si : $\forall n \geq 2, \quad \forall (x_1, \dots, x_n) \in I^n, \quad \forall (\lambda_1, \dots, \lambda_n) \in (\mathbb{R}_+)^n$ tels

$$\text{que } \sum_{j=1}^n \lambda_j = 1, \quad f\left(\sum_{j=1}^n \lambda_j x_j\right) \leq \sum_{j=1}^n \lambda_j f(x_j).$$

► Propriété (inégalité des pentes) :

Il y a équivalence entre les trois assertions suivantes :

i) f est convexe sur I ;

$$ii) \forall (x, y, z) \in I^3, \quad x < y < z, \quad \frac{f(y) - f(x)}{y - x} \leq \frac{f(z) - f(x)}{z - x};$$

$$iii) \forall (x, y, z) \in I^3, \quad x < y < z, \quad \frac{f(y) - f(x)}{y - x} \leq \frac{f(z) - f(x)}{z - x} \leq \frac{f(z) - f(y)}{z - y}.$$

► Propriété :

Une fonction est convexe sur I si et seulement si pour tout $x \in I$, la fonction « pente issue de x » : $t \mapsto \frac{f(t) - f(x)}{t - x}$ est croissante sur $I \setminus \{x\}$.

► Convexité et maximum

Une fonction f convexe sur $[a, b]$ admet un maximum global, qui est pris à une extrémité (au moins) du segment.

► Exercice :

Une fonction convexe et majorée sur \mathbb{R} est constante.

► Propriété :

Soit f une fonction convexe sur I et $x_0 \in I$ un point qui n'est pas l'une des extrémités de I , alors f est dérivable à droite et à gauche en x_0 et on a de plus $f'_g(x_0) \leq f'_d(x_0)$.

► Corollaire :

Si f est convexe sur $[a, b]$ alors f est continue sur $]a, b[$.

► Convexité et minimum

Soit f une fonction convexe sur I :

- Si f admet un minimum local y_0 , il s'agit d'un minimum global.
- Si f atteint un minimum local en deux points x_1, x_2 de I tels que $x_1 < x_2$, alors f est constante sur $[x_1, x_2]$.

► Propriété :

- Si f est dérivable sur I , alors f est convexe sur I si et seulement si f' est croissante sur I .
- Si f est deux fois dérivable sur I , alors f est convexe si et seulement si $f'' \geq 0$ sur I .

► Remarque :

On déduit de la croissance de la fonction dérivée que le graphe d'une fonction dérivable convexe est situé au dessus de ses tangentes.

Chapitre 12 Arithmétique

■ Rudiments d'arithmétique :

► **Définition :** On appelle ensemble des entiers naturels et on note \mathbb{N} un ensemble ordonné *non vide* vérifiant les trois propriétés suivantes :

- **N1** • toute partie non vide admet un plus petit élément.
- **N2** • toute partie non vide et majorée admet un plus grand élément.
- **N3** • \mathbb{N} n'a pas de plus grand élément.

On admet qu'un tel ensemble existe et est unique à bijection croissante près.

► **Définition :** Multiples et diviseurs d'un entier.

► Propriété (division euclidienne dans \mathbb{N}) :

$$\forall (a, b) \in \mathbb{N} \times \mathbb{N}^*, \quad \exists!(q, r) \in \mathbb{N} \times \{0, 1\}, \quad a = bq + r$$

► **Vocabulaire :** On dit que a est le *dividende*, b le *diviseur*, q le *quotient*, r le *reste* de la division euclidienne de a par b .

► **Définition :** PGCD et PPCM de deux entiers naturels non nuls.

Si a et b sont deux entiers non nuls, on note $a \wedge b$ le pgcd de a et b , et $a \vee b$ le ppcm de a et b .

► **Algorithme :** Algorithme d'Euclide pour le calcul du *pgcd*.

► **Propriété (propriété de Bézout) :** Si $(a, b) \in (\mathbb{N}^*)^2$, il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = a \wedge b$.

