Lycée Faidherbe

Classe de MP⋆

Cours de Mathématiques

Programme officiel et compléments

Année 2019-2020

Table des matières

Dans tout le cours, les éléments explicitement au programme sont précédés par **Théorème**, **Définition**, **Propriété**, **Proposition**. Les remarques, corollaires et conséquences sont généralement importants. Les **Résultats** ou éléments démontrés sans indication quant à leur nature sont des compléments de cours (hors programme). Tous les compléments de cours ont leur intérêt, mais il n'est pas nécessaire de tous les connaître.
Les démonstrations manquantes sont jugées suffisamment facile à retrouver rapidement. Lorsqu'une démonstration est admise, elle apparaît toujours sous la forme :

Démonstration. Admis(e). □

Chapitre I

Analyse asymptotique

Sommaire

1 Développements limités – Rappels

Cette section ne contient que des rappels de sup.

Définition (Développement limité).

> Un développement limité de $f : V \longrightarrow \mathbf{R}$ à l'ordre n au voisinage V de a (qu'on abrègera $\mathrm{DL}_n(a)$ de f) est une écriture du type :
>
> $$f(x) = \underbrace{a_0 + a_1(x-a) + \cdots + a_n(x-a)^n}_{\text{partie polynômiale}} + o_a((x-a)^n)$$

Remarque.

Lorsqu'un $\mathrm{DL}_n(a)$ existe, il y a unicité de la partie polynômiale.

Remarque.

Les DL usuels sont à connaître.

$$\begin{aligned}
e^x &= 1 + x + \frac{x^2}{2} + \ldots + \frac{x^n}{n!} && + o_0(x^n) \\
\sin x &= x - \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots + (-1)^p \frac{x^{2p+1}}{(2p+1)!} && + o_0(x^{2p+1}) \\
\cos x &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots + (-1)^p \frac{x^{2p}}{(2p)!} && + o_0(x^{2p}) \\
\frac{1}{1-x} &= 1 + x + x^2 + + x^3 + \ldots + x^n && + o_0(x^n) \\
\ln(1-x) &= -x - \frac{x^2}{2} - \frac{x^3}{3} - \frac{x^4}{4} - \ldots - \frac{x^n}{n} && + o_0(x^n) \\
(1+x)^\alpha &= 1 + \alpha x + \alpha(\alpha-1)\frac{x^2}{2!} + \ldots \\
&\quad + \alpha(\alpha-1)\ldots(\alpha-n+1)\frac{x^n}{n!} && + o_0(x^n)
\end{aligned}$$

Les règles de calcul sont aussi à connaître (vues en sup : composition, troncature, multiplication)

Définition (Voisinage).

Un voisinage de $a \in \mathbf{R}$ est un intervalle du type $]a-\varepsilon, a+\varepsilon[$. Si V est un voisinage de a, on note $V \in \mathscr{V}(a)$.

Si $V \in \mathscr{V}(0)$ et si pour $x \in V \setminus \{0\}$, $f(x) = a_0 + a_1 x + a_p x^p + o_p(x^p)$, $a_p \neq 0$ et $p \geqslant 2$ alors

- f est prolongeable en 0 et $f(0) = a_0$
- f est dérivable en 0 et $f'(0) = a_1$
- $y = a_0 + a_1 x$ est l'équation cartésienne de la tangente au graphe de f en 0
- $f(x) - a_0 - a_1 x$ a le même signe que $a_p x^p$ au voisinage de 0.

Remarque.

f admet un $\mathrm{DL}_1(a)$ si et seulement si f est dérivable en a. Ça n'est pas vrai pour les ordres supérieurs de dérivation.

Exemple. On pose

$$f : x \in]-\pi;\pi[\setminus\{0\} \longmapsto \frac{1}{x} - \frac{1}{\sin x}$$

et on a (en utilisant les DL usuels et les règles de calcul)

$$\forall x \in D_f, \quad f(x) = \frac{1}{x} - \frac{1}{x - \frac{x^3}{3} + o_0(x^3)} = \frac{1}{x}\left(1 - \left(1 + \frac{x^2}{6} + o_0(x^2)\right)\right) = -\frac{1}{6}x + o_0(x)$$

donc f est prolongeable en 0 avec $f(0) = 0$, $f'(0) = -\frac{1}{6}$.

La fonction f est $\mathscr{C}^1$ sur son domaine de définition, l'est-elle en 0 ? On a

$$\forall x \in D_f, \qquad f'(x) = -\frac{1}{x^2} + \frac{\cos x}{\sin^2 x} = \frac{1}{x^2}\left(-1 + \frac{1 - \frac{x^2}{2} + o_0(x^2)}{(1 - \frac{x^2}{6} + o_0(x^2))^2}\right) = -\frac{1}{6} + o_0(1) \xrightarrow[x\to 0]{} -\frac{1}{6}$$

donc f est $\mathscr{C}^1$ en 0

2 Taylor-Young

Théorème (Taylor-Young).

(H) $f \in \mathscr{C}^n(V \in \mathscr{V}(0), \mathbf{R})$

(C)

$$\forall x \in V, \qquad f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} x^k + o_0(x^n)$$

Remarque.

On n'a en fait besoin que de $f \in \mathscr{C}^{n-1}(V, \mathbf{R})$ et $f^{(n-1)}$ dérivable en 0

Remarque.

On ne peut en général pas dériver termes à termes. Si f est $\mathscr{C}^n$, on peut dériver termes à termes pour obtenir le $\mathrm{DL}_{n-1}(0)$ de f'.

Exemple (a). Pour obtenir un $\mathrm{DL}_3(1)$ de arctan, on note $f = \arctan$ et

$$f(1) = \frac{\pi}{4} \qquad f'(1) = \frac{1}{2} \qquad f''(1) = -\frac{1}{2} \qquad f^{(3)}(1) = \frac{1}{2}$$

donc

$$\forall x \in \left]-\frac{\pi}{2}; \frac{\pi}{2}\right[, \qquad f(x) = \frac{\pi}{4} + \frac{x-1}{2} - \frac{(x-1)^2}{4} + \frac{(x-1)^3}{12} + o_1((x-1)^3)$$

Exemple (b). On note $f \in \mathscr{C}^\infty([-1;1], \mathbf{R})$ telle que $\forall n \in \mathbf{N}^\star$,

$$\begin{aligned} f\left(\frac{1}{n}\right) &= \frac{\sqrt{n}}{\sqrt{n+1} + \sqrt{n}} \\ &= \frac{1}{1 + \sqrt{1 + \frac{1}{n}}} \\ &= \frac{\sqrt{1+\frac{1}{n}} - 1}{\frac{1}{n}} \\ &= n\left(\sum_{k=1}^{2020} \binom{1/2}{k} \frac{1}{n^k} + o_{+\infty}\left(\frac{1}{n^{2020}}\right)\right) \\ &= \sum_{k=0}^{2019} \frac{f^{(k)}(0)}{k!} \frac{1}{n^k} + o_{+\infty}\left(\frac{1}{n^{2019}}\right) \end{aligned}$$

Puis $n \to +\infty$ donne

$$\binom{1/2}{1} = f(0)$$

et $nf(1/n)$ avec $n \to +\infty$ donne

$$\binom{1/2}{2} = \frac{f'(0)}{1!}$$

et en itérant on obtient

$$\binom{1/2}{2020} = \frac{f^{(2019)}(0)}{2019!}$$

3 Utilisation standard des développements limités

a) Calcul de limite

On va calculer

$$\lim_{x \to 0^+} \frac{x^{\operatorname{sh} x} - (\operatorname{sh} x)^x}{(\sin x)^x - x^{\sin x}}$$

Et on a

$$\operatorname{sh} x = x + \frac{x^3}{6} + o_0(x^3) \qquad \sin x = x - \frac{x^3}{6} + o_0(x^3)$$

donc, après calculs,

$$\frac{x^{\operatorname{sh} x} - (\operatorname{sh} x)^x}{(\sin x)^x - x^{\sin x}} = \frac{\frac{x^3}{6}\ln x + o_0(x^3 \ln x) - \frac{x^3}{6} + o_0(x^3)}{\frac{-x^3}{6} + o_0(x^3) + \frac{x^3}{6}\ln x + o_0(x^3\ln x)} \underset{0+}{\sim} -1$$

b) Développement limité d'une réciproque

Exercice.

> Soit $x \in \mathbf{R}$. Montrer $\exists! \psi(x) \underset{\text{def}}{=} y \in \mathbf{R}, e^{x+y} + y = 1$. Montrer que ψ admet un $\mathrm{DL}_2(0)$ que l'on donnera

Résolution (Idée 1). On étudie $y \longmapsto e^{x+y} + y - 1$ à x fixé. Problème : comment trouver un DL_2 en x ? $\square$

Résolution (Idée 2). «On perturbe le problème.»

$$e^{x+y} + y = 1 \iff e^{x+y} + x + y = 1 + x \iff \varphi(x+y) = 1 + x$$

avec $\varphi : t \longmapsto e^t + t \in \mathscr{C}^\infty(\mathbf{R}, \mathbf{R})$ strictement croissante de dérivée jamais nulle. C'est donc une bijection de $\mathbf{R}$ dans $\mathbf{R}$ de bijection réciproque dérivable :

$$\varphi^{-1'} = \frac{1}{\varphi' \circ \varphi^{-1}} \in \mathscr{C}^1$$

donc $\varphi^{-1} \in \mathscr{C}^2$ (en fait $\mathscr{C}^\infty$) donc φ^{-1} admet un $\mathrm{DL}_2(a)$ en $a \in \mathbf{R}$.

On a $\psi(x) = -x + \varphi^{-1}(1+x)$ donc ψ a un $\mathrm{DL}_2(0)$. Donc on écrit

$$\psi(x) = a_0 + a_1 x + a_2 x^2 + o_0(x^2)$$

et

$$\psi(\varphi(x) - 1) = -\varphi(x) + 1 + x = -x - \frac{x^2}{2} + o_0(x^2) = \psi\left(2x + \frac{x^2}{2} + o_0(x^2)\right)$$

donc

$$-x + \frac{x^2}{2} + o_0(x^2) = a_0 + 2a_1 x + \left(\frac{a_1}{2} + 4a_2\right) x^2 + o_0(x^2)$$

et on identifie les coefficients $\square$

4 Utilisation non standard des développements limités

a) Calul de primitive

On veut calculer une primitive de

$$F : x \longmapsto \frac{1}{x^{2019}(1+x^2)}.$$

On a

$$F(x) = \sum_{k=0}^{1010} (-1)^k x^{2k-2019} + o_0(x)$$

donc

$$F(x) - \sum_{k=0}^{1009} (-1)^k x^{2k-2019} = o_0(1)$$

est une fraction rationnelle sans partie polaire en 0, donc

$$\sum_{k=0}^{1009} (-1)^k x^{2k-2019}$$

est la partie polaire de F en 0 et

$$F(x) = \sum_{k=0}^{1009} (-1)^k x^{2k-2019} + \frac{\alpha x + \beta}{1+x^2}$$

et en injectant i, $\alpha i + \beta = i$ d'où $\alpha = 1, \beta = 0$. Puis on peut intégrer termes à termes

b) Développement limité d'un terme général

On note f une fonction $\mathscr{C}^2$ sur un voisinage V de 0 telle que $f(0) = 0$. On définit pour n suffisament grand,

$$u_n = \sum_{k=1}^{n} f\left(\frac{k}{n^2}\right)$$

On va faire l'étude de u_n.

$$\forall k \in [\![1, n]\!], \quad f\left(\frac{k}{n^2}\right) = \frac{f'(0)k}{n^2} + \frac{f''(0)}{2} \cdot \frac{k^2}{n^4} + \frac{k^2}{n^4} \cdot \varepsilon\left(\frac{k}{n^2}\right), \qquad \varepsilon(x) \xrightarrow[x \to 0]{} 0$$

donc

$$u_n = \frac{f'(0)}{n^2} \sum_{k=1}^{n} k + \underbrace{\frac{f''(0)}{2n^4} \sum_{k=1}^{n} k^2}_{\longrightarrow 0} + \underbrace{\frac{1}{n^4} \sum_{k=1}^{n} k^2 \varepsilon\left(\frac{k}{n^2}\right)}_{\longrightarrow 0 \text{ car } \varepsilon \text{ bornée}} \xrightarrow[n \to +\infty]{} \frac{f'(0)}{2}$$

c) Polynôme sous contrainte

Exercice.

> Trouver un polynôme P_n tel que $P_n^2(x) = 1 + x + o_0(x^n)$. En déduire une racine carrée de
>
> $$A = \begin{pmatrix} 4 & 1 \\ -9 & -2 \end{pmatrix}$$

Démonstration.

$$P_n = \sum_{k=1}^{n} \binom{1/2}{k} x^k$$

convient et

$$A = I_n + \underbrace{\begin{pmatrix} 3 & 1 \\ -9 & -3 \end{pmatrix}}_{\underset{\text{def}}{=} N}, \qquad N^2 = 0$$

donc $P_1^2(N) = I_n + N + \frac{N^2}{4} = I_n + N = A$ donc $P_1(N)$ convient. □

d) Formule combinatoire

On va montrer que si $0 \leqslant m \leqslant n$ alors

$$\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^m = \delta_{n,m} n!$$

On écrit

$$(e^x - 1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} e^{kx} = (x + o(x))^n = x^n + o_0(x^n)$$

et pour $m < n$, on identifie le coefficient de x^m (il est nul). Sinon, $n = m$ et le résultat est le bon.

5 Majorer, minorer, encadrer

a) Rappels

$$|x| \leqslant a \iff -a \leqslant x \leqslant a$$

$$\begin{cases} x \leqslant x' \\ y \leqslant y' \end{cases} \implies \begin{cases} x + y \leqslant x' + y' \end{cases}$$

$$\begin{cases} 0 \leqslant x \leqslant x' \\ 0 \leqslant y \leqslant y' \end{cases} \implies xy \leqslant x'y'$$

$$||x| - |y|| \leqslant |x + y| \leqslant |x| + |y|$$

b) Sommation terme à terme

Si $a_1 \leqslant b_1, \cdots, a_n \leqslant b_n$ alors

$$a_1 + \cdots + a_n \leqslant b_1 + \cdots + b_n$$

avec égalité ssi $a_1 = b_1, \cdots a_n = b_n$. Le résultat se généralise identiquement aux séries convergentes.

Exemple. pour $n \geqslant 3$,

$$\frac{1}{n^3} \leqslant \frac{1}{n(n-1)(n-2)} = \frac{1}{2n} - \frac{1}{n-1} + \frac{1}{2(n-2)}$$

et en sommant,

$$\zeta(3) = \sum_{k=1}^{+\infty} \frac{1}{k^3} < \frac{11}{8}$$

c) Inégalité de Cauchy-Schwarz

On va montrer l'inégalité de Cauchy-Schwarz de deux manières différentes

Identité de Lagrange. On note $a_1, \cdots, a_n, b_1, \cdots, b_n \in \mathbf{R}$.

$$\begin{aligned}
\left(\sum_{i=1}^n a_i^2\right) \cdot \left(\sum_{i=1}^n b_i^2\right) - \left(\sum_{i=1}^n a_i b_i\right)^2 &= \sum_{i=1}^n \sum_{j=1}^n \underbrace{a_i^2 b_j^2 - a_i b_i a_j b_j}_{=0 \text{ si } i=j} \\
&= \sum_{i<j} (a_i^2 b_j^2 + a_j^2 b_i^2) - 2 a_i b_i a_j b_j \\
&= \sum_{i<j} (a_i b_j - a_j b_i)^2 \geqslant 0
\end{aligned}$$

Utilisation de l'homogénéité. On suppose les b_i non tous nuls. On pose

$$f : (a, b) \longrightarrow \left(\sum_{i=1}^n a_i^2\right) \cdot \left(\sum_{i=1}^n b_i^2\right) - \left(\sum_{i=1}^n a_i b_i\right)^2$$

On a, pour $\lambda, \mu \geqslant 0$, $f(\lambda a, \mu b) = \lambda^2 \mu^2 f(a, b)$ de même signe que $f(a, b)$. Il existe $\lambda, \mu \geqslant 0$ tels que

$$\sum_{i=1}^n \lambda^2 a_i^2 = \sum_{j=1}^n b_j^2 \mu^2 = 1$$

de sorte qu'on peut supposer sans perte de généralité

$$\sum_{i=1}^n a_i^2 = \sum_{j=1}^n b_j^2 = 1$$

Puis $|a_i b_i| \leqslant \frac{a_i^2 + b_i^2}{2}$ donc

$$\sum_{i=1}^n |a_i b_i| \leqslant \frac{1+1}{2} = 1$$

d'où C

d) Inégalités fonctionnelles

Montrer que si $0 < p < 1$ et $\theta \in \left[0; \frac{\pi}{2}\right]$ alors

$$\cos^p \theta \leqslant \cos(p\theta)$$

On pose

$$f_p : \theta \in \left[0; \frac{\pi}{2}\right] \longmapsto -\cos^p \theta + \cos(p\theta)$$

de sorte que

$$f_p'(\theta) = -p \sin(p\theta) + p \sin\theta \cos^{p-1} \theta$$

or $\sin(p\theta) \leqslant \sin\theta \leqslant \sin\theta \cos^{p-1}\theta$ donc $f_p'(\theta) \geqslant 0$ et f_p croissante, ce qui conclut puisque $f_p(0) = 0$

e) Inégalité de réordonnement

On note

$$\begin{cases} a_1 \leqslant \cdots \leqslant a_n \\ b_1 \leqslant \cdots \leqslant b_n \end{cases}$$

et $\sigma \in \mathfrak{S}_n$. Puis, on définit

$$S_\sigma \underset{\text{def}}{=} \sum_{i=1}^{n} a_i b_{\sigma(i)}.$$

S_σ est maximal pour $\sigma = \mathrm{id}$, et minimal pour $\sigma = (n \;\; n-1 \;\; \cdots \;\; 1)$. On suppose que σ maximise S_σ. On note $\sigma' = (1 \;\; \sigma(1)) \circ \sigma$ donc

$$S_{\sigma'} - S_\sigma = a_1 b_1 + a_{\sigma^{-1}(1)} b_{\sigma(1)} - a_1 b_{\sigma(1)} - a_{\sigma^{-1}(1)} b_1 = (a_1 - a_{\sigma^{-1}(1)})(b_1 - b_{\sigma(1)}) \geqslant 0$$

donc on peut supposer $\sigma(1) = 1$. En itérant, $\sigma = \mathrm{id}$ est maximisante. On procède de la même manière pour la permutation minimisante.

Exemple (Application 1)**.** On note $f : \mathbf{N}^\star \to \mathbf{N}^\star$ bijective. On cherche la nature de $\sum \dfrac{1}{nf(n)}$. On note $a_1 < \cdots < a_n$ les éléments $f(1), \cdots, f(n)$ ordonnés. Alors

$$\sum_{k=1}^{n} \frac{1}{kf(k)} \leqslant \frac{1}{na_n} + \cdots \frac{1}{a_1} \leqslant \frac{1}{n^2} + \cdots + \frac{1}{1^2} \leqslant \zeta(2)$$

donc la série converge.

Exemple (Inégalité AM-GM)**.** On note $x_1, \cdots, x_n \geqslant 0$, et on note

$$f(x_1, \cdots, x_n) = \frac{1}{n} \sum x_i - \sqrt[n]{\prod x_i}$$

de sorte que $f(\lambda x_1, \cdots, \lambda x_n) = \lambda f(x_1, \cdots, x_n)$ pour $\lambda \geqslant 0$ donc on peut supposer $\prod x_i = 1$. En notant

$$a_k = \prod_{i=1}^{k} x_i \qquad\qquad b_i = \frac{1}{a_i}$$

on a

$$n = a_1 b_1 + \cdots a_n b_n \leqslant \underbrace{a_1 b_n}_{x_1} + \underbrace{a_2 b_1}_{x_2} + \cdots + a_n b_{n-1} = x_1 + \cdots + x_n$$

ce qui conclut.

f) Échelles de références

Définition (Rappels)**.**

Si f et g sont définies sur un voisinage de $a \in \overline{\mathbf{R}}$ alors

$$f(x) = o_a(g(x)) \iff \exists V' \subset V, V' \in \mathscr{V}(a), \exists \varepsilon : V' \to \mathbf{R}, \forall x \in V', f(x) = \varepsilon(x) g(x) \text{ et } \varepsilon(x) \xrightarrow[x \to a]{} 0$$

$$f(x) = O_a(g(x)) \iff \exists M > 0, \exists V' \subset V, V \in \mathscr{V}(a), \forall x \in V', |f(x)| \leqslant M |g(x)|$$

$$f(x) \underset{a}{\sim} g(x) \iff f(x) = g(x) + o_a(g(x))$$

Exemple.

$$x^\alpha |\ln x|^\beta = o_0(x^{\alpha'} |\ln x|^{\beta'}) \iff \alpha > \alpha' \quad \text{ou} \quad \alpha = \alpha' \text{ et } \beta < \beta'$$

$$x^\alpha (\ln x)^\beta = o_{+\infty}(x^{\alpha'} (\ln x)^{\beta'}) \iff \alpha < \alpha' \quad \text{ou} \quad \alpha = \alpha' \text{ et } \beta < \beta' \underset{\text{def}}{\iff} (\alpha, \beta) \prec (\alpha', \beta')$$

Conséquence 1. $(x \in \mathbf{R}_+^\star \longmapsto x^\alpha |\ln x|^\beta)_{\alpha,\beta}$ est une famille libre (pour une famille finie, on ordonne $(\alpha_1, \beta_1) \prec \cdots \prec (\alpha_n, \beta_n)$ et on prend la limite en $+\infty$)

6 Suites numériques

a) Caractérisation de la borne supérieure

Théorème.

(H) $\varnothing \neq A \subset \mathbf{R}$, $M \in \mathbf{R}$.

(C) Il y a équivalence entre

(a) $M = \sup A$

(b) M majore A et $\exists a = (a_n)_n \in A^{\mathbf{N}}, \quad a_n \longrightarrow M$

Démonstration.

1. ($a \implies b$) M majore A par définition et pour tout n, il existe $a_n \in A$ tel que

$$M - \frac{1}{n} < a_n$$

donc $a_n \longrightarrow M$

2. ($b \implies a$) Supposons qu'il existe un majorant $M' < M$ de A. Alors toute suite convergente de A a une limite $\ell \leqslant M' < M$ donc $a_n \longrightarrow M \implies M \leqslant M'$ absurde. Donc M est le plus petit majorant.

□

b) Limite supérieure et inférieure

On se donne u une suite réelle bornée. On pose pour $n \in \mathbf{N}$,

$$u_n^+ = \sup\{u_k, \quad k \geqslant n\} \qquad\qquad u_n^- = \inf\{u_k, \quad k \geqslant n\}$$

de sorte que $u_0^- \leqslant u_n^- \leqslant u_n \leqslant u_n^+ \leqslant u_0^+$ et les deux suites u^+, u^- étant monotones bornées, elles sont convergentes.

Définition.

Pour une suite réelle u, on appelle limite supérieure et limite inférieure les quantités

$$\limsup_{n\to+\infty} u_n \underset{\text{def}}{=} \lim_{n\to+\infty} u_n^+ \qquad\qquad \liminf_{n\to+\infty} u_n \underset{\text{def}}{=} \lim_{n\to+\infty} u_n^-$$

On va construire une extractice φ de la manière suivante :

- $\varphi(0) = 0$. On a $u_1^+ - 1 < u_1^+$ donc $\exists k_1 \geqslant 1, u_1^+ - 1 < u_{k_1} \leqslant u_1^+$
- $\varphi(1) = k_1$. On a $u_2^+ - \frac{1}{2} < u_2^+$ donc $\exists k_2 \geqslant k_1, u_2^+ - \frac{1}{2} < u_{k_2} \leqslant u_2^+$
- $\cdots$

On construit ainsi une sous-suite convergente (qui converge vers $\limsup u$).

Remarque.

On a montré le théorème de Bolzano-Weierstrass

c) Suites sous-additives

Résultat (Lemme de Fekete, Lemme sous-additif).

On dit que $(u_n)_n$ est sous-additive si

$$\forall n, m \in \mathbf{N}^\star, u_{n+m} \leqslant u_n + u_m$$

Dans ce cas,

$$\frac{u_n}{n} \xrightarrow[n\to+\infty]{} \inf\left\{\frac{u_k}{k}, \quad k \geqslant 1\right\} \underset{\text{def}}{=} \ell$$

Démonstration. On suppose $\ell \in \mathbf{R}$ (le cas $\ell = -\infty$ se traite similairement).

On note $\varepsilon > 0$. Il existe $k_0 \in \mathbf{N}^\star$ tel que

$$\ell \leqslant \frac{u_{k_0}}{k_0} \leqslant \ell + \varepsilon' \underset{\text{def}}{=} \ell + \frac{\varepsilon}{2}$$

Pour $n \in \mathbf{N}\star$, on écrit $n = pk_0 + r$ la division euclidienne de n par k_0. Alors,

$$u_n \leqslant pu_{k_0} + u_r \implies \frac{u_n}{n} \leqslant \frac{u_{k_0}}{k_0} + \frac{u_{r_0}}{n} \leqslant \ell + \varepsilon' + \frac{u_{r_0}}{n} \xrightarrow[n\to+\infty]{} \ell + \varepsilon'$$

donc à partir d'un certain rang,

$$\ell \leqslant \frac{u_n}{n} \leqslant \ell + 2\varepsilon' = \ell + \varepsilon$$

de sorte que

$$\frac{u_n}{n} \xrightarrow[n\to+\infty]{} \ell$$

□

Exemple (Application aux chemins auto-évitants)**.** On munit $\mathbf{Z}^2$ de l'ensemble d'arêtes

$$\{\{(a,b),(a+\varepsilon, b+(1-\varepsilon))\}, \quad \varepsilon \in \{0,1\}, a, b \in \mathbf{Z}\}$$

de sorte à obtenir un graphe sommet-transitif[1] qui correspond au réseau «classique» $\mathbf{Z}^2$. On note ce graphe G, et la transitivité permet d'en choisir arbitrairement un sommet O qui sera l'origine des chemins. Un chemin auto-évitant sur G de taille n est un chemin sur G (suite de sommets adjacents qui commence par l'origine O) de longueur n qui ne passe pas deux fois par le même sommet. On note c_n le nombre de chemins auto-évitants de longueur n.

On a clairement $c_{n+m} \leqslant c_n c_m$ (car un chemin de longueur $n+m$ est la juxtaposition d'un chemin de longueur n et un autre de longueur m), de sorte que $(\ln c_n)_n$ est sous-additive positive. On a donc

$$\frac{1}{n}\ln c_n \xrightarrow[n\to+\infty]{} \ell = \ln \mu$$

donc

$$c_n^{1/n} \xrightarrow[n\to+\infty]{} \mu$$

Cette limite μ est appelée *constante de connectivité* de G. Le raisonnement que l'on vient de mener montre que tout graphe sommet-transitif admet une constante de connectivité.

Exemple (Application aux quasi-morphismes de $\mathbf{Z}$)**.** On dit que

$$f : \mathbf{Z} \longrightarrow \mathbf{R}$$

est un quasi-morphisme s'il existe $C > 0$ tel que

$$\forall m, n \in \mathbf{Z}, \quad |f(n+m) - f(n) - f(m)| \leqslant C$$

On va montrer par récurrence $|f(n_1 + \cdots + n_p) - f(n_1) - \cdots - f(n_p) \leqslant pC$

- Pour $p = 1$, c'est vrai.

1. chaque sommet joue le même rôle : entre chaque sommets, il existe un automorphisme de graphe qui envoie l'un sur l'autre

- On suppose que c'est vrai pour p.

$$\begin{aligned}
&|f(n_1+\cdots+n_{p+1}) - f(n_1) - \cdots f(n_{p+1})| \\
&\qquad\leqslant |f(n_1+\cdots+n_p) - f(n_1) - \cdots - f(n_p)| \\
&\qquad\quad + |f(n_1+\cdots+n_{p+1}) - f(n_1+\cdots+n_p) - f(n_{p+1})| \\
&\qquad\leqslant (p+1)C
\end{aligned}$$

On a alors

$$|f(pn) - pf(n)| \leqslant pC \qquad |f(pn) - nf(p)| \leqslant nC$$

donc

$$\left|\frac{f(pn)}{pn} - \frac{f(n)}{n}\right| \leqslant \frac{C}{n} \qquad \left|\frac{f(pn)}{pn} - \frac{f(p)}{p}\right| \leqslant \frac{C}{p}$$

donc

$$\left|\frac{f(n)}{n} - \frac{f(p)}{p}\right| \leqslant \frac{C}{n} + \frac{C}{p}$$

On note

$$u_n = \frac{f(2^n)}{2^n}$$

de sorte que $|u_{n+1} - u_n|$ est le terme général d'une série convergente, donc (u_n) converge vers un réel ℓ. Puis

$$\Big|\frac{f(n)}{n} - \underbrace{u_n}_{\longrightarrow \ell}\Big| \leqslant \frac{C}{n} + \frac{C}{2^n} \xrightarrow[n\to+\infty]{} 0$$

donc

$$\frac{f(n)}{n} \xrightarrow[n\to+\infty]{} \ell$$

Exercice (Application aux quasi-morphismes réels).

Soit $f : \mathbf{R} \longrightarrow \mathbf{R}$ un quasi-morphisme.

1. Montrer qu'il existe un morphisme φ tel que $\forall x \in \mathbf{R}, |f(x) - \varphi(x)| \leqslant C$
2. Montrer que si f est continue, φ est linéaire.

7 Parties entières

Définition.

Soit $x \in \mathbf{R}$. On appelle **partie entière** de x l'unique entier p tel que

$$p \leqslant x < p+1$$

On la note $E(x)$ ou $\lfloor x \rfloor$

Conséquence 1.

$$\left|x - \frac{\lfloor 10^p x\rfloor}{10^p}\right| \leqslant \frac{1}{10^p} \xrightarrow[p\to+\infty]{} 0$$

donc $\mathbf{Q}$ dense dans $\mathbf{R}$

Exemple (Approximation d'un irrationnel)**.** On note $\alpha \in \mathbf{R}_+ \setminus \mathbf{Q}$, et $\left(\dfrac{p_n}{q_n}\right)_n$ une suite de rationnels qui converge vers α. Que dire de $(p_n)_n$ et $(q_n)_n$?

Pour $N \in \mathbf{N}^\star$, on note $I_N = \{k\alpha, k \in [\![1, N]\!]\}$. On note d un entier naturel qui minimise la distance à I_N. Cette distance (notée $d(I_n, \mathbf{Z})$) est > 0 car I_N ne contient que des irrationnels. À partir d'un certain rang,

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{d(I_N, \mathbf{Z})}{N} \iff |q_n\alpha - p_n| < \frac{d(I_n, \mathbf{Z})}{N} q_n$$

Donc $q_n \notin [\![1, N]\!]$ donc $q_n > N$ d'où

$$q_n \to +\infty$$

et

$$p_n \underset{+\infty}{\sim} \alpha q_n \to +\infty$$

8 Suites récurrentes doubles et déterminant tridiagonal

On note

$$\Delta_n = \begin{vmatrix} a & c & & (0) \\ b & \ddots & \ddots & \\ & \ddots & \ddots & c \\ (0) & & b & a \end{vmatrix}$$

Après calculs, pour $n \geqslant 3$,

$$\Delta_n = a\Delta_{n-1} - bc\Delta_{n-2}.$$

Exemple. Si $a = b = -c = 1$, alors $\Delta_n = Ar_+^n + Br_-^n$ avec r_+, r_- solutions de $r^2 = r + 1$ et

$$A = \frac{\begin{vmatrix} 1 & 1 \\ 1 & r_- \end{vmatrix}}{r_- - r_+} \qquad\qquad B = \frac{\begin{vmatrix} 1 & 1 \\ r_+ & 1 \end{vmatrix}}{r_- - r_+}.$$

Exercice.

Montrer que si $a = 2\cos\theta$ et $b = c = 1$ alors pour $\theta \notin \pi\mathbf{Z}$,

$$\Delta_n = \frac{\sin((n+1)\theta)}{\sin\theta}.$$

9 Développements asymptotiques – Équivalents

a) Développement asymptotique d'une suite implicite

Exercice.

Montrer qu'il existe un unique $u_n \in [0,1]$ tel que $u_n^5 + nu_n - 1 = 0$. En donner un DA à deux termes.

Résolution. L'existence et l'unicité sont faciles. On a

$$u_n = \frac{1}{n} - \frac{u_n^5}{n} \xrightarrow[n\to+\infty]{} 0$$

puis

$$\frac{u_n^5}{n} = o\left(\frac{1}{n}\right) \implies u_n \underset{+\infty}{\sim} \frac{1}{n}$$

donc

$$u_n = \frac{1}{n} - \frac{\left(\frac{1}{n} + o\left(\frac{1}{n}\right)\right)^5}{n} = \frac{1}{n} - \frac{1}{n^6} + o\left(\frac{1}{n^6}\right)$$

□

b) Développement asymptotique d'une fonction implicite

Exercice.

Montrer que pour $x \in \mathbf{R}$, il existe un unique $y > 0$ tel que $\dfrac{y}{\ln y} = x$. On le note $\psi(x)$. Donne un DA en $+\infty$ de ψ

Résolution. L'unicité et l'existence sont faciles. On a

$$\psi(x) = x\ln\psi(x) \geqslant x \implies \psi(x) \xrightarrow[x\to+\infty]{} +\infty$$

et

$$\ln\psi(x) = \ln x + \ln(\ln\psi(x)) = \ln x + o_{+\infty}(\ln\psi(x)) \sim \ln x$$

donc

$$x\ln\psi(x) = \psi(x) \sim x\ln x$$

puis

$$\psi(x) = x\ln\psi(x) = x\ln(x\ln x \cdot (1 + o(1))) = x\ln x + x\ln(\ln x) + x\ln(1 + o(1))$$

□

Remarque.

Si on note π la fonction qui compte les nombres premiers : $\pi : n \longmapsto \#\mathbb{P} \cap [\![1, n]\!]$, alors on admet (difficile) le théorème des nombres premiers :

$$\pi(n) \underset{+\infty}{\sim} \frac{n}{\ln n}$$

d'où

$$p_n = n\ln(p_n)(1+o(1)) \implies \ln p_n = \ln n + \ln p_n + \ln(1+o(1))$$

donc

$$\ln p_n \sim \ln n \implies p_n \sim n \ln p_n \sim n \ln n$$

10 Cesàro-Stolz

Théorème (Cesàro-Stolz).

(H) (a_n) une suite réelle, (b_n) suite réelle strictement croissante strictement positive qui tend vers $+\infty$. On suppose

$$\frac{a_{n+1}-a_n}{b_{n+1}-b_n} \xrightarrow[n\to+\infty]{} \ell \in \overline{\mathbf{R}}$$

(C)

$$\frac{a_n}{b_n} \xrightarrow[n\to+\infty]{} \ell$$

Démonstration. On va montrer le cas $\ell \in \mathbf{R}$. Soit $\varepsilon > 0$. À partir d'un certain rang N,

$$\left(\ell - \frac{\varepsilon}{2}\right)(b_n - b_{n-1}) \leqslant a_n - a_{n-1} \leqslant \left(\ell + \frac{\varepsilon}{2}\right)(b_n - b_{n-1}).$$

On somme :

$$\left(\ell - \frac{\varepsilon}{2}\right)(b_n - b_{N-1}) \leqslant a_n - a_{N-1} \leqslant \left(\ell + \frac{\varepsilon}{2}\right)(b_n - b_{N-1})$$

d'où

$$\underbrace{\frac{a_{N-1}}{b_n}}_{\to 0} + \left(\ell - \frac{\varepsilon}{2}\right)\underbrace{\frac{b_n - b_{N-1}}{b_n}}_{\to 1} \leqslant \frac{a_n}{b_n} \leqslant \left(\ell + \frac{\varepsilon}{2}\right)\underbrace{\frac{b_n - b_{N-1}}{b_n}}_{\to 1} + \underbrace{\frac{a_{N-1}}{b_n}}_{\to 0}$$

et en passant à la limite,

$$\frac{a_n}{b_n} \xrightarrow[n\to+\infty]{} \ell$$

□

Remarque.

Le cas particulier

$$u_n = \sum_{k=1}^{n} x_k$$

et $b_n = 1$ donne le théorème de Cesàro.

Remarque (Lemme de l'escalier).

Avec $b_n = n$, on trouve

$$a_{n+1} - a_n \longrightarrow \ell \in \mathbf{R}^\star \implies a_n \underset{+\infty}{\sim} n\ell$$

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre II

Suites et séries numériques

Sommaire

1 Rappels sur les séries numériques

Définition.

Soit $u \in \mathbf{R}^{\mathbf{N}}$. On appelle **série de terme général** u_n la suite $(S_n(u))_n$ définie par

$$S_n(u) \underset{\text{def}}{=} \sum_{k=1}^{n} u_k$$

On dira que cette série converge si $(S_n(u))$ converge, et on écrira

$$\lim_{n \to +\infty} S_n(u) = \sum_{k=1}^{+\infty} u_k$$

Dans ce cas, on pose

$$R_n(u) \underset{\text{def}}{=} \sum_{k=1}^{+\infty} u_k - S_n(u)$$

qu'on appelle reste d'ordre n de la série. La série de terme général u_k sera notée $\sum u_k$

Remarque.

Le terme général d'une séries convergente tend vers 0. Si $u_n \longrightarrow \ell \in \overline{\mathbf{R}} \setminus \{0\}$ alors la série diverge grossièrement. Si $\sum u_n$ converge alors $R_n(u) \longrightarrow 0$ et on peut noter

$$R_n(u) = \sum_{k=n+1}^{+\infty} u_k$$

Remarque.

On peut remplacer $\mathbf{R}$ par $\mathbf{C}$ ou n'importe quel espace vectoriel normé (traité dans un chapitre ultérieur)

Exemple. Si $u_n = a^n$ pour un complexe a, alors

$$S_n(u) = \begin{cases} n+1 & \text{si } a = 1 \\ \dfrac{1-a^{n+1}}{1-a} & \text{sinon} \end{cases}$$

d'où

$$\sum u_n \text{ CV} \iff |a| < 1$$

et

$$\sum_{k=0}^{+\infty} u_k = \frac{1}{1-a}$$

Exemple. On a

$$\ln\left(1 + \frac{2}{n(n+3)}\right) = \ln(n+1) + \ln(n+2) - \ln(n) - \ln(n+3)$$

donc

$$\sum_{k=1}^{n} \ln\left(1 + \frac{2}{k(k+3)}\right) = \ln 3 + \ln\left(\frac{n+1}{n+3}\right) \xrightarrow[n\to+\infty]{} \ln 3$$

2 Opérations

Proposition.

(H) $\sum u_n, \sum v_n$ deux séries numériques, $\lambda \in \mathbf{C}$

(C)
1. $\lambda \sum u_n + \sum v_n = \sum(\lambda u_n + v_n)$
2. Si les séries convergent, alors $\sum(\lambda u_n + v_n)$ converge (+ égalité des limites)

Remarque.

On en déduit

CV	+	CV	=	CV
DV	+	CV	=	DV
DV	+	DV	=	?

Proposition.

(H) $u \in \mathbf{C}^{\mathbf{N}}$

(C)

$$(u_n) \text{ CV} \iff \sum(u_{n+1} - u_n) \text{ CV}$$

Exemple (Séries de Riemann)**.** On veut étudier $\sum \frac{1}{n^\alpha}$.

- Si $\alpha \leqslant 0$ alors la série diverge grossièrement
- Si $\alpha > 0$ alors

$$\frac{1}{(n+1)^\alpha} - \frac{1}{n^\alpha} = \frac{1}{n^\alpha}\left(-\frac{\alpha}{n} + O\left(\frac{1}{n}\right)\right) \sim -\frac{\alpha}{n^\alpha}$$

  or $(\frac{1}{n^\alpha})_n$ converge vers 0 donc $\sum \frac{1}{(n+1)^\alpha} - \frac{1}{n^\alpha}$ aussi et donc, par équivalence [1], $\sum \frac{1}{n^{\alpha+1}}$ aussi.
- Pour $\alpha < 0$, on trouve alors que $\sum \frac{1}{n^{\alpha+1}}$ diverge

Il ne reste que le cas $\alpha = 1$ à traiter : la série diverge. On a donc

$$\sum \frac{1}{n^\alpha} \text{ CV} \iff \alpha > 1$$

1. c'est une propriété qui sera vue dans la prochaine partie

On va maintenant s'intéresser à la série harmonique

$$H_n = \sum_{k=1}^{n} \frac{1}{k}.$$

On a

$$\ln(n+1) - \ln(n) \sim \frac{1}{n} \implies \sum \frac{1}{k} \text{ DV}$$

et par équivalence des sommes partielles [2] (ou bien par comparaison série-intégrale),

$$H_n \sim \ln(n).$$

On note $u_n = H_n - \ln n$. On a

$$u_{n+1} - u_n = \frac{1}{n+1} - \ln\left(1 + \frac{1}{n}\right) = \frac{1}{n} \times \frac{1}{1+\frac{1}{n}} - \frac{1}{n} - \frac{1}{2n^2} + o\left(\frac{1}{n^2}\right) = -\frac{2}{n^2} + o\left(\frac{1}{n^2}\right)$$

donc $\sum u_{n+1} - u_n$ converge donc (u_n) converge vers un réel γ. On note

$$v_n = H_n - \ln n - \gamma$$

et

$$v_{n+1} - v_n = -\frac{1}{2n^2} + o\left(\frac{1}{n^2}\right)$$

donc (v_n) converge. Par équivalence des restes (série CV),

$$\sum_{k=n}^{+\infty} v_{k+1} - v_k \sim \sum_{k=n} -\frac{1}{2}\left(\frac{1}{n} - \frac{1}{n+1}\right)$$

d'où $v_n \sim \frac{1}{2n}$. On pose

$$\omega_n = H_n - \ln n - \gamma - \frac{1}{2n}$$

Après calculs (vérifiez-le),

$$\omega_{n+1} - \omega_n = \frac{1}{6n^3} + o\left(\frac{1}{n^3}\right) \sim \frac{1}{6n^3} \sim \frac{1}{12} \cdot \left(\frac{1}{n^2} - \frac{1}{(n+1)^2}\right)$$

d'où $\omega_n \sim \frac{1}{12n^2}$

Bilan. (Question X)

$$H_n = \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\left(\frac{1}{n^2}\right)$$

Exercice (Mines-Ponts).

> On note
>
> $$k_n = \min\{k \in \mathbf{N}, \quad H_k > n\}$$
>
> Calculer
>
> $$\lim_{n \to +\infty} \frac{k_{n+1}}{k_n}$$

3 Séries à termes positifs

Proposition.

> (H) u est une suite positive
>
> (C) $\sum u_n$ converge si et seulement si $(S_n(u))$ est majorée

2. vu plus tard

Proposition.

(H) u, v des suites positives

(C)
1. Si $u_n \leqslant v_n$ à partir d'un certain rang et si $\sum v_n$ converge alors $\sum u_n$ aussi
2. Si $u_n = O(v_n)$ et $\sum v_n$ converge alors $\sum u_n$ aussi
3. Si $u_n \sim v_n$ alors $\sum u_n$ et $\sum v_n$ ont la même nature

Démonstration.

1. Si $u_n \leqslant v_n$ à partir du rang N,
$$S_n(u) \leqslant \sum_{k=0}^{N} u_k + \sum_{k=N+1}^{+\infty} v_k$$
donc $(S_n(u))$ croissante est majorée donc converge.
2. Idem à constante multiplicative près
3. $u_n \sim v_n$ donne $u_n = O(v_n)$ et $v_n = O(u_n)$ et on applique 2.

□

Exercice.

On note $(a_n)_{n\geqslant 1}$ une suite positive telle que $\sum a_n$ converge. Donner la nature de
$$\sum a_n \sin(a_n), \qquad \sum \frac{a_n}{1+a_n^2}, \qquad \sum \frac{\sqrt{a_n}}{n}$$

Résolution. À partir d'un certain rang, $0 \leqslant a_n \sin(a_n) \leqslant a_n$ puis
$$\frac{a_n}{1+a_n^2} \sim a_n$$
et enfin (AM-GM)
$$0 \leqslant \frac{\sqrt{a_n}}{n} \leqslant \frac{1}{2}\left(a_n + \frac{1}{n^2}\right)$$
donc les trois séries convergent. □

Exercice (X).

Soit x une suite positive. Montrer que si $\sum x_n$ converge, alors
$$\sum x_n^{\frac{n}{n+1}}$$
aussi

Résolution. Idée : On fait un découpage. On pose
$$I = \{n \in \mathbf{N}, \quad x_n \geqslant 0 \text{ et } x_n^{-\frac{1}{n+1}} > 2\}$$
Si $n \in I$ alors
$$\frac{1}{2} > x_n^{\frac{1}{n+1}} \iff \frac{1}{2^{n+1}} > x_n \implies \frac{1}{2^n} > y_n$$
Sinon,
$$x_n = 0 \implies y_n = 0 \leqslant 2x_n$$
et
$$x_n^{-\frac{1}{n+1}} \leqslant 2 \implies y_n \leqslant 2x_n$$
donc dans tous les cas,
$$0 \leqslant y_n \leqslant \frac{1}{2^n} + 2x_n$$

□

4 Absolue convergence, semi-convergence

Définition.

Soit a une suite réelle.

1. On dira que $\sum a_n$ est absolument convergnete si $\sum |a_n|$ converge
2. On dira que $\sum a_n$ est semi convergente si elle est convergente mais pas absolument convergente

Théorème.

L'absolue convergence entraîne la convergence

Démonstration. On écrit $a_n = a_n^+ - a_n^-$ avec $a_n^+ = \max(a_n, 0)$ et $a_n^- = \max(-a_n, 0)$ de sorte que $|a_n| = a_n^+ + a_n^-$ □

Remarque.

$$\begin{array}{ccccc} \text{ACV} & + & \text{ACV} & = & \text{ACV} \\ \text{ACV} & + & \text{SCV} & = & \text{SCV} \\ \text{SCV} & + & \text{SCV} & = & ? \end{array}$$

5 Comparaison logarithmique

Proposition.

(H) u, v deux suites strictement positives telles que APCR N

$$\frac{u_{n+1}}{u_n} \leqslant \frac{v_{n+1}}{v_n}$$

(C) $u_n = O(v_n)$

Démonstration.

$$\forall n > N, \prod_{k=N}^{n-1} \frac{u_{k+1}}{u_k} = \frac{u_n}{u_N} \leqslant \frac{v_n}{v_N} \implies u_n \leqslant v_n \frac{u_N}{v_N} = O(v_n)$$

□

Théorème (Règle de D'Alembert).

(H) a une suite positive telle que

$$\frac{a_{n+1}}{a_n} \xrightarrow[n \to +\infty]{} \ell \in \overline{\mathbf{R}}$$

(C)
1. Si $0 \leqslant \ell < 1$ alors $\sum a_n$ converge
2. Si $\ell > 1$ alors $\sum a_n$ diverge

Démonstration.

- $\exists \varepsilon > 0, \quad 0 < \ell' = \ell + \varepsilon < 1$ et on applique la proposition précédente à $u = a$, $v = (\ell'^n)_n$.
- $\exists \varepsilon > 0, \quad 1 < \ell' = \ell - \varepsilon$ et on fait pareil.

□

Remarque.

Il faut faire attention à avoir (a_n) jamais nulle à partir d'un certain rang. Le critère est intéressant lorsque $\frac{a_{n+1}}{a_n}$ a une expression simple.

Exercice.

Donner la nature de $\sum \frac{n^n}{n!^\alpha}$ en fonction de α

Résolution. On a

$$\frac{a_{n+1}}{a_n} = \frac{(n+1)^{n+1}}{n^n} \times \frac{1}{(n+1)^\alpha} = \frac{\left(1+\frac{1}{n}\right)^n}{(n+1)^{\alpha-1}} \xrightarrow[n\to+\infty]{} \begin{cases} 0 & \text{si } \alpha > 1 \\ e & \text{si } \alpha = 1 \\ +\infty & \text{si } \alpha < 1 \end{cases}$$

et on conclut avec la règle de d'Alembert □

Exercice.

On note a une suite réelle telle que

$$|a_n|^{\frac{1}{n}} \xrightarrow[n\to+\infty]{} \ell \in \mathbf{R} \cup \{+\infty\}$$

Donner la nature de $\sum |a_n|$ en fonction de ℓ

Résolution. Si $\ell > 1$ alors $\exists \varepsilon > 0, 1 < \ell' = \ell - \varepsilon \leqslant |a_n|^{\frac{1}{n}}$ donc $\ell'^n \leqslant |a_n|$ et la série diverge.

Si $\ell < 1$ alors par un raisonnement similaire, la série converge.

Si $\ell = 1$ alors on ne peut pas conclure en général :

$$\left|\frac{1}{n^2}\right|^{\frac{1}{n}} \xrightarrow[n\to+\infty]{} 1 \qquad \text{et} \qquad \sum \frac{1}{n^2} \text{ CV}$$

$$\left|\left(1+\frac{1}{n}\right)^n\right|^{\frac{1}{n}} \xrightarrow[n\to+\infty]{} 1 \qquad \text{et} \qquad \sum \left(1+\frac{1}{n}\right)^n \text{ DV grossièrement}$$

□

6 Sommation des relations de comparaion

Théorème.

(H) u, v sont des suites réelles positives et $\sum v_n$ converge.

(C)
1. Si $u_n = O(v_n)$ alors $\sum u_n$ converge et
$$R_n(u) = O(R_n(v))$$
2. Si $u_n = o(v_n)$ alors $\sum u_n$ converge et
$$R_n(u) = o(R_n(v))$$
3. Si $u_n \sim v_n$ alors $\sum u_n$ converge et
$$R_n(u) \sim R_n(v)$$

Démonstration. La convergence est déjà vue, on ne montre que les relations de comparaison

1. Il existe un rang N et une constante $C > 0$ tels que $\forall n \geqslant N, u_n \leqslant Cv_n$. On a alors
$$\forall m \geqslant n \geqslant N, \qquad \sum_{k=n}^{N} u_k \leqslant C \sum_{k=n}^{m} v_k$$
puis $m \to +\infty$ donnc $R_n(u) \leqslant CR_n(v)$ ie (C)
2. Soit $\varepsilon > 0$. Il existe un rang N après lequel $u_n \leqslant \varepsilon v_n$. Par le même raisonnement, $R_n(u) \leqslant \varepsilon R_n(v)$ après N donc (C)
3. $|u_n - v_n| = o(v_n)$ donc
$$|R_n(u) - R_n(v)| = |R_n(u-v)| \leqslant R_n(|u-v|) = o(R_n(v))$$

□

Théorème.

(H) u, v suites réelles positives et $\sum u_n$ diverge.

(C)

1. Si $u_n = O(v_n)$ alors $\sum v_n$ diverge et
$$S_n(u) = O(S_n(v))$$
2. Si $u_n = o(v_n)$ alors $\sum v_n$ diverge et
$$S_n(u) = o(S_n(v))$$
3. Si $u_n \sim v_n$ alors $\sum v_n$ diverge et
$$S_n(u) \sim S_n(v)$$

Démonstration. La divergence est déjà vue, on ne montre que le reste.

1. Il existe $C > 0$, et un rang N à partir duquel $u_n \leqslant C v_n$.
$$\forall n \geqslant N, \quad \underbrace{S_n(u)}_{\longrightarrow +\infty} = \sum_{k=0}^{N-1} u_k + \sum_{k=N}^{n} u_k \leqslant \sum_{k=0}^{N-1} + C \underbrace{\sum_{k=0}^{n} v_k}_{S_n(v) \longrightarrow +\infty} - C \sum_{k=0}^{N-1} v_k$$
donc à partir d'un certain rang,
$$\frac{S_n(u)}{S_n(v)} \leqslant C + \frac{\sum_{k=0}^{N-1} u_k - C \sum_{k=0}^{N-1} v_k}{S_n(v)} \xrightarrow[n \to +\infty]{} C$$
d'où (C)
2. Idem
3. $S_n(|u - v|) = o(S_n(v))$ (attention aux hypothèses, si $\sum |u - v|$ converge ok sinon on applique 2.)

□

Exemple. On va montrer
$$\sum_{k=n}^{+\infty} \frac{\ln(k+1)}{k^2} \sim \frac{\ln n}{n}$$

Démonstration. La série converge puisque $\frac{\ln n}{n^2} = o\left(\frac{1}{n^{3/2}}\right)$. Puis, on a
$$\frac{\ln(n+1)}{n+1} - \frac{\ln n}{n} = \frac{\ln\left(\frac{n+1}{n}\right)}{n+1} + \frac{\ln n}{n+1} - \frac{\ln n}{n} = \ln n \left(\frac{1}{n+1} - \frac{1}{n}\right) + \ln\left(1 + \frac{1}{n}\right) \frac{1}{n+1} \sim -\frac{\ln n}{n^2}.$$
d'où la conclusion. □

Exercice.

Donner un développement asymptotique de
$$R_n = \sum_{k=n}^{+\infty} \frac{1}{k^2}$$

Résolution.
$$\frac{1}{n^2} \sim \frac{1}{n} - \frac{1}{n+1}$$
donc
$$R_n \sim \frac{1}{n}$$

puis

$$R_n - \frac{1}{n} = \sum_{k=n}^{+\infty} \left(\frac{1}{k^2} - \frac{1}{k} + \frac{1}{k+1} \right) = \sum_{k=n}^{+\infty} \frac{1}{k^2(k+1)}$$

or

$$\frac{1}{n^3} \sim \frac{1}{2n^2} - \frac{1}{2(n+1)^2}$$

donc

$$R_n = \frac{1}{n} + \frac{1}{2n^2} + o\left(\frac{1}{n^2}\right)$$

□

Exemple (Équivalent de Stirling)**.** On va trouver un équivalent de $u_n = n!$. On a

$$\ln(u_n) = \sum_{k=1}^{n} \ln k$$

or

$$(k+1)\ln(k+1) - k\ln k \sim \ln k$$

qui est le terme général positif d'une série divergente donc

$$\ln(u_n) \sim \sum_{k=1}^{n} ((k+1)\ln(k+1) - k\ln k) \sim n\ln n.$$

On note $v_n = \ln u_n - n\ln n$ puis

$$v_{n+1} - v_n = \ln(n+1) - (n+1)\ln(n+1) + n\ln n = -n\ln\left(1 + \frac{1}{n}\right) \sim -1$$

qui est le terme général négatif (mais de signe constant) d'une série divergente donc

$$v_n \sim -n$$

On note $w_n = v_n + n$ et

$$w_{n+1} - w_n = -n\left(1 + \frac{1}{n}\right) + 1 = -n\left(\frac{1}{n} - \frac{1}{2n^2} + o\left(\frac{1}{n^2}\right)\right) + 1 = \frac{1}{2n} + o\left(\frac{1}{n}\right) \sim \frac{1}{2n} \sim \frac{1}{2}(\ln(n+1) - \ln n)$$

donc

$$w_n \sim \frac{\ln n}{2}$$

On pose $y_n = w_n - \frac{1}{2}\ln n$ et

$$y_{n+1} - y_n = -n\ln\left(1 + \frac{1}{n}\right) + 1 - \frac{1}{2}\ln\left(1 + \frac{1}{n}\right) \sim \frac{1}{6n^2}$$

qui est le terme général d'une séries ACV donc y_n converge vers un réel ℓ. On a donc

$$\ln(u_n) = n\ln n - n + \frac{1}{2}\ln n + \ell + o(1)$$

donc

$$u_n \sim e^{\ell}\sqrt{n}\, n^n e^{-n}$$

Dans le chapitre d'intégration (**Intégrales de Wallis** p.44) on montrera $e^{\ell} = \sqrt{2\pi}$

Exemple (Raabe-Duhamel)**.** On note u une suite réelle jamais nulle à partir d'un certain rang telle que

$$\frac{u_{n+1}}{u_n} = 1 - \frac{\lambda}{n} + o\left(\frac{1}{n}\right), \qquad \lambda > 0$$

On va chercher la nature de $\sum u_n$ en fonction de λ

On a

$$\frac{u_{n+1}}{u_n} \sim 1$$

donc u_n est de signe constant à partir d'un certain rang, on suppose spdg que c'est positif.

$$\ln u_{n+1} - \ln u_n \sim -\frac{\lambda}{n}$$

qui est le terme général d'une série divergente (signe constant) donc

$$\ln u_n \sim -\lambda H_n \sim -\lambda \ln n$$

d'où $\ln u_n = -\lambda \ln n + o(\ln n)$ donc $u_n = n^{-\lambda + o(1)} = \dfrac{1}{n^{\lambda + o(1)}}$.

Si $\lambda > 1$ alors $\sum u_n$ converge, si $\lambda < 1$ alors $\sum u_n$ diverge et si $\lambda = 1$ on ne peut pas conclure (e.g. $u_n = 1/n$ et $u_n = 1/(n \ln^2 n)$).

Remarque.

Si $\ell \neq 0$, $u_n \sim \ell$ (tg série DV) donc $\sum_{k=1}^n u_k \sim n\ell$ d'où le théorème de Cesàro. Si $\ell = 0$ alors $u_n = o(1)$ et $\sum_{k=1}^n u_k = o(n)$ et on retrouve aussi Cesàro.
Plus généralement, si

$$\frac{a_{n+1} - a_n}{b_{n+1} - b_n} \longrightarrow \ell \neq 0$$

avec b_n croissante qui tend vers $+\infty$, alors

$$a_{n+1} - a_n \sim \ell(b_{n+1} - b_n)$$

qui est le terme général d'une série divergente donc

$$\sum_{k=1}^{n-1} a_{n+1} - a_n = a_n - a_1 \sim \ell(b_n - b_1) \implies a_n \sim \ell b_n \implies \frac{a_n}{b_n} \longrightarrow \ell$$

d'où le théorème de Cesàro-Stolz (dans le cas $\ell \in \mathbf{R}^\star$)

7 Comparaison série-intégrale [3]

On note f décroissante continue positive au voisinage de $+\infty$ (pour simplifier on prend $\mathbf{R}_+$ comme voisinage). On a

$$f(k+1) \leqslant \int_k^{k+1} f \leqslant f(k)$$

Exemple. On trouve de cette manière

$$H_n \sim \ln n \qquad \text{et} \qquad H_{2n} - H_n \sim \ln 2.$$

Théorème.

(H) f est continue décroissante positive sur $\mathbf{R}_+$, $u_n = \displaystyle\int_{n-1}^n f - f(n)$

(C) $\sum u_n$ converge et $u_n \geqslant 0$

Démonstration. $u_n \leqslant f(n-1) - f(n)$ tg série CV car f converge en $+\infty$ □

Exercice.

On note u une suite positive, $S_n = \sum_{k=0}^n u_k$ et quand c'est possible, $R_n = \sum_{k=n}^{+\infty} u_k$

1. Montrer que si $\sum u_n$ diverge alors $\sum \frac{u_n}{S_n^\alpha}$ converge ssi $\alpha > 1$
2. Montrer que si $\sum u_n$ converge alors $\sum \frac{u_n}{R_n^\alpha}$ converge ssi $\alpha < 1$

3. Épisode 1

Résolution (uniquement 1.)

1. On a $S_n \longrightarrow +\infty$, (S_n) croissante. On suppose $\alpha > 1$.

$$\frac{u_n}{S_n^\alpha} = \frac{S_n - S_{n-1}}{S_n^\alpha} \leqslant \int_{S_{n-1}}^{S_n} \frac{\mathrm{d}t}{t^\alpha} \implies \sum_{k=1}^{n} \frac{u_k}{S_k^\alpha} \leqslant \frac{1}{\alpha-1}\left(\frac{1}{S_0^{\alpha-1}} - \frac{1}{S_n^{\alpha-1}}\right) \leqslant \frac{1}{\alpha-1} S_0^{1-\alpha} \text{ donc CV}$$

Si $\alpha \geqslant 0$ alors APCR, $\frac{u_n}{S_n^\alpha} \geqslant u_n$ donc la série diverge.
Si $\alpha = 1$, on a

$$\sum_{k=n}^{p} \frac{u_k}{S_k} \geqslant \frac{1}{S_p} \sum_{k=n}^{p} u_k = \frac{S_p - S_{n-1}}{S_p} \geqslant 1 - \frac{S_{n-1}}{S_p}$$

Si $\sum \frac{u_k}{S_k}$ converge alors $p \longrightarrow +\infty$ donne $\sum_{k=n}^{+\infty} \frac{u_k}{S_k} \geqslant 1$ absurde, donc la série diverge. Pour $\alpha \in]0,1]$,

$$\frac{u_k}{S_k^\alpha} \underset{\text{APCR}}{\geqslant} \frac{u_k}{S_k}$$

donc la série diverge.

□

8 Théorème des séries alternées

Théorème.

(H) a une suite décroissante positive qui tend vers 0.

(C) 1. $\sum a_n(-1)^n$ converge

2.
$$\sum_{k=n+1}^{+\infty} (-1)^k a_k$$

a le même signe que $(-1)^{n+1}a_{n+1}$ (le premier terme de la somme)

3.
$$\left|\sum_{k=n+1}^{+\infty} (-1)^k a_k\right| \leqslant a_{n+1}$$

Démonstration.

1. Les suites S_{2n} et S_{2n+1} sont adjacentes donc convergentes de limite ℓ.
2. Vu le calcul fait en 1.,

$$\sum_{k=2p}^{+\infty} (-1)^k a_k = \ell - S_{2p-1} \geqslant 0$$

du même signe que son premier terme. C'est la même chose pour les restes d'indices impair.

3.
$$0 \leqslant \ell - S_{2p-1} \leqslant S_{2p} - S_{2p-1} \implies 0 \leqslant \sum_{k=2n} (-1)^k a_k \leqslant a_{2n}$$

et on fait dans l'autre sens pour les impairs.

□

9 Transformation d'Abel

On part de deux suites (a_n) et (b_n) et d'une somme $\displaystyle\sum_{k=0}^{n} a_k b_k$. On pose

$$S_n = \sum_{k=0}^{n} a_k$$

On a $a_n = S_n - S_{n-1}$ pour $n \geqslant 0$ avec $S_{-1} = 0$. Alors,

$$\sum_{k=0}^{n} a_k b_k = \sum_{k=0}^{n} (S_n - S_{n-1}) b_k = \sum_{k=0}^{n-1} S_k (b_k - b_{k+1}) + S_n b_n$$

Exemple. On suppose $|S_n|$ majorée par M et (b_n) décroissante de limite nulle.

$$b_n S_n \longrightarrow 0$$

et

$$|S_k(b_k - b_{k+1})| \leqslant M(b_k - b_{k+1})$$

donc

$$\sum S_k(b_k - b_{k+1}) \text{ ACV}$$

donc $\sum a_k b_k$ converge.

Exemple. $\sum \frac{\sin n}{n}$ converge car $S_n(\sin n)$ est bornée (on peut faire le calcul) et $\frac{1}{n}$ est décroissante de limite nulle.

Exemple. On va chercher la nature de $\sum \frac{\sin\sqrt{n}}{n}$. On note S_n les sommes partielles de sorte que

$$\forall n \geqslant 1, \qquad \sin\sqrt{n} = S_n - S_{n-1}$$

et

$$\sum_{k=1}^{n} \frac{\sin\sqrt{n}}{n} = \sum_{k=1}^{n} \frac{S_k - S_{k-1}}{k} = \sum_{k=1}^{n-1} S_k \left(\frac{1}{k} - \frac{1}{k+1}\right) + \frac{S_n}{n}.$$

Pour $x \in [k, k+1]$, il existe $c_x \in [k, k+1]$ tel que

$$\sin\sqrt{x} - \sin\sqrt{k} = (x-k)\frac{\cos\sqrt{c_x}}{2\sqrt{c_x}}$$

donc

$$|\sin\sqrt{x} - \sin\sqrt{k}| \leqslant \frac{1}{2\sqrt{k}}$$

et

$$\left|\sin k - \int_k^{k+1} \sin\sqrt{t}\ \mathrm{d}t\right| \leqslant \int_k^{k+1} |sin\sqrt{k} - \sin\sqrt{t}|\,\mathrm{d}t \leqslant \frac{1}{2\sqrt{k}}$$

donc

$$\left|\sum_{k=1}^{n}\left(\sin\sqrt{k} - \int_k^{k+1}\sin\sqrt{t}\ \mathrm{d}t\right)\right| = \left|S_n - \int_1^{n+1}\sin\sqrt{t}\ \mathrm{d}t\right| \leqslant \sum_{k=1}^{n}\frac{1}{2\sqrt{k}}$$

or

$$\int_1^{n+1} \sin\sqrt{t}\ \mathrm{d}t = \int_1^{\sqrt{n+1}} 2u\sin u\,\mathrm{d}u = 2[-u\cos u + \sin u]_1^{\sqrt{n+1}} = O(\sqrt{n}).$$

Puis,

$$\frac{1}{2\sqrt{k}} \sim \sqrt{k+1} - \sqrt{k} \implies \sum_{k=1}^{n} \frac{1}{2\sqrt{k}} \sim \sqrt{n}$$

On a donc

$$|S_n| - \left|\int_1^{n+1} \sin\sqrt{t}\ \mathrm{d}t\right| \leqslant \sum_{k=1}^{n}\frac{1}{2\sqrt{k}} = O(\sqrt{n}) \implies S_n = O(\sqrt{n})$$

donc

$$S_k\left(\frac{1}{k} - \frac{1}{k+1}\right) = O\left(\frac{1}{n^{3/2}}\right)$$

et la série converge.

10 Utilisation des paquets

Remarque.

Si $\sum a_n$ converge alors pour toute suite d'entiers (u_n) telle que $u_n \geqslant n$, on a

$$\sum_{k=n}^{u_n} a_k = S_{u_n}(a) - S_{n-1}(a) \xrightarrow[n\to+\infty]{} 0$$

En particulier, si

$$\sum_{k=n}^{u_n} a_k \not\xrightarrow[n\to+\infty]{} 0$$

alors la série diverge.

Exemple (Série harmonique)**.**

$$\sum_{k=n}^{2n} \frac{1}{k} \geqslant \frac{n+1}{2n+1} \xrightarrow[n\to+\infty]{} \frac{1}{2} \neq 0$$

donc la série harmonique diverge.

Exemple (Oscillations lentes)**.** On va déterminer la nature de

$$\sum \frac{\cos(\ln n)}{n}$$

Pour $N \geqslant 1$,

$$\sum_{-\frac{\pi}{3}+2N\pi \leqslant \ln n \leqslant \frac{\pi}{3}+2N\pi} \frac{\cos(\ln n)}{n} \geqslant \frac{1}{2} \sum_{e^{-\frac{\pi}{3}} e^{2N\pi} \leqslant n \leqslant e^{\frac{\pi}{3}} e^{2N\pi}} \frac{1}{n} \geqslant \frac{1}{2} \frac{\left\lfloor e^{\frac{\pi}{3}} e^{2N\pi} \right\rfloor - \left\lfloor e^{-\frac{\pi}{3}} e^{2N\pi} \right\rfloor}{e^{\frac{\pi}{3}} e^{2N\pi}} \xrightarrow[n\to+\infty]{} \frac{1}{2}(1-e^{-\frac{2\pi}{3}}) \neq 0$$

donc la série diverge.

Exemple (Série lacunaire)**.** On note

$$u_n = \begin{cases} \frac{1}{n^\alpha} & \text{si } n \text{ n'a pas de 9 dans son écriture décimale} \\ 0 & \text{sinon} \end{cases}$$

Les sommes partielles sont croissantes donc la série $\sum u_n$ converge si et seulement si (S_n) a une suite extraite convergente. On va considérer des paquets du type

$$\sum_{k=10^n}^{10^{n+1}-1} u_k \leqslant \frac{1}{10^{n\alpha}} \times \underbrace{8 \times 9^n}_{\text{nb d'entiers sans 9}}$$

On a ainsi

$$\underbrace{\left(\frac{9}{10^\alpha}\right)^n}_{\text{tg série CV} \iff \frac{9}{10^\alpha}<1} \frac{8}{10^\alpha} \leqslant \sum_{k=10^n}^{10^{n+1}-1} u_k = S_{10^{n+1}-1} - S_{10^n-1} \leqslant \left(\frac{9}{10^\alpha}\right)^n \cdot 8$$

donc $(S_{10^n-1})_n$ converge ssi $\alpha > \dfrac{\ln 9}{\ln 10}$

11 Développement décimal illimité

Pour $x \in \mathbf{R}$, on pose $a_0 = \lfloor x \rfloor$ et

$$a_n = \lfloor 10^n x \rfloor - 10 \left\lfloor 10^{n-1} x \right\rfloor \in [\![0, 9]\!]$$

Par récurrence, on montre

$$\frac{\lfloor 10^n x \rfloor}{10^n} = \sum_{k=0}^{n} \frac{a_k}{10^k} = \overline{a_0, a_1 \cdots a_n}$$

Puis, $\sum \frac{a_k}{10^k}$ converge et sa somme vaut x.

Remarque.

La suite (a_n) n'est pas stationnaire égale à 9.

Démonstration. On suppose que la suite est stationnaire égale à 9 : $a_{N-1} \neq 9$ et $(a_n)_{n\geqslant N}$ constante égale à 9. Dans ce cas,

$$x = \sum_{k=0}^{N} \frac{a_k}{10^k} + \underbrace{\sum_{k=N}^{+\infty} \frac{9}{10^k}}_{=\frac{1}{10^{N-1}}}$$

et c'est absurde en calculant explicitement a_{N-1} □

On dit que le développement obtenu est le **développement décimal propre** de x

Proposition.

x est rationnel si et seulement si son développement propre est ultimement périodique (périodique à partir d'un certain rang)

Démonstration. On supose (a_k) T-périodique à partir du rang N. On a

$$x = \underbrace{\sum_{k=0}^{N-1} \frac{a_k}{10^k}}_{\in\mathbf{Q}} + \underbrace{\sum_{k=0}^{+\infty} \frac{1}{10^{kT}}}_{=\frac{1}{1-\frac{1}{10^T}}\in\mathbf{Q}} \underbrace{\left(\frac{a_N}{10^N} + \cdots + \frac{a_{N+T-1}}{10^{N+T-1}}\right)}_{\in\mathbf{Q}} \in \mathbf{Q}$$

On suppose $x = \frac{p}{q} \in \mathbf{Q}$. Il y a un nombre fini de restes modulo p donc il existe $n < m$ tels que $10^n p \equiv 10^m p \pmod{q}$.

On a $10^n p = q_n q + r_n$ avec $q_n \in \mathbf{N}$, donc $10^n x = q_n + \frac{r_n}{q}$. On a alors, pour $n, i \in \mathbf{N}^\star$,

$$\begin{aligned}
a_{n+i} &= E(10^{n+i}x) - 10E(10^{n+i-1}x) \\
&= E\left(10^i\left(q_n + \frac{r_n}{q}\right)\right) - 10E\left(10^{i-1}\left(q_n + \frac{r_n}{q}\right)\right) \\
&= E\left(10^i\frac{r_n}{q}\right) + 10^i q_n - 10E\left(10^{i-1}\frac{r_n}{q}\right) - 10^i q_n \\
&= E\left(10^i\frac{r_n}{q}\right) - 10E\left(10^{i-1}\frac{r_n}{q}\right)
\end{aligned}$$

On pose $T = m - n$. On a, pour tout $i \geqslant 1$, $a_{n+i+T} = a_{m+i} = a_{n+i}$. Donc $(a_k)_k$ est périodique à partir du rang n. □

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre III

Familles sommables

Sommaire

1 Dénombrabilité

Définition.

Un ensemble est dénombrable si et seulement si il est en bijection avec $\mathbf{N}$

Exemple. $\mathbf{N}, 2\mathbf{N}, \mathbf{N}^\star, \mathbf{Z}$

Proposition.

1. Toute partie infinie de $\mathbf{N}$ est dénombrable
2. Toute partie de $\mathbf{N}$ est finie ou dénombrable

Démonstration. Soit A une partie de $\mathbf{N}$ infinie. On note $\varphi(0) = \min A$ et

$$\varphi(n) = \min(A \setminus [\![0, \varphi(n-1)]\!])$$

de sorte que φ est croissante donc injective, et surjective car si $a \in A$ n'a pas d'antécédent, $I = \{k, \quad a < \varphi(k)\}$ est non vide et a un minimum p, et $\varphi(0) < a$ donc $p \geqslant 1$ d'où $\varphi(p-1) < a < \varphi(p)$ absurde. □

Proposition.

1. Si $f : A \to B$ est injective et B dénombrable alors A est fini ou dénombrable
2. Si $f : A \to B$ est surjective et A dénombrable alors B est fini ou dénombrable.

Démonstration.

1. B est en bijection avec $\mathbf{N}$ donc on peut supposer $B = \mathbf{N}$. Si A est fini alors ok, sinon $f(A)$ est une partie infinie de $\mathbf{N}$ en bijection avec A.
2. On note $\psi(b)$ un élément de $f^{-1}(\{b\})$. $f \circ \psi = \mathrm{id}_B$ injective donc ψ est injective et on utilise 1.

□

Proposition.

1. Si I est non-vide, fini ou dénombrable, et $(A_i)_{i\in I}$ est une famille d'ensembles finis ou dénombrables, alors
$$\bigcup_{i\in I} A_i$$
est fini ou dénombrable
2. $E_1, \cdots, E_n$ des ensembles finis ou dénombrables, non vides. $E_1 \times \cdots \times E_n$ est fini ou dénombrable et $E_1 \times \cdots \times E_n$ est dénombrable si et seulement si au moins l'un des E_i est dénombrable.

Démonstration.

1. On note $\varphi : \mathbf{N} \to I$ surjective et pour chaque i on note $f_i : \mathbf{N} \to A_i$ bijective de sorte que
$$\psi : (p, q) \in \mathbf{N}^2 \longmapsto f_{\varphi(q)}(p) \in \bigcup_{i\in I} A_i$$
est surjective, et $\mathbf{N}^2$ est dénombrable.
2. Chaque E_i est en bijection avec une partie de $\mathbf{N}$, on peut supposer $E_i \subseteq \mathbf{N}$. On note $p_1, \cdots, p_n$ des premiers disjoints.
$$f : E_1 \times \cdots \times E_n \longrightarrow \mathbf{N}, \quad (a_1, \cdots, a_n) \longmapsto p_1^{a_1} \cdots p_n^{a_n}$$
est injective et $\mathbf{N}$ dénombrable. Si tous les E_i sont finis alors le produit est fini et si l'un est infini alors le produit est infini.