► **Propriété (de Gauss) :** Si a et b sont deux entiers premiers entre eux ($a \wedge b = 1$) et si $a \mid bc$, alors $a \mid c$.

► **Propriété :** Si a et b sont deux entiers non nuls, $ab = (a \wedge b)(a \vee b)$.

► **Définition :** Un entier positif est dit *premier* s'il admet exactement 2 diviseurs distincts dans \mathbb{N}^* .

► **Théorème :** Tout entier $n \in \mathbb{N} \setminus \{0, 1\}$ est divisible par un entier premier.

► **Théorème :** Il existe une infinité d'entiers premiers.

► **Théorème :** Tout entier $n \geq 2$ se décompose en produit de nombres premiers ; on *admet* que cette décomposition est unique à l'ordre près des facteurs.

Chapitre 13 Systèmes linéaires, calcul matriciel

■ Calcul matriciel :

► **Définition :** Ensemble des matrices à n lignes et p colonnes (ou de type (n, p)) à coefficients dans \mathbb{K} , noté $\mathcal{M}_{n,p}(\mathbb{K})$.

► **Définition :** Addition de matrices de type (n, p) ; multiplication d'une matrice par une constante ; produit d'une matrice de type (n, p) par une matrice de type (p, q) .

► **Propriétés (admisses) :** Le produit matriciel est pseudo-associatif, pseudo-distributif à droite et à gauche ; compatible avec la multiplication par un scalaire ; pour résumer :

$$\forall A \in \mathcal{M}_{n,p}, \quad \forall B \in \mathcal{M}_{p,q}, \quad \forall C \in \mathcal{M}_{q,r}, \quad (AB)C = A(BC)$$

$$\forall A \in \mathcal{M}_{n,p}, \quad \forall (B, C) \in \mathcal{M}_{p,q}^2, \quad A(B + C) = AB + AC$$

$$\forall (A, B) \in \mathcal{M}_{n,p}^2, \quad \forall C \in \mathcal{M}_{p,q}^2, \quad (A + B)C = AC + BC$$

$$\forall \lambda \in \mathbb{K}, \quad \forall A \in \mathcal{M}_{n,p}, \quad \forall B \in \mathcal{M}_{p,q}, \quad (\lambda A)B = \lambda(AB) = A(\lambda B)$$

► Exemples -- Vocabulaire :

- matrices carrées d'ordre n ;
- matrices diagonales (notation $\text{diag}(\alpha_1, \dots, \alpha_n)$) ;
- matrice identité (notation I_n) ;
- matrices triangulaires supérieures et inférieures.
- matrices élémentaires $E_{i,j}$ en taille (n, p)

■ Généralités sur les systèmes linéaires :

► **Définitions :** Équation linéaire à p inconnues ; système linéaire de n équations à p inconnues.

Matrice associée à un système linéaire.

Si $n \in \mathbb{N}^*$ et $p \in \mathbb{N}^*$, on considère $(a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \in \mathcal{M}_{n,p}(\mathbb{K})$,

► **Propriété :** Le produit matriciel est associatif. Le produit de matrices carrées d'ordre n est non commutatif si $n > 1$.

► **Notation :** Symbole de Kronecker : $\delta_{\alpha,\beta} = \begin{cases} 1 & \text{si } \alpha = \beta \\ 0 & \text{sinon} \end{cases}$.

► **Exercice :** Cas particulier du produit des matrices élémentaires (pour des matrices de tailles compatibles) : $E_{i,j} \times E_{k,\ell} = \delta_{j,k} E_{i,\ell}$.

► **Définition :** *Matrices d'opérations élémentaires* : matrices de transvection, de transposition et de dilatation.

Traduction des opérations élémentaires en produits matriciels.