□

2 Exemples d'ensembles classiques

Exemple. $\mathbf{Q}$ est dénombrable car $\mathbf{Z} \times \mathbf{N}^\star$ est dénombrable et $(p, q) \in \mathbf{Z} \times \mathbf{N}^\star \longmapsto \frac{p}{q}$ est surjective

Exemple. L'ensemble des nombres algébriques est dénombrable :
$$\mathscr{A} = \bigcup_{n\in\mathbf{N}^\star} \bigcup_{P\in\mathbf{Z}_n[X]} \mathscr{Z}_{\mathbf{C}}(P)$$

Exemple (Diagonale de Cantor)**.** $\mathbf{R}$ n'est pas dénombrable. Si $\mathbf{R}$ est dénombrable alors $[0, 1[$ est dénombrable, et on note $(r_n)_{n\in\mathbf{N}}$ une énumération des éléments de $[0, 1[$. On construit le réel $x \in [0, 1[$ de la manière suivante : si la n-ième décimale de r_n vaut 1 alors la n-ième décimale de x vaut 0, sinon elle vaut 1. Le réel ainsi construit ne peut pas être un r_n car sa n-ième décimale est différente de celle de r_n. On a donc trouvé un réel qui n'est pas dans l'énumération, c'est absurde.

3 Discontinuités d'une fonction monotone

On note $f : [a, b] \in \mathbf{R}$ croissante. On va montrer que l'ensemble des points de discontinuité de f est fini ou dénombrable.

On note pour $x \in]a, b[$,
$$\delta(x) = \lim_{\substack{t\to x\\ t>x}} f(t) - \lim_{\substack{t\to x\\ t<x}} f(t)$$

- f est croissante donc δ est positive et f est continue en a ssi $\delta(a) = 0$.
- Pour tout $n \in \mathbf{N}^\star$, on note
$$I_n = \left\{ x \in]a, b[, \qquad \delta(x) \geqslant \frac{f(b) - f(a) + 1}{n} \right\}$$

- Si I_n est de cardinal $\geqslant n+1$ alors on peut trouver $x_1 < \cdots < x_{n+1}$ dans I_n, et on se donne $a < t_1 < x_1 < \cdots < x_{n+1} < t_{n+2} < b$ pour avoir

$$f(b) - f(a) = \underbrace{f(b) - f(t_{n+2})}_{\geqslant 0} + \underbrace{f(t_{n+2}) - f(b_{n+1})}_{\geqslant \delta(x_{n+1})} + \cdots + \underbrace{f(t_2) - f(t_1)}_{\geqslant \delta(x_1)} + \underbrace{f(t_1) - f(b)}_{\geqslant 0}$$

donc

$$f(b) - f(a) \geqslant \delta(x_{n+1}) + \cdots + \delta(x_1) \geqslant n\frac{f(b) - f(a) + 1}{n}$$

absurde donc I_n est fini. $x \in]a, b[$ est un point de discontinuité si et seulement si $\delta(x) > 0$ ssi $\exists n \in \mathbf{N}, x \in I_n$ ssi

$$x \in \bigcup_{n \in \mathbf{N}^\star} I_n$$

4 Familles sommables de réels positifs

Pour un ensemble dénombrable I, on note $\mathscr{P}_f(I)$ l'ensemble des parties finies de I

Définition.

Soit $(a_i)_{i\in I} \in (\mathbf{R}_+)^I$. On dira que la famille $(a_i)_{i\in I}$ est **sommable** si

$$\left\{\sum_{j\in J} a_j, \quad J \in \mathscr{P}_f(I)\right\}$$

est majoré. On note alors

$$\sum_{i\in I} a_i = \sup \left\{\sum_{j\in J} a_j, \quad J \in \mathscr{P}_f(I)\right\}$$

Si la famille n'est pas sommable on peut parfois écrire

$$\sum_{i\in I} a_i = +\infty$$

Proposition.

(H) $(a_i)_{i\in I}$ famille dénombrable de réels positive et $S \in \mathbf{R}$

(C) $(a_i)_{i\in I}$ est sommable et $S = \sum_{i\in I} a_i$ si et seulement si les deux conditions suivantes sont réunies :

- $\forall J \in \mathscr{P}_f(I), \quad \sum_{j\in J} a_j \leqslant S$
- $\forall \varepsilon > 0, \exists J \in \mathscr{P}_f(J), \quad S - \varepsilon \leqslant \sum_{j\in J} a_j$

Démonstration. C'est une caractérisation de la borne supérieure. □

Remarque.

Dans le cas $I = \mathbf{N}$ et $(a_i)_{i\in\mathbf{N}}$ positive, la sommabilité équivaut à la convergence de $\sum a_i$. Si la famille est sommable, (S_n) est croissante majorée donc la série converge, et si la série converge, alors les sommes sur un segment sont majorées par la somme de la série.

Proposition.

(H) $(a_i)_{i\in I}$, $(b_i)_{i\in I}$ des familles de réels positifs

(C) 1. Si $0 \leqslant a_i \leqslant b_i$ pour tout $i \in I$ et $(b_i)_i$ est sommable, alors $(a_i)_i$ est sommable et

$$\sum_{i\in I} a_i \leqslant \sum_{i\in I} b_i$$

2. Pour $\lambda \in \mathbf{R}_+$, si $(a_i)_i$ et $(b_i)_i$ sont sommables, $(\lambda a_i + b_i)_i$ aussi et

$$\lambda \sum_{i\in I} a_i + \sum_{i\in I} b_i = \sum_{i\in I}(\lambda a_i + b_i)$$

Démonstration.

1. Ok
2. Pour tout $J \in \mathscr{P}_f(I)$,

$$\sum_{j\in J}(\lambda a_j + b_j) = \lambda \sum_{j\in J} a_j + \sum_{j\in J} b_j \leqslant \lambda \sum_{i\in I} a_i + \sum_{i\in I} b_i \underset{\text{def}}{=} M$$

Soit $\varepsilon > 0$. Il existe $J_1, J_2 \in \mathscr{P}_f(I)$ tels que

$$\sum_{j\in I} a_j - \varepsilon' \leqslant \sum_{j\in J_1} a_j \qquad \text{et} \qquad \sum_{j\in I} b_j - \varepsilon' \leqslant \sum_{j\in J_2} b_j$$

donc pour $J = J_1 \cup J_2$,

$$M - \lambda\varepsilon' - \varepsilon' = M - \varepsilon \leqslant \sum_{j\in J}(\lambda a_j + b_j)$$

donc (C)

□

5 Familles sommables de complexes

Définition – Proposition.

(H) $(a_k)_{k\in I}$ une famille dénombrable de complexes, $\alpha_k = \mathfrak{Re}(a_k)$ et $\beta_k = \mathfrak{Im}(a_k)$

(C) 1. $(a_k)_{k\in I}$ est sommable ssi $(|a_k|)_{k\in I}$ est sommable.

2. Dans ce cas, (α_k^+), (α_k^-), (β_k^+) et (β_k^-) sont sommables [a] et on pose

$$\sum_{i\in I} a_i \underset{\text{def}}{=} \sum_{i\in I} \alpha_i^+ - \sum_{i\in I} \alpha_i^- + i \sum_{i\in I} \beta_i^+ - i \sum_{i\in I} \beta_i^-$$

3. Si $(a_i)_i$ et $(b_i)_i$ sont sommables et $\lambda \in \mathbf{C}$ alors $(\lambda a_i + b_i)_{i\in I}$ est sommable et

$$\lambda \sum_{i\in I} a_i + \sum_{i\in I} b_i = \sum_{i\in I}(\lambda a_i + b_i)$$

a. $u_n^+ = \max(u_n, 0)$, $\quad u_n^- = \max(-u_n, 0)$ pour écrire $u_n = u_n^+ - u_n^-$

Démonstration.

1. Définition
2. $0 \leqslant \alpha_k^\pm \leqslant |\alpha_k| \leqslant |a_k|$ pour la sommabilité
3. L'inégalité triangulaire donne la sommabilité. La linéarité est admise car la démo est lourde.

□

Théorème (Sommation par paquets).

(H) I dénombrable, $(I_n)_{n\in\mathbf{N}}$ une partition de I, $(a_i)_{i\in I} \in \mathbf{C}^I$

(C) Il y a équivalence entre

a. la famille $(a_i)_i$ est sommable

b. Pour tout $n \in \mathbf{N}$, $(a_i)_{i\in I_n}$ est sommable et

$$\sum_{i\in I_n} a_i$$

est le terme général d'une série absolument convergente. Dans ce cas,

$$\sum_{i\in I} a_i = \sum_{n\in\mathbf{N}} \sum_{i\in I_n} a_i$$

Démonstration. La démonstration n'est pas au programme. On la fait dans le cas $(a_i)_i$ réelle positive.

- $(b \implies a)$ On prend J une partie finie de I,

$$I = \bigcup_{n\in\mathbf{N}} I_n$$

donc il existe n_0 tel que

$$J \subset \bigcup_{n\leqslant n_0} I_n$$

On a

$$0 \leqslant \sum_{j\in J} a_j \leqslant \sum_{k=0}^{n_0} \sum k \in I_n a_k \leqslant \sum_{n\in\mathbf{N}} \sum_{k\in I_n} a_k$$

donc $(a_i)_i$ sommable.

- $(a \implies b)$ Pour tout J fini inclus dans I_n, $J \subset I$ donc

$$0 \leqslant \sum_{j\in J} a_j \leqslant \sum_{j\in I} a_j$$

donc $(a_i)_{i\in I_n}$ est sommable. Soit $n_0 \in \mathbf{N}$ et $J_0, \cdots, J_{n_0}$ finis tels que $J_k \subset I_k$. $J = J_0 \cup \cdots \cup J_{n_0}$ est fini et

$$\sum_{j\in J} a_j = \sum_{i\in J_0} a_i + \cdots + \sum_{i\in J_{n_0}} a_i \leqslant \sum_{j\in I} a_j$$

On a alors

$$\sum_{j\in J_0} a_j \leqslant \sum_{i\in I} a_i - \sum_{j\in J_1} a_j - \cdots - \sum_{j\in J_{n_0}} a_j$$

et le membre de droite est indépendant de J_0. On passe à la borne supérieure par rapport à J_0 :

$$\sum_{i\in I_0} a_i = \sup_{\substack{J_0\subset I_0 \\ J_0 \text{ fini}}} \sum_{j\in J_0} a_j \leqslant \sum_{i\in I} a_i - \sum_{j\in J_1} a_j - \cdots - \sum_{j\in J_{n_0}} a_j$$

puis on recommence pour $J_1, \cdots, J_{n_0}$. On obtient ainsi

$$\sum_{i\in I_0} a_i + \cdots + \sum_{i\in I_{n_0}} a_i \leqslant \sum_{j\in I} a_j.$$

Les sommes partielles sont croissantes et majorées donc

$$\sum \left(\sum_{k\in I_n} a_k \right)$$

est absolument convergente (convergente + termes positifs). Puis, $n_0 \to +\infty$ donne

$$\sum_{n=0}^{+\infty} \sum_{k \in I_n} a_k \leqslant \sum_{i \in I} a_i$$

Enfin,

$$\sum_{j \in J} a_j \leqslant \sum_{k=0}^{n_0} \sum_{j \in I_k} a_j \leqslant \sum_{k=0}^{+\infty} \sum_{j \in I_k} a_j$$

puis on passe au sup pour J et on trouve la conclusion.

Pour (a_i) complexe, on utilise la linéarité. □

Corollaire (Fubini discret).

(H) $(a_{n,m})_{(n,m)\in\mathbf{N}^2} \in \mathbf{C}^{\mathbf{N}^2}$

(C) Il y a équivalence entre :

a. $(a_{n,m})_{(n,m)\in\mathbf{N}^2}$ est sommable
b. $\forall n \in \mathbf{N}, (a_{n,m})_{m\in\mathbf{N}}$ est sommable et $\sum_{m\in\mathbf{N}} |a_{n,m}|$ est le terme général d'une série convergente. Dans ce cas,

$$\sum_{(n,m)\in\mathbf{N}^2} a_{n,m} = \sum_{n\in\mathbf{N}} \sum_{m\in\mathbf{N}} a_{n,m} = \sum_{m\in\mathbf{N}} \sum_{n\in\mathbf{N}} a_{n,m}$$

Exemple.

$$\sum_{n \geqslant 2} (\zeta(n) - 1)$$

On a $\zeta(n) - 1 = \sum_{k \geqslant 2} \frac{1}{k^n}$. La famille $\left(\dfrac{1}{k^n}\right)_{n,k\geqslant 2}$ est-elle sommable ?

Pour $k \geqslant 2$, $\left(\frac{1}{k^n}\right)_{n\geqslant 2}$ est sommable (géométrique) et

$$\sum_{n\geqslant 2} \frac{1}{k^n} = \frac{1}{k^2} \frac{1}{1-\frac{1}{k}} = \frac{1}{k(k-1)}$$

est le terme général d'une série convergente, donc la famille est sommable et

$$\sum_{m\geqslant 2} \sum_{n\geqslant 2} \frac{1}{k^n} = \sum_{k\geqslant 2} \frac{1}{k-1} - \frac{1}{k} = 1 = \sum_{n\geqslant 2} \sum_{k\geqslant 2} \frac{1}{k^n} = \sum_{n\geqslant 2} (\zeta(n) - 1)$$

donc

$$\sum_{n\geqslant 2} (\zeta(n) - 1) = 1$$

Remarque.
Une suite réelle est sommable si et seulement si elle est le terme général d'une série absolument convergente. Dans ce cas,

$$\sum_{n\in\mathbf{N}} a_n = \sum_{n=0}^{+\infty} a_n$$

Proposition (Convergence cumulative).

(H) $(a_n)_{n\in\mathbf{N}}$ est une suite complexe

(C) Il y a équivalence entre

a. (a_n) est sommable
b. $\sum a_n$ est absolument convergente
c. $\forall \sigma \in \mathfrak{S}(\mathbf{N}), (a_{\sigma(n)})$ est sommable

Démonstration.

- ($a \iff b$) OK
- ($b \implies c$) Soit $\sigma \in \mathfrak{S}(\mathbf{N})$ et J fini.

$$\sum_{k\in J} |a_{\sigma(k)}| = \sum_{k\in\sigma(J)} |a_k| \leqslant \sum_{k\in\mathbf{N}} |a_k|$$

- ($c \implies a$) $\sigma = \mathrm{id}$

□

Théorème (Produit de Cauchy).

H $(a_p)_{p\in\mathbf{N}}$, $(b_q)_{q\in\mathbf{N}}$ des familles complexes sommables et

$$c_n = \sum_{p+q=n} a_p b_q = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{n} a_{n-k} b_k$$

C 1. $(c_n)_{n\in\mathbf{N}}$ est sommable
2.
$$\sum_{n=0}^{+\infty} c_n = \left(\sum_{p=0}^{+\infty} a_p\right) \cdot \left(\sum_{q=0}^{+\infty} b_q\right)$$

Démonstration. On note

$$I_n = \{(p,q) \in \mathbf{N}^2, \quad p+q=n\}$$

de sorte que (I_n) est une partition de $\mathbf{N}^2$. On note

$$J_n = \{n\} \times \mathbf{N}$$

de sorte que (J_n) est aussi une partition de $\mathbf{N}^2$. La famille $(a_n b_q)_{q\in\mathbf{N}}$ est sommable et

$$\sum_{q\in\mathbf{N}} |a_n b_q| = |a_n| \underbrace{\sum_{q\in\mathbf{N}} |b_q|}_{\text{fixé}}$$

est le terme général d'une série convergente ((a_n) sommable). On a donc $(a_p b_q)_{(p,q)\in\mathbf{N}^2}$ sommable et on somme par paquets sur les I_n :

$$\sum_{(p,q)\in\mathbf{N}^2} a_p b_q = \sum_{n=0}^{+\infty} \sum_{p+q=n} a_p b_q = \sum_{n\in\mathbf{N}} c_n$$

□

Remarque.

On peut généraliser avec

$$\sum_{i_1,\cdots,i_r} a_{1,i_1} \cdots a_{r,i_r} = \sum_{n=0}^{+\infty} \sum_{i_1+\cdots+i_r=n} a_{1,i_1} \cdots a_{r,i_r}$$

6 Exemples

a) Théorème de réarrangement de Steinitz

On note $(a_n)_n$ une suite réelle telle que $\sum a_n$ est semi-convergente. On va montrer que pour tout $\ell \in \overline{\mathbf{R}}$, il existe $\sigma \in \mathfrak{S}(\mathbf{N})$ tel que

$$\sum_{n=0}^{+\infty} a_{\sigma(n)} = \ell$$

On note $a_n = a_n^+ - a_n^-$ donc $\sum a_n^+$ et $\sum a_n^-$ divergent car $\sum a_n$ semi-convergente. On fixe $\alpha \in \mathbf{R}$,

$$I^+ = \{n \in \mathbf{N}, a_n \geqslant 0\} \qquad I^- = \{n \in \mathbf{N}, a_n < 0\}$$

On note $(i_n)_n$ (resp. $(j_n)_n$) la suite croissante de tous les éléments de I^+ (resp. I^-). On note k_1 le plus petit indice $k \geqslant 0$ tel que

$$-\alpha + a_{i_1} + \cdots + a_{i_{k_1}} > 0$$

et ρ_1 le plus petit indice tel que

$$-\alpha + a_{i_1} + \cdots + a_{i_{k_1}} + a_{j_1} + \cdots + a_{j_{\rho_1}} < 0$$

On itère le processus pour construire $\sigma = (i_1, \cdots, i_{k_1}, j_1, \cdots j_{\rho_1}, i_{k_1+1}, \cdots, i_{k_2}, \cdots) \in \mathfrak{S}(n)$ (c'est bijectif car $I^+ \sqcup I^- = \mathbf{N}$).

Puis,

$$\left| -\alpha + \sum_{k=0}^{n} a_{\sigma(k)} \right| \leqslant |a_{p_n}| + |a_{q_n}| \xrightarrow[n \to +\infty]{} 0$$

avec p_n le plus grand entier tel que $\rho_{p_n} \leqslant \sigma(n)$ et q_n le plus petit entier tel que $\sigma(n) \leqslant \rho_{q_n}$ Pour $\ell = \pm\infty$ c'est le même principe.

b) Inégalité de Carleman

On suppose que $\sum a_n$ converge pour (a_n) positive. On va montrer que

$$\sum_{k=1}^{+\infty} (a_1 \cdots a_k)^{\frac{1}{k}} \leqslant e \sum_{k=1}^{+\infty} a_n$$

On note $(c_n)_n$ une suite à préciser.

$$(a_1 \cdots a_n)^{\frac{1}{n}} = (c_1 a_1 \cdots c_n a_n)^{\frac{1}{n}} \cdot (c_1 \cdots c_n)^{-\frac{1}{n}}$$

On va prendre $c_k = \dfrac{(k+1)^k}{k^{k-1}}$ de sorte que $(c_1 \cdots c_n)^{\frac{1}{n}} = n+1$. On a alors

$$\begin{aligned} (a_1 \cdots a_n)^{\frac{1}{n}} &\leqslant \frac{1}{n(n+1)} \sum_{k=1}^{n} c_k a_k && \text{(AM-GM)} \\ &\leqslant \frac{e}{n(n+1)} \sum_{k=1}^{n} k a_k = \sum_{k=1}^{n} \frac{e k a_k}{n(n+1)} \end{aligned}$$

car $c_k = k\left(1 + \frac{1}{k}\right)^k \leqslant ek$. On pose

$$u_{k,n} \underset{\text{def}}{=} \begin{cases} \dfrac{eka_k}{n(n+1)} & \text{si } k \leqslant n \\ 0 & \text{sinon} \end{cases}$$

Pour $k \in \mathbf{N}^\star$,

$$\sum_{n=1}^{+\infty} u_{k,n} = \sum_{n=k}^{+\infty} \frac{eka_k}{n(n+1)} = eka_k \sum_{n=k}^{+\infty} \left(\frac{1}{k} - \frac{1}{k+1} \right) = ea_k$$

qui est le tg d'une série convergente, donc $(u_{k,n})_{k,n}$ est sommable, puis (Fubini)

$$\sum (a_1 \cdots a_n)^{\frac{1}{n}} \text{ CV}$$

et

$$\sum_{n=1}^{+\infty} (a_1 \cdots a_n)^{\frac{1}{n}} \leqslant \sum_{k=1}^{+\infty} \sum_{n=1}^{+\infty} u_{k,n} = e \sum_{k=1}^{+\infty} a_k$$

Remarque.

La constante e est optimale.

Pour le voir, on pose

$$a_k = \begin{cases} \frac{1}{k} & \text{si } k \leqslant n \\ 0 & \text{sinon} \end{cases}$$

et c une autre constante qui convient.

$$\sum_{k=1}^{n} (a_1 \cdots a_k)^{\frac{1}{k}} = \sum_{k=1}^{n} \left(\frac{1}{k!}\right)^{\frac{1}{k}} \leqslant c \sum_{k=1}^{n} \frac{1}{k}$$

et

$$\left(\frac{1}{k!}\right)^{\frac{1}{k}} = \exp\left(-\frac{1}{k}\sum_{i=1}^{k} \ln i\right)$$

avec

$$\ln i \sim i \ln i - (i-1)\ln(i-1) \implies \sum_{i=1}^{k} \ln i \sim k \ln k$$

Puis on pose $u_k = \displaystyle\sum_{i=1}^{k} \ln i - k \ln k$ de sorte que

$$u_{k+1} - u_k = \ln(k+1) - (k+1)\ln(k+1) + k \ln k \sim -1$$

C'est le terme général d'une série divergente (signe constant APCR) donc $u_k \sim -k$ et

$$-\frac{1}{k}\sum_{i=1}^{k} \ln i = -\ln k + 1 + o(1)$$

donc

$$\left(\frac{1}{k!}\right)^{\frac{1}{k}} \sim \frac{e}{k}.$$

C'est le terme général d'une série divergente donc

$$\sum_{k=1}^{n} (a_1 \cdots a_k)^{\frac{1}{k}} \sim e \sum_{k=1}^{n} \frac{1}{k} \sim e \ln n$$

donc $e \leqslant C$

7 Produits infinis

Soit (a_n) une suite numérique et

$$p_n = \prod_{k=0}^{n} (1 + a_k)$$

On dira que le produit $\prod(1 + a_k)$ converge si et seulement si p_n a une limite réelle **non nulle**

Résultat.

Si $\sum a_k$ est absolument convergente et (a_n) ne vaut jamais -1, alors $\prod(1 + a_k)$ converge

Démonstration. On le montre dans le cas réel. On a $a_n \longrightarrow 0$ donc à partir d'un certain rang n_0, $(1 + a_n)$ est strictement positive. Pour $N > n_0$,

$$p_n = \underbrace{\prod_{k=0}^{n_0} (1 + a_k)}_{\text{fixe } \neq 0} \times \prod_{k=n+1}^{N} \underbrace{(1 + a_k)}_{>0}$$

Or pour $k \geqslant n_0$, $|\ln(1+a_k)| \sim |a_k|$ donc $\sum \ln(1+a_k)$ ACV et sa somme vaut $\ell \in \mathbf{R}$. On a alors

$$p_n = e^{\ln p_n} \xrightarrow[n\to+\infty]{} e^{\ell} \prod_{k=0}^{n_0}(1+a_k) \neq 0$$

□

Remarque.

Le resultat est vrai avec une suite complexe.

Exemple. On note $f : \mathbf{N}^{\star} \longrightarrow \mathbf{R}_+$ complètement multiplicative [1] (le résultat que l'on va montrer est toujours vrai pour f multiplicative [2])

On suppose que $\sum f(n)$ est absolument convergente. On va montrer que

$$\prod_{p \text{ premier}} \frac{1}{1-f(p)} = \sum_{n=1}^{+\infty} f(n)$$

On note $(p_i)_i$ la suite croissante des nombres premiers. Si il existe un premier p tel que $f(p) = 1$ alors $f(p^n) = 1$ et $f(n) \not\to 0$ ce qui est absurde, donc pour tout p premier, $f(p) \neq 1$. On a alors $\sum f(p_i)$ ACV donc et $f(p_i) \neq 1$ donc $\prod(1-f(p_i))$ converge donc $\prod \frac{1}{1-f(p_i)}$ aussi. Puis,

$$P_N = \prod_{i=1}^{N} \frac{1}{1-f(p_i)} = \prod_{i=1}^{N}\sum_{k=0}^{+\infty} f(p_i)^k \underset{\Pi \text{ de Cauchy}}{=} \sum_{k_1,\cdots,k_N} f(p_1^{k_1}\cdots p_N^{k_N})$$

d'où

$$\sum_{n=0}^{M_N} f(n) \leqslant P_N \leqslant \sum_{n=0}^{+\infty} f(n)$$

avec $M_N = \max\{k, \quad [\![1,k]\!] \text{ se décompose avec } p_1,\cdots p_N\}$. Puis, $N \to +\infty$ donne le résultat.

Avec $s > 1$ et $f : n \longmapsto \frac{1}{n^s}$, on trouve l'identité d'Euler :

$$\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}} = \zeta(s)$$

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

1. $\forall x, y, f(xy) = f(x)f(y)$
2. $\forall x, y, x \wedge y = 1 \implies f(xy) = f(x)f(y)$

Chapitre IV

Intégration sur un intervalle quelconque

Sommaire

1 Rappels

L'opération d'intégration sur $\mathscr{C}^0_{PM}([a,b],\mathbf{R})$ est linéaire positive croissante. On a

$$\left|\int_a^b f\right| \leqslant \int_a^b |f| \leqslant (b-a)\sup_{[a,b]}|f|$$

et similairement

$$\left|\int_a^b fg\right| \leqslant \sup_{[a,b]}|f| \int_a^b |g|$$

Si f est continue alors
$$\left|\int_a^b f\right| = \int_a^b |f| \iff f \text{ de signe constant}$$
et si g est continue positive,
$$\inf_{[a,b]} f \int_a^b g \leqslant \int_a^b fg \leqslant \sup_{[a,b]} f \int_a^b g$$
et si g n'est pas identiquement nulle,
$$\int_a^b g > 0 \implies \frac{\int_a^b fg}{\int_a^b g} \in [\inf f, \sup f] = f([a,b]) \implies \exists c, \quad \int_a^b fg = f(c)\int_a^b g.$$
Le résultat reste vrai si g est identiquement nulle. Si f est continue positive sur $[a,b]$ et $\int_a^b f = 0$ alors $f = 0$. Si f et g sont de classe $\mathscr{C}^1$ alors
$$\int_a^b fg' = [fg]_a^b - \int_a^b f'g$$
et si $\varphi : [\alpha,\beta] \to [a,b]$ est $\mathscr{C}^1$, f continue sur $\varphi([\alpha,\beta])$ alors
$$\int_{\varphi(\alpha)}^{\varphi(\beta)} f(u)\,\mathrm{d}u = \int_\alpha^\beta f(\varphi(t))\varphi'(t)\,\mathrm{d}t$$
Si f est continue par morceaux sur $[a,b]$ alors
$$\frac{1}{b-a}\sum_{k=0}^{n-1} f\left(a + k\frac{b-a}{n}\right) \xrightarrow[n\to+\infty]{} \int_a^b f$$

Théorème (Taylor avec reste intégral).

(H) f de classe $\mathscr{C}^n$ sur $[a,b]$

(C)
$$f(b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\,\mathrm{d}t$$

Démonstration. Vu en sup. □

Remarque.

On peut échanger a et b dans la formule.

Exemple (Irrationnalité de $\cos 1$). Supposons $\cos 1 = \frac{p}{q} \in \mathbf{Q}$ de sorte que
$$\cos 1 = \sum_{k=0}^{q} \frac{\cos^{(k)}(0)}{k!} + \int_0^1 \frac{(1-t)^q}{q!}\cos^{(q+1)}(t)\,\mathrm{d}t \implies 0 \leqslant \underbrace{q!\left|\cos 1 - \sum_{k=0}^{q}\frac{\cos^{(k)}(0)}{k!}\right|}_{\in\mathbf{N}} = \left|\int_0^1 (1-t)^q \cos^{(q+1)}(t)\,\mathrm{d}t\right| < 1$$
donc
$$\cos 1 = \sum_{k=0}^{q} \frac{\cos^{(k)}(0)}{k!}$$
d'où
$$\int_a^b \underbrace{(1-t)^q\cos^{(q+1)}(t)}_{\mathscr{C}^0 \text{ de signe constant}}\,\mathrm{d}t = 0 \implies (1-t)^q\cos^{(q+1)}(t) \equiv 0$$
ce qui est aburde.

2 Intégrales de Wallis

On appelle intégrales de Wallis les intégrales

$$W_n \underset{\text{def}}{=} \int_0^{\frac{\pi}{2}} \cos^n \underset{u=\frac{\pi}{2}-t}{=} \int_0^{\frac{\pi}{2}} \sin^n$$

On a

$$W_0 = \frac{\pi}{2} \qquad\qquad W_1 = [\sin t]_0^{\frac{\pi}{2}} = 1$$

Pour $n \geqslant 2$,

$$W_n = \int_0^{\frac{\pi}{2}} \cos\cdot\cos^{n-1} = [\sin\cos^{n-1}]_0^{\frac{\pi}{2}} + \int_0^{\frac{\pi}{2}} \underbrace{\sin^2}_{1-\cos^2}\cdot(n-1)\cos^{n-2} = (n-1)W_{n-2} - (n-1)W_n$$

donc

$$W_n = \frac{n-1}{n}W_{n-2}$$

de sorte que

$$W_{2p} = \frac{(2p)!}{2^{2p}(p!)^2}\frac{\pi}{2} \qquad\qquad W_{2p+1} = \frac{2^{2p}p!^2}{(2p+1)!}.$$

Pour $t \in [0, \frac{\pi}{2}]$, on a $\cos^{n+1} t \leqslant \cos^n t$ donc $W_{n+1} \leqslant W_n$. Puis

$$W_{n+2} = \frac{n+1}{n+1}W_n \leqslant W_{n+1} \leqslant W_n \implies \frac{W_{n+1}}{W_n} \xrightarrow[n\to+\infty]{} W_{n+1} \sim W_n.$$

La suite $((n+1)W_nW_{n+1})_n$ est constante égale à $W_0W_1 = W_0$ donc

$$\frac{\pi}{2}(n+1)W_{n+1}W_n \sim nW_n^2 \implies W_n \sim \sqrt{\frac{\pi}{2n}}$$

or

$$W_{2p} \sim \frac{C\sqrt{2p}(2p)^{2p}e^{-2p}}{2^{2p}C^2(\sqrt{p}p^pe^{-p})^2}\frac{\pi}{2} \sim \frac{\sqrt{2}}{C\sqrt{p}}\sqrt{\frac{\pi}{2}} \underset{\text{aussi}}{\sim} \sqrt{\frac{\pi}{4p}}$$

donc

$$C = \sqrt{2\pi}$$

3 Fonctions continues par morceaux

Définition (Rappel).

$f : [a,b] \longrightarrow \mathbf{R}$ (ou $\mathbf{C}$) est dite continue par morceaux s'il existe une subdivision finie $\sigma = (a_1, \cdots, a_n)$ ($a_1 = a$, $a_n = b$) de $[a,b]$ telle que f est continue sur $]a_n, a_{n+1}[$, et admet une limite à droite et à gauche (ou d'un seul côté aux bords de l'intervalle) en chacun des points de la subdivision.
L'ensemble de ces fonction est noté $\mathscr{C}^0_{PM}([a,b],\mathbf{R})$

Définition.

Si I est un intervalle non trivial de $\mathbf{R}$, on dira que f est continue par morceaux sur I si f est continue par morceaux sur tous segments inclus dans I.

Exemple. La partie entière est $\mathscr{C}^0_{PM}$ sur $\mathbf{R}$. L'application

$$x \longmapsto \left\lfloor \frac{1}{x} \right\rfloor$$

est $\mathscr{C}^0_{PM}$ sur $]0,1]$

Proposition.

(H) I est un intervalle réel non trivial, $f, g \in \mathscr{C}^0_{PM}(I,\mathbf{R})$

(C)
1. Pour tout $\lambda \in \mathbf{R}$ (ou $\mathbf{C}$), $\lambda f + g \in \mathscr{C}^0_{PM}(I,\mathbf{R})$
2. fg est $\mathscr{C}^0_{PM}$
3. $|f|$ est $\mathscr{C}^0_{PM}$. En particulier, $\max(f,g)$ et $\min(f,g)$ aussi

Démonstration. On se ramène à un segment de I et c'est vu en sup.

$$\max(f, g) = \frac{f + g + |f - g|}{2}$$

□

Théorème (Rappel).

(H) f continue sur $[a, b]$

(C) 1. On note $E(I, \mathbf{R})$ l'ensemble des fonctions en escaliers de I dans $\mathbf{R}$.

$$\forall \varepsilon > 0, \exists \varphi \in E([a, b], \mathbf{R}), \quad \sup_{[a,b]} |f - \varphi| \leqslant \varepsilon$$

2.

$$\exists (\varphi_n)_n \in E([a, b] \in \mathbf{R})^{\mathbf{R}}, \forall n \in \mathbf{N}^\star, \quad \sup_{[a,b]} |f - \varphi_n| \leqslant \frac{1}{n}$$

Idée de la preuve. f est uniformément continue (Heine) donc avec une subdivision régulière assez petite on a bien l'approximation. □

4 Intégration sur un intervalle quelconque

On note I un intervalle non trivial de $\mathbf{R}$ et $f \in \mathscr{C}^0_{PM}(I, \mathbf{R})$.

Définition.

1. Si $I = [a, b[$ avec $b \in \mathbf{R} \cup \{+\infty\}$, alors

$$\int_I f = \int_a^b f \underset{\text{def}}{=} \lim_{x \to b} \int_a^x f$$

lorsque cette limite existe (on dira alors que l'intégrale est convergente).

2. Si $I =]a, b[$ alors de même, lorsque la limite existe on définit

$$\int_I f = \int_a^b f \underset{\text{def}}{=} \lim_{x \to a} \lim_{y \to b} \int_x^y f$$

On peut inverser les deux limites car pour $c \in I$,

$$\int_x^y f = \int_x^c f + \int_c^y f$$

3. Lorsque

$$\int_I |f|$$

converge, on dit que f est intégrable sur I. Si f n'est pas intégrable, on dira que $\displaystyle\int_I f$ est semi-convergente si elle converge.

Exemple. L'application $t \longmapsto e^{-t}$ est $\mathscr{C}^0_{PM}$ sur $\mathbf{R}_+$ et

$$\int_0^x e^{-t} \,\mathrm{d}t = 1 - e^x \xrightarrow[x \to +\infty]{} 1 \implies \int_0^{+\infty} e^{-t} \,\mathrm{d}t = 1$$

a) Lien avec les primitives

Si f est continue sur $[a, b[$ et F est une primitive de f, alors pour $x \in [a, b[$,

$$\int_a^x f = F(x) - F(a)$$

donc $\int_a^b f$ CV $\iff$ F a une limite finie en b.

Exemple.

$$\int_0^1 \frac{\mathrm{d}t}{t^\alpha} \text{ CV} \iff t \longmapsto \begin{cases} \dfrac{t^{-\alpha+1}}{1-\alpha} & \text{si } \alpha \neq 1 \\ \ln|t| & \text{sinon} \end{cases} \quad \text{a une limite finie en } 0^+ \iff \alpha < 1$$

$$\int_1^{+\infty} \frac{\mathrm{d}t}{t^\alpha} \text{ CV} \iff \alpha > 1$$

5 Propriétés algébriques

Proposition.

(H) $f, g \in \mathscr{C}^0_{PM}(I, \mathbf{C})$ telles que $\int_I f$ et $\int_I g$ convergent

(C) 1.

$$\forall \lambda \in \mathbf{C}, \quad \int_I (\lambda f + g) \text{ CV et } \int_I (\lambda f + g) = \lambda \int_I f + \int_I g$$

2. Si $f \geqslant 0$ alors

$$\int_I f \geqslant 0$$

et si $f \leqslant g$ alors

$$\int_I f \leqslant \int_I g$$

3. Si f est intégrable sur I alors

$$\left| \int_I f \right| \leqslant \int_I |f|$$

Démonstration.

1. 2. On l'écrit sur un segment dans I puis on passe à la limite
3. Dans le cas réel,

$$\pm \int_I f \leqslant \int_I |f|.$$

Si f est à valeurs complexes, le cas $\int_I f = 0$ est immédiat et sinon il existe $\theta \in \mathbf{R}$ tel que

$$e^{-i\theta} \int_I f > 0$$

et

$$\left| \int_I f \right| = e^{-i\theta} \int_I f = \int_I e^{-i\theta} f = \mathfrak{Re}\left(\int_I e^{-i\theta} \right) = \int_I \mathfrak{Re}(e^{-i\theta} f) \leqslant \int_I |e^{-i\theta} f| = \int_I |f|$$

□

Proposition.

(H) $f \in \mathscr{C}^0_{PM}(I, \mathscr{C}), c \in I$ et $\int_I f$ convergente

(C) 1. Les intégrales

$$\int_{I \cap [c, +\infty[} f \qquad \text{et} \qquad \int_{I \cap]-\infty, c]} f$$

sont convergentes

2. On a l'égalité

$$\int_I f = \int_{I \cap [c, +\infty[} f + \int_{I \cap]-\infty, c]} f$$

Démonstration. Si $I = [a, b[$, alors $I \cap [c, +\infty[= [c, b[$ et

$$\int_a^x f - \int_a^c f = \int_c^x f \implies \int_c^b f \qquad \text{CV}$$

On fait pareil pour les autres configurations. □

Remarque.

Si $f \in \mathscr{C}^0([a, b[, \mathbf{C})$ et

$$\varphi : x \in [a, b[\longmapsto \int_x^c f$$

alors pour $c \in [a, b[$,

$$\varphi(x) = \int_x^c f + \int_c^b f$$

donc φ dérivable et

$$\varphi'(x) = -f(x)$$

6 Utilisation de la positivité

Proposition.

(H) $f \in \mathscr{C}^0_{PM}(I, \mathbf{R}), f \geqslant 0$ sur I

(C)
1. f est intégrable sur I si et seulement s'il existe $M \geqslant 0$ tel que

$$\forall x, y \in I, \qquad x \leqslant y \implies \int_x^y f \leqslant M$$

soit encore, de manière équivalente,

$$\forall J \subset I, J \text{ segment}, \qquad \int_J f \leqslant M$$

Et dans ce cas

$$\int_I f = \sup \left\{ \int_J f, \quad J \subset I, J \text{ segment} \right\}$$

2. Si $0 \leqslant f \leqslant g$ et g intégrable sur I alors f est aussi intégrable
3. Si $I = [a, b[$, $f = O_b(g)$ et g intégrable au voisinage de b alors f est intégrable sur I.

Démonstration.

1. ($\implies$) Pour $I = [a, b[$ et $a \leqslant x \leqslant y < b$,

$$\int_x^y f \leqslant \int_x^y f + \int_a^x f = \int_a^y f \xrightarrow[y \to b]{} \int_a^b f \underset{\text{def}}{=} M.$$

($\impliedby$)

$$\int_a^y f \leqslant M \implies \lim_{y \to b} \int_a^y f = \int_I f \quad \text{existe (fonction croissante majorée)}$$

donc f est intégrable sur I. On a clairement

$$\underbrace{\sup \left\{ \int_I f, \quad J \subset I, J \text{ segment} \right\}}_{\underset{\text{def}}{=} \mathscr{E}} \leqslant \int_I f$$

puis

$$\int_a^{b - \frac{1}{n}} f \xrightarrow[n \to +\infty]{} \int_I f$$

donc
$$\sup \mathscr{E} = \int_I f$$

2. Pour tout J segment de I,
$$\int_J f \leqslant \int_J g \leqslant \int_I g$$
donc en passant à la borne supérieure on optient l'intégrabilité.
3. Il existe $C > 0$ et $c \in I$ tels que
$$\forall x \in [c, b[, \qquad 0 \leqslant f(x) \leqslant C \underbrace{|g(x)|}_{\text{intégrable}}$$
donc f est intégrable sur $[c, b[$ et $\mathscr{C}^0_{PM}$ sur $[a, c]$ donc intégrable sur I.

□

Remarque.

Dans le cas général, si $f = u + iv$ intégrable avec u, v des fonctions à valeurs réelles alors u et v sont intégrables car
$$|u| \leqslant |\mathfrak{Re}(f)| \leqslant |f| \qquad \text{et} \qquad |v| \leqslant |\mathfrak{Im}(f)| \leqslant |f|$$

Exercice.

Donner la nature de
$$\int_0^{+\infty} \frac{1 + \cos t}{1 + t^2} \,\mathrm{d}t$$

Résolution. L'application est continue sur l'intervalle d'intégration et intégrable en $+\infty$ en tant que $O(\frac{1}{t^2})$, donc l'intervalle converge absolument. □

Exercice.

Donner la nature de
$$\int_0^1 \frac{\mathrm{d}t}{\sin \sqrt{t}}$$

7 Absolue convergence et semi-convergence

Proposition.

(H) $f \in \mathscr{C}^0_{PM}(I, \mathbf{C})$

(C) Si $\displaystyle\int_I f$ est absolument convergente (ou f est intégrable sur I), alors $\displaystyle\int_I f$ converge

Démonstration. Si f est réelle, on a $f = f^+ - f^-$ avec $f^+ = \max(f, 0)$ et $f^- = \max(-f, 0)$, de sorte qu'il suffit d'avoir la convergence de $\displaystyle\int_I f^\pm$, qui est donnée par
$$0 \leqslant f^\pm \leqslant |f|$$
Si f est à valeurs complexes, on écrit $f = u^+ - u^- + i(v^+ - v^-)$ et on fait pareil. □

Exercice.

Donner la nature de
$$\int_0^{+\infty} \frac{\sin t}{1 + t^2} \,\mathrm{d}t$$

Résolution. L'application
$$f : t \in \mathbf{R}_+ \longmapsto \frac{\sin t}{1 + t^2}$$
est continue et
$$\forall t \geqslant 1, \qquad |f(t)| \leqslant \frac{1}{t^2} \text{ intégrable en } +\infty$$

donc f est intégrable sur $[1, +\infty[$ et f est continue par morceaux sur $[0, 1]$ donc l'intégrale est absolument convergente donc convergente. □

Exercice.

Donner la nature de

$$\int_0^{+\infty} \frac{\sin t}{t\sqrt{t}} \, \mathrm{d}t$$

Résolution.

- $\left|\dfrac{\sin t}{t\sqrt{t}}\right| = O_0\left(\dfrac{1}{\sqrt{t}}\right)$ intégrable en 0
- $\left|\dfrac{\sin t}{t\sqrt{t}}\right| = O_{+\infty}\left(\dfrac{1}{t\sqrt{t}}\right)$ intégrable en $+\infty$

donc l'intégrale est absolument convergente. □

Exercice.

Donner la nature de

$$\int_0^{+\infty} \frac{\sin t}{t} \, \mathrm{d}t$$

Résolution. L'application

$$\varphi : t \longmapsto \frac{\sin t}{t}$$

est continue (avec un prolongement en 0) sur $\mathbf{R}_+$ et

$$\int_1^x \varphi = \left[-\frac{\cos t}{t}\right]_1^x + \int_1^x \frac{\cos t}{t^2} \, \mathrm{d}t \xrightarrow[x \to +\infty]{} \cos(1) + \int_1^{+\infty} \frac{\cos t}{t^2} \, \mathrm{d}t$$

et cette dernière intégrale converge absolument. L'intégrale

$$\int_0^{+\infty} \varphi$$

est donc convergente. On va montrer qu'elle n'est pas absolument convergente. On a

$$\forall t \geqslant 0, \qquad |\varphi(t)| = \frac{|\sin t|}{t} \geqslant \frac{\sin^2 t}{t} = \frac{1 - \cos(2t)}{2t}$$

donc

$$\int_1^x |\varphi| \geqslant \int_1^x \frac{\mathrm{d}t}{2t} - \underbrace{\int_1^x \frac{\cos(2t)}{2t} \, \mathrm{d}t}_{\text{limite finite}} \xrightarrow[x \to +\infty]{} +\infty$$

donc l'intégrale est semi-convergente. □

8 Intégration des relations de comparaison

Théorème.

(H) $f, g \in \mathscr{C}^0_{PM}([a, b[, \mathbf{R}_+)$ des fonctions positives, g intégrable sur $[a, b[$

(C)
1. Si $f = O_b(g)$ alors
$$\int_x^b f = O_b\left(\int_x^b g\right)$$
2. Si $f = o_b(g)$ alors
$$\int_x^b f = o_b\left(\int_x^b g\right)$$
3. Si $f \underset{b}{\sim} (g)$ alors
$$\int_x^b f \underset{b}{\sim} \int_x^b g$$

Démonstration.

1. Il existe $M > 0$ et un $c \in [a, b[$ tel que

$$\forall t \in [c, b[, \qquad f(t) \leqslant Mg(t) \implies \forall x \in [c, b[, \qquad \int_x^b f \leqslant M \int_x^b g$$

2. Soit $\varepsilon > 0$. Il existe $c \in [a, b[$ tel que sur $[c, b[$, $f \leqslant \varepsilon g$ donc

$$\forall x \in [c, b[, \qquad \int_x^b f \leqslant \varepsilon \int_x^b g$$

3. $f \underset{b}{\sim} g \iff f - g = o_b(g)$ donc

$$\int_x^b (f-g) = O_b\left(\int_x^b |f-g|\right) = O_b\left(o_b\left(\int_x^b g\right)\right) = o_b\left(\int_x^b g\right) \implies \int_x^b f \sim \int_x^b g$$

□

Remarque.

Si f est de signe quelconque, alors

$$f = O_b(g) \iff |f| = O_b(g) \implies \int_x^b f = O_b\left(\int_x^b |f|\right) = O_b\left(\int_x^b g\right)$$

donc le signe de f n'est pas important.

Théorème.

(H) $f, g \in \mathscr{C}^0_{PM}([a, b[, \mathbf{R})$ positives

(C)
1. Si f est non intégrable et $f = O_b(g)$ alors g n'est pas intégrable et

$$\int_a^x f = O_b\left(\int_a^x g\right)$$

2. Si f est non intégrable et $f = o_b(g)$ alors g n'est pas intégrable et

$$\int_a^x f = o_b\left(\int_a^x g\right)$$

3. Si f est non intégrable et $f \underset{b}{\sim} g$ alors g n'est pas intégrable et

$$\int_a^x f \underset{b}{\sim} \int_a^x g$$

Démonstration. Dans les trois cas il existe $C > 0$ et $c \in [a, b[$ tels que

$$\forall x \in [c, b[, \qquad 0 \leqslant f(x) \leqslant Cg(x)$$

donc

$$\forall x \geqslant c, \qquad \int_a^x f = \underbrace{\int_a^x f + \int_c^x f}_{\xrightarrow[x\to b]{} +\infty} \leqslant C \int_c^x g + \int_a^c f$$

donc

$$\int_c^x g \xrightarrow[x\to b]{} +\infty$$

et g n'est pas intégrable.

On montre le point 2. (les points 1. et 3. se traitant similairement). Soit $\varepsilon > 0$. Il existe $c \in [a, b[$ tel que

$$\forall x \in [c, b[, \qquad 0 \leqslant f(x) \leqslant \varepsilon' g(x) \underset{\text{def}}{=} \frac{\varepsilon}{2} g(x) \implies \int_c^x f \leqslant \varepsilon' \int_c^x g \implies \int_a^x f \leqslant \varepsilon' \underbrace{\int_a^x g}_{\xrightarrow[x \to b]{} +\infty} + \int_a^c f - \varepsilon' \int_a^c g$$

donc pour x assez grand,

$$0 \leqslant \frac{\displaystyle\int_a^x f}{\displaystyle\int_a^x g} \leqslant \varepsilon' + \frac{\displaystyle\int_a^c f - \varepsilon' \int_a^c g}{\displaystyle\int_a^x g} \underset{x \text{assez grand}}{\leqslant} 2\varepsilon' = \varepsilon$$

d'où C □

Exemple. On veut déterminer un équivalent de $\displaystyle\int_x^{+\infty} e^{-t^2}\,\mathrm{d}t$. On écrit

$$\int_x^{+\infty} e^{-t^2}\,\mathrm{d}t = \int_x^{+\infty} \frac{1}{2t}(2te^{-t^2})\,\mathrm{d}t \underset{\text{IPP}}{=} \frac{e^{-x^2}}{2x} - \int_x^{+\infty} \frac{e^{-t^2}}{2t^2}\,\mathrm{d}t$$

de sorte que

$$\int_x^{+\infty} e^{-t^2}\,\mathrm{d}t + \int_x^{+\infty} \frac{e^{-t^2}}{2t^2}\,\mathrm{d}t = \frac{e^{-x^2}}{2x}$$

or

$$\frac{e^{-t^2}}{2t^2} = o_{+\infty}(e^{-t^2}) \implies \int_x^{+\infty} \frac{e^{-t^2}}{2t^2}\,\mathrm{d}t = o_{+\infty}\left(\int_x^{+\infty} e^{-t^2}\,\mathrm{d}t\right)$$

donc

$$\int_x^{+\infty} e^{-t^2}\,\mathrm{d}t \underset{+\infty}{\sim} \frac{e^{-x^2}}{2x}$$

9 Propriétés héritées

Proposition.

1. Si $f \in \mathscr{C}^0(I, \mathbf{R}_+)$ et $\int_I f = 0$ alors $f \equiv 0$ sur I.
2. Soit $f \in \mathscr{C}^0(]a, b[, \mathbf{C})$ et φ de classe $\mathscr{C}^1$ bijective croissante de $]\alpha, \beta[$ dans $]a, b[$.
   (a) $\int_a^b f$ et $\int_\alpha^\beta f \circ \varphi \times \varphi'$ ont même nature (CV, ACV, DV)
   (b) En cas de convergence, ces intégrales sont égales
3. Soit f, g de classe $\mathscr{C}^1$ sur $]a, b[$ à valeurs complexes. On a

$$\int_a^b f'g = [fg]_a^b - \int_a^b fg'$$

à condition que deux des trois termes convergent.

Démonstration.

1. Pour J segment de I, c'est vrai. On passe à la limite.
2. Sur les semgents c'est vrai, on passe à la limite.
3. Si deux des trois termes convergent, le troisième aussi

□

10 Méthodes pour établir l'intégrabilité

a) Intégrabilité de $x \longmapsto x^a(1-\exp(-1/\sqrt{x}))$ sur $\mathbf{R}_+$

On cherche la nature de

$$\int_0^{+\infty} x^a(1-e^{-\frac{1}{\sqrt{x}}})\,\mathrm{d}x$$

La fonction

$$f : x \longmapsto x^a(1-e^{-\frac{1}{\sqrt{x}}})$$

est continue sur $\mathbf{R}_+^\star$ et

$$f(x) \underset{0^+}{\sim} x^a = \frac{1}{x^{-a}}$$

donc f est intégrable en 0 ssi $a > -1$. Puis,

$$f(x) \underset{+\infty}{\sim} \frac{x^a}{\sqrt{x}}$$

donc f est intégrable en $+\infty$ ssi $a < -\frac{1}{2}$.

L'intégrale est donc absolument convergente ($\iff$ convergente vu la positivité) ssi $-1 < a < -\frac{1}{2}$

b) Intégrales de Bertrand

On cherche la nature de

$$\int_0^{\frac{1}{e}} \frac{1}{x^\alpha |\ln x|^\beta}\,\mathrm{d}x$$

On note

$$f : t \longmapsto \frac{1}{x^\alpha |\ln x|^\beta} \in \mathscr{C}^0(]0,\frac{1}{e}],\mathbf{R})$$

- Si $\alpha < 0$ alors on peut prolonger par continuité en 0, la fonction est intégrable
- Si $0 \leqslant \alpha < 1$ alors
$$\frac{t^{\frac{1+\alpha}{2}}}{t^\alpha |\ln t|^\beta} = \frac{t^{\frac{t-\alpha}{2}}}{|\ln t|^\beta} \xrightarrow[t\to 0^+]{} 0 \implies f(t) = o_{0^+}\left(\frac{1}{t^{\frac{1+\alpha}{2}}}\right)$$
et $\frac{1+\alpha}{2} < 1$ donc f est intégrable.
- Si $\alpha \geqslant 1$ alors
$$\int_x^{\frac{1}{e}} f = \int_{-\ln x}^{-\ln\frac{1}{e}} \frac{-e^{-u}}{(e^{-u})^\alpha u^\beta}\,\mathrm{d}t = \int_{-\ln\frac{1}{e}}^{-\ln x} \frac{e^{(\alpha-1)u}}{u^\beta}\,\mathrm{d}t$$
Si $\alpha > 1$ alors $\dfrac{e^{(\alpha-1)u}}{u^\beta} \xrightarrow[u\to+\infty]{} +\infty$ donc on n'a pas l'intégrabilité Si $\alpha = 1$ alors on a l'intégrabilité ssi $\beta > 1$.

Exercice.

> Montrer que
> $$\int_e^{+\infty} \frac{\mathrm{d}t}{t^\alpha|\ln t|^\beta} \quad \text{CV} \iff (\alpha > 1) \text{ ou } (\alpha = 1 \text{ et } \beta > 1)$$

c) Nature d'une intégrale

On va déterminer la nature de

$$\int_0^1 \frac{1-\cos t}{t^\alpha\sqrt{\sin t}}\,\mathrm{d}t$$

L'intégrande est continue sur $]0,1]$ et en 0,

$$\frac{1-\cos t}{t^\alpha\sqrt{\sin t}} \underset{0}{\sim} \frac{t^2}{t^{\alpha-\frac{1}{2}}}$$

donc l'intégrale converge ssi $\alpha < \dfrac{5}{2}$

d) Calcul de $\int_0^{+\infty} \frac{\sin t}{t} \, \mathrm{d}t$

Résultat (Lemme de Riemann-Lebesgue).

Si $f \in \mathscr{C}^0([a,b] \in \mathbf{C})$ alors

$$\int_a^b f(t)e^{int} \, \mathrm{d}t \xrightarrow[n\to+\infty]{} 0$$

Démonstration. Le cas où f est $\mathscr{C}^1$ est plus facile à montrer :

$$\int_a^b f(t)e^{int} \, \mathrm{d}t \underset{\text{IPP}}{=} \underbrace{\frac{f(b)e^{inb} - f(a)e^{ina}}{in}}_{\xrightarrow[n\to+\infty]{} 0} - \underbrace{\frac{1}{in} \int_a^b f'(t)e^{int} \, \mathrm{d}t}_{\xrightarrow[n\to+\infty]{} 0}$$

Dans le cas où f n'est que continue, on note

$$E = \left\{ f \in \mathscr{C}^0_{PM}([a,b], \mathbf{C}), \qquad \int_a^b f(t)e^{int} \, \mathrm{d}t \xrightarrow[n\to+\infty]{} 0 \right\}$$

E est un sev de $\mathscr{C}^0_{PM}([a,b], \mathbf{C})$ et toutes les fonctions de type $\mathbb{1}_{[\alpha,\beta]}$ sont dans E donc toutes les fonctions en escalier aussi.

Pour f continue et $\varepsilon > 0$, on approche f à ε' près par φ fonction en escalier de sorte que

$$\int_a^b f(t)e^{int} \, \mathrm{d}t = \underbrace{\int_a^b (f - \varphi)(t)e^{int} \, \mathrm{d}t}_{|\,| \leqslant (b-a)\varepsilon'} + \underbrace{\int_a^b \varphi(t)e^{int} \, \mathrm{d}t}_{\xrightarrow[n\to+\infty]{} 0}$$

donc APCR N,

$$\forall n \geqslant N, \qquad \left| \int_a^b f(t)e^{int} \right| \leqslant (b-a)\varepsilon' + \varepsilon' = \varepsilon$$

donc $f \in E$ □

On note

$$f : t \longmapsto \frac{1}{\sin t} - \frac{1}{t}$$

Cette fonction est prolongeable en 0 en une fonction $\mathscr{C}^1$ qu'on note toujours f. Puis on définit

$$I_n = \int_0^{(n+1)\frac{\pi}{2}} \frac{\sin t}{t} \, \mathrm{d}t \qquad J_n = \int_0^{\frac{\pi}{2}} \frac{\sin((2n+1)t)}{\sin t} \, \mathrm{d}t$$

On a

$$I_n = \int_0^{\frac{\pi}{2}} \frac{\sin((2n+1)t)}{t} \, \mathrm{d}t$$

donc

$$J_n - I_n = \int_0^{\frac{\pi}{2}} f(t) \sin((2n+1)t) \, \mathrm{d}t \xrightarrow[n\to+\infty]{\text{Riemann-Lebesgue}} 0$$

Puis

$$J_{n+1} - J_n = \int_0^{\frac{\pi}{2}} \frac{\sin((2n+3)t) - \sin((2n+1)t)}{\sin t} \, \mathrm{d}t = \int_0^{\frac{\pi}{2}} \frac{2\cos((2n+2)t)\sin t}{\sin t} \, \mathrm{d}t = 0$$

donc (J_n) est contante égale à $J_0 = \frac{\pi}{2}$ d'où

$$I_n \xrightarrow[n\to+\infty]{} \frac{\pi}{2}$$

11 Espaces de fonctions intégrables

a) $\mathscr{L}^1(I,\mathbf{C})$

Définition.

On note $\mathscr{L}^1(I,\mathbf{C})$ l'ensemble des fonctions ($\mathscr{C}^0_{PM}$) intégrables sur I à valeurs dans $\mathbf{C}$, et

$$\mathscr{L}^1_c(I,\mathbf{C}) = \mathscr{L}^1(I,\mathbf{C}) \cap \mathscr{C}^0(I,\mathbf{C})$$

Proposition.

(H) Soit I un intervalle non trivial

(C) 1. Si $f,g \in \mathscr{L}^1(I,\mathbf{C})$, alors $f+g \in \mathscr{L}^1(I,\mathscr{C})$ et

$$\int_I |f+g| \leqslant \int_I |f| + \int_I |g|$$

2. $\mathscr{L}^1(I,\mathbf{C})$ et $\mathscr{L}^1_c(I,\mathbf{C})$ sont des sev de $\mathscr{C}^0_{PM}(I,\mathbf{C})$

Démonstration. Facile □

Remarque.

Pour $f,g \in \mathscr{L}^1(I,\mathbf{C})$,

$$\int_I ||f|-|g|| \leqslant \int_I |f-g|$$

b) $\mathscr{L}^2(I,\mathbf{C})$

Théorème – Définition.

1. $$\mathscr{L}^2(I,\mathbf{C}) \underset{\text{def}}{=} \left\{ f \in \mathscr{C}^0_{PM}(I,\mathbf{C}), \qquad \int_I |f|^2 \text{ CV} \right\}$$
   On dit que les fonctions de cet ensemble sont de carré intégrable.
2. (Inégalité de Cauchy-Schwarz)Si $f,g \in \mathscr{L}^2(I,\mathbf{C})$ alors $fg \in \mathscr{L}^1(I,\mathbf{C})$ et
   $$\left|\int_I fg\right| \leqslant \sqrt{\left(\int_I |f|^2\right)\left(\int_I |g|^2\right)} \qquad (\star)$$
3. On a égalité dans $(\star)$ si et seulement si f et g sont proportionnelles

Démonstration.

1. $$|fg| \leqslant \frac{|f|^2}{2} + \frac{|g|^2}{2}$$
2. C'est vrai sur un segment, on passe à la borne supérieure :
   $$\int_I |fg| \leqslant \left(\int_I |f|^2\right)^{\frac{1}{2}} \left(\int_I |g|^2\right)^{\frac{1}{2}}$$
   et
   $$\left|\int_I fg\right| \leqslant \int_I |fg|$$
3. (autre preuve) Si f et g sont de carré intégrable, alors
   - Premier cas :
     $$\int_I |g|^2 = 0 \implies g \equiv 0 \implies g = 0 \times f$$
     et il y a égalité.

- Second cas :

$$\int_I |g|^2 \neq 0.$$

On pose alors

$$P(x) = \int_I (f+xg)^2 = \int_I f^2 + 2x \int_I fg + x^2 \int_I g^2$$

et on a égalité si et seulement si

$$\Delta = 0 \iff \exists \lambda \in \mathbf{R}, \quad P(x) = 0 \iff \lambda g = -f$$

□

Théorème.

1. $\mathscr{L}^2$ et $\mathscr{L}^2_c$ sont des sev de $\mathscr{C}^0_{PM}$
2. Si f, g sont de carré intégrable alors

$$\left(\int_I |f+g|^2\right)^{\frac{1}{2}} \leqslant \left(\int_I |f|^2\right)^{\frac{1}{2}} + \left(\int_I |g|^2\right)^{\frac{1}{2}}$$

Démonstration.

1. $|\lambda f + g|^2 = |\lambda|^2 |f| + \lambda f \overline{g} + \overline{\lambda f} g + |g|^2$ intégrable
2.

$$\begin{aligned}
\left(\int_I |f+g|^2\right)^{\frac{1}{2}} &\leqslant \left(\int_I |f|^2\right)^{\frac{1}{2}} + \left(\int_I |g|^2\right)^{\frac{1}{2}} \\
&\iff \int_I |f+g|^2 \leqslant \int_I |f|^2 + 2\left(\left(\int_I |f|^2\right)\left(\int_I |g|^2\right)\right)^{\frac{1}{2}} + \int_I |g|^2 \\
&\iff \int_I f\overline{g} + \overline{f} g \leqslant 2\left(\left(\int_I |f|^2\right)\left(\int_I |g|^2\right)\right)^{\frac{1}{2}}
\end{aligned}$$

qui est vrai par Cauchy-Schwarz vu précédemment

□

Remarque.

Sur $\mathscr{L}^2_c(I, \mathbf{R})$, cette inégalité est l'inégalité triangulaire pour la norme canoniquement associée au produit scalaire

$$(f|g) = \int_I fg$$

Remarque.

En général, il n'y a pas de relation d'inclusion entre $\mathscr{L}^1$ et $\mathscr{L}^2$. Par exemple, l'application $x \longmapsto \frac{1}{\sqrt{x}}$ est intégrable sur $]0,1]$ mais n'est pas de carré intégrable sur cet intervalle. L'application $x \longmapsto \frac{1}{x}$ est de carré intégrable sur $]1;+\infty[$ mais elle n'est pas intégrable sur cet intervalle.
Dans le cas d'un intervalle borné, si f est de carré intégrable alors comme $\mathbb{1}_I$ aussi, $f\mathbb{1}_I$ est intégrable et vaut f. Il y a donc une inclusion dans ce cas.

Exercice.

Soir $f \in \mathscr{C}^2(\mathbf{R}_+, \mathbf{R})$ telle que $f, f'' \in \mathscr{L}^2_c(\mathbf{R}_+, \mathbf{R})$. Montrer que $f' \in \mathscr{L}^2_c(\mathbf{R}_+, \mathbf{R})$ et

$$\int_0^{+\infty} f'^2 \leqslant \int_0^{+\infty} f^2 + \int_0^{+\infty} f''^2$$

Résolution. On raisonne par l'absurde et on suppose que f'^2 n'est pas intégrable, c'est-à-dire

$$\int_0^x f'^2 \xrightarrow[x\to+\infty]{} +\infty$$

On a

$$\int_0^x ff'' = [ff']_0^x - \int_0^x f'^2 = f(x)f'(x) - f(0)f'(0) - \int_0^x f'^2$$

Or ff'' est intégrable donc, la limite étant finie des deux côtés, $f(x)f'(x) \xrightarrow[x\to+\infty]{} +\infty$ de sorte que

$$\int_0^x ff' = \frac{1}{2}f^2(x) - \frac{1}{2}f^2(0) \implies f^2(x) \xrightarrow[x\to+\infty]{} +\infty$$

ce qui est absurde. Ainsi, f'^2 est intégrable.

Ensuite,

$$(f+f'+f'')^2 - ((f+f')^2)' = f^2 + f''^2 - f'2$$

puis

$$\int_0^x (f+f'+f'')^2 - ((f+f')^2)' = \underbrace{\int_0^x (f+f'+f'')^2}_{\geqslant 0} - \underbrace{(f+f')^2(x)}_{\xrightarrow[x\to+\infty]{} 0?} + \underbrace{(f+f')^2(0)}_{\geqslant 0}$$

Il ne reste plus qu'à vérifier $(f+f')^2(x) \xrightarrow[x\to+\infty]{} 0$. Pour le voir :

$$f^2(x) = f^2(0) + 2\int_0^x ff' \xrightarrow[x\to+\infty]{ff'\in\mathscr{L}^1} \ell \in \mathbf{R} \underset{f^2\in\mathscr{L}^1}{\implies} f^2(x) \xrightarrow[x\to+\infty]{} 0$$

et de même pour $f'^2(x)$ □

Exercice ($\star$) (Cas particulier de Landau-Kolmogorov).

> Montrer que dans ce cas,
>
> $$\int_0^{+\infty} f'^2 \leqslant 2\sqrt{\int_0^{+\infty} f^2 \times \int_0^{+\infty} f''^2}$$
>
> Indication : remplacer $f(x)$ par $f(\lambda x)$ et choisir λ

12 Calcul d'intégrales [1]

a) Calcul de $I = \int_0^{\frac{\pi}{2}} \ln\circ\sin$

- $t \longmapsto \ln(\sin t)$ est continue sur $]0, \frac{\pi}{2}]$
- $\ln(\sin t) = \ln t + \ln(1 + o_0(t))$ intégrable

donc I est ACV donc CV. De même, $\displaystyle\int_0^{\frac{\pi}{2}} \ln(\cos t)\,\mathrm{d}t$ est absolument convergente. Le changement de variable $u = \frac{\pi}{2} - t$ dans I donne $I = J$ puis

$$I + J = \int_0^{\frac{\pi}{2}} \ln(\sin\times\cos) = \int_0^{\frac{\pi}{2}} \ln\frac{1}{2}\,\mathrm{d}t + \int_0^{\frac{\pi}{2}} \ln(\sin(2t))\,\mathrm{d}t = \int_0^{\frac{\pi}{2}} \ln\frac{1}{2}\,\mathrm{d}t + \frac{1}{2}\underbrace{\int_0^{\pi} \ln(\sin u)\,\mathrm{d}u}_{=2I}$$

donc $2I - I = -\frac{\pi}{2}\ln 2$

b) Calcul par compensation

On se donne $f \in \mathscr{C}(\mathbf{R}_+, \mathbf{R})$, $0 < a < b$ et $f(x) \xrightarrow[x\to+\infty]{} \ell \in \mathbf{R}$

On va justifier que

$$\int_0^{+\infty} \frac{f(ax) - f(bx)}{x}\,\mathrm{d}x$$

converge et calculer sa valeur.

1. «Les intégrales qui font le plaisir des taupins»

On a

$$\forall 0<\varepsilon<R, \qquad \int_\varepsilon^R \frac{f(ax)-f(bx)}{x}\,\mathrm{d}x = \int_\varepsilon^R \frac{f(ax)}{x}\,\mathrm{d}x - \int_\varepsilon^R \frac{f(bx)}{x}\,\mathrm{d}x$$
$$= \int_{a\varepsilon}^{aR} \frac{f(u)}{u}\,\mathrm{d}u - \int_{b\varepsilon}^{bR} \frac{f(u)}{u}\,\mathrm{d}u$$
$$= \int_{a\varepsilon}^{b\varepsilon} \frac{f(u)}{u}\,\mathrm{d}u - \int_{aR}^{bR} \frac{f(u)}{u}\,\mathrm{d}u$$

Or

$$\left|\int_{a\varepsilon}^{b\varepsilon} \frac{f(u)}{u}\,\mathrm{d}u - f(0)\ln\left(\frac{b}{a}\right)\right| = \left|\int_{a\varepsilon}^{b\varepsilon} \frac{f(u)-f(0)}{u}\,\mathrm{d}u\right| \leqslant \sup_{[a\varepsilon,b\varepsilon]} |f-f(0)|\cdot\ln\left(\frac{b}{a}\right) \xrightarrow[\varepsilon\to 0^+]{} 0$$

De même,

$$\left|\int_{aR}^{bR} \frac{f(u)}{u}\,\mathrm{d}u - \ell\ln\left(\frac{b}{a}\right)\right| \leqslant \sup_{[aR,bR]} |f-\ell|\ln\left(\frac{b}{a}\right) \xrightarrow[R\to+\infty]{} 0$$

donc

$$\int_0^{+\infty} \frac{f(ax)-f(bx)}{x}\,\mathrm{d}x = (f(0)-\ell)\ln\left(\frac{b}{a}\right)$$

Exemple.

$$\int_0^{+\infty} \frac{\arctan x - \arctan(2x)}{x}\,\mathrm{d}x = -\frac{\pi}{2}\ln 2$$

13 Méthodes asymptotiques

a) Comparaison séries-intégrales [2]

Soit f continue sur $\mathbf{R}_+$, positive décroissante. Dans ce cas,

$$\forall k\in\mathbf{N}, \qquad f(k+1) \leqslant \int_k^{k+1} f \leqslant f(k)$$

donc

$$\sum_{k=1}^n f(k) \leqslant \int_0^n f \qquad \text{et} \qquad \sum_{k=0}^n f(k) \geqslant \int_0^{n+1} f$$

Si $\sum f(k)$ est convergente alors

$$\int_0^n f \leqslant \sum_{k=0}^{+\infty} f(k)$$

pour $n\geqslant 1$ donc $\left(\int_0^n f\right)$ est croissante majorée convergente vers un réel ℓ et

$$\int_0^{\lfloor x\rfloor} f \leqslant \int_0^x f \leqslant \int_0^{\lfloor x\rfloor+1} f \implies \int_0^x f \xrightarrow[x\to+\infty]{} \ell$$

et f est intégrable.

Réciproquement si f est intégrable sur $\mathbf{R}_+$ alors

$$\sum_{k=1}^n f(k) \leqslant \int_0^n f \leqslant \int_0^{+\infty} f \implies \sum f(k) \text{ CV}$$

Puis si f n'est pas intégrable en $+\infty$, on va calculer un équivalent des sommes partielles de $\sum f(k)$. On a

$$\int_0^n f \xrightarrow[n\to+\infty]{} +\infty \implies \sum f(k) \text{ DV}$$

2. Épisode 2

et

$$\int_1^{n+1} f \leqslant \sum_{k=1}^{n} f(k) \leqslant \int_0^n f$$

donc si $\displaystyle\int_0^n f \sim \int_0^{n+1} f$, alors pour un a fixé,

$$\sum_{k=1}^{n} f(k) \sim \int_0^n f \sim \int_a^n f$$

or $0 \leqslant f \leqslant f(0)$ donc

$$\int_0^{n+1} f = \int_0^n f + \int_n^{n+1} f \sim \int_0^n f$$

On en déduit ainsi la proposition suivante :

Proposition.

(H) $f \in \mathscr{C}^0_{PM}(\mathbf{R}_+, \mathbf{R})$ décroissante et positive sur un voisinage de $+\infty$

(C)
1. $\sum f(k)$ et $\int_0^{+\infty} f$ ont la même nature
2. Si f n'est pas intégrable en $+\infty$ alors

$$\sum_{k=0}^{n} f(k) \sim \int_a^n f$$

pour a fixé assez grand

b) Sommes de Riemann généralisées

On note f continue par morceaux décroissante intégrable sur $\mathbf{R}_+$ (donc $\geqslant 0$) et

$$S(h) = h\sum_{k=1}^{+\infty} f(kh), \qquad h > 0$$

On va montrer que

$$S(h) \xrightarrow[h\to 0^+]{} \int_0^{+\infty} f$$

Remarque.

On ne sait pas encore que $S(h)$ a un sens

On a

$$(0 \leqslant) \qquad hf((k+1)h) \leqslant \int_{kh}^{(k+1)h} f \leqslant hf(kh)$$

or l'intégrale est le terme général d'une série convergente donc $hf(kh)$ aussi et $S(h)$ est bien défini, puis

$$S(h) - hf(0) \leqslant \int_0^{+\infty} f \leqslant S(h)$$

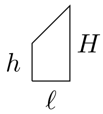
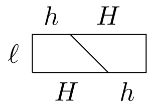
ce qui conclut avec $h \to 0^+$

Exemple.

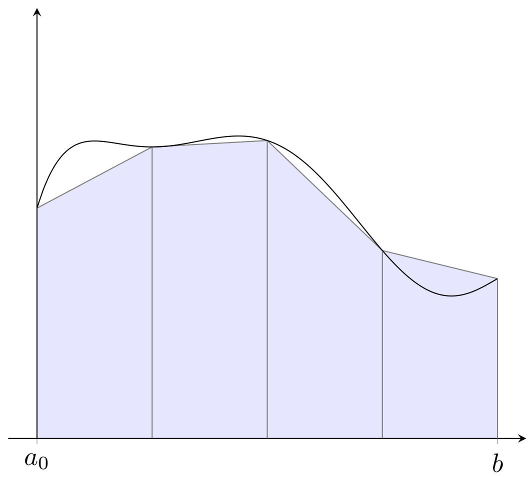
$$x\sum_{k=0}^{+\infty} e^{-k^2x^2} \xrightarrow[x\to 0^+]{} \int_0^{+\infty} e^{-t^2}\,\mathrm{d}t$$

c) Méthode du trapèze

Remarque.

> L'aire du trapèze 
>
> vaut $\dfrac{h+H}{2}\ell$. Pour le voir, 
>

On se donne $f \in \mathscr{C}^2([a,b],\mathbf{R})$



On note

$$a_k = a + k\frac{b-a}{n}$$

et on va montrer que

$$S_n(f) = \sum_{k=0}^{n-1} \frac{f(a_k)+f(a_{k+1})}{2} \times \frac{b-a}{n}$$

approche l'intégrale et on va majorer l'erreur commise. Pour ça, on note

$$g_k(x) = f(a_k)\frac{x-a_{k+1}}{a_k-a_{k+1}} + f(a_{k+1})\frac{x-a_k}{a_{k+1}-a_k}$$

de sorte que

$$\int_a^b f - S_n(f) = \sum_{k=0}^{n-1} \int_{a_k}^{a_{k+1}} f - g_k$$

donc

$$\left|\int_a^b f - S_n(f)\right| \leqslant \sum_{k=0}^{n-1} \int_{a_k}^{a_{k+1}} |f-g_k|.$$

Pour $x \in]a_k, a_{k+1}[$, on note $\lambda \in \mathbf{R}$ tel que

$$f(x) = g_k(x) + \frac{\lambda}{2}(x-a_k)(x-a_{k+1}).$$

La fonction

$$h : t \in [a_k, a_{k+1}] \longmapsto f(t) - g_k(t) - \frac{\lambda}{2}(t-a_k)(t-a_{k+1})$$

s'annule en trois points donc en appliquant Rolle deux fois, il existe γ tel que

$$h''(\gamma) = 0 \implies \lambda = f''(\gamma)$$

Par suite,

$$|f(x) - g_k(x)| \leqslant \frac{1}{2} \sup_{[a_k, a_{k+1}]} |f''| \cdot |(x - a_k)(x - a_{k+1})|$$

d'où on tire

$$\left| \int_a^b f - S_n(f) \right| \leqslant \frac{1}{2} \|f''\|_\infty \sum_{k=0}^{n-1} \int_{a_k}^{a_{k+1}} (a_k - t)(t - a_{k+1})\, \mathrm{d}t = \|f''\|_\infty \frac{(b-a)^3}{12n^2}$$

Remarque.