Si $i \neq j$ et $\lambda \in \mathbb{K}$, on définit les matrices carrées d'ordre n :

$$\bullet S_{i,j}^n = I_n + E_{i,j} + E_{j,i} - E_{i,i} - E_{j,j}.$$

$$\bullet T_{i,j}^n(\lambda) = I_n + \lambda E_{i,j}.$$

$$\bullet \text{Si } \lambda \neq 0, \text{ on pose } H_i(\lambda) = I_n + (\lambda - 1)E_{i,i}.$$

$$\circ L_i \leftrightarrow L_j \quad M \leftrightarrow S_{i,j}^n M$$

$$\circ L_i \leftarrow L_i + \lambda L_j \quad M \leftrightarrow T_{i,j}^n(\lambda) M$$

$$\circ L_i \leftarrow \lambda L_i \quad M \leftrightarrow H_i(\lambda) M$$

► **Propriété :** Effet de la multiplication à gauche (ou à droite - énoncé mais pas prouvé) par une matrice élémentaire.

Conséquence pour les matrices d'opérations élémentaires

$(b_i)_{1 \leq i \leq n} \in \mathbb{K}^n$, et le système :

$$(S) : \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,p}x_p = b_1 \\ \vdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \dots + a_{n,p}x_p = b_n \end{cases}$$

La matrice augmentée associée à ce système linéaire est la matrice $(A | B) \in \mathcal{M}_{n, p+1}(\mathbb{K})$ obtenue en plaçant à la droite de la matrice du système, la colonne des seconds membres.

- **Définition (opérations élémentaires):** Opérations élémentaires sur les lignes d'un système ou d'une matrice :
 - échange des lignes L_{i_1} et L_{i_2} : $L_{i_1} \leftrightarrow L_{i_2}$
 - ajout de λL_{i_2} à L_{i_1} pour $i_1 \neq i_2$: $L_{i_1} \leftarrow L_{i_1} + \lambda L_{i_2}$
 - multiplication de L_i par $\mu \neq 0$: $L_i \leftarrow \mu L_i$
- **Propriété:** Deux systèmes équivalents ont le même ensemble de solutions.

■ Matrices inversibles :

- **Définition:** Matrices inversibles, inverse. Propriétés des matrices inversibles (structure de groupe - sans définir l'axiomatique d'un groupe).
- **Propriété:** Inverse d'un produit de matrices inversibles.
- **Propriété:** Les matrices d'opérations élémentaires sont inversibles et leurs inverses sont encore des matrices d'opérations élémentaires.
- **Exercice:** Définition de l'ensemble des matrices diagonales, triangulaires. Stabilité de ces ensembles par les opérations matricielles.

- **Propriété:** Si l'on passe d'un système S à un autre système S' par une suite finie d'opérations élémentaires sur les lignes, la matrice augmentée de S' s'obtient en effectuant la même suite d'opérations élémentaires sur la matrice augmentée de S .
- **Propriété:** Pour un système linéaire, si on dispose d'une solution particulière s_0 , alors l'ensemble des solutions est $\{s_0 + h, h \in \mathcal{S}_H\}$, où \mathcal{S}_H est l'ensemble des solutions du système homogène associé (c'est-à-dire celui ayant même matrice que le système initial, mais des seconds membres nuls).

Propriété: Pour une matrice $A \in \mathcal{M}_n(\mathbb{K})$, les propriétés suivantes sont équivalentes :

- A est inversible
- Pour tout B , le système $AX = B$ admet une unique solution ;

Remarque : le théorème complet démontré en cours est : Pour une matrice $A \in \mathcal{M}_n(\mathbb{K})$, les propriétés suivantes sont équivalentes :

- A est inversible
- Pour tout B , le système $AX = B$ admet une unique solution ;
- A peut se ramener à la matrice I_n en effectuant un nombre fini d'opérations élémentaires sur les lignes ;
- Pour tout B , le système $AX = B$ admet au moins une solution ;
- L'unique solution du système $AX = 0$ est la solution nulle.

- **Propriété:** Caractérisation des matrices inversibles parmi les matrices triangulaires supérieures (ou inférieures).