La majoration est un $O\left(\frac{1}{n^2}\right)$, ce qui est meilleur que la méthode des rectangles.

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre V

Suites et Séries de fonctions

Sommaire

Dans tout le chapitre, I est un intervalle non trivial, A est une partie non vide de $\mathbf{R}$ et $K = \mathbf{R}$ ou $\mathbf{C}$. Plus tard, on pourra remplacer A par une partie d'un e.v.n (de dimension finie généralement) et K un e.v.n.

1 Différents types de convergence

Définition.

On note $(f_n)_n$ une suite de fonctions de I dans K.

1. On dit que $(f_n)_n$ *converge simplement* (CVS) s'il existe $f : I \to K$ telle que $\forall x \in I, f_n(x) \xrightarrow[n\to+\infty]{} f(x)$
2. On dit que $(f_n)_n$ *converge uniformément* (CVU) s'il existe $f : I \to K$ telle que
   - $(f_n - g)$ est bornée à partir d'un certain rang
   - $\sup_I |f_n - g| \xrightarrow[n\to+\infty]{} 0$
3. On dit que (f_n) converge uniformément sur tout segment (CVUTS) si pour tout segment $J \subset I$, on a $f_n \xrightarrow[J]{\text{CVU}} f$

Dans chacun des cas, on peut remplacer I par A.

Remarque.

- CVU $\Longrightarrow$ CVUTS $\Longrightarrow$ CVS
- CVS $\not\Longrightarrow$ CVUTS $\not\Longrightarrow$ CVU

Remarque.

La limite uniforme d'une suite uniformément convergente est identique à la limite simple de cette suite. En particulier, on a unicité de la limite pour les trois convergences.

2 Opérations simples sur les convergences

Proposition.

(H) $(u_n)_n, (v_n)_n$ sont des suites de fonctions de I dans K, $u, v : I \to K$, $\lambda \in K$.

(C) Si $u_n \to u$, $v_n \xrightarrow{v}$ avec de la convergence simple (resp. CVUTS, CVU) alors

$$(\lambda u_n + v_n) \to \lambda u + v$$

avec la convergence simple (resp. CVUTS, CVU).

Démonstration. Évident. □

Remarque.

Pour la convergence simple, on a $u_n v_n \longrightarrow uv$, mais pas pour la CVU ou la CVUTS. Par exemple,

$$u : \begin{array}{ccc} \mathbf{R}_+ & \longrightarrow & \mathbf{R} \\ x & \longmapsto & e^x + \frac{1}{n} \end{array}$$

On a

$$u_n \xrightarrow[\mathbf{R}_+]{\text{CVU}} u$$

On a aussi

$$u_n^2 \xrightarrow[\mathbf{R}_+]{\text{CVS}} u^2$$

donc si u_n^2 converge uniformément,

$$u_n^2(x) - u^2(x) = \frac{2e^x}{n} + \frac{1}{n^2} \xrightarrow[n\to+\infty]{} 0$$

ce qui est absurde

Proposition (Propriétées héritées par CVS).

(H) $u_n : I \to \mathbf{K}$, $u_n \xrightarrow{\text{CVS}} u$ sur I

(C) La monotonie, la convexité, le caractère k-lipschitzien, la positivité sont hérités.

Démonstration. On écrit les inégalités et on passe à la limite. □

3 Propriétés héritées par CVU

Théorème (Double limite).

(H) $u_n \xrightarrow{\text{CVU}} u$ sur A, a point adhérent de A, $u_n(x) \underset{x\to a}{\longrightarrow} \ell_n \in \mathbf{K}$

(C) 1. (ℓ_n) converge vers $\ell \in \mathbf{K}$

2. La fonction u a pour limite ℓ en a, i.e.

$$\lim_{\substack{x\to a\\ x\in A}} \lim_{x\to+\infty} u_n(x) = \lim_{n\to+\infty} \lim_{\substack{x\to a\\ x\in A}} u_n(x)$$

Démonstration.

1. (admis) On va construire (n_k) strictement croissante telle que $\forall n \geqslant n_k, |\ell_n - \ell_{n_k}| \leqslant \dfrac{1}{2^k}$.
   - $\forall \varepsilon > 0, \exists N \in \mathbf{N}, \forall n \geqslant N, \forall x \in A, |u_n(x) - u(x)| \leqslant \varepsilon'$
   - $\forall n, p \geqslant N, |u_n(x) - u_p(x)| \leqslant |u_n(x) - u(x)| + |u(x) - u_p(x)| \leqslant 2\varepsilon' = \varepsilon$ et $x \longrightarrow a$ donne $|\ell_n - \ell_p| \leqslant \varepsilon$
   - Pour $\varepsilon = 1$, il existe $n_0 \in \mathbf{N}$ tel que $\forall n \geqslant n_0, |\ell_n - \ell_{n_0}| \leqslant 1$
   - Pour $k \in \mathbf{N}$, si on suppose $n_0 < \cdots < n_k$ construits, pour $\varepsilon = \frac{1}{2^{k+1}}$, il existe $N \in \mathbf{N}$ tel que $\forall p \geqslant N, |\ell_n - \ell_p| \leqslant \varepsilon$. On prend $n_{k+1} = \max(N, n_0, \cdots, n_k + 1)$.

   Puis $|\ell_{n_{k+1}} - \ell_{n_k}| \leqslant \frac{1}{2^k}$, c'est le terme général d'une série convergente donc (ℓ_{n_k}) converge.
   Soit $\varepsilon > 0$. Il existe K tel que $k \geqslant K$, $\frac{1}{2^k} \leqslant \varepsilon'$ et $|\ell - \ell_{n_k}| \leqslant \varepsilon'$ donc pour $n \geqslant n_k$,

   $$|\ell_n - \ell| \leqslant |\ell_n - \ell_{n_k}| + |\ell_{n_k} - \ell| \leqslant 2\varepsilon' = \varepsilon$$

   donc $\ell_n \longrightarrow \ell$
2. On suppose $a \in \mathbf{R}$. Soit $\varepsilon > 0$.
   - $\exists N \in \mathbf{N}, \forall n \geqslant N, \forall x \in A, \quad |u_n(x) - u(x)| \leqslant \varepsilon'$
   - $\exists N_1 \in \mathbf{N}, \forall n \geqslant N_1, \quad |\ell_n - \ell| \leqslant \varepsilon'$
   - $M = \max(N, N_1)$. $\qquad \exists \delta > 0, \forall x \in]a - \delta, a + \delta[\cap A, |u_M(x) - \ell_M| \leqslant \varepsilon'$.

   Donc $|u(x) - \ell| \leqslant |u(x) - u_M(x)| + |u_M(x) - \ell_M| + |\ell_M - \ell| \leqslant 3\varepsilon' = \varepsilon$

□

Remarque.

a est un point adhérent si et seulement si $\exists (a_n) \in A^{\mathbf{N}}, a_n \longrightarrow a$

Corollaire.

(H) (u_n) une suite de fonctions continues sur A qui converge uniformément sur A vers u

(C) u est continue sur A

Démonstration. $a \in A$ donc a est un point adhérent de A, $u_n \xrightarrow[A]{\text{CVU}} u$ et $\forall n \in \mathbf{N}$,

$$\lim_{\substack{x\to a\\ x\in A}} u_n(x) = u_n(a) \quad (= \ell_n)$$

et TDL :

$$\lim_{\substack{x\to a\\ x\in A}} u(x) = \lim_{n\to+\infty} u_n(x) = u(a)$$

□

4 Convergence uniforme, dérivation, intégration

Théorème.

(H) $u_n : I \to K$, $u : I \to K$ et $u_n \xrightarrow[I]{\text{CVUTS}} u$, $a \in I$, u_n et u sont $\mathscr{C}^0_{PM}(I, \mathbf{K})$. On note $U_n : x \in I \longmapsto \int_a^x u_n$ et $U : x \in I \longmapsto \int_a^x u$

(C) $U_n \xrightarrow[I]{\text{CVUTS}} U$ et en particulier $\forall \alpha, \beta \in I$, $\int_\alpha^\beta u_n \xrightarrow[n\to+\infty]{} \int_\alpha^\beta u$

Démonstration. $[\alpha, \beta] \subset I$, J plus petit segment qui contient a, α, β. On a sur J, avec $\mu(J) = \int_J \mathrm{d}x$ (constant) :

$$\|U_n - U\|_\infty \leqslant \mu(J)\|u_n - u\|_\infty \xrightarrow[n\to+\infty]{} 0$$

donc $U_n \xrightarrow[J]{\text{CVU}} U$ d'où la conclusion sur la CVUTS. Puis,

$$\int_\alpha^\beta u_n = U_n(\beta) - U_n(\alpha) \xrightarrow[n\to+\infty]{} U(\beta) - U(\alpha)$$

□

Exemple. $u_n : x \in [0,1] \longmapsto n^2 x^n (1-x)$ converge simplement vers la fonction nulle. Puis

$$\int_0^1 u_n = n^2 \left(\frac{1}{n+1} - \frac{1}{n+2} \right) \xrightarrow[n\to+\infty]{} 1 \neq \int_0^1 0 = 0$$

donc il n'y a pas CVU.

Théorème (Dérivation).

(H) (u_n) suite de fonctions $\mathscr{C}^1$ sur I, telles que

$$u_n \xrightarrow[I]{\text{CVS}} u \qquad \text{et} \qquad u_n' \xrightarrow[I]{\text{CVUTS}} v$$

(C)
1. $u_n \xrightarrow[I]{\text{CVUTS}} u$
2. v est continue et $u' = v$

Démonstration. On se donne $a \in I$ fixé, on écrit

$$u_n(x) = u_n(a) + \int_a^x u_n'$$

et $n \to +\infty$ donne

$$u(x) = u(a) + \int_a^x v$$

donc u est $\mathscr{C}^1$ et $u' = v$. Puis,

$$\int_a^x u_n \xrightarrow[I]{\text{CVUTS}} \int_a^x u'$$

donc

$$u_n \xrightarrow[I]{\text{CVUTS}} u$$

□

Théorème (Dérivation itérée).

(H) (u_n) fonctions $\mathscr{C}^p$,

$$\forall k \in [\![0, p-1]\!], \qquad u_n^{(i)} \xrightarrow[I]{\text{CVS}} \varphi_i$$

et

$$u_n^{(p)} \xrightarrow[I]{\text{CVUTS}} \varphi_p$$

(C)
1. Il y a CVUTS à la place de la CVS pour toutes les dérivées d'ordre $\leqslant p$
2. φ_0 est $\mathscr{C}^p$ et $\varphi_0^{(k)} = \varphi_k$

Démonstration. Admis. (Récurrence) □

Théorème (Convergence dominée).

(H) $(u_n), u$ des fonctions $\mathscr{C}^0_{PM}(I, \mathbf{K})$, $u_n \xrightarrow[I]{\text{CVS}} u$
$\exists \varphi \in \mathscr{L}^1(I, \mathbf{R}_+), \quad \forall x \in I, \forall n \in \mathbf{N}, \quad |u_n(x)| \leqslant \varphi(x)$

(C)
1. u_n et u intégrable sur I
2. $\lim\limits_{n \to +\infty} \int_I u_n = \int_I u$

Démonstration. Admis □

Remarque.

On note

$$f_n : \begin{array}{ccc} \mathbf{R}_+ & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \dfrac{x^n e^{-x}}{n!} \end{array}$$

Les f_n sont $\mathscr{C}^1$ et

$$f_n'(x) = \frac{e^{-x}}{n!}\left(-x^n + nx^{n-1}\right) = \frac{x^{n-1}e^x(n-x)}{n!}$$

Le calcul donne

$$\sup_{\mathbf{R}_+} |f_n| \xrightarrow[n \to +\infty]{} 0 \qquad \text{donc} \qquad f_n \xrightarrow[\mathbf{R}_+]{\text{CVU}} 0$$

Les f_n sont intégrables (ce sont des $o(\frac{1}{x^2})$) et

$$\int_0^{+\infty} f_n = \underbrace{\left[-\frac{x^n e^{-x}}{n!}\right]_0^{+\infty}}_{=0} + \int_0^{+\infty} \frac{x^{n-1}}{(n-1)!} e^{-x} \,\mathrm{d}x = \cdots = \int_0^{+\infty} e^{-x} \,\mathrm{d}x = 1$$

Ainsi

$$\lim_{n \to +\infty} \int_0^{+\infty} \frac{x^n e^{-x}}{n!} \,\mathrm{d}x = 1 \neq \int_0^{+\infty} \left(\lim_{n \to +\infty} f_n(x)\right) \mathrm{d}x = 0$$

Le théorème ne s'applique pas sans hypothèse de domination

Exemple.

$$\Gamma : x \longmapsto \int_0^{+\infty} e^{-t} t^{x-1} \,\mathrm{d}t$$

Cette fonction est bien définie car l'intégrande est intégrable. On note

$$f_n : t \longmapsto \mathbb{1}_{[0,n]}(t) \left(t - \frac{t}{n}\right)^n t^{x-1}$$

Ce sont des fonctions $\mathscr{C}^0_{PM}$ sur $\mathbf{R}_+^\star$. On a

$$f_n \xrightarrow[\mathbf{R}_+^\star]{\text{CVS}} e^{-t} t^{x-1}$$

Donc $\forall n \in \mathbf{N}^\star$,

$$\forall t > 0, \qquad 0 \leqslant f_n(t) \leqslant \mathbb{1}_{[0,n]} \exp\left(n \ln\left(1 - \frac{t}{n}\right)\right) \leqslant e^{-t} t^{x-1}$$

et le membre de droite est $\mathscr{C}^0_{PM}$ intégrable. Par convergence dominée,

$$\int_0^{+\infty} f_n \xrightarrow[t \to +\infty]{} \int_0^{+\infty} f = \Gamma(x)$$

Puis (calculer)

$$\int_0^{+\infty} f_n = \frac{n^x n!}{x(x+1)\cdots(x+n)}$$

donc

$$\frac{n^x n!}{x(x+1)\cdots(x+n)} \xrightarrow[n \to +\infty]{} \Gamma(x)$$

5 Méthodes pour la convergence uniforme

On suppose que l'on a une suite $(u_n)_n$ de fonctions de I dans $\mathbf{C}$ et u de I dans $\mathbf{C}$ telle que

$$u_n \xrightarrow[I]{\text{CVS}} u$$

Comment établir $u_n \xrightarrow[I]{\text{CVS}} u$?

- Étude de $|u_n - u|$ (ou $u_n - u$ pour les fonctions réelles)
- On trouve (a_n) tel que $\forall x \in I, \quad |u_n(x) - u(x)| \leqslant a_n$ et $a_n \longrightarrow 0$
- Autre (il faut réfléchir)

Comment montrer qu'il n'y a pas CVU ?

- Étudier $\sup_I |u_n - u|$ et vérifier que ça ne tend pas vers 0
- Trouver (x_n) tel que $(u_n - u)(x_n)$ ne tend pas vers 0
- Trouver un segment I tel que $\int_I u_n$ ne tend pas vers $\int_I u$
- Régularité de la limite simple
- Autre (réfléchir)

a) Un premier exemple

$$f_n(x) = \begin{cases} \dfrac{\sin(n^2 x)^2}{n \sin x} & \text{si } x \in]0, \frac{\pi}{2}] \\ 0 & \text{si } x = 0 \end{cases}$$

On a

$$f_n \xrightarrow{\text{CVS}} 0$$

mais

$$f_n\left(\frac{1}{n}\right) \sim \sin(n)^2 \not\to 0$$

donc il n'y a pas CVU.

b) Un deuxième exemple

$$\varphi_n : \begin{array}{ccc} [0, \frac{\pi}{2}] & \longrightarrow & \mathbf{R} \\ x & \longmapsto & n \cos^n x \sin x \end{array}$$

La suite (φ_n) converge simplement vers la fonction nulle, or

$$\int_0^{\frac{\pi}{2}} \varphi_n = \frac{n}{n+1} \xrightarrow[n \to +\infty]{} 1 \neq 0$$

Donc il n'y a pas CVU.

c) Approximation de l'exponentielle

On va montrer que pour tout $R > 0$,

$$\left(1+\frac{z}{n}\right)^n \xrightarrow[\mathscr{D}_f(0,R)]{\text{CVU}} e^z$$

On remarque d'abord (Taylor)

$$\forall z \in \mathscr{D}_f(0,R), \qquad \left|e^z - \sum_{k=0}^{n} \frac{z^k}{k!}\right| = \left|z^{n+1}\int_0^1 \frac{(1-t)^n}{n!} e^{tz}\,\mathrm{d}t\right| \leqslant \sup_{|z|\leqslant R} |e^z| \frac{R^{n+1}}{(n+1)!} = a_n \xrightarrow[n\to+\infty]{} 0$$

donc

$$P_n(z) \underset{\text{def}}{=} \sum_{k=0}^{n} \frac{z^k}{k!} \xrightarrow[\mathscr{D}_f(0,R)]{\text{CVU}} e^z.$$

Puis,

$$P_n(z) - \left(1-\frac{z}{n}\right)^n = \sum_{k=0}^{n} \underbrace{\left(\frac{1}{k!} - \frac{n(n-1)\cdots(n-k+1)}{k!n^k}\right)}_{\geqslant 0} z^k$$

donc

$$\left|P_n(z) - \left(1+\frac{z}{n}\right)^n\right| \leqslant P_n(R) - \left(1+\frac{R}{n}\right)^n \xrightarrow[n\to+\infty]{} 0$$

et finalement

$$e^z - \left(1+\frac{z}{n}\right)^n = \underbrace{e^z - P_n(z)}_{\text{CVU vers } 0} + \underbrace{P_n(z) - \left(1+\frac{z}{n}\right)^n}_{\text{CVU vers } 0} \xrightarrow[\mathscr{D}_f(0,R)]{\text{CVU}} 0$$

d) Suite récurrente de fonctions

On se place sur $[0, \frac{\pi}{2}]$ et on pose

$$u_0 = \mathrm{id} \qquad \forall n \geqslant 0, \quad u_{n+1} = \sin(u_n)$$

On observe que les u_n sont croissantes donc

$$0 \leqslant u_n(x) \leqslant u_n\left(\frac{\pi}{2}\right) \xrightarrow[n\to+\infty]{} 0$$

Donc $u_n \xrightarrow{\text{CVU}} 0$

6 Résultats de densité

a) Fonctions en escalier

On a montré que $f \in \mathscr{C}^0_{PM}([a,b],\mathbf{C})$ est limite uniforme de fonctions en escalier sur $[a,b]$ (vu en sup).

b) Fonctions continues affines par morceaux

On va montrer que toutes les fonctions continues sur un segment sont limites uniforme de fonctions continues affines par morceaux.

On prend $f \in \mathscr{C}([a,b],\mathbf{C})$. Soit $\varepsilon > 0$. Il existe φ en escalier qui approche f à $\varepsilon' = \frac{\varepsilon}{3}$ près. On note $\sigma = (a_0, \cdots, a_n)$ une subdivision adaptée à φ (on note $|\sigma|$ le pas de cette subdivision, c'est à dire le minimum des écarts entre deux termes consécutifs). On note $\delta > 0$ tel que $\delta < \frac{|\sigma|}{2}$, et on note c_i la valeur de φ sur $]a_i, a_{i+1}[$. On a :

$$\forall i \in [\![1, n-1]\!], \quad |c_i - f(a_{i+1})| \leqslant \varepsilon' \text{ et } |c_{i+1} - f(a_{i+1})| \leqslant \varepsilon' \qquad \text{donc} \qquad |c_{i+1} - c_i| \leqslant 2\varepsilon'$$

On pose g l'unique fonction continue affine sur les intervalles du type $[a_i - \delta, a_i + \delta]$ et qui coïncide avec φ ailleurs. On a dans tous les cas $|g(x) - \varphi(x)| \leqslant 2\varepsilon'$ et donc

$$\forall x \in [a,b], \qquad |g(x) - f(x)| \leqslant 3\varepsilon'$$

c) Théorème de Weierstrass

Théorème (Weierstrass).

(H) $f \in \mathscr{C}^0([a,b],\mathbf{R})$

(C) f est limite uniforme de polynômes :

$$\forall \varepsilon > 0, \exists P \in \mathbf{R}[X], \forall x \in [a,b], \quad |f(x) - P(x)| \leqslant \varepsilon$$

Démonstration par les polynômes de Bernstein. On commence par le cas $[a,b] = [0,1]$. Pour $f \in \mathscr{C}^0([0,1],\mathbf{R})$, on note

$$B_n(f)(x) \underset{\text{def}}{=} \sum_{k=0}^{n} \binom{k}{n} x^k (1-x)^{n-k} f\left(\frac{k}{n}\right)$$

Le calcul donne

- $B_n(1)(x) = 1$
- $B_n(X)(x) = x$
- $B_n(X^2)(x) = \dfrac{x}{n}(nx - x + 1) = x^2 + \dfrac{x - x^2}{n}$ donc

$$B_n(X^2)(x) \xrightarrow[{[0,1]}]{\text{CVU}} x^2$$

On en déduit

$$\sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k} (k - nx)^2 = n^2 B_n(X^2)(x) - 2n^2 x B_n(X)(x) + n^2 B_n(1)(x) = nx(1-x)$$

On va montrer que $B_n(f)$ converge uniformément vers f sur $[0,1]$. La fonction f est continue sur un segment donc (Heine) elle est uniformément continue. Soit $\alpha > 0$, il existe $\delta > 0$ associé tel que

$$|x - y| \leqslant \delta \implies |f(x) - f(y)| \leqslant \alpha$$

On a

$$\begin{aligned} B_n(f)(x) - f(x) = & \sum_{\substack{k=0 \\ |\frac{k}{n} - x| \leqslant \delta}}^{n} \left(f\left(\frac{k}{n}\right) - f(x) \right) \binom{n}{k} x^k (1-x)^{n-k} \\ & + \sum_{\substack{k=0 \\ |\frac{k}{n} - x| > \delta}}^{n} \left(f\left(\frac{k}{n}\right) - f(x) \right) \binom{n}{k} x^k (1-x)^{n-k} \end{aligned}$$

On note M un majorant de $|f|$ sur $[0,1]$, et en remarquant que $\left|\frac{k}{n} - x\right| > \delta \iff (n\delta)^2 < (k - nx)^2$, on a

$$\begin{aligned} (n\delta)^2 \sum_{\substack{k=0 \\ |\frac{k}{n} - x| > \delta}}^{n} \binom{n}{k} x^k (1-x)^{n-k} & \leqslant \sum_{\substack{k=0 \\ |\frac{k}{n} - x| > \delta}}^{n} (k - nx)^2 \binom{n}{k} x^k (1-x)^{n-k} \\ & \leqslant \sum_{k=0}^{n} (k - nx)^2 \binom{n}{k} x^k (1-x)^{n-k} \\ & = nx(1-x) \leqslant \frac{n}{4} \end{aligned}$$

d'où finalement

$$\sum_{\substack{k=0 \\ |\frac{k}{n} - x| > \delta}}^{n} \binom{n}{k} x^k (1-x)^{n-k} \leqslant \frac{1}{4n\delta^2}$$

et

$$|B_n(f)(x) - f(x)| \leqslant \frac{2M}{4n\delta^2} + \alpha < \varepsilon$$

d'où la CVU.

Pour le cas général, on compose à droite par une application affine (polynômiale). $\square$

7 Séries de fonctions

Définition.

On note $(f_n)_{n\in\mathbf{N}}$ une suite de fonctions de I dans $\mathbf{K}$.

- On appelle série de fonctions associée à $f = (f_n)$ la suite $(S_n(f))_n$, où

$$S_n(f) : x \in I \longmapsto \sum_{k=0}^{n} f_k(x)$$

  On la note $\sum f_n$
- On dira que $\sum f_n$ converge simplement ou uniformément si la suite sous-jacente $(S_n(f))$ aussi.
- On dira que $\sum f_n$ converge normalement si $\|f_n\|_\infty$ est le terme général d'une série convergente.

Remarque.

La convergence normale entraine tous les autres types de convergences, c'est une contrainte plus forte. En effet, si $\sum f_n$ converge normalement, alors il y a CVS car $\sum |f_n(x)|$ converge. On note S la limite simple et on a

$$\forall x \in I, \forall n \in N, \qquad |S_n(f)(x) - S(x)| = \left| \sum_{k=n+1}^{+\infty} f_k(x) \right| \leqslant \sum_{k=n+1}^{+\infty} \|f_k\|_\infty \xrightarrow[n\to+\infty]{} 0$$

d'où la CVU.

8 Propriétés héritées

Proposition.

(H) $f_n : I \to \mathbf{K}$ continues, $\sum f_n$ CVU

(C) $S : x \in I \longmapsto \sum_{n=0}^{+\infty} f_n(x)$ est continue

Démonstration. Les $S_n(f)$ sont continues et il y a CVU. □

Proposition (Dérivation).

(H) $f_n : I \to \mathbf{K} \quad \in \mathscr{C}^1$, $\sum f_n$ CVU et $\sum f_n'$ CVUTS

(C) $S : x \in I \longmapsto \sum_{n=0}^{+\infty} f_n(x)$ est $\mathscr{C}^1$ et

$$S'(x) = \sum_{n=0}^{+\infty} f_n'(x)$$

Proposition (Double limite).

(H) $f_n : I \to \mathbf{K}$, a adhérent à I, $\sum f_n$ CVU, $\qquad \lim\limits_{\substack{x\to a\\ x\in I}} f_n(x) = \ell_n \in \mathbf{K}$

(C)
1. $\sum \ell_n$ converge
2. $\lim\limits_{x\to a} \sum_{n=0}^{+\infty} f_n(x) = \sum_{n=0}^{+\infty} \ell_n$

Proposition (Dérivation itérée).

(H) $f_n \in \mathscr{C}^p(I, \mathbf{K})$, $\sum f_n, \cdots, \sum f_n^{(p-1)}$ CVS et $\sum f_n^{(p)}$ CVUTS

(C) Les CVS sont des CVUTS et

$$\forall \ell \in [\![0, p]\!], \quad S^{(\ell)}(x) = \sum_{n=0}^{+\infty} f_n^{\ell}(x)$$

9 Exemples

a) Étude de $\sum_{n\geqslant 0} \frac{1}{n!(x+n)}$

On a bien CVS sur $\mathbf{R}_+^\star$ et pour $k > 0$

$$\left|\frac{1}{k!(x+k)}\right| \leqslant \frac{1}{k!} \text{ tg série CV}$$

donc il y a CVN et CVU. La somme S est continue et on a

$$S(x) = \frac{1}{x} + \underbrace{\sum_{n\geqslant 1} f_n}_{\text{borné}} \underset{0^+}{\sim} \frac{1}{x}$$

Puis, $xS(x)$ converge normalement et

$$\lim_{x\to+\infty} \frac{x}{n!(x+n)} = \frac{1}{n!}$$

Donc par théorème de la double limite,

$$xS(x) \xrightarrow[x\to+\infty]{} e \qquad \text{donc} \qquad S(x) \underset{+\infty}{\sim} \frac{e}{x}$$

On étudie $S(x) - \frac{e}{x}$.

$$S(x) - \frac{e}{x} = \sum_{n=0}^{+\infty} \frac{1}{n!} \frac{-n}{x(x+n)} = -\frac{1}{x} \sum_{n=1}^{+\infty} \frac{1}{(n-1)!(x+n)} = -\frac{1}{x} S(1+x) \underset{+\infty}{\sim} \frac{e}{x^2}$$

D'où finalement

$$S(x) = \frac{e}{x} - \frac{e}{x^2} + o_{+\infty}\left(\frac{1}{x^2}\right)$$

La fonction S est $\mathscr{C}^1$ sur $\mathbf{R}_+^\star$ car

- Les f_n sont $\mathscr{C}^1$
- Il y a CVS
- Sur un segment $[a, b]$, $\|f_n'\|_\infty \leqslant \frac{1}{n!(a+n)^2}$ qui est le terme général d'une série convergente, indépendant de x. Donc $\sum f_n'$ CVN donc CVUTS

b) Étude de $\sum(-1)^n \ln(1 + 1/n^2x^2)$

On pose

$$\forall x \in \mathbf{R}_+^\star, \qquad f(x) = \sum_{n\geqslant 1} (-1)^n \ln\left(1 + \frac{1}{n^2x^2}\right)$$

La série converge absolument donc on a bien la CVS, les f_n sont continus puis il y a CVN sur chaque segment donc f est continue.

Puis, sur $[1, +\infty[$, on a $x^2 \ln(1 + \frac{1}{n^2x^2}) \leqslant \frac{1}{n^2}$ donc il y a CVN et

$$\forall n \in \mathbf{N}^\star, \quad \lim_{x\to+\infty} (-1)^n x^2 \ln\left(1 + \frac{1}{n^2x^2}\right) = \frac{(-1)^n}{n^2}$$

donc (double limite) :

$$f(x) \underset{+\infty}{\sim} \frac{1}{x^2} \sum_{n\geqslant 1} \frac{(-1)^n}{n^2}$$

Remarque.

$$\zeta(2) = \frac{\pi^2}{6} = \underbrace{\sum_{n\geqslant 1} \frac{1}{(2n)^2}}_{\frac{1}{4}\cdot\frac{\pi^2}{6}} + \sum_{n\geqslant 0} \frac{1}{(2n+1)^2}$$

donc

$$\sum_{n=1}^{+\infty} \frac{(-1)^n}{n^2} = \frac{1}{4}\cdot\frac{\pi^2}{6} - \frac{\pi^2}{8} = -\frac{\pi^2}{12}$$

et $f(x) \underset{+\infty}{\sim} -\dfrac{\pi^2}{12x^2}$

10 Intégration terme à terme

L'intégration terme à terme dans le cas uniforme est identique au cas des suites.

Théorème (Intégration terme à terme uniforme).

(H) $f_n \in \mathscr{C}^0_{PM}([a,b], \mathbf{R})$, $\sum f_n$ CVU et $\sum_{n\geqslant 0} f_n$ $\mathscr{C}^0_{PM}$

(C) $\displaystyle\int_a^b \sum f_n = \sum \int_a^b f_n$

Théorème (Intégration dominée).

(H) $f_n \in \mathscr{C}^0_{PM}$ sur I, intégrable. $\sum f_n$ CVS, $\sum_{n\geqslant 0} f_n$ $\mathscr{C}^0_{PM}$ et $\sum \int_I |f_n|$ converge

(C) $\sum_{n\geqslant 0} f_n$ est intégrable sur I et

$$\int_I \sum_{n\geqslant 0} f_n = \sum_{n\geqslant 0} \int_I f_n$$

Exemple. Calcul de $\displaystyle\int_0^{+\infty} \frac{t}{e^t - 1}\,\mathrm{d}t$.

Pour $t > 0$,

$$\frac{t}{e^t-1} = \frac{t}{e^t(1-e^{-t})} = \frac{t}{e^t}\sum_{k=0}^{+\infty} e^{-tk} = \sum_{k=0}^{+\infty} te^{-(k+1)t}$$

On note $f_k : t \longmapsto te^{-(k+1)t} \in \mathscr{C}^0_{PM}(\mathbf{R}_+^\star)$. On a $\sum f_n$ CVS sur $\mathbf{R}_+^\star$ et $\sum_{n\geqslant 0} f_n$ est continue sur $\mathbf{R}_+^\star$. Puis, pour $k \geqslant 0$,

$$\int_0^{+\infty} |f_k| = \int_0^{+\infty} te^{-(k+1)t}\,\mathrm{d}t = \frac{1}{(k+1)^2} \text{ tg série CV}$$

donc on peut intégrer terme à terme :

$$\int_0^{+\infty} \frac{t}{e^t-1}\,\mathrm{d}t = \sum_{k=0}^{+\infty} \int_0^{+\infty} te^{-(k+1)t}\,\mathrm{d}t = \frac{\pi^2}{6}$$

Exemple. Calcul de $I = \displaystyle\int_0^{+\infty} \frac{\ln u}{1+u}\,\mathrm{d}u$.

Première méthode. $u = e^{-t}$ donne $I = -\displaystyle\int_0^{+\infty} \frac{t}{e^t-1}\,\mathrm{d}t$ et on a calculé cette intégrale

Seconde méthode. $\dfrac{\ln u}{1+u} = \displaystyle\sum_{k\geqslant 0} (-1)^k u^k \ln u$ et on applique le théorème d'intégration terme à terme (version simple)

11 Méthodes pour la convergence uniforme

Pour montrer la convergence uniforme, on peut montrer

- la convergence normale
- la convergence simple puis la convergence uniforme du reste vers 0
- autre (il faut réfléchir)

a) TSA uniforme

Si (u_n) est une suite de fonctions de I dans $\mathbf{R}_+$, que $\forall x \in I, (u_n(x))$ décroît et u_n converge uniformément vers 0, alors $\sum(-1)^k u_k$ converge simplement sur I par TSA et

$$\forall x \in I, \qquad , \left| \sum_{k=n+1}^{+\infty} (-1)^k u_k(x) \right| \leqslant u_{n+1}(x) \xrightarrow[I]{\text{CVU}} 0$$

donc $\sum u_n$ CVU.

b) Étude de ζ

On note

$$\forall s > 1, \qquad \zeta(s) = \sum_{k \geqslant 1} \frac{1}{k^s}$$

et

$$\forall x > 0, \qquad \varphi(x) = \sum_{n \geqslant 1} \frac{(-1)^{n-1}}{n^x}$$

On note $u_n : x \longmapsto \dfrac{1}{n}$

Étude de régularité. On va montrer que ζ est $\mathscr{C}^\infty$. Soit $n > 1$.

- Les u_k sont $\mathscr{C}^\infty$
- Pour $i \in [\![0, n-1]\!]$, on a
$$u_k^{(i)}(x) = \frac{(-1)^i \ln^i(k)}{k^x}$$
donc pour $x > 1$,
$$u_k^{(i)}(x) = o_{+\infty}\left(\frac{1}{k^{\frac{x+1}{2}}}\right) \text{ tg série CV}$$
donc $\sum u_k^{(i)}$ CVS
- Soit $[a, b] \subset]1, +\infty[$. Alors
$$\forall x \in [a, b], \forall k \geqslant 1, \qquad |u_k^{(n)}(x)| \leqslant \frac{\ln^n k}{k^a} = o_{+\infty}\left(\frac{1}{k^{\frac{1+a}{2}}}\right)$$
d'où la CVUTS.

ζ est donc $\mathscr{C}^n$ pour tout n, donc $\zeta \in \mathscr{C}^\infty$ et

$$\zeta^{(n)}(s) = \sum_{k \geqslant 1} \frac{(-1)^n \ln^n k}{k^s}$$

Des arguments identiques montrent le même résultat pour φ sur $\mathbf{R}_+^\star$ (pour montrer la CVUTS on utilise le TSA à partir d'un certain rang).

Étude en 1^+. Pour $x > 1$ et $n \geqslant 1$,

$$\frac{1}{(n+1)^x} \leqslant \int_n^{n+1} \frac{\mathrm{d}t}{t^x}$$

donc

$$\zeta(x) - 1 \leqslant \left[\frac{t^{x+1}}{1-x}\right]_1^{+\infty} = \frac{1}{x-1} \leqslant \zeta(x)$$

et finalement

$$\zeta(x) \underset{1^+}{\sim} \frac{1}{x-1}$$

Pour aller plus loin, on note

$$f_n : x \longmapsto \frac{1}{n^x} - \int_n^{n+1} \frac{\mathrm{d}t}{t^x}$$

On a CVS car

$$\forall x \geqslant 1, \forall n \geqslant 0, \quad 0 \leqslant f_n(x) \leqslant \frac{1}{n^x} - \frac{1}{(n+1)^x} \text{ tg série CV}$$

et il y a CVU sur $[1, +\infty[$ car

$$\forall x \geqslant 1, n \geqslant 1, \quad 0 \leqslant \sum_{k=n+1}^{+\infty} f_k(x) \leqslant \sum_{k=n+1}^{+\infty} \frac{1}{k^x} - \frac{1}{(k+1)^x} = \frac{1}{(n+1)^2} \leqslant \frac{1}{n+1} \xrightarrow[n\to+\infty]{} 0$$

Ainsi,

$$S : x \longmapsto \sum_{n\geqslant 1} f_n(x)$$

est continue et

$$\zeta(s) - \frac{1}{s-1} \xrightarrow[s\to 1^+]{} S(1) = \sum_{n\geqslant 1} \lim_{s\to 1^+} f_n(s) = \sum_{n\geqslant 1} \left(\frac{1}{n} - (\ln(n+1) - \ln n)\right) = \gamma$$

donc finalement

$$\zeta(s) = \frac{1}{s-1} + \gamma + o(1)$$

Étude en $+\infty$.

$$\forall s \geqslant 1, \forall n \geqslant 1, \qquad n^s \left(\zeta(s) - \sum_{k=1}^{n} \frac{1}{k^s}\right) = \sum_{k=n+1}^{+\infty} \left(\frac{n}{k}\right)^s$$

et

$$\forall s \geqslant 2, \forall k \geqslant n+1, \qquad \left(\frac{n}{k}\right)^s \leqslant \left(\frac{n}{k}\right)^2 \text{ tg série CV (variable } k)$$

donc $\sum (\frac{n}{k})^s$ converge normalement sur $[2, +\infty[$ Une interversion des limites donne

$$\lim_{s\to+\infty} \left(\frac{n}{k}\right)^s = 0 \qquad \text{donc} \qquad \zeta(s) = \sum_{k=1}^{n} \frac{1}{k^s} + o(\frac{1}{n^s})$$

Lien entre φ et ζ.

$$\forall s \geqslant 1, \qquad -\varphi(s) + \zeta(s) = \sum_{n\geqslant 1} \frac{1-(-1)^{n-1}}{k^s} = 2\sum_{n\geqslant 1} \frac{1}{(2n)^s}$$

donc

$$\zeta(s) = \frac{1}{1 - \dfrac{1}{2^{s-1}}} \varphi(s)$$

On en déduit ainsi un prolongement de ζ sur $]0, 1[$.

12 Méthodes pour les équivalents

a) Un développement asymptotique à trois termes

On note
$$a_n = \int_0^1 \frac{\mathrm{d}t}{1+t^n}$$
On a
$$a_n - 1 = -\frac{1}{n}\int_0^1 \frac{u^{\frac{1}{n}}}{1+u}\,\mathrm{d}u$$
On note donc
$$f_n : u \longmapsto \frac{u^{\frac{1}{n}}}{1+u} \in \mathscr{C}([0,1],\mathbf{R})$$
On a la convergence simple suivante :
$$f_n(u) \xrightarrow[{[0,1]}]{\text{CVS}} \begin{cases} \dfrac{1}{1+u} & \text{si } u>0 \\ 0 & \text{sinon} \end{cases}$$
Puis
$$\forall n\in\mathbf{N}, \forall u\in[0,1], \qquad |f_n(u)| \leqslant \frac{1}{1+u} \text{ continu intégrable sur } [0,1]$$
donc par convergence dominée,
$$\int_0^1 \frac{u^{\frac{1}{n}}}{1+u}\,\mathrm{d}u \xrightarrow[n\to+\infty]{} \int_0^1 \frac{\mathrm{d}u}{1+u} = \ln 2$$
donc
$$a_n = 1 - \frac{\ln 2}{n} + o\left(\frac{1}{n}\right)$$
Puis
$$a_n - 1 + \frac{\ln 2}{n} = \frac{1}{n}\int_0^1 \frac{1-u^{\frac{1}{n}}}{1+u}\,\mathrm{d}u$$
et (Taylor-Lagrange), pour $u\in[0,1]$,
$$\left|u^{\frac{1}{n}} - 1 - \frac{1}{n}\ln u\right| \leqslant \frac{(\ln u)^2}{n^2} \sup_{[\ln(u)/n,0]} |\exp| \leqslant \frac{(\ln u)^2}{n^2}$$
En appliquant la même méthode,
$$a_n = 1 - \frac{\ln 2}{n} - \frac{1}{n^2}\int_0^1 \frac{\ln u}{1+u}\,\mathrm{d}u + o\left(\frac{1}{n^2}\right)$$

b) Étude d'une norme

Étude en 0^+. On définit
$$I(\alpha) = \left(\int_0^1 f^\alpha\right)^{\frac{1}{\alpha}} = \|f\|_\alpha$$
avec $f\in\mathscr{C}([0,1],\mathbf{R}_+^\star)$. Pour $x\in[0,1]$ fixé,
$$f^\alpha(x) = e^{\alpha\ln f(x)} = 1 + \alpha\ln(f(x)) + \varepsilon(\alpha,x)$$
donc
$$I(\alpha) = \exp\left(\frac{1}{\alpha}\ln\left(1 + \alpha\int_0^1 \ln f + \underbrace{\int_0^1 \varepsilon(\alpha,x)\,\mathrm{d}x}_{o(\alpha)?}\right)\right)$$
Taylor-Lagrange donne, si α est assez petit pour avoir $[\alpha\ln(f(x)),0]\subset[-2,2]$,
$$|\varepsilon(\alpha,x)| \leqslant \frac{(\alpha\ln f(x))^2}{2}e^2$$

donc

$$\int_0^1 \varepsilon(\alpha,x)\,\mathrm{d}x = o(\alpha)$$

et

$$I(\alpha) \xrightarrow[\alpha\to 0^+]{} \exp\left(\int_0^1 \ln f\right)$$

Étude en $+\infty$. On va montrer que $\|f\|_\alpha \xrightarrow[\alpha\to+\infty]{} \|f\|_\infty = \max|f|$ (cette valeur existe car f est définie sur un segment). On note x_0 un antécédent du maximum de $|f|$.

On suppose $x_0 \in]0,1[$. Soit $\varepsilon > 0$, $\delta > 0$ associé tel que

$$\forall x \in [x_0-\delta, x_0+\delta] \subset [0,1], \quad M - \varepsilon' \leqslant f(x) \leqslant M$$

de sorte que

$$(M-\varepsilon')^\alpha 2\delta \leqslant \int_{x_0-\delta}^{x_0+\delta} f^\alpha \leqslant \int_0^1 f^\alpha \leqslant M^\alpha$$

et

$$\underbrace{(M-\varepsilon')(2\delta)^{\frac{1}{\alpha}}}_{\xrightarrow[\alpha\to+\infty]{} M-\varepsilon'} \leqslant I(\alpha) \leqslant M$$

Donc il existe $A > 0$ tel que pour $\alpha > A$, $M - 2\varepsilon' = M - \varepsilon \leqslant I(\alpha) \leqslant M$ donc

$$I(\alpha) = \|f\|_\alpha \xrightarrow[\alpha\to+\infty]{} M = \|f\|_\infty$$

c) Une série de primitives

On note $f_0 : [a,b] \to \mathbf{R}$ continue et pour $n \geqslant 1$,

$$f_n : \begin{array}{ccc} [a,b] & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \displaystyle\int_a^x f_{n-1} \end{array}$$

Que dire de $\sum_{n\geqslant 1} f_n$?

On note $M = \|f\|_\infty = \sup\limits_{[a,b]} |f|$. Par récurrence, on montre que

$$\forall x \in [a,b], \qquad |f_n(x)| \leqslant M\frac{(x-a)^n}{n!}$$

Puis

$$\forall x \in [a,b], \qquad |f_n(x)| \leqslant M\frac{(b-a)^n}{n!} \text{ tg série CV}$$

donc $\sum f_n$ converge normalement sur $[a,b]$. On note S la somme de cette série.

Les f_n dont $\mathscr{C}^1$ donc S aussi (facile) et

$$S' = \sum_{n\geqslant 1} f_{n-1} = f_0 + S$$

Avec $S(a) = 0$, on déduit

$$\forall x \in [a,b], \qquad S(x) = e^x \int_a^x e^{-t} f_0(t)\,\mathrm{d}t$$

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre VI

Algèbre générale

Sommaire

1 Groupes

Rappel. $(G, \star)$ est un groupe ssi

- $\star$ est une loi de composition interne associative

- $\star$ a un neutre dans G
- Tous les éléments de G ont un inverse dans G pour $\star$

Notation.

Si $\star$ est commutative, on la notera en général $+$ et l'inverse sera alors noté $-x$. Sinon, on notera souvent la loi $\cdot$ et l'inverse x^{-1}. Le neutre de G se note e_G (parfois 0_G ou 0 dans le cas d'une loi notée additivement)

Si G est de cardinal fini, alors on note $|G|$ ou $\#G$ son cardinal.

2 Constructeurs de groupes

Proposition.

1. Si $(G, \cdot)$ est un groupe et X un ensemble non vide alors on muni l'ensemble de fonction de X dans G de la loi $\star$ en posant
$$\forall f, g : X \longrightarrow G, \quad f \star g : x \longmapsto f(x) \cdot g(x)$$
$(\mathscr{F}(X, G), \star)$ est alors un groupe.
2. Soit $(G, \wedge)$, $(G', \star)$ deux groupes. On munit $G \times G'$ de la loi $\cdot$ en posant
$$(x, x') \cdot (y, y') = (x \wedge x', y \star y')$$
$(G \times G', \cdot)$ est alors un groupe.

Démonstration. Facile mais pénible. □

3 Sous-groupes

Théorème – Définition.

Ⓗ $(G, \cdot)$ un groupe, $H \subset G$

Ⓒ On dira que H est un sous-groupe de G si $H \neq \varnothing$, $\cdot$ est une l.c.i. sur H et $(H, \cdot)$ est un groupe. Dans ce cas, $e_H = e_G$. Il y a équivalence entre :

(a) H est un sous-groupe de G

(b) $H \subset G$, $H \neq \varnothing$ et $\forall x, y \in H, x \cdot y^{-1} \in H$

Notation.

$(G, \cdot)$ groupe, $H \subset G$, $a \in G$.
$$aH = \{a \cdot h, \quad h \in H\}$$
$$H^{-1} = h^{-1}, \quad h \in H$$
et si $A \subset G$,
$$AH = \{a \cdot h, \quad a \in A, h \in H\}$$

Ainsi $H \subseteq G$ est un sous-groupe de G si et seulement si $H \neq \varnothing$ et $HH^{-1} \subseteq H$

Exercice.

Soient H, K des sous-groupes de G. Montrer que HK est un sous groupe si et seulement si $HK = KH$.

Résolution. Si HK sous-groupe de G alors $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. Si $HK = KH$ alors $HK(HK)^{-1} = HKK^{-1}H = HKKH = HHKK \subseteq HK$ □

a) Centre d'un groupe

Définition.

Le centre d'un groupe G est le groupe
$$Z(G) = \{x \in G, \quad \forall y \in G, xy = yx\}$$

Remarque.

C'est un sous-groupe de G, on peut le vérifier manuellement.

b) Normalisateur

On note H un sous-groupe de G. On appelle **normalisateur** de H l'ensemble

$$N(H) = \{x \in G, \quad xHx^{-1} = H\}$$

On peut vérifier que c'est un sous-groupe de G. On dira que H est un sous-groupe distingué de G si $N(H) = G$.

Remarque.

> On note $\mathscr{R}$ la relation
> $$x\mathscr{R}y \iff y^{-1}x \in H$$
> C'est bien une relation d'équivalence (réfléxive symétrique transitive) et si $a \in H$, $x \in \overline{a} \iff x \in aH$. De même, $x\mathscr{R}'y \iff xy^{-1} \in H$ définit une autre relation d'équivalence dont les classes sont les Ha. Lorsque H est distingué (on notera $H \triangleleft G$), $aH = Ha$

c) Sous-groupe de torsion

Soit G un groupe *abélien*. On note

$$\tau(G) = \{g \in G, \quad \exists n \in \mathbf{N}^\star, g^n = e_G\}$$

C'est un sous-groupe [1] de G appelé sous-groupe de torsion.

d) Sous-groupes de Z et R

On va montrer que les sous-groupe de $\mathbf{Z}$ sont de la forme $d\mathbf{Z}$, et d est unique au signe près. On va pour cela montrer la propriété plus générale suivante (hors-programme) : si A est un anneau euclidien, alors c'est un anneau principal.

Définition (Hors-Programme).

> Un anneau A commutatif est dit euclidien lorsqu'il existe une application $v : A \setminus \{0\} \to \mathbf{N}$ qui satisfait les propriétés suivantes :
>
> 1. $$\forall (a,b) \in A \times A \setminus \{0\}, \exists q, r \in A, \qquad a = qb + r \quad \text{et} \quad r = 0 \text{ ou } v(r) < v(b)$$
> 2. $$\forall a, b \in A \setminus \{0\}, \qquad v(b) \leqslant v(ab)$$
>
> Une telle application sera appelée **stathme euclidien** sur A. Une application qui ne satisfait que la première propriété sera appelée **préstathme euclidien** sur A.
> Un anneau A commutatif sera dit principal lorsque tous ses idéaux [a] (sous-groupes I de $(A,+)$ tels que pour tout $a \in A$, $aI \subset I$) sont principaux (i.e. de la forme aA)
>
> a. notion abordée plus en détail dans la section **Idéal d'un anneau**

L'anneau $\mathbf{Z}$ est euclidien (la valeur absolue est un stathme euclidien sur $\mathbf{Z}$). Si H est un sous-groupe de $\mathbf{Z}$ alors pour tout $k \in \mathbf{Z}$, $kH = H + H + \cdots + H \subset H$ donc H est un idéal de l'anneau $\mathbf{Z}$. Il sera donc suffisant de montrer que tout anneau euclidien est principal.

Proposition (Hors-Programme).

> Un anneau euclidien est principal

Démonstration. Soit A un anneau commutatif euclidien (de stathme v), et I un idéal de A. On va montrer que I s'écrit aA pour un $a \in A$. Si $I = \{0\}$ alors $a = 0$ convient.

On suppose $I \neq \{0\}$. L'ensemble $v(I \setminus \{0\})$ admet un minimum, on note $a \in I \setminus \{0\}$ un élément minimal pour v. On a clairement $aA \subset I$ car $a \in I$ et I idéal. On prend $b \in I$ et

$$\exists q, r, \qquad b = qa + r \quad \text{et} \quad r = 0 \text{ ou } v(r) < v(a).$$

On a $r = b - qa \in I$ donc $v(r) < v(a)$ est impossible par définition de a, donc $r = 0$ et $b = qa$. On a donc $I \subset aA$ d'où $aA = I$ □

1. on a besoin de l'hypothèse de commutativité de G, ça n'est pas vrai sinon

Remarque.

Si I est un idéal principal, il s'écrit $I = aA$. S'il s'écrit également $a'A$ alors $a \mid a'$ et $a' \mid a$ donc $a = \varepsilon a'$ pour $\varepsilon \in \mathscr{U}(A)$ (le groupe des inversibles de A). Dans $\mathbf{Z}$, les inversibles sont -1 et 1, d'où l'unicité du générateur positif.

Remarque.

On aurait pu écrire la démonstration directement pour $A = \mathbf{Z}$, $v : x \mapsto |x|$

On va maintenant montrer qu'un sous groupe H non trivial de $\mathbf{R}$ est soit dense dans $\mathbf{R}$ soit de la forme $a\mathbf{Z}$. On note $\ell = \inf H \cap \mathbf{R}_+^\star$. Il y a deux cas :

- $\ell > 0$. Si $l \notin H$ alors il existe $a \in \mathbf{R}_+^\star$ tel que $a \in]\ell, 2\ell[$ et $a \in H$, il existe $b \in H$ tel que $b \in]\ell, a[$ donc $a - b \in H \cap \mathbf{R}_+^\star$ ce qui est absurde car $a - b > \ell$ par définition de ℓ. Donc $\ell \in H$ et $\ell\mathbf{Z} \subset H$. Pour l'autre inclusion, fait comme pour $\mathbf{Z}$: on écrit $x = \lfloor x/\ell \rfloor \ell + r$ et $r = 0$.
- $\ell = 0$. Soient $0 < x < y$. Il existe $\alpha \in H \cap \mathbf{R}_+^\star$ tel que $0 < \alpha < y - x$ et

$$x < \underbrace{\left\lfloor \frac{x}{\alpha} \right\rfloor}_{\in H} + \alpha < x + y - x = y$$

donc H est dense dans $\mathbf{R}$ (les autres configurations de x et y se traitent similairement)

Par exemple, $a\mathbf{Z} + b\mathbf{Z}$ est dense dans $\mathbf{R}$ si et seulement si $\frac{a}{b} \notin \mathbf{Q}$, de sorte que $\cos(\mathbf{N})$ est dense dans $\mathbf{R}$ car $\mathbf{Z} + 2\pi\mathbf{Z}$ est dense dans $\mathbf{R}$

4 Opérations sur les sous-groupes

Proposition.

(H) $(H_i)_{i\in I}$ famille de sous-groupes de G

(C) L'ensemble

$$\bigcap_{i\in I} H_i$$

est un sous-groupe de G

Remarque.

En général, l'union de deux sous-groupes n'est pas un sous-groupe

5 Sous-groupes engendrés

Théorème – Définition.

(H) $(G, \cdot)$ un groupe, $A \subset G$, $S_A = \{H \in \mathscr{P}(G), A \subset H, H \text{ sg de } G\}$

(C)

1. On appelle sous-groupe engendré par A l'ensemble

$$\langle A \rangle = \bigcap_{H \in S_A} H$$

2. Si H est un sous-groupe de G contenant A alors $\langle A \rangle \subseteq H$
3. $$\langle A \rangle = \{e_G\} \cup \{x_1 \cdots x_n, \quad n \in \mathbf{N}, x_1, \cdots, x_n \in A \cup A^{-1}\}$$

Démonstration.

3. On note $E = \{e_G\} \cup \{x_1 \cdots x_n, \quad n \in \mathbf{N}, x_1, \cdots, x_n \in A \cup A^{-1}\}$. On a

$$E \subset \langle A \rangle \qquad \text{car } A, A^{-1} \subset \langle A \rangle$$

et $A \subset E$ donc $\langle A \rangle \subset E$ par 2. donc $E = \langle A \rangle$

□

Exemple. • $\langle \exp\left(\frac{2i\pi}{n}\right)\rangle = \mathbb{U}_n$
- $\mathbf{Z} = \langle 1\rangle = \langle 2, 3\rangle$
- $\mathfrak{S}_n = \langle \tau_{1,2}, (1\ \cdots\ n)\rangle$

Définition.
Un groupe G est dit monogène s'il existe $a \in G$ tel que $G = \langle a\rangle$. Si de plus G est fini, on dira qu'il est cyclique

6 Morphismes

Définition.
Soient $(G, \cdot), (G', \star)$ deux groupes. Une application $f : G \to G'$ est un morphisme ssi

$$\forall x, y \in G, f(x \cdot y) = f(x) \star f(y)$$

Notation.
$f : G \to G'$ est un endomorphisme ssi c'est un morphisme. C'est un isomorphisme si c'est une bijection. Si $G = G'$, on dira qu'un morphisme de G dans G' est un endomorphisme de G. Un endomorphisme bijectif est appelé automorphisme. On note $\mathrm{Hom}(G, G')$ l'ensemble des morphisme de G dans G' et $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

Proposition.

H $f \in \mathrm{Hom}(G, G')$

C
1. $f(e_G) = e_G$
2. $\forall x \in G, \quad f(x^{-1}) = f(x)^{-1}$
3. On note $\mathrm{Ker}\, f = f^{-1}(\{e_G\})$.
   (a) $\mathrm{Ker}\, f$ est un sous groupe de G
   (b) f est injective si et seulement si $\mathrm{Ker}\, f = \{e_G\}$
4. f^{-1} est un isomorphisme si f est un isomorphisme.
5. $g \circ f$ est un morphisme si $f : G \to G'$ et $g : G' \to G''$ le sont

Conséquence 1. $(\mathrm{Aut}(G), \circ)$ est un groupe

Conséquence 2. Les $i_a : x \in G \longmapsto axa^{-1}$ pour $a \in G$ sont appelés automorphismes intérieurs. $\varphi : a \longmapsto i_a$ est un morphisme.

Les morphismes ont la propriété intéressante suivante :

Proposition.
L'image et la préimage d'un groupe par un morphisme est un groupe.

Démonstration. Facile mais pénible □

7 Groupes finis

a) Théorème de Lagrange

On note G un groupe fini et H un sous groupe de G. On va montrer que $|H|$ divise $|G|$. On a vu que

$$x\mathscr{R}y \iff x^{-1}y \in H$$

définit une relation d'équivalence sur G, les classes d'équivalence forment donc une partition de G. On a ainsi ($\sqcup$ désigne l'union disjointe)

$$G = \bigsqcup_{i=1}^{p} a_i H \implies |G| = p|H|$$

b) $|G| = |\operatorname{Ker} f| \cdot |\operatorname{Im} f|$

On note G un groupe fini et $f : G \to G'$ un morphisme. On note $\operatorname{Im} f = \{y_1, \cdots, y_p\}$ de sorte que

$$G = \bigsqcup_{i=1}^{p} f^{-1}(\{y_i\}) \implies |G| = \sum_{i=1}^{p} \left|f^{-1}(\{y_i\})\right|$$

On se donne $y \in \operatorname{Im} f$ fixé et $x \in f^{-1}(\{y\})$. On pose

$$\varphi : t \in \operatorname{Ker} f \longmapsto xt \in f^{-1}(\{y\}).$$

Cette application est injective et si $u \in f^{-1}(\{y\})$ alors $u = \varphi(x^{-1}u)$ donc elle est aussi surjective. Elle est donc bijective, d'où

$$|f^{-1}(\{y\})| = |\operatorname{Ker} f| \quad \implies \quad |G| = |\operatorname{Ker} f| \cdot |\operatorname{Im} f|$$

c) Ordre d'un élément

Définition – Proposition.

(H) G un groupe fini, $a \in G$

(C)
1. $\varphi : \mathbf{Z} \longrightarrow G, n \longmapsto a^n$ est un morphisme. Il existe un unique entier naturel non nul tel que $\operatorname{Ker}\varphi = d\mathbf{Z}$, qu'on appelle **ordre** de a dans G, noté $\operatorname{ord}_G(a)$ ou $\operatorname{ord}(a)$
2. $\operatorname{ord}(a) = |\langle a\rangle| = \min\{n \in \mathbf{N}^\star, a^n = e_G\}$
3. $a^n = e_G \iff \operatorname{ord}(a) \mid n$ et
$$\operatorname{ord}(a^p) = \frac{\operatorname{ord}(a)}{p \wedge \operatorname{ord}(a)}$$

Démonstration.

1. φ n'est pas injective car G fini donc $\operatorname{Ker}\varphi$ est un sous-groupe non trivial de $\mathbf{Z}$, ce qui conclut
2. $d = \min \operatorname{Ker}\varphi \cap \mathbf{N}^\star = \min\{n \in \mathbf{N}^\star, a^n = e_G\}$ puis
$$a^k = a^{dq+r} = a^r$$
avec $r \in [\![0, d-1]\!]$ donc $\langle a\rangle = \{e_G, a, \cdots, a^{d-1}\}$ et pour $0 \leqslant r_1 < r_2 < d$, $a^{r_1} = a^{r_2} \implies r_2 - r_1 \in d\mathbf{Z} \cap]\!]0, d-1[\![$ absurde donc $|\langle a\rangle| = d$
3. $a^n = e_G \iff n \in \operatorname{Ker}\varphi = d\mathbf{Z} \iff d \mid n$ puis
$$(a^p)^{\frac{\operatorname{ord}(a)}{p\wedge\operatorname{ord}(a)}} = a^{k\operatorname{ord}(a)} = e_G \quad \text{donc} \quad \operatorname{ord}(a^p) \,\Big|\, \frac{\operatorname{ord}(a)}{p \wedge \operatorname{ord}(a)}$$
et
$$(a^p)^{\operatorname{ord}(a^p)} = e_G \implies \operatorname{ord}(a) \,\Big|\, p\operatorname{ord}(a^p) \implies \frac{\operatorname{ord}(a)}{p \wedge \operatorname{ord}(a)} \,\Big|\, \frac{p}{p \wedge \operatorname{ord}(a)} \times \operatorname{ord}(a^p)$$
donc par le lemme de Gauss,
$$\frac{\operatorname{ord}(a)}{p \wedge \operatorname{ord}(a)} \,\Big|\, \operatorname{ord}(a^p)$$
d'où l'égalité

□

Remarque.

Si G est fini abélien et $a, b \in G$,

$$(ab)^{\operatorname{ord}(a)\vee\operatorname{ord}(b)} = e_G \implies \operatorname{ord}(ab) \mid \operatorname{ord}(a) \vee \operatorname{ord}(b)$$

Si $\operatorname{ord}(a)$ et $\operatorname{ord}(b)$ sont premiers entre eux alors

$$(ab)^{\operatorname{ord}(ab)\operatorname{ord}(b)} = e_G = a^{\operatorname{ord}(ab)\operatorname{ord}(b)} \implies \operatorname{ord}(a) \mid \operatorname{ord}(b)\operatorname{ord}(ab) \underset{\text{Gauss}}{\implies} \operatorname{ord}(a) \mid \operatorname{ord}(ab)$$

et par symétrie, $\operatorname{ord}(b) \mid \operatorname{ord}(ab)$ don $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$

Proposition.

(H) $(G, \cdot)$ groupe fini, $a \in G$

(C) $\mathrm{ord}(a) \mid \#G$

Démonstration. C'est évident avec le théorème de Lagrange. Sinon,

$$\prod_{x \in G} x = \prod_{x \in G} ax = a^{|G|} \prod_{x \in G} x \implies a^{|G|} = e_G$$

□

d) Groupe de cardinal p^2

On note p un nombre premier et on suppose que G est un groupe d'ordre p^2. Les seuls ordres possibles sont $1, p$ et p^2. S'il y a un élément d'ordre p^2, alors $G = \langle a \rangle$ est abélien et a^p est d'ordre p. Sinon, tous les éléments sont d'ordres p. Dans les deux cas, il y a un élément d'ordre p.

e) Groupe de cardinal divisible par p

On note p premier et G un groupe d'ordre kp. On va montrer qu'il existe un élément d'ordre p. Il suffit de montrer qu'un élément est d'ordre p. On note

$$E = \{(x_1, \cdots, x_p) \in G^p, \quad x_1 \cdots x_p = e_G\} \qquad \#E = \#G^{p-1}.$$

Cet ensemble est stable par permutation circulaire (car $x_1 \cdots x_p = e_G \implies x_2 \cdots x_p x_1 = e_G$). On note σ la permutation circulaire $(1\ \ 2\ \ \cdots\ \ p)$. On va faire agir $\langle \sigma \rangle$ sur E. Pour $C \in \mathfrak{S}_n$, $x = (x_1, \cdots, x_p) \in E$, on note $C.x = (x_{\sigma(1)}, \cdots, x_{\sigma(p)})$.

Pour $x \in E$, on note $O_x = \{C.x, C \in \langle \sigma \rangle\}$ l'orbite de x. La relation $x\mathscr{R}y \iff y \in O_x$ est une relation d'équivalence sur E de sorte que les O_x forment une partition de E. On note

$$\varphi_x : c \in \langle \sigma \rangle \longmapsto c.x \in O_x.$$

Si φ_x est injective alors $O_x = \operatorname{Im} \varphi_x$ et $|O_x| = |\langle \sigma \rangle| = p$. Sinon, il existe $1 \leqslant k_1 < k_2 \leqslant p$ tel que $\sigma^{k_1}.x = \sigma^{k_2}.x$ donc $\sigma^{k_2 - k_1}.x = x$. On a alors $\forall n \geqslant 0, \sigma^n.x = \sigma^{n+k_2-k_1}.x$ donc $\forall i \in [\![1, p]\!]$, $x_i = x_{i+n(k_2-k_1) \pmod p}$ or $k_2 - k_1$ engendre $(\mathbf{Z}_p, +)$ (car p premier) donc $(n(k_2 - k_1))_n$ parcourt tous les entiers modulo p et $x = (x_1, \cdots, x_1)$, d'où finalement $\#O_x = 1$

Ainsi, les orbites sont de cardinal p ou 1. On note $O_{x_1}, \cdots, O_{x_r}$ les orbites de cardinal p et $O_{x'_1}, \cdots, O_{x'_s}$ celles de cardinal 1. On a

$$\#E = rp + s = \#G^{p-1} \equiv 0 \pmod p \implies r \equiv 0 \pmod p$$

donc $r \geqslant p \geqslant 2$ et il existe $x = (a, \cdots, a) \neq (e_G, \cdots, e_G)$ dans E, donc $a^p = e_G$ et $a \neq e_G$ donc $\mathrm{ord}(a) = p$ (car p premier n'est divisible que par 1 et p).

f) Moyenne dans un groupe

On note E un K-e.v., G un sous-groupe de $\mathrm{GL}(E)$ fini d'ordre n. On note

$$p = \frac{1}{|G|} \sum_{g \in G} g$$

Si $g_0 \in G$, alors $g \longmapsto g_0 \circ g$ est bijective et

$$g_0 p = \frac{1}{|G|} \sum_{g \in G} g_0 g = p = p g_0$$

donc

$$p \circ p = p \circ \left(\frac{1}{|G|} \sum_{g \in G} g \right) = \frac{1}{|G|} \sum_{g \in G} \underbrace{pg}_{=p} = \frac{1}{|G|} |G| p = p$$

donc p est un projecteur

Exercice.

- [3/2] On note $f \in \mathscr{L}(E)$,
$$f^\star = \frac{1}{|G|}\sum_{g\in G} g^{-1}\circ f\circ g$$
Montrer que $f^\star$ commute avec les éléments de G et $f^{\star\star} = f^\star$
- [5/2] Montrer que si F est un s.e.v stable par tous les éléments de G alors il a un supplémentaire stable par tous les éléments de G.

8 Groupes cycliques

Définition.

Un groupe cyclique est un groupe fini monogène

a) Sous-groupes d'un groupe cyclique

On note $G = \langle a\rangle$ cyclique d'ordre n. On note H un sous-groupe de G, et $r = \min\{p \in \mathbf{N}^\star, a^p \in H\}$. On a

- $\langle a^r\rangle \subseteq H$
- Soit $x = a^m \in H$. On écrit $m = rq + s$, $s \in [\![0, r-1]\!]$ de sorte que $a^s \in H$ donc $s = 0$ et donc $x \in \langle a^p\rangle = H$

Ainsi, H est cyclique.

b) Générateurs d'un groupe cyclique

Avec les mêmes notations, on considère
$$\varphi : n \longmapsto \{k \in [\![1, n]\!],\quad k\wedge n = 1\}.$$
On appelle cette application l'indicatrice d'Euler. $g = a^p$ est un générateur de G ssi $\mathrm{ord}(a^p) = n$ ssi $n = \frac{n}{p\wedge n}$ ssi $p\wedge n = 1$. Il y a donc $\varphi(n)$ générateurs de G.

Plus généralement, il y a $\varphi(d)$ éléments d'ordre d (on peut le voir en appliquant ce raisonnement à un sous-groupe d'ordre $d \mid n$). On a ainsi
$$\sum_{d\,\mid\,n}\varphi(d) = n$$

c) Sous-groupes d'ordre d

On note H un sous-groupe de cardinal d de G (donc d divise n).

- H a $\varphi(d)$ générateurs (donc d'ordre d)
- G a $\varphi(d)$ éléments d'ordre d

donc H contient tous les éléments d'ordre d, il est donc unique.

9 Le groupe $\mathfrak{S}_n$

Le n-ième groupe symétrique $(\mathfrak{S}_n, \circ)$ est un groupe d'ordre $n!$. On note $\tau_{i,j}$ la transposition de support $\{i, j\}$. Si $\sigma \in \mathfrak{S}_n$, alors σ s'identifie au n-uplet
$$(\sigma(1), \cdots, \sigma(n))$$
On note $c = (i_1\ \ i_2\ \ \cdots\ \ i_p)$ la permutation
$$c : n \in [\![1, n]\!] \longmapsto \begin{cases} i_{k+1} & \text{si } n = i_k, k < p\\ i_1 & \text{si } n = i_p\\ n & \text{sinon}\end{cases}$$
On dira que c est un cycle de support $\{i_1, \cdots, i_p\}$ et d'ordre[2] p (on prend les i_k deux à deux distincts)

2. il s'agit bien de l'ordre au sens de $\mathrm{ord}_{\mathfrak{S}_n}(c)$

a) Décomposition en cycles

On note $\sigma \in \mathfrak{S}_n$ et $O_1, \cdots O_p$ les orbites pour l'action de $\langle \sigma \rangle$ sur $[\![1, n]\!]$ (c'est à dire les classes d'équivalence pour $x\mathscr{R}y \iff \exists k, y = \sigma^k(x)$)

Les orbites s'écrivent $O_k = \{i_k, \sigma(i_k), \cdots, \sigma^{p_k}(i_k)\}$. On note $c_k = (i_k \;\; \sigma(i_k) \;\; \cdots \;\; \sigma^{p_k}(i_k))$ de sorte que

$$\sigma = c_1 \circ \cdots \circ c_p$$

On a alors

$$\sigma^k = \mathrm{id} \iff c_1^k = \cdots = c_p^k = \mathrm{id} \iff \mathrm{ord}(c_1) \vee \cdots \vee \mathrm{ord}(c_p) \mid k$$

b) Signature

Une inversion pour $\sigma \in \mathfrak{S}_n$ est un couple $(i, j) \in [\![1, n]\!]^2$ tel que $i < j$ et $\sigma(j) < \sigma(i)$. On note N_σ le nombre de ces inversions et

$$\varepsilon : \sigma \longmapsto (-1)^{N_\sigma}$$

est appelée **signature** de σ

Proposition.

1. $$\forall \sigma \in \mathfrak{S}_n, \qquad \varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j} = \prod_{\{i,j\} \in \mathscr{P}_2([\![1,n]\!])} \frac{\sigma(i) - \sigma(j)}{i - j}$$
2. $\varepsilon : \mathfrak{S}_n \to \mathbb{U}_2$ est un morphisme
3. La signature d'une transposition vaut -1

Démonstration.

1. La seconde égalité est claire. Puis,
$$\left| \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j} \right| = \frac{\prod_{i<j} |\sigma(i) - \sigma(j)|}{\prod_{i<j} |i - j|} = 1$$
et le signe est bon.
2. $\sigma, \sigma' \in \mathfrak{S}_n$.
$$\varepsilon(\sigma \circ \sigma') = \prod_{i<j} \frac{\sigma \circ \sigma'(i) - \sigma \circ \sigma'(j)}{\sigma'(i) - \sigma'(j)} \times \frac{\sigma'(i) - \sigma'(j)}{i - j} = \varepsilon(\sigma)\varepsilon(\sigma')$$
3. On compte les inversions de $\tau_{1,2}$ et $\sigma \circ \tau_{i,j} \circ \sigma^{-1} = \tau_{1,2}$.

□

c) Théorème de Cayley

On note $G = \{g_1, \cdots, g_n\}$ un groupe fini. On a

$$\varphi : G \to \mathfrak{S}(G), x \longmapsto (t \longmapsto xt)$$

Cette application est injective car

$$\varphi(x) = \varphi(x') \implies \varphi(x)(e_G) = \varphi(x')(e_G) \implies x = x'$$

C'est un morphisme car $\varphi(xx')(t) = xx't = x\varphi(x')(t) = \varphi(x) \circ \varphi(x')(t)$. Ainsi, G est isomorphe à $\varphi(G)$ sous-groupe de $\mathfrak{S}(G)$ qui est isomorphme à $\mathfrak{S}_n$. Donc, G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

10 Anneaux et corps

Définition.

Un ensemble A muni des lois $+$ et $\times$ est un anneau si

- $(A, +)$ est un groupe abélien de neutre 0_A
- $(A \setminus \{0\}, \times)$ est un monoïde [a] de neutre 1_A
- $\times$ est distributive par rapport à $+$

a. mêmes hypothèses que la structure de groupe sans l'inversibilité

Définition.

Un anneau commutatif est intègre si tous ses éléments sont réguliers pour $\times$

Définition.

$(A, +, \times)$ est un corps si $(A \setminus \{0\}, \times)$ est un groupe abélien.

Remarque.

Un anneau intègre fini est un corps, car $\forall a \in A \setminus \{0\}, x \longmapsto ax$ est injective donc bijective donc tous les éléments sont inversibles.

a) Calcul dans un anneau

Proposition (Binôme de Newton).

(H) $a, b \in A$ un anneau, $ab = ba$.

(C)

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Démonstration. Vu en sup, facile mais long. [3] □

Remarque.

On prend la convention

$$\forall k \notin [\![0, n]\!], \qquad \binom{n}{k} = 0$$

La formule du binôme se généralise ainsi : pour $a_1, \cdots, a_p \in A$ qui commutent 2 à 2 et pour $n \in \mathbf{N}$,

$$(a_1 + \cdots + a_p)^n = \sum_{a_1 + \cdots + a_p = n} \binom{n}{n_1, \cdots, n_p} a_1^{n_1} \cdots a_p^{n_p}$$

avec

$$\binom{n}{n_1, \cdots, n_p} = \frac{n!}{n_1! \cdots n_p!}$$

Pour le voir, on va développer $(a_1 + \cdots + a_p) \times \cdots \times (a_1 + \cdots + a_p)$. On obtient une somme de termes en $a_1^{n_1} \cdots a_p^{n_p}$ avec $n_1 + \cdots + n_p = n$.

- Il y a $\binom{n}{n_1}$ blocs pour a_1
- Il y a $\binom{n-n_1}{n_2}$ pour a_2
- $\cdots$
- Il y a $\binom{n-n_1-\cdots-n_{p-1}}{n_p}$ blocs pour a_p

Donc les coefficients valent

$$\prod_{i=1}^{p} \binom{n - n_1 - \cdots - n_{i-1}}{n_i} = \frac{n!}{n_1! \cdots n_p!} = \binom{n}{n_1, \cdots, n_p}$$

Techniques pour les sommes de coefficients binomiaux

3. «Moralement, c'est vrai»

- $(1+X)^p(1+X)^q = (1+X)^{p+q}$ donc

$$\binom{p+q}{\ell} = \sum_{i+j=\ell} \binom{p}{i}\binom{q}{j}$$

En particulier,

$$\binom{2n}{n} = \sum_{i=0}^{p} \binom{p}{i}^2$$

- Si on note $S : x \longmapsto (1+x)^n$

$$S'(x) = n(1+x)^{n-1} = \sum_{k=0}^{n} \binom{n}{k} k x^{k-1}$$

donc

$$\sum_{k=0}^{n} \binom{n}{k} k = n 2^{n-1}$$

- **Sommes lacunaires** : On note $p \in \mathbf{N}^\star$ fixé, on va calculer

$$S_n = \sum_{pk \leqslant n} \binom{n}{pk}$$

On note $\omega = \exp\left(\frac{2i\pi}{p}\right)$ de sorte que

$$1 + \omega^k + \cdots + \omega^{(p-1)k} = \begin{cases} p & \text{si } w^k = 1 \text{ i.e. } p \mid k \\ 0 & \text{sinon} \end{cases}$$

On pose $f(x) = (1+x)^n$ et

$$f(1) + f(\omega) + \cdots + f(\omega^{p-1}) = \sum_{k=1} \binom{n}{k} (1 + \cdots + \omega^{k(p-1)}) = pS_n$$

d'où

$$S_n = \frac{1}{p}\left(f(1) + \cdots + f(\omega^{p-1})\right)$$

b) Élément nilpotent

Définition.