Chapitre 14 Polynômes

■ Définitions, Construction :

- **Définition:** Dans toute cette partie, \mathbb{K} désigne un corps ; en pratique, il s'agit de \mathbb{R} ou \mathbb{C} . On appelle *support* de la suite $(a_n) \in \mathbb{K}^{\mathbb{N}}$ l'ensemble $\{n \in \mathbb{N}, a_n \neq 0\}$.
Un polynôme à une indéterminée à coefficients dans \mathbb{K} est une suite de $\mathbb{K}^{\mathbb{N}}$ à *support fini* (on parle également de suite *presque nulle*) ; on note $\mathbb{K}[X]$ l'ensemble des polynômes.

► Exemples et vocabulaire :

- ◊ La suite nulle est appelée polynôme nul et noté 0
- ◊ L'ensemble des polynômes constants est : $\{(a_n) \in \mathbb{K}^{\mathbb{N}}, \forall n \geq 1, a_n = 0\}$.
- ◊ On dit qu'un polynôme est un monôme si un seul des coefficients est non nul.

► Remarque : $\mathbb{K}[X] \neq \mathbb{K}^{\mathbb{N}}$.

► Définitions : Soit $P \in \mathbb{K}[X] \setminus \{0\}$

- ◊ On appelle *degré* de P et on note $\deg(P)$ l'entier $\max\{n \in \mathbb{N}, a_n \neq 0\}$.

- ◊ $a_{\deg(P)}$ est le *coefficient dominant* de P .
- ◊ On dit que P est *unitaire* si son coefficient dominant vaut 1.
- ◊ Par convention $\deg(0) = -\infty$.

► Proposition -- Définition : On définit l'addition de $P = (a_n) \in \mathbb{K}[X]$ et $Q = (b_n) \in \mathbb{K}[X]$ par $P + Q = (a_n + b_n)_{n \in \mathbb{N}} \in \mathbb{K}[X]$.

- ◊ On a $\forall (P, Q) \in \mathbb{K}[X]^2$:
 - $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ et si $\deg(P) \neq \deg(Q)$, il y a égalité.

► Proposition - Définition : On définit la multiplication de 2 polynômes $P = (a_n) \in \mathbb{K}[X]$ et $Q = (b_n) \in \mathbb{K}[X]$ par $P \times Q = PQ = (c_n)_{n \in \mathbb{N}} \in \mathbb{K}[X]$ où :

$$\forall n \in \mathbb{N}, c_n = \sum_{k=0}^n a_k b_{n-k} = \sum_{i+j=n} a_i b_j$$

On a $\forall (P, Q) \in \mathbb{K}[X]^2, \deg(PQ) = \deg(P) + \deg(Q)$.

► Proposition : Les éléments inversibles (pour la loi \times) de cet anneau sont les polynômes constants non nuls.

► Proposition - Définition : On définit un produit externe sur $\mathbb{K} \times \mathbb{K}[X]$: pour $\lambda \in \mathbb{K}$ et $P = (a_n) \in \mathbb{K}[X]$, on note $\lambda \cdot P = \lambda P = (\lambda a_n)_{n \in \mathbb{N}} \in \mathbb{K}[X]$.

► Proposition - Définition : On dit que $(\mathbb{K}[X], +, \cdot)$ admet une structure d'espace vectoriel sur \mathbb{K} (ou de \mathbb{K} -espace vectoriel, ou en abrégé \mathbb{K} -e.v.) ; cela signifie :

- $(\mathbb{K}[X], +)$ groupe abélien.
- \cdot est une loi externe de $\mathbb{K} \times \mathbb{K}[X]$ dans $\mathbb{K}[X]$ telle que :

$$\forall (\alpha, \beta) \in \mathbb{K}^2, \forall (P, Q) \in \mathbb{K}[X]^2 : \begin{cases} (\alpha + \beta) \cdot P = \alpha \cdot P + \beta \cdot P \\ \alpha \cdot (P + Q) = \alpha \cdot P + \alpha \cdot Q \\ \alpha \cdot (\beta \cdot P) = (\alpha\beta) \cdot P \\ 1_{\mathbb{K}} \cdot P = P \end{cases}$$

■ Arithmétique sur $\mathbb{K}[X]$:

- **Définition:** Si $(A, B) \in \mathbb{K}[X]^2$, on dit que A est un multiple de B ou que B divise A si et seulement s'il existe $C \in \mathbb{K}[X]$ tel que $A = BC$, et on note $B | A$.