> Un élément $a \in A$ (A est un anneau) est **nilpotent** si il existe un entier naturel n tel que $a^n = 0_A$. On appelle **indice de nilpotence** l'entier naturel minimal tel que $a^n = 0_A$

Si a, b sont nilpotents et commutent alors

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k} = 0_A$$

avec n et m les indices de nilpotence respectifs de a et b. Ainsi, $a+b$ est nilpotent. Si A est un anneau commutatif alors l'ensemble $\mathcal{N}$ des éléments nilpotents est un idéal de A. Pour a nilpotent, $a^n = 0_A$ et

$$1 = 1 - a^n = (1-a)(1 + a + \cdots + a^{n-1})$$

donc $a - 1$ est inversible.

11 Constructeurs d'anneaux, sous-anneaux, sous-corps

Comme pour les groupes, si A, A' sont des anneaux et X un ensemble non vide, $A \times A'$ a une structure d'anneau et $\mathfrak{F}(X, A)$ aussi

Définition – Proposition.

1. On dira que A' est un sous-anneau de A si
   - $A' \subset A$
   - $1_A \in A$
   - $\forall x, y \in A', x - y \in A'$ et $xy \in A'$
2. On dira que K' est un sous-corps de K si
   - $K' \subset K$
   - $1_K \in K$
   - $\forall x, y \in K', x - y \in K'$ et si $y \neq 0$, $xy^{-1} \in K'$

Exemple.

- $\mathbf{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbf{R}$
- $\mathbf{Q}[\sqrt{2}]$ est un sous-corps de $\mathbf{R}$ qu'on note $\mathbf{Q}(\sqrt{2})$
- $\mathbf{Q}[\omega]$ pour ω algébrique est un sous-corps de $\mathbf{R}$ (c'est un espace vectoriel de dimension finie et φ : $t \longmapsto tx$ est injective donc bijective car linéaire ce qui montre l'inversibilité)

Remarque.

Si on fixe n et on note

$$S_n = \left\{ \sum_{i=1}^{n} x_i^2 \ , \qquad x_1, \cdots, x_n \in K \right\}$$

alors on peut montrer que S_n est stable par $\times$ si $n = 2^k$

12 Idéal d'un anneau

Définition.

Un idéal à gauche (resp. à droite) $I \subset A$ d'un anneau A est un sous-groupe de $(A, +)$ tel que

$$\forall a \in A, x \in I, \quad ax \in I \quad (\text{resp. } xa \in I)$$

Un idéal bilatère (ou simplement idéal) est un idéal à gauche et à droite.

Remarque.

Pour un anneau commutatif A et $a \in A$, $I = aA$ est un idéal.

L'ensemble des idéaux d'un anneau commutatif est stable par somme et par intersection. De plus, si I et J sont des idéaux, alors

$$IJ \underset{\text{def}}{=} \left\{ \sum_{k \in K} i_k j_k, \quad K \subset \mathbf{N} \text{ fini }, i_k \in I, j_k \in J \right\}$$

est aussi un idéal. Le radical $\sqrt{I}$ de I, définit par

$$\sqrt{I} \underset{\text{def}}{=} \{x \in A, \quad \exists n \in \mathbf{N}, x^n \in I\},$$

est également un idéal (c'est un sous-groupe par binôme de Newton).

Définition (Hors-Programme).

Un anneau A est principal si tous ses idéaux sont principaux, c'est à dire de la forme $I = aA$. Un anneau est noéthérien si toute suite croissante d'idéaux est stationnaire

Exercice.

Décrire les idéaux de $\mathbf{K}^2$ pour un corps $\mathbf{K}$

13 Groupe des inversibles d'un anneau

Pour un anneau A, on note $A^\star$ le groupe des inversibles de A.

Exemple. On note $A = \mathbf{Z}[\sqrt{2}]$, on va décrire $\mathbf{Z}[\sqrt{2}]^\star$.

On note $G = \mathbf{Z}[\sqrt{2}]^\star$ de sorte que $G_+ = G \cap \mathbf{R}_+^\star$ est un groupe pour $\times$. Le logarithme est un morphisme injectif donc $\ln(G_+)$ est un sous-groupe de $\mathbf{R}$, donc dense si et seulement si $a = \inf(\ln(G_+) \cap \mathbf{R}_+^\star) = 0$.

On a $e^a = \inf(G_+ \cap]1; +\infty[)$ et

$$1 \leqslant e^a < 1 + \sqrt{2} \implies \exists p, q \in \mathbf{Z}, 1 \leqslant e^a \leqslant \underbrace{p + q\sqrt{2}}_{\in G_+} < 1 + \sqrt{2}$$

Si $p > 0, q < 0$ alors $1 \leqslant p + q\sqrt{2} \leqslant p - q\sqrt{2} < p^2 - 2q^2 = 1$ (la dernière égalité vient de l'inversibilité de $p + \sqrt{2}q$, cf. remarque). C'est absurde. On arrive à la même conclusion si $p < 0, q > 0$. On a donc $e^a = 1 + \sqrt{2}$ et $G = \langle 1 + \sqrt{2} \rangle$

Remarque.

Dans un anneau euclidien A de stathme v, les éléments inversibles sont exactement les éléments qui minimisent le stathme. Si u minimise le stathme, $1 = qu + r$ avec $r = 0$ ou $v(r) < v(u)$ donc $r = 0$ et $1 = qu$ donc u inversible. Sinon, $v(u) > v(1)$ donc $v(u) \geqslant 2$ donc $\forall q, 2 \leqslant v(uq)$ donc u n'est pas inversible.
Par exemple, dans $\mathbf{Z}$ euclidien pour le stathme $|\cdot|$, les inversibles sont -1 et 1. Dans $\mathbf{Q}[X]$ euclidien pour le stathme deg, les inversibles sont tous les polynômes de degré 0 (les polynômes constants).

14 Morphismes d'anneaux

Définition.

Pour A, A' des anneaux, $\varphi : A \to A'$ est un morphisme d'anneau si

- $f(1_A) = 1_{A'}$
- $\forall x, y \in A, f(x + y) = f(x) + f(y)$
- $\forall x, y \in A, f(xy) = f(x)f(y)$

Comme dans les groupes ou les espaces vectoriels (dans les e.v. les applications linéaires jouent le rôle de morphismes), les morphismes d'anneaux préservent la structure (l'image et la préimage d'un anneau par un morphisme est un anneau).

15 Structure d'algèbre

Définition.

On note $(A, +, \times, \cdot)$ muni de deux lois internes $+$ et $\times$ et d'une loi externe $\cdot$ sur le corps K. On dira que A est une K-algèbre si $(A, +, \times)$ est un anneau, $(A, +, \cdot)$ est un K-e.v, et

$$\forall \lambda \in K, \forall x, y \in A, \lambda \cdot (x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y)$$

Remarque.

Un corps K est toujours une K-algèbre, la multiplication servant de loi interne et externe.

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre VII

Arithmétique

Sommaire

1 Arithmétique classique

a) Rappels

On se place dans l'anneau $(\mathbf{Z}, +, \times)$, et on note $\mathbb{P}$ l'ensemble des nombres premiers.

Théorème (Division Euclidienne).

Pour $a, b \in \mathbf{Z}$, b non nul, il existe des uniques entiers q, r tels que

$$a = qb + r \qquad \text{et } 0 \leqslant r < |b|$$

Remarque.

L'existence d'un tel r montre que $\mathbf{Z}$ est euclidien pour le stathme $|\cdot|$

Théorème (Théorème fondamental de l'arithmétique).

Tout entier relatif n non nul s'écrit de manière unique (à l'ordre près des facteurs et à une constante inversible près) comme produit de puissances de premiers :

$$\forall n \in \mathbf{Z}^\star, \exists! p_1, \cdots, p_r \in \mathbb{P}, \exists! \alpha_1, \cdots, \alpha_r \in \mathbf{N}^\star, \exists \varepsilon \in \mathscr{U}_{\mathbf{Z}} = \{-1, 1\}, \qquad n = \varepsilon p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Théorème – Définition (Bézout, PGCD).

Pour $a, b \in \mathbf{Z}$, il existe un unique entier positif d tel que $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$. On appelle cet entier le PGCD de a et b, et on le note $d = a \wedge b = (a, b) = \mathrm{PGCD}(a, b)$. Si $d = a \wedge b$ alors il existe $u, v \in \mathbf{Z}$ tels que $au + bv = d$ (c'est la propriété de Bézout)

Remarque.

Cette définition du PGCD coïncide avec la définition usuelle.

Théorème – Définition (Identité de Bézout, Coprimalité).

Deux entiers a et b sont dits premiers entre eux si les ensembles de leurs diviseurs stricts sont disjoints. C'est équivalent à

$$\exists u, v \in \mathbf{Z}, \qquad au + bv = 1$$

Théorème (Lemme de Gauss).

Si $a, b, c \in \mathbf{Z}$ et $a \wedge c = 1$ alors

$$a \mid bc \implies a \mid b$$

b) Utilisation d'un Vandermonde

On note $a_1, \cdots, a_n \in \mathbf{Z}$. On veut montrer que

$$\prod_{1 \leqslant i < j \leqslant n} (j - i) \,\Bigg|\, \prod_{1 \leqslant i < j \leqslant n} (a_j - a_i)$$

On introduit

$$\Delta(X_1, \cdots, X_n) = \begin{vmatrix} \binom{X_1}{0} & \cdots & \binom{X_1}{n-1} \\ \vdots & \ddots & \vdots \\ \binom{X_n}{0} & \cdots & \binom{X_n}{n-1} \end{vmatrix} \qquad \text{avec } \binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!}$$

On a

$$\binom{X}{n-1} = \frac{X^{n-1}}{(n-1)!} + \underbrace{c_{n-2}X^{n-2} + \cdots + c_0}_{\in \mathrm{Vect}\left(\binom{X}{0}, \cdots, \binom{X}{n-2}\right)}$$

de sorte que dans le déterminant on peut remplacer la dernière colonne par

$$\begin{pmatrix} \frac{X_1^{n-1}}{(n-1)!} \\ \vdots \\ \frac{X_n^{n-1}}{(n-1)!} \end{pmatrix}$$

et en itérant sur les colonnes de droite à gauche,

$$\Delta(X_1, \cdots, X_n) = \begin{vmatrix} 1 & \frac{X_1}{1} & \cdots & \frac{X_1^{n-1}}{(n-1)!} \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 1 & \cdots & \cdots & \frac{X_n^{n-1}}{(n-1)!} \end{vmatrix}$$

et

$$\Delta(a_1, \cdots, a_n) = \frac{1}{1!2!\cdots(n-1)!} V(a_1, \cdots, a_n) = \frac{1}{\prod_{1 \leqslant i < j \leqslant n}(j - i)} \prod_{1 \leqslant i < j \leqslant n} (a_j - a_i)$$

or $\Delta(a_1, \cdots, a_n)$ est bien un entier car les $\binom{a_i}{k}$ sont des entiers, ce qui conclut.

c) Méthode de la descente infinie

On note p premier et pour $n \geqslant 3$, on considère l'équation $x^n + py^n = p^2 z^n$.

- $(0,0,0)$ est solution. On suppose qu'il y en a d'autres et on note $(x,y,z) \neq (0,0,0)$ une solution minimale pour $|x|+|y|+|z|$.
- On a $p \mid p^2z^n - py^n = x^n$ donc p divise x : on écrit $x = px'$. On a

$$p^{n-1}x'^n + y^n = pz^n$$

  donc p divise y qu'on écrit $y = py'$ et donc p divise z qui s'écrit $z = pz'$. On a ainsi trouvé une nouvelle solution (x',y',z') strictement inférieure à la précédente, ce qui est absurde. Ainsi, la seule solution est la solution nulle.

d) Formule de Legendre

Définition.

> Pour tout premier p, on définit la **valuation p-adique** v_p par :
>
> $$v_p : n \in \mathbf{Z}^\star \longmapsto \max\{k \in \mathbf{N}, \quad p^k \mid n\}$$

On va montrer la formule de Legendre :

$$v_p(n!) = \sum_{i=1}^{+\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Pour cela, on remarque

$$v_p(n!) = \sum_{m=1}^{n} v_p(m) = \sum_{m=1}^{n} \sum_{k=1}^{v_p(m)} 1 = \sum_{k=1}^{+\infty} \sum_{\substack{k \leqslant v_p(m) \\ 1 \leqslant m \leqslant n}} 1 = \sum_{k=1}^{+\infty} \sum_{d \leqslant m = p^k u \leqslant n} 1 = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Exercice (X).

> Pour $m, n \in \mathbf{N}$, montrer
>
> $$\frac{(2m)!(2n)!}{(m+n)!n!m!} \in \mathbf{N}$$

e) Coefficients du binôme

On note p un premier et q un entier naturel non divisible par p. On va calculer

$$v_p\left(\binom{p^k q}{p^k}\right)$$

pour $k \in \mathbf{N}$. On a

$$\binom{p^k q}{p^k} = \frac{(p^k q)!}{p^k!(p^k(q-1))!} = \frac{p^k q(p^k q - 1)\cdots(p^k(q-1)+1)}{p^k!}.$$

- $$\forall i \in [\![0, p^k - 1]\!], \quad v_p(p^k - i) = v_p(i)(1 - \delta_{i,0}) + k\delta_{i,0}$$
- $$v_p(p^k q(p^k q - 1)\cdots(p^k(q-1)+1)) = k + \sum_{k=1}^{p^k - 1} v_p(i) = v_p(p^k!)$$

Donc,

$$v_p\left(\binom{p^k q}{p^k}\right) = v_p(p^k q(p^k q - 1)\cdots(p^k(q-1)+1)) - v_p(p^k!) = 0$$

2 L'anneau $\mathbf{Z}_n$

Soit A un anneau commutatif et I un idéal de A. On définit la relation d'équivalence suivante : $x\mathscr{R}y \iff x - y \in I$. On note A/I l'ensemble des classes d'équivalences : c'est un anneau commutatif avec les lois $\overline{x+y} = \overline{x} + \overline{y}$ et $\overline{x \times y} = \overline{x} \times \overline{y}$.

Pour $A = \mathbf{Z}$, $I = n\mathbf{Z}$, il y a n classes d'équivalence dans $\mathbf{Z}_n \underset{\text{def}}{=} \mathbf{Z}/n\mathbf{Z}$, ce sont les $\overline{0}, \cdots, \overline{n-1}$.

3 Groupe $\mathbf{Z}_n^\star$ des inversibles de $\mathbf{Z}_n$

Proposition.

- La classe de $a \in \mathbf{Z}$ est inversible dans $\mathbf{Z}_n$ si et seulement si $a \wedge n = 1$
- $\#\mathbf{Z}_n^\star = \varphi(n)$
- (Euler) Pour $\overline{a}$ inversible, $\overline{a}^{\varphi(n)} \equiv \overline{1} \pmod n$

Démonstration.

1. $\overline{a} \in \mathbf{Z}_n^\star \iff \exists \overline{u} \in \mathbf{Z}_n, \overline{a} \times \overline{u} \equiv 1 \pmod n \iff \exists u, v \in \mathbf{Z}, au = 1 + nv \iff a \wedge n = 1$
2. C'est évident vu 1.
3. $\operatorname{ord}(\overline{a}) \mid \#\mathbf{Z}_n^\star = \varphi(n)$

□

Corollaire (Petit théorème de Fermat).

Pour tout $a \in \mathbf{Z}$, $\quad \overline{a}^p \equiv \overline{a} \pmod p$ pour p premier

4 Caractérisations des corps

Proposition.

$\mathbf{Z}_n$ est un corps si et seulement si n est premier

Démonstration. $\varphi(n) = n - 1 \iff n \in \mathbb{P}$ □

a) Théorème de Wilson

Résultat (Théorème de Wilson).

$p \geqslant 3$ est premier si et seulement si $(p-1)! \equiv -1 \pmod p$

Démonstration.

- ($\implies$) Dans $\mathbf{Z}_p$, $x^2 \equiv 1$ n'a que deux solutions : 1 et -1 (car on est dans un corps donc un anneau intègre). Ce sont donc les deux seuls éléments qui sont leurs propres inverses, les autres sont couplés deux à deux dans l'écriture de $(p-1)!$. On a donc

$$(p-1)! \equiv 1 \times (2 \times \cdots \times (p-2)) \times (p-1) \equiv 1 \times (p-1) \equiv -1 \pmod p$$

- ($\impliedby$) On note $n \geqslant 3$ non premier, il s'écrit donc $n = ab$ avec $a \wedge b = 1$ et $a, b \geqslant 2$. Si $a \neq b$ alors $ab \mid (n-1)!$. Sinon, $n = a^2$ et $a \geqslant 2$ donc $a^2 \mid (n-1)!$ car a et $2a$ apparaissent dans l'écriture de la factorielle. Dans les deux cas, $(n-1)! \equiv 0 \pmod n$

□

b) RSA

On va voir (rapidement) le principe du chiffrement RSA. On choisit p, q des nombres premiers distincts, et on note $n = pq$. On note a, b tels que $ab \equiv 1 \pmod{\varphi(n)}$. Les nombres n et a sont publics, et b (qu'on appelle clé privée) n'est connu que de Bob, qui veut recevoir un message chiffré d'alice

Alice veut transmettre $x \in \mathbf{Z}_n^\star$. Elle calcule $x^n \equiv y \pmod n$, et y est le message chiffré.

Bob calcule $y^b \equiv x^{ab} \equiv x \times x^{\varphi(n)k} \equiv x \pmod n$

c) $\mathbf{Z}_{p^\alpha}^\star$ pour p premier impair

$\mathbf{Z}_p^\star$ est cyclique

On va d'abord montrer les résultats suivants, vrais dans tous les groupes abéliens finis :
- L'ensemble des ordres est stable par ppcm
- L'exposant d'un groupe est l'ordre d'un élément

On utilisera ensuite la structure de corps de $\mathbf{Z}/p\mathbf{Z}$ pour conclure.

Soit $(G, \cdot)$ un groupe abélien fini. On va montrer que l'ensemble des ordres est stable par ppcm. Soient a, b deux éléments d'ordres respectifs m, n. On cherche un élément d'ordre $m \vee n$. On note $d = m \wedge n$ de telle sorte que $m = dm'$, $n = dn'$ et $m \wedge n' = 1$. De cette manière, on a $m \vee n = mn'$

$$\operatorname{ord}(a) = m \qquad \operatorname{ord}\left(b^d\right) = n'$$

et donc $c = ab^d$ est un élément d'ordre $mn' = m \vee n$, ce qui conclut.

On définit l'exposant λ du groupe G comme l'ordre maximal des éléments de G. L'ensemble des ordres étant stable par ppcm, et le ppcm de tous les ordres majorant l'ensemble, le maximum des ordres λ est le ppcm des ordres des éléments. Puis, la stabilité garantit qu'il existe un élément d'ordre λ.

On va maintenant montrer que $\mathbf{Z}_p^\star$ est cyclique. $\mathbf{Z}_p$ est un corps (déjà vu). Ainsi, un polynôme de $\mathbf{Z}_p[X]$ admet au plus autant de racines que son degré. On pose $P = X^\lambda - 1$. Ce polynôme admet au moins $p - 1$ racines distinctes (les éléments non nuls du corps) par définition de λ. On a donc $\lambda \geqslant p - 1$. Puis, λ est un ordre donc divise $\#\mathbf{Z}_p^\star = p - 1$ (Lagrange). Ainsi, $\lambda \mid p - 1$ et $\lambda = p - 1$.

L'exposant du groupe vaut le cardinal du groupe, ce groupe est donc cyclique (un élément d'ordre λ est automatiquement un générateur du groupe).

$\mathbf{Z}_{p^\alpha}^\star$ est cyclique

On va d'abord montrer par récurrence

$$\forall n \in \mathbf{N}, \quad (1+p)^{p^n} \equiv 1 + p^{n+1} \pmod{p^{n+2}}.$$

- Le cas $n = 0$ est direct.
- On suppose le résultat vrai au rang n :

$$(1+p)^{p^n} = 1 + p^{n+1} + p^{n+2} q.$$

  On a alors

$$\begin{aligned}
(1+p)^{p^{n+1}} &\equiv (1 + p^{n+1} + p^{n+2}q)^p \\
&\equiv 1 + \sum_{k=1}^{p} \binom{p}{k} p^{(n+1)k} (1+pq)^k \\
&\equiv 1 + p^{n+1}(1+pq)p \\
&\equiv 1 + p^{n+2} && \pmod{p^{n+3}}.
\end{aligned}$$

  Donc l'égalité est vraie pour tout entier naturel n.

Il est suffisant de trouver un élément de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\star$ d'ordre $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$ (cette égalité s'obtient via la définition de l'indicatrice d'Euler), et vu la stabilité des ordres par ppcm vue précédemment, il est suffisant de trouver un élément d'ordre $p - 1$ et un élément d'ordre $p^{\alpha-1}$.

On va d'abord exhiber un élément d'ordre $p^{\alpha-1}$. On a

$$(1+p)^{p^{\alpha-2}} \equiv 1 + p^{\alpha-1} \pmod{p^\alpha}$$

et

$$(1+p)^{p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}.$$

Donc $\operatorname{ord}(1+p) \mid p^{\alpha-1}$ mais $\operatorname{ord}(1+p) \nmid p^{\alpha-2}$ donc $\operatorname{ord}(1+p) = p^{\alpha-1}$.

Il reste à trouver un élément d'ordre $p - 1$. On sait que $\mathbf{Z}_p^\star$ est cyclique, on note g un générateur. On a :

$$\forall k < p-1, \quad p \nmid g^k - 1 \quad \text{ie} \quad p^\alpha \nmid g^k - 1$$

et $p \mid g^{p-1} - 1$ donc $\operatorname{ord} g = k(p-1)$ est g^k et d'ordre $p - 1$.

5 Théorème chinois

Théorème.

(H) $m, n \in \mathbf{N}^\star$, $m \wedge n = 1$

(C)
1. La classe de $\overline{x} \in \mathbf{Z}_{mn}$ dans $\mathbf{Z}_n$ ne dépend pas du choix de représentant dans $\mathbf{Z}_{mn}$
2. L'application
$$\varphi : \begin{array}{ccc} \mathbf{Z}_{mn} & \longrightarrow & \mathbf{Z}_n \times \mathbf{Z}_m \\ \overline{x} & \longmapsto & (\overline{x}, \overline{x}) \end{array}$$
est un isomorphisme d'anneaux
3. φ est une bijection de $\mathbf{Z}_{m,n}^\star$ dans $\mathbf{Z}_n^\star \times \mathbf{Z}_m^\star$
4. Pour $a, b \in \mathbf{Z}$ fixés, le système
$$\begin{cases} x = a \pmod n \\ x = b \pmod m \end{cases}$$
admet une unique solution modulo mn

Démonstration.
1. a, b de représentants de $\overline{x}$ dans $\mathbf{Z}_{m,n}$. $a \equiv b \pmod m n \implies a \equiv b \pmod n$ donc $\overline{a} = \overline{b}$ dans $\mathbf{Z}_n$
2. C'est bien un morphisme, il est injectif car $\operatorname{Ker} \varphi = \{\overline{0}\}$ donc c'est un isomorphisme car les ensembles d'antécédents et d'images sont équipotents finis.
3. C'est clair ($a \wedge n \neq 1 \implies a \wedge mn \neq 1$ d'où on déduit l'injectivité).
4. C'est 2.

□

Remarque.
Le point 3. donne la multiplicativité de l'indicatrice d'euler : pour m, n premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$

Remarque.
On peut généraliser le résultat à $n_1, \cdots, n_r$ deux à deux premiers entre eux

Remarque.
Si $un + vm = 1$ alors $x = avm + bun$ est une solution

a) Puissances parfaites

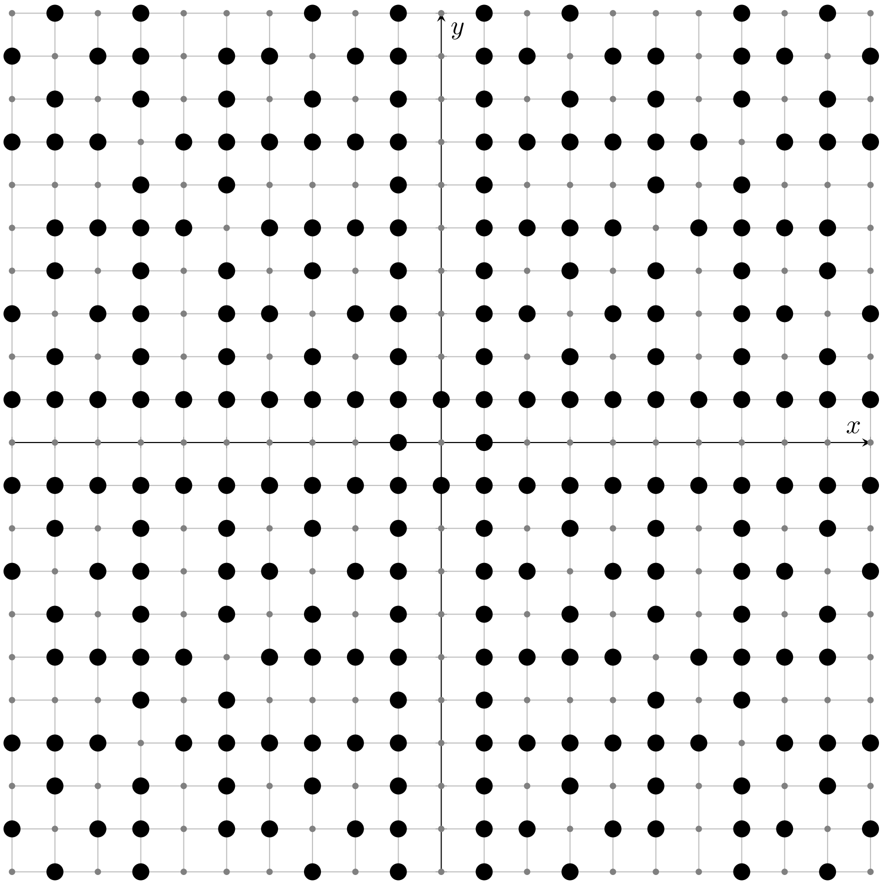
On va montrer qu'il existe n entiers consécutifs qui ne sont pas des puissances parfaites.

On note $p_1, \cdots, p_n$ des premiers deux à deux distincts. Le système

$$\begin{cases} x \equiv p_1 - 1 \pmod{p_1^2} \\ \qquad \vdots \\ x \equiv p_n - n \pmod{p_n^2} \end{cases}$$

possède une solution $x \in \mathbf{N}$ et $v_{p_i}(x + i) = 1$ donc $x + i$ n'est pas une puissance parfaite (car $x + i \neq p_i$ quitte à translater x de $p_1^2 \cdots p_n^2$)

b) Points visibles



On considère l'ensemble des points (qu'on appelle *points visibles*) de $\mathbf{Z}^2$ tels que pour un point (x, y), l'ensemble $\{(1-t)(0,0)+t(x,y), \quad t \in]0,1[\}$ ne contient pas de point de $\mathbf{Z}^2$. On veut montrer qu'il existe des rectangles pleins arbitrairement grands hors de cet ensemble, c'est à dire que pour tout $n \in \mathbf{N}$, il existe (a,b) tel que $\forall i, j \leqslant n, (a+i, b+j)$ est invisible.

On vérifie facilement que cet ensemble est l'ensemble $\{(a,b) \in \mathbf{Z}^2, \quad a \wedge b = 1\}$. On note A une matrice $k \times k$ dont les coefficients sont des nombres premiers deux à deux distincts. On note m_i le produit de la i-ième ligne, M_i le produit de la i-ième colonne. Le théorème chinois donne l'existence de a, b tels que

$$\begin{cases} a \equiv -1 \pmod{m_1} \\ \quad \vdots \\ a \equiv -k \pmod{m_k} \end{cases} \qquad \begin{cases} b \equiv -1 \pmod{M_1} \\ \quad \vdots \\ b \equiv -k \pmod{M_k} \end{cases}$$

de sorte que $(a+i) \wedge (b+j)$ est divisible par $m_i \wedge M_j \neq 1$.

c) Les congruences de Lucas

On note $p \in \mathbb{P}$ et

$$n \underset{\text{def}}{=} \sum_{k=0}^{N} a_k p^k \geqslant \sum_{k=0}^{N} b_k p^k \underset{\text{def}}{=} m$$

On va montrer que

$$\binom{n}{m} \equiv \binom{a_0}{b_0} \cdots \binom{a_N}{b_N} \pmod{p}$$

On a $(1+X)^p = 1 + X^p$ dans $\mathbf{Z}_p[X]$. Puis,

$$(1+X)^n = \prod_{i=0}^{N} ((1+X)^p)^{a_i} = \prod_{i=0}^{n} \sum_{k=0}^{a_i} \binom{a_i}{k} X^{kp^i}$$

et il suffit d'identifier le coefficient de X^m

6 Principe d'inclusion-exclusion

Pour E fini, $A_1, \cdots, A_N \in \mathscr{P}(E)$,

$$\#A_1 \cup \cdots \cup A_N = \sum_{i_1=1}^{N} \#A_{i_1} - \sum_{i_1<i_2} \#A_{i_1} \cap A_{i_2} + \cdots + (-1)^{N-1} \sum_{i_1<\cdots<i_N} \#A_1 \cap \cdots \cap A_N$$

Pour le voir, on remarque :

$$\sum_{x\in E} \mathbb{1}_A(x) = \#A \qquad \mathbb{1}_{A\cap B} = \mathbb{1}_A \cdot \mathbb{1}_B \qquad \mathbb{1}_{A^c} = 1 - \mathbb{1}_A$$

et

$$(A_1 \cup \cdots \cup A_N)^c = A_1^c \cap \cdots \cap A_N^c$$

donc

$$\mathbb{1}_{(A_1\cup\cdots\cup A_N)^c} = \prod_{i=1}^{N} (1 - \mathbb{1}_{A_i^c})$$

puis on développe le produit et on somme la fonction prise sur les éléments de E

Exemple (Application aux permutations sans points fixes)**.** On note d_n le nombre de permutations de $\mathfrak{S}_n$ sans points fixes.

Il y a $\binom{n}{i} d_{n-i}$ permutations qui ont i points fixes donc

$$n! = \sum_{i=0}^{n} \binom{n}{i} d_{n-i} = \sum_{i=0}^{n} \binom{n}{i} d_i.$$

Matriciellement,

$$\begin{pmatrix} n! \\ \vdots \\ \vdots \\ 0! \end{pmatrix} = \underbrace{\begin{pmatrix} \binom{n}{n} & \cdots & \cdots & \binom{n}{0} \\ 0 & \binom{n-1}{n-1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \binom{0}{0} \end{pmatrix}}_{\underset{\text{def}}{=} A_n \in \mathrm{GL}_n(\mathbf{R})} \begin{pmatrix} d_n \\ \vdots \\ d_1 \\ d_0 \end{pmatrix}$$

On a $A_n^\top = \mathscr{M}_{\text{base canonique}}(f)$ avec $f : P \in \mathbf{R}_n[X] \longmapsto P(X+1)$. Puis, $(A_n^\top)^{-1} = (A_n^{-1})^\top = \mathscr{M}(f^{-1})$ or $f^{-1} : P \longmapsto P(X-1)$ d'où

$$(A_n^{-1})^\top = \begin{pmatrix} \binom{n}{n} & 0 & \cdots & 0 \\ -\binom{n}{n-1} & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ (-1)^n \binom{n}{0} & \cdots & \cdots & \binom{0}{0} \end{pmatrix}$$

d'où

$$d_n = \sum_{i=0}^{n} \binom{n}{n-i} (n-i)!(-1)^i = \sum_{i=0}^{n} \frac{(-1)^i n!}{i!} \sim \frac{n!}{e}$$

7 Principe des tiroirs

Proposition (Principe des tiroirs).

> Si on place n éléments dans k tiroirs, alors l'un des tiroirs contient au moins $\lceil \frac{n}{k} \rceil$ éléments

Démonstration. Par l'absurde. □

a) Problème d'Erdős

On choisit $n+1$ éléments distincts de $[\![1, 2n]\!]$. On va montrer que l'un divise un autre.

Tous les entiers s'écrivent $2^n(2s+1)$, $2s+1 \in [\![1, n]\!]$. On en a choisit $n+1$ (parmi n possibilités) donc deux entiers ont la même partie impaire ce qui conclut.

b) Existence d'univers parallèles (moyennant quelques hypothèses physiques)

On définit un volume de Hubble : une boule de $4 \cdot 10^{26}$m de rayon qui contient 10^{115} cases contenant ou non un proton.

L'univers est en expansion, donc la lumière se fait rare et il fait noir. Mais, il ne fait pas noir. Donc il y a des volumes de Hubble qui apparaissent.

Il n'y a qu'un nombre fini de volumes de Hubble possibles, ainsi, il y a deux volumes de Hubble identiques dans l'univers.

c) Tiroirs de Dirichlet

On se donne $\alpha \in \mathbf{R} \setminus \mathbf{Q}$. On va montrer qu'il existe une infinité de (h, k) tels que

$$k > 0, \qquad \left|\alpha - \frac{h}{k}\right| \leqslant \frac{1}{k^2}$$

On note $\{p\alpha\} = p\alpha - \lfloor p\alpha \rfloor$ la partie décimale de $p\alpha$ pour $p \in [\![0, n]\!]$. Il y a $n+1$ valeurs possibles, donc il existe $k \in [\![0, n-1]\!]$ tel que

$$\{p\alpha\}, \{q\alpha\} \in \left[\frac{k}{n}; \frac{k+1}{n}\right[, \qquad \text{et} \qquad p < q$$

Puis,

$$|\{p\alpha\} - \{q\alpha\}| = |(q-p)\alpha - (\lfloor q\alpha \rfloor - \lfloor p\alpha \rfloor)| < \frac{1}{n}$$

donc

$$\Bigg|\alpha - \underbrace{\frac{\lfloor q\alpha \rfloor - \lfloor p\alpha \rfloor}{q-p}}_{=\frac{h}{k} \quad \text{convient}}\Bigg| < \frac{1}{n(q-p)} \leqslant \frac{1}{(q-p)^2}$$

S'il y a un nombre fini de (h, k) solutions alors l'un d'eux réalise le minimum (> 0), donc il existe n tel que

$$\frac{1}{n} < \left|\alpha - \frac{h}{k}\right|$$

et vu ce qui précède il existe $p \neq q$ tel que

$$\left|\alpha - \frac{\lfloor q\alpha \rfloor - \lfloor p\alpha \rfloor}{q-p}\right| < \frac{1}{n|q-p|} \leqslant \left|\alpha - \frac{h}{k}\right|$$

absurde

8 Dénombrement de partitions

Soient $n, p \in \mathbf{N}^\star$. On appelle partition de n en p parties un p-uplet $(x_1, \cdots, x_p) \in [\![0, n]\!]^p$ tel que $x_1 + \cdots + x_p = n$

Pour compter les partitions de n en p-uplets, on compte le nombre de manière de positionner $p-1$ signes $+$ parmi $n+p-1$ emplacements (le nombre d'emplacements entre le i-ième signe $+$ et le $i+1$-ième sera x_{i+1}). Le nombre de p-partitions de n est donc

$$\binom{n+p-1}{p-1}$$

Si on impose que les x_i soient non nuls, alors il n'y a plus que $\binom{n-1}{p-1}$ possibilités.

9 Une congruence subtile

On se donne $a, b \in \mathbf{N}$, $a \geqslant b$. On va montrer que pour p premier

$$\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p^2}$$

On considère l'ensemble E des matrices de $\mathscr{M}_{a,p}(\mathbf{Z}_2)$ dont tous les coefficients sont nuls sauf pb d'entre eux. On munit E de la relation d'équivalence

$$A\mathscr{R}B \iff \exists c_1, \cdots, c_a \text{ permutations circulaires de } [\![1, p]\!], \quad (a_{i,c_i(j)})_{\substack{1 \leqslant i \leqslant a \\ 1 \leqslant j \leqslant p}} = A$$

Par exemple,

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \mathscr{R} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \mathscr{R} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \mathscr{R} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Les classes d'équivalences sont de cardinal 1 si et seulement si les lignes ont chacune un seul des coefficients 1 ou 0 (p est premier). Il y a b parmi a telles classes. Puis, si une ligne contient deux coefficients distincts alors il y a au moins une autre telle ligne (car on a choisi pb coefficients 1). Ainsi, si une classe d'équivalence n'est pas un singleton, son cardinal est divisible au moins par p^2. On a donc

$$\binom{pa}{pb} - \binom{a}{b} = \sum_{\#\overline{x} \geqslant 2} \#\overline{x} = p^2 k$$

d'où le résultat.