- **Proposition - Définition :** Pour résumer le fait que $(\mathbb{K}[X], +, \times)$ est un anneau et $(\mathbb{K}[X], +, \cdot)$ est un \mathbb{K} -e.v. ainsi que la relation de compacité :

$$\forall \lambda \in \mathbb{K}, \forall (P, Q) \in \mathbb{K}[X]^2, (\lambda \cdot P) \times Q = \lambda \cdot (P \times Q) = P \times (\lambda \cdot Q)$$

on dit que $\mathbb{K}[X]$ est une *algèbre sur \mathbb{K}* (ou encore \mathbb{K} -algèbre).

- **Notation :** X désigne le polynôme $(0, 1, 0, \dots) \in \mathbb{K}[X]$, on convient de noter $X^0 = 1, X^1 = X$ et $\forall k \in \mathbb{N}^*, X^k = \underbrace{(0, \dots, 0, 1, 0, \dots)}_{k \text{ termes}}$.

Par construction, tout polynôme s'écrit comme combinaison linéaire finie à coefficients dans \mathbb{K} de polynômes de $\{X^j, j \in \mathbb{N}\}$. Pour tout $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n .

- **Définition :** Si $P = \sum_{n=0}^N a_n X^n \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$; on définit le

$$\text{polynôme composé, noté } P \circ Q \text{ ou } P(Q), \text{ par } P \circ Q = \sum_{n=0}^N a_n Q^n.$$

- **Proposition :** $\forall (P, Q) \in \mathbb{K}[X]^2$ avec Q polynôme non constant, on a : $\deg(P \circ Q) = \deg(P) \deg(Q)$.

- **Propriétés :** $\forall (P, Q, R) \in \mathbb{K}[X]^3, \forall \alpha \in \mathbb{K}$:

- ◊ $(P + \alpha Q) \circ R = P \circ R + \alpha Q \circ R$;
- ◊ $(PQ) \circ R = (P \circ R)(Q \circ R)$;
- ◊ $(P \circ Q) \circ R = P \circ (Q \circ R)$;
- ◊ $X \circ P = P \circ X = P$.

- **Définition :** Pour tout $P = \sum_{n=0}^N a_n X^n \in \mathbb{K}[X]$, on note P' ou $D(P)$ le

$$\text{polynôme dérivé de } P \text{ par } P' = \sum_{n=1}^N n a_n X^{n-1} = \sum_{n=0}^{N-1} (n+1) a_{n+1} X^n.$$

On a en particulier $\forall P \in \mathbb{K}[X], \deg(P) \geq 1, \deg(P') = \deg(P) - 1$ et $\deg(P') = -\infty$ si $\deg(P) \leq 0$.

On définit par récurrence la dérivée n -ième d'un polynôme.

► Cas particulier important :

$$\forall (k, n) \in \mathbb{N}^2, D^k(X^n) = \begin{cases} \frac{n!}{(n-k)!} X^{n-k} & \text{si } k \leq n \\ 0 & \text{si } k > n \end{cases}$$

- **Propriétés :** $\forall (P, Q) \in \mathbb{K}[X]^2, \forall \alpha \in \mathbb{K} : (P + \alpha Q)' = P' + \alpha Q', (PQ)' = P'Q + PQ'$ et $\forall n \in \mathbb{N}, (PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}$.

- **Définition :** Deux polynômes $(A, B) \in (\mathbb{K}[X] \setminus \{0\})^2$, sont *associés* ssi il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$ (cela équivaut à $P | Q$ et $Q | P$).