10 Méthodes combinatoires

On note E un ensemble fini et $A_1, \cdots, A_k \in \mathscr{P}(E)$. On va compter les k-uplets d'ensembles qui vérifient certaines propriétés

a) Suite croissante pour l'inclusion

On va démonbrer le nombre de $A_1, \cdots, A_k$ tels que $A_1 \subset A_2 \subset \cdots \subset A_n$

$$\boxed{\text{Poubelle} \underset{\text{def}}{=} A_0} \qquad \boxed{A_1} \subset \boxed{A_2} \subset \cdots \subset \boxed{A_k}$$

On associe à chaque $x \in E$ le plus petit $i \in [\![1, k]\!]$ tel que $x \in A_i$ (0 sinon), on note $f : C \to \mathfrak{F}(E, [\![0, k]\!])$ cette fonction, avec C l'ensemble des k-uplets qui satisfont la condition.

Cette fonction est clairement bijective donc $\#C = (k+1)^{\#E}$

b) Union disjointe

On veux dénombrer le nombre de k-uplets tels que $A_i \cap A_j = \varnothing$ pour $i \neq j$ C'est le même principe : on note

$$f : (A_1, \cdots, A_k) \in C \longmapsto (x \longmapsto \text{ unique } i \text{ tel que } x \in A_i)$$

avec A_0 l'ensemble des éléments qui n'apparaissent dans aucun des A_i. Cette application est aussi clairement bijective ce qui permet de conclure.

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre VIII

Algèbre Linéaire

Sommaire

1 Rappels

Définition.

Pour un corps $\mathbf{K}$, $(E,+,\cdot)$ est un $\mathbf{K}$-espace vectoriel si

- $(E,+)$ est un groupe abélien
- $\forall \lambda \in \mathbf{K}, \quad \forall x,y \in E, \quad \lambda(x+y) = \lambda x + \lambda y$
- $\forall \lambda,\mu \in \mathbf{K}, \quad \forall x \in E, \quad (\lambda+\mu)x = \lambda x + \mu x$ et $\lambda(\mu x) = (\lambda\mu)x$
- $\forall x \in E, \quad 1_{\mathbf{K}} \cdot x = x$

a) Calculs dans un espace vectoriel

Remarque (Rappel).

$(E,+,\cdot)$ un $\mathbf{K}$-ev. Alors

- $\forall x \in E, \quad 0_{\mathbf{K}} = 0_E$
- $\forall \lambda \in \mathbf{K}, \quad \lambda \cdot 0_E = 0_E$ et $\qquad \lambda x = 0_E \iff \lambda = 0_K$ ou $x = 0_E$

Définition.

On note $(E,+,\cdot)$ un $\mathbf{K}$-ev et I un ensemble non vide quelconque. On appelle **famille de vecteurs** de E indexée par I la donnée d'une fonction $x : I \to E$. On la note $(x_i)_{i\in I}$ avec $x_i = x(i)$

On appelle **combinaison linéaire** de $(x_i)_{i\in I}$ la donnée de $J \subset I$ fini, d'une famille $(\lambda_j)_{j\in J}$ de scalaires de $\mathbf{K}$ et du vecteur

$$\sum_{j\in J} \lambda_j x_j$$

À faire: Compléter cette section

2 Les sous-espaces vectoriels

a) Constructeurs d'espaces vectoriels

Si $(E,+,\cdot)$ et $(F,+,\cdot)$ sont des $\mathbf{K}$-ev alors $(E\times F,+,\cdot)$ est un $\mathbf{K}$-ev avec les lois qui s'appliquent terme à terme.

Si X est un ensemble non vide, et E est un $\mathbf{K}$-ev, alors $\mathscr{F}(X,E)$ est un $\mathbf{K}$-ev

b) Rappels

Définition.

F est un **sous-espace vectoriel** du $\mathbf{K}$-e.v. E si et seulement si c'est un $\mathbf{K}$-e.v. pour les mêmes lois et qu'il est inclus dans E, ou bien de manière équivalente, F est tel que

- $F \subset E$
- $F \neq \varnothing$
- $\forall \lambda \in \mathbf{K}, \quad \forall x,y \in F, \qquad \lambda x + y \in F$

Définition – Proposition.

(H) E un $\mathbf{K}$-ev, $(F_i)_i$ une famille de sev de E

(C)
1. $\bigcap\limits_{i\in I} F_i$ sev de E
2. On note A une partie de E, $\mathscr{E}_A$ l'ensemble des sev de E qui contiennent A
   (a) $\bigcap\limits_{F\in\mathscr{E}_A} F$ est le sous-espace engendré par A, on le note aussi $\mathrm{Vect}(A)$ ou $\langle A\rangle$
   (b) $F \in \mathscr{E}_A \implies \mathrm{Vect}(A) \subset F$
   (c) $\mathrm{Vect}(A) = \left\{ \sum\limits_{i=1}^{n} \lambda_i a_i, \qquad n \in \mathbf{N}, \lambda_i \in \mathbf{K}, a_i \in A \right\}$

Remarque.

> Pour montrer qu'un ensemble est un sev on peut : revenir à la définition, reconnaître un espace engendré, montrer que c'est le noyau ou l'image d'une application linéaire.

c) Union de sous-espaces vectoriels

On note E un $\mathbf{K}$-espace vectoriel. On va montrer que si $\mathbf{K}$ est infini, alors la réunion d'un nombre fini de sous espaces stricts de E ne peut pas valoir E.

Soient $E_1, \cdots, E_n$ des sev de E tels que

$$\bigcup_{i=1}^{n} E_i = E$$

Quitte à éliminer les redondances et supposer n minimal, on peut faire en sorte (sans modifier l'union) que

$$E_1 \not\subset \bigcup_{j=2}^{n} E_j$$

Ainsi, si $u \in E_1 \setminus \bigcup_{i=2}^{n} E_i$ et $v \in E \setminus E_1$, l'ensemble $v + \mathbf{K}u$ est disjoint de E_1 et contient au plus un vecteur de chaque autre espace vectoriel (car si $\alpha_1 \neq \alpha_2$ sont tels que $v + \alpha_1 u, v + \alpha_2 u \in E_i$, alors $u \in E_i$ absurde). Ainsi,

$$v + \mathbf{K}u = \bigcup_{j=1}^{n} (E_j \cap (v + \mathbf{K}u))$$

est un ensemble fini de cardinal au plus $n - 1$, ce qui est absurde si $\mathbf{K}$ est infini.

Application aux endomorphismes cycliques. On note $f \in \mathscr{L}(E)$ pour E un $\mathbf{C}$-ev et on suppose que f n'a qu'un nombre fini de sous espaces stables. On définit les espaces (stables) suivants :

$$\forall x \in E, \qquad E_{f,x} \underset{\text{def}}{=} \operatorname{Vect}(f^k(x), k \in \mathbf{N})$$

Supposons que $\forall x \in E, E_{f,x} \neq E$. On construit alors la suite $(x_k)_{k \in \mathbf{N}^\star}$ ainsi :

- $x_1 \in E \setminus \{0\}$
- $x_2 \in E \setminus E_{f,x_1}$ et $E \neq E_{f,x_1} \cup E_{f,x_2}$
- $\cdots$
- $x_{n+1} \in E \setminus (E_{f,x_1} \cup \cdots \cup E_{f,x_n})$ et $E \neq E_{f,x_1} \cup \cdots \cup E_{f,x_{n+1}}$

Les $E_{f,x}$ sont stables par f est deux à deux distincts puisqu'on peut construire la suite. On en a une infinité, c'est absurde donc il existe $x \in E$ tel que $E_{f,x} = E$. On dit alors que f est **cyclique**

Si E est de dimension finie, alors on note r le plus grand entier tel que $(x, \cdots, f^r(x))$ est libre. Cette famille constitue alors une base de $E_{f,x} = E$ (si on rajoute un autre vecteur de la partie génératrice, c'est une CL d'éléments de la famille libre exprimée). La matrice de f dans cette base s'écrit

$$\mathscr{M}_{\mathscr{B}}(f) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & a_0 \\ 1 & 0 & \ddots & \vdots & \vdots \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & a_r \end{pmatrix}$$

C'est une matrice compagnon.

3 Somme simple, somme directe

On note E un $\mathbf{K}$-ev, $E_1, \cdots, E_n$ des sev de E et on pose

$$E_1 + \cdots + E_n = \{x_1 + \cdots + x_n, \quad \forall i \in [\![1, n]\!], x_i \in E_i\}$$

C'est un sev de E en tant qu'image d'une application linéaire.

Théorème – Définition.

(H) $E_1, \cdots, E_n$ sev de E

(C) 1. La somme $E_1 + \cdots + E_n$ est dite **directe** si

$$\forall (x_1, \cdots, x_n) \in E_1 \times \cdots \times E_n, \qquad x_1 + \cdots + x_n = 0 \implies (x_1, \cdots, x_n) = 0$$

On notera alors $E_1 \oplus \cdots \oplus E_n$

2. C'est équivalent à ce que l'une des trois propositions suivantes soit vérifiée :
   (a) $\forall j \in [\![2, n]\!], \qquad (E_1 + \cdots + E_{j-1}) \cap E_j = \{0\}$
   (b) $\dim(E_1 + \cdots + E_n) = \dim E_1 + \cdots + \dim E_n$
   (c) La concaténations de bases des E_i est une base de la somme simple.

Démonstration.
- (def $\implies$ a) Facile
- ($a \implies c$) $\mathscr{B}$ génératrice de $E_1 + \cdots + E_n$, $\mathscr{B}_\ell = (e_{i,\ell})_i$ base de E_ℓ. On considère une CL nulle, on isole un coefficient : il est nul. On itère.
- ($c \implies b$) Immédiat
- ($b \implies c$) Une famille génératrice du cardinal de la dimension est une base
- ($c \implies$ def) On décompose sur la base concaténée : tous les coefs sont nuls donc les x_i sont nuls.

□

a) Application linéaire définie par morceaux

Théorème.

(H) $E_1, \cdots, E_n$ des sev de E

(C) 1. $E_1 \oplus \cdots \oplus E_n$ si et seulement si

$$\forall x \in E_1 + \cdots + E_n, \exists! (x_1, \cdots, x_n) \in E_1 \times \cdots \times E_n, \quad x = x_1 + \cdots + x_n$$

2. Dans ce cas,
   (a) L'application

$$\varphi : \begin{array}{ccc} E_1 \times \cdots \times E_n & \longrightarrow & E_1 \oplus \cdots \oplus E_n \\ (x_1, \cdots, x_n) & \longmapsto & x_1 + \cdots + x_n \end{array}$$

   est un isomorphisme
   (b) On a :

$$\forall x \in E_1 \oplus \cdots \oplus E_n, \forall i \in [\![1, n]\!], \exists! x_i \in E_i, \qquad x - x_i \in \bigoplus_{\substack{j=1 \\ j \neq i}}^{n} E_j$$

   On note $\pi_i(x) = x_i$
   (c) Les π_i sont des projecteurs et $\sum \pi_i$ est l'application identité sur $E_1 \oplus \cdots \oplus E_n$. On les appelle les **projecteurs associés à la décomposition**

3. F un $\mathbf{K}$-ev, $f_1 \in \mathscr{L}(E_1, F), \cdots, f_n \in \mathscr{L}(E_n, F)$.

$$\exists! f \in \mathscr{L}(E_1 \oplus \cdots \oplus E_n, F), \qquad f_{|E_i} = f_i$$

et

$$f = \sum_i f_i \circ \pi_i$$

Démonstration. Facile □

b) Lemme de décomposition et d'isomorphisme

Si $E = F \oplus G$ et H, alors

$$\begin{array}{rccc} \psi : & \mathscr{L}(E,H) & \longrightarrow & \mathscr{L}(F,H) \times \mathscr{L}(G,H) \\ & f & \longmapsto & (f_{|F}, f_{|G}) \end{array}$$

est un isomorphisme.

Si π_1, π_2 sont les projecteurs associés à $(F_1 \times \{0\}) \oplus (\{0\} \times F_2)$, alors

$$\begin{array}{rccc} \varphi : & \mathscr{L}(E,F_1 \times F_2) & \longrightarrow & \mathscr{L}(E,F_1) \times \mathscr{L}(E,F_2) \\ & f & \longmapsto & (\pi_1 \circ f, \pi_2 \circ f) \end{array}$$

est aussi un isomorphisme.

c) Lemme de factorisation

Premier lemme Soient $u \in \mathscr{L}(E,F), v \in \mathscr{L}(E,G)$ tels que $\operatorname{Ker} u \subset \operatorname{Ker} v$. On va montrer qu'il existe $w \in \mathscr{L}(F,G)$ telle que $v = w \circ u$.

On note V un supplémentaire de $\operatorname{Ker} u$ dans E. $u_{|V}$ est un isomorphisme de V dans $\operatorname{Im} u$. On peut prendre $w_{|\operatorname{Im} u} = v_{|V} \circ (u_{|V}^{-1})$ et w nulle sur un supplémentaire de $\operatorname{Im} u$

Second lemme $u \in \mathscr{L}(E,G), v \in \mathscr{L}(F,G)$ et $\operatorname{Im} u \subset \operatorname{Im} v$. Il existe $w \in \mathscr{L}(E,F)$ telle que $u = v \circ w$

La démonstration est similaire.

4 Théorème du rang

Théorème (Rang).

> (H) E, F des $\mathbf{K}$-ev et $f \in \mathscr{L}(E,F)$
>
> (C) 1. Si V est un supplémentaire de $\operatorname{Ker} f$ dans E alors $f_{|V}$ est un isomorphisme de V dans $\operatorname{Im} f$
> 2. $\dim E < +\infty \implies \dim(\operatorname{Im} f) < +\infty$ et $\dim E = \dim \operatorname{Ker} f + \operatorname{rg} f$

Démonstration. Simple (sup) □

Remarque.

> Le rang est invariant par composition de son argument avec un isomorphisme : si u, v sont des isomorphismes, $\operatorname{rg} f = \operatorname{rg} f \circ v = \operatorname{rg} u \circ f$

Exercice.

> $f, g \in \mathscr{L}(E)$. Montrer que
> $$|\operatorname{rg} f - \operatorname{rg} g| \leqslant \operatorname{rg}(f+g) \leqslant \operatorname{rg} f + \operatorname{rg} g$$

Résolution. $(f+g)(E) \subset f(E) + g(E)$ d'où l'inégalité de droite. Puis

$$\operatorname{rg} f = \operatorname{rg}(f+g-g) \leqslant \operatorname{rg}(f+g) + \operatorname{rg}(-g) = \operatorname{rg}(f+g) + \operatorname{rg} g$$

et par symétrie des rôles, on a l'autre inégalité. □

5 Monotonie des noyaux itérés, décomposition de Fitting

Résultat (Propriété d'essoufflement des noyaux itérés).

On note f un endomorphisme en dimension finie n. La suite

$$\left(\mathrm{Ker}(f^k)\right)_k.$$

est strictement croissante sur d premiers termes (on peut avoir $d = 0$) puis stationnaire. De plus, la suite $(\delta_n)_n$ définie par

$$\forall k \in \mathbf{N}, \delta_k = \dim(\mathrm{Ker}(f^{k+1})) - \dim(\mathrm{Ker}(f^k))$$

est décroissante (cette monotonie est appelée **propriété d'essoufflement**).

Démonstration. La croissance simple de la suite des noyaux est directe : si $f^k(x) = 0$ alors $f(f^k(x)) = f(0) = 0$. On a forcément croissance stricte sur les premiers termes jusqu'à atteindre une égalité (éventuellement la croissance stricte ne concerne aucun termes). Cette égalité est atteinte car la suite $(\dim(\mathrm{Ker}(f^k)))$ est une suite entière croissante majorée donc stationnaire. Il reste à montrer que dès qu'une égalité est atteinte, la suite devient constante. Supposons

$$\mathrm{Ker}(f^k) = \mathrm{Ker}(f^{k+1})$$

Alors,

$$\mathrm{Ker}(f^{k+2}) = \{x, \quad f(f^{k+1}(x)) = 0\} = \{x, \quad f(f^k(x)) = 0\} = \mathrm{Ker}(f^k)$$

La suite est donc bien strictement croissante puis stationnaire. On va maintenant montrer la décroissance de $(\delta_n)_n$. On a, en appliquant le théorème du rang,

$$\begin{aligned}\dim(\mathrm{Im}(f^k)) &= \dim\left(\mathrm{Ker}\left(f\left|_{\mathrm{Im}(f^k)}\right.\right)\right) + \dim\left(\mathrm{Im}\left(f\left|_{\mathrm{Im}(f^k)}\right.\right)\right)\\ &= \dim\left(\mathrm{Ker}\left(f\left|_{\mathrm{Im}(f^k)}\right.\right)\right) + \dim(\mathrm{Im}(f^{k+1}))\end{aligned}$$

d'où

$$\delta_k = \dim(\mathrm{Im}(f^k)) - \dim(\mathrm{Im}(f^{k+1})) = \dim\left(\mathrm{Ker}\left(f\left|_{\mathrm{Im}(f^k)}\right.\right)\right) = \dim(\mathrm{Im}(f^k) \cap \mathrm{Ker}(f)).$$

Or la suite des images est décroissante donc $(\delta_k)_k$ décroît. □

Résultat (Décomposition de Fitting).

Si r est tel que $\mathrm{Ker}\, f^r = \mathrm{Ker}\, f^{r+1}$, alors $E = \mathrm{Ker}\, f^r \oplus \mathrm{Im}\, f^r$

Démonstration. Si $x \in \mathrm{Im}\, f^r \cap \mathrm{Ker}\, f^r$ alors $x = f^r(t)$ et $f^r(x) = 0$ donc $t \in \mathrm{Ker}\, f^{2r} = \mathrm{Ker}\, f^r$ et $x = 0$, ce qui donne la somme directe. Puis on a la bonne dimension avec le théorème du rang. □

6 Formes linéaires

a) Rappels

Définition.

Si E est un $\mathbf{K}$-ev, on appelle **forme linéaire** sur E une application de $\mathscr{L}(E, \mathbf{K}) \underset{\text{def}}{=} E^\star$. On appelle **hyperplan** le noyau d'une forme linéaire non nulle.

Théorème.

(H) E un $\mathbf{K}$-ev, H un sev de E

(C) Il y a équivalence entre

1. H est un hyperplan de E
2. $\forall a \in E \setminus H, \quad H \oplus \mathbf{K}a = E$
3. $\exists a \in E \setminus H, \quad H \oplus \mathbf{K}a = E$
4. $\dim H = \dim E - 1$ si E est de dimension finie
5. $\exists \varphi \in \mathscr{L}(E, \mathbf{K}) \setminus \{0\}, \quad H = \mathrm{Ker}\, \varphi$

Démonstration.
(1 $\iff$ 5) c'est la déf
(1 $\implies$ 2) Si φ est une FL non nulle telle que $\operatorname{Ker}\varphi = H$ et si $a \in E \setminus H$ alors $\varphi(a) \neq 0$ et

$$x = \left(x - \frac{\varphi(x)}{\varphi(a)}a\right) + \frac{\varphi(x)}{\varphi(a)}a$$

d'où $E = H + \mathbf{K}a$. L'intersection vaut $\{0\}$ donc la somme est directe.
(2 $\implies$ 3) Trivial
(3 $\implies$ 1) $\varphi_H = 0$, $\varphi(a) = 1$. □

b) Base antéduale

Exercice.
On note E un $\mathbf{K}$-ev de dimension n et $(\varphi_1, \cdots, \varphi_n)$ une base de $E^\star$. Montrer qu'il existe $(x_1, \cdots, x_n) \in E^n$ tels que $\varphi_i(x_j) = \delta_{i,j}$

Démonstration. On note

$$\begin{aligned}\psi : E &\longrightarrow \mathbf{K}^n \\ x &\longmapsto (\varphi_1(x), \cdots, \varphi_n(x))\end{aligned}$$

Si ψ n'est pas surjective alors $\dim \operatorname{Im}(\psi) < n$ donc $\operatorname{Im}\psi$ est inclus dans un hyperplan de $\mathbf{K}^n$. Il existe $(a_1, \cdots, a_n) \in \mathbf{K}^n \setminus \{0\}$ tels que

$$\forall x \in E, a_1\varphi_1(x) + \cdots + a_n\varphi_n(x) = 0$$

donc $(\varphi_1, \cdots, \varphi_n)$ est liée, ce qui est absurde. L'application ψ est donc une AL surjective et $\dim E = \dim \mathbf{K}^n = n$ donc ψ est un isomorphisme.

On note $x_1 = \psi^{-1}(1, 0, \cdots, 0)$, $x_2 = \psi^{-1}(0, 1, \cdots, 0)$, $\cdots$, $x_n = \psi^{-1}(0, , \cdots, 1)$ et la famille $(x_1, \cdots, x_n)$ convient.

C'est une base car c'est l'image par ψ^{-1} de la base canonique de $\mathbf{K}^n$. Cette base s'appelle la **base antéduale** de $(\varphi_1, \cdots, \varphi_n)$

□

c) Base duale

Si on note $(e_1, \cdots, e_n)$ est une base de E, alors pour chaque i, on note $e_i^\star$ la forme linéaire donnée par $e_i^\star(e_j) \underset{\text{def}}{=} \delta_{i,j}$.

La famille $(e_1^\star, \cdots, e_n^\star)$ est une famille de n vecteurs en dimension n, qui est libre donc c'est une base, appelée **base duale** de $(e_1, \cdots, e_n)$

d) Un exercice classique

Exercice.
Soit E un $\mathbf{K}$-ev de dimension finie n. On note $\varphi_1, \cdots, \varphi_p \in E^\star$
Montrer que $\varphi \in \operatorname{Vect}(\varphi_1, \cdots, \varphi_p) \iff \operatorname{Ker}\varphi_1 \cap \cdots \cap \operatorname{Ker}\varphi_p \subset \operatorname{Ker}\varphi$

Résolution.
($\implies$) Si $\varphi \in \operatorname{Vect}(\varphi_1, \cdots, \varphi_p)$ alors il existe $a_1, \cdots, a_p \in \mathbf{K}$ tels que :

$$\varphi = a_1\varphi_1 + \cdots + a_p\varphi_p$$

et $\forall x \in \operatorname{Ker}\varphi_1 \cap \cdots \cap \operatorname{Ker}\varphi_p$,

$$\varphi(x) = a_1\varphi_1(x) + \cdots + a_p\varphi_p(x) = 0 + \cdots + 0 = 0$$

donc $x \in \operatorname{Ker} \varphi$ d'où l'inclusion et le sens direct.
($\Longleftarrow$) On suppose que $(\varphi_1, \cdots, \varphi_p)$ est libre, et on complète en une base $(\varphi_1, \cdots, \varphi_p, \varphi_{p+1}, \cdots, \varphi_n)$. Ainsi, il existe $(a_1, \cdots, a_n) \in \mathbf{K}^n$ tels que

$$\varphi = a_1\varphi_1 + \cdots + a_n\varphi_n$$

On note $(x_1, \cdots, x_n)$ la base antéduale de $(\varphi_1, \cdots, \varphi_n)$. Alors, $x_{p+1} \in \operatorname{Ker} \varphi_1 \cap \cdots \cap \operatorname{Ker} \varphi_p$ donc $x_{p+1} \in \operatorname{Ker}(\varphi)$ ce qui donne $\varphi(x_{p+1}) = 0 = a_{p+1}$. En recommençant pour $x_{p+2}, \cdots, x_n$, on trouve $a_{p+1} = \cdots = a_n = 0$ d'où la conclusion.

Dans le cas général, on extrait de $(\varphi_1, \cdots, \varphi_p)$ une base de $\operatorname{Vect}(\varphi_1, \cdots, \varphi_p)$ qu'on note $(\varphi_1, \cdots, \varphi_r)$ (on renomme si besoin). On a $\operatorname{Ker} \varphi_1 \cap \cdots \cap \operatorname{Ker} \varphi_r \subset \operatorname{Ker} \varphi_{r+1}, \cdots, \operatorname{Ker} \varphi_p$

□

e) Intersection

On note E un $\mathbf{K}$-ev, $\varphi_1, \cdots, \varphi_p \in E^\star$ et $H_i = \operatorname{Ker} \varphi_i$. On va montrer que $\dim(H_1 \cap \cdots \cap H_p) \geqslant n - p$ avec égalité si et seulement si $(\varphi_1, \cdots, \varphi_p)$ est libre.

- $\dim H_1 \geqslant n - 1$
- $\varphi_{2|H_1}$ est une FL sur H_1 donc $\dim(\operatorname{Ker} \varphi_{2|H_1}) = \dim(\operatorname{Ker} \varphi_2 \cap \operatorname{Ker} \varphi_1) = \dim H_1 - 1 \geqslant n - 2$
- $\cdots$

Puis il y a égalité si et seulement si on a une égalité à chaque étape.

- $\varphi_1 \neq 0$ donc (φ_1) libre.
- $H_1 \not\subset H_2$ donc $\varphi_2 \notin \operatorname{Vect}(\varphi_1)$ et (φ_1, φ_2) libre
- $\cdots$

7 Idéaux de $\mathscr{L}(E)$

On note E un $\mathbf{K}$-ev de dimension n. Quitte à se donner une base $\mathscr{B}$, on a $\mathscr{L}(E) \cong \mathscr{M}_n(\mathbf{K})$ (c'est un isomorphisme d'algèbres).

I est un idéal à gauche (resp. à droite) si $(I, +)$ est un groupe et $\forall M \in I, \forall A \in \mathscr{M}_n(\mathbf{K}), MA \in I$ (resp. $AM \in I$). Un idéal est bilatère si c'est un idéal à droite et à gauche.

a) Idéaux bilatères

$I = \{0\}$ en est un, on suppose désormais que $I \neq \{0\}$. Il existe donc $A \in I$ tel que $\operatorname{rg}(A) = r > 0$ donc il existe $P, Q \in \mathrm{GL}_n(\mathbf{K})$ telles que

$$A = P \underbrace{\begin{array}{l}\left(\begin{array}{ccc|ccc} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & \vdots \\ \hline \vdots & & \ddots & 0 & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 \end{array}\right) \\ \quad\underbrace{\hphantom{0 \quad \cdots \quad \cdots}}_{r} \end{array}}_{J_r} Q \text{ donc } J_r = P^{-1}AQ^{-1} \in I.$$

Puis $J_1 = J_r J_1 \in I$. Les matrices de rang 1 sont équivalentes à J_1 donc sont dans I, ce qui est le cas des matrices de la base canonique $E_{i,j}$, donc $I = \mathscr{M}_n(\mathbf{K})$

Les idéaux bilatères de $\mathscr{M}_n(\mathbf{K})$ sont donc $\{0\}$ et $\mathscr{M}_n(\mathbf{K})$.

b) Idéaux à gauche

Remarque.

Un idéal de $\mathscr{M}_n(\mathbf{K})$ est toujours un espace vectoriel.

On note $(A_1, \cdots, A_r)$ une base de I et $M \in I$ de rang maximal. On a $M \cdot \mathscr{M}_n(\mathbf{K}) \subset I$. Soit $A \in I$, si $\operatorname{Im} A \subset \operatorname{Im} M$ alors il existe B tel que $A = MB$ (lemme de factorisation) donc $A \in M\mathscr{M}_n(\mathbf{K})$.

Soit $A \in I$. Par l'absurde si $\operatorname{Im} A \not\subset \operatorname{Im} M$ alors M non inversible et il existe X un vecteur colonne tel que $AX \notin \operatorname{Im} M$. On note $(X_1, \cdots, X_n)$ une base d'un supplémentaire de $\operatorname{Ker} M$. On note $(X_{r+1}, \cdots, X_n)$ une base de $\operatorname{Ker} M$ et on note B telle que.

$$\begin{cases} BX_1 = \cdots = BX_r = 0 \\ BX_{r+1} = X \\ BX_{r+2} = \cdots = BX_n = 0 \end{cases}$$

La matrice $M + AB$ est dans I et son image contient $(MX_1, \cdots, MX_r, AX)$ donc $rg(M+AB) \geqslant r+1 > r$ absurde donc $\operatorname{Im} A \not\subset \operatorname{Im} M$.

Les idéaux à gauche de $\mathscr{M}_n(\mathbf{K})$ sont docn les ensembles du type $A\mathscr{M}_n(\mathbf{K})$ avec $A \in \mathscr{M}_n(\mathbf{K})$.

8 Matrices élémentaires

a) Rappels

Remarque (Produit de matrices $E_{i,j}$).

Dans $\mathscr{M}_n(\mathbf{K})$,

$$E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}$$

Définition.

On définit les matrices élémentaires suivantes :

- Matrices de transposition :

$$T_{i,j} = I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i} = \begin{array}{cc} \begin{matrix} & & & i & & & & j & & & \end{matrix} & \\ \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & (0) & \\ & & 1 & & & & & & & & \\ & & & 0 & & \cdots & & 1 & & & \\ & & & & 1 & & & & & & \\ & & & \vdots & & \ddots & & \vdots & & & \\ & & & & & & 1 & & & & \\ & & & 1 & & \cdots & & 0 & & & \\ & & & & & & & & 1 & & \\ & (0) & & & & & & & & \ddots & \\ & & & & & & & & & & 1 \end{pmatrix} & \begin{matrix} \\ \\ \\ \leftarrow i \\ \\ \\ \\ \leftarrow j \\ \\ \\ \\ \end{matrix} \end{array}$$

- Matrices de transvection : pour $i \neq j$,

$$T_{i,j}(\lambda) = I_n + \lambda E_{i,j} = \begin{pmatrix} 1 & & & & \\ & 1 & & \lambda & \\ & & \ddots & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}$$

- Matrices de dilataion :

$$D_i(\lambda) = I_n + (\lambda - 1)E_{i,i} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

b) Actions des matrices élémentaires

La multiplication à gauche par une matrice élémentaire agit sur les lignes, et la multiplication à droite agit sur les colonnes.

- La multiplication à gauche par $T_{i,j}$ fait $L_i \leftrightarrow L_j$
- La multiplication à gauche par $T_{i,j}(\lambda)$ fait $L_i \leftarrow L_i + \lambda L_j$
- La multiplication à gauche par $D_i(\lambda)$ fait $L_i \leftarrow \lambda L_i$
- La multiplication à gauche par $E_{i,j}$ fait $L_k \leftarrow \delta_{k,i} L_j$

Les opérations sont identiques mais avec les colonnes pour la multiplication à droite

c) Générateurs de $\mathrm{GL}_n(\mathbf{K})$ et $\mathrm{SL}_n(\mathbf{K})$

On va montrer que les éléments de $\mathrm{GL}_n(\mathbf{K})$ s'écrivent comme un produit de transvections et d'une dilatation.

Remarque.

L'inverse d'une transvection est une transvection : $T_{i,j}(\lambda)^{-1} = T_{i,j}(-\lambda)$

On procède par récurrence pour montrer que si A est inversible, il existe $T_1, \cdots, T_r$ des transvections telles que

$$T_1 \cdots T_r A = D_n(\det A)$$

- L'initialisation est trivialle : pour $n = 1$, toutes les matrices sont des matrices de dilatation.
- Soit $n > 1$. On suppose la propriété vraie au rang $n-1$ et on note $A \in \mathrm{GL}_n(\mathbf{K})$. On note $(a_{i,j})$ les coefficients de A. Quitte à multiplier par une transvection, on peut supposer $a_{1,1} \neq 0$ et l'utiliser comme pivot :

$$\begin{pmatrix} a_{1,1} & & \\ \vdots & & \\ & \star & \\ \vdots & & \\ a_{n,1} & & \end{pmatrix} \xrightarrow{\text{pivot avec} a_{1,1}} \left(\begin{array}{c|c} a_{1,1} & \star \\ \hline 0 & \\ \vdots & \star \\ 0 & \end{array}\right)$$

$$\xrightarrow{L_2 \leftarrow L_2 + L_1} \left(\begin{array}{c|c} a_{1,1} & \star \\ \hline a_{1,1} & \\ \vdots & \star \\ 0 & \end{array}\right)$$

$$\xrightarrow{L_1 \leftarrow L_1 + (1-a_{1,1})L_2} \left(\begin{array}{c|c} 1 & \star \\ \hline a_{1,1} & \\ \vdots & \star \\ 0 & \end{array}\right)$$

$$\xrightarrow{L_2 \leftarrow L_2 - a_{1,1}L_1} \left(\begin{array}{c|c} 1 & \star \\ \hline 0 & \\ \vdots & \star \\ 0 & \end{array}\right)$$

$$\xrightarrow{\text{HR}} \left(\begin{array}{c|cccc} 1 & & \star & & \\ \hline 0 & 1 & & & \\ \vdots & & \ddots & & \\ \vdots & & & 1 & \\ 0 & & & & \det A \end{array}\right)$$

$$\xrightarrow{C_i \leftarrow C_i - a_{1,i}C_1} \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & \det A \end{pmatrix}$$

d'où la conclusion.

Exercice.

> Montrer que $\mathrm{SL}_n(\mathbf{K}) = \ker(\det) = \{A \in \mathrm{GL}_n(\mathbf{K}), \det A = 1\}$ est engendré par les matrices de transvection

Résolution. On vient de le voir. □

9 Matrices

a) Rappels

$\mathscr{B} = (e_1, \cdots, e_p)$, $\mathscr{F} = (f_1, \cdots, f_n)$ des bases de E, F et $f \in \mathscr{L}(E, F)$. On note $\mathscr{M}_{\mathscr{B},\mathscr{F}}(f)$ la matrice de taille $n \times p$ dans laquelle la colonne i est le vecteur des coordonées de $f(e_i)$ dans le base $\mathscr{F}$

Si $\mathscr{B}' = (e'_1, \cdots, e'_p)$ est une base de E alors on définit la matrice de passage $P_{\mathscr{B},\mathscr{B}'}$ par

$$P_{\mathscr{B},\mathscr{B}'} \underset{\text{def}}{=} \mathscr{M}_{\mathscr{B},\mathscr{B}'}(f)$$

où $f : e_i \longmapsto e'_i$. Si x s'écrit $X_{\mathscr{B}}$ dans $\mathscr{B}$ et $X_{\mathscr{B}'}$ dans $\mathscr{B}'$, alors

$$X_{\mathscr{B}} = P_{\mathscr{B},\mathscr{B}'} X_{\mathscr{B}'}$$

b) Interprétation combinatoire

On note $G = (S, A)$ un graphe simple orienté avec $|S| = n$. La matrice d'adjacence $M \in \mathscr{M}_n(\mathbf{K})$ est la matrice de terme général $(\mathbb{1}_A((i,j)))_{i,j\in[\![1,n]\!]}$

Exercice.

Montrer que $[A^m]_{i,j}$ est le nombre de chemins de longueur m de i vers j. On pourra procéder par récurrence sur m.

c) Crochet de Lie

On s'intéresse au commutateur comme crochet de Lie dans $\mathscr{M}_n(\mathbf{K})$: $[A, B] \underset{\text{def}}{=} AB - BA$

Exercice.

Montrer l'identité de Jacobi :

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$$

Exercice.

Si A et $[A, B]$ commutent, alors

$$\forall k \in \mathbf{N}^\star, \qquad [A^k, B] = k[A, B]A^{k-1}$$

Démonstration. Par récurrence en écrivant $AB = [A, B] + BA$ □

Exercice.

Montrer que si $A \in \mathscr{M}_n(\mathbf{C})$ est de trace nulle, alors il existe B, C tels que $A = [B, C]$

Résolution. On commence par le cas où A est de diagonale nulle. On pose $B = \operatorname{diag}(1, \cdots, n)$. Si C existe alors

$$A = [B, C] \underset{\text{calcul}}{\iff} \forall i, j, \quad A_{i,j} = (i - j)C_{i,j}$$

donc la matrice C existe bien (on prend 0 pour la diagonale)

On va maintenant montrer que toute matrice de trace nulle est semblable à une matrice de diagonale nulle, ce qui conclura. On procède par récurrence sur la dimension.

- L'initialisation est évidente
- $A \in \mathscr{M}_{n+1}(\mathbf{C})$, $\operatorname{Tr}(A) = 0$. Il y a deux cas :
  — $\forall X \in \mathscr{M}_{n+1,1}(\mathbf{C}), \quad (X, AX)$ liée. Donc $A = \lambda I_{n+1} = 0$.
  — $\exists X \in \mathscr{M}_{n+1,1}(\mathbf{C}), \quad (X, AX)$ libre.

  Il n'y a que le second cas à traiter. On complète (X, AX) en une base $\mathscr{B}$ et la matrice de A dans cette base s'écrit

$$\left(\begin{array}{c|c} 0 & \star \\ \hline 1 & \\ 0 & \\ \vdots & A' \\ 0 & \end{array}\right)$$

  et $\operatorname{Tr}(A') = \operatorname{Tr}(A)$. Puis l'hypothèse de récurrence permet de conclure (considérer les matrices $\hat{P} = \operatorname{diag}(1, P)$ pour $P \in \mathscr{M}_n(\mathbf{C})$ matrice de passage)

□

10 Déterminants

a) Rappels

On note $\mathscr{B} = (e_1, \cdots, e_n)$ une base de E et $\mathscr{F} = (f_1, \cdots, f_n)$ une famille de vecteurs de E. On note $f_{i,j}$ la coordonnée de f_j sur e_i dans $\mathscr{B}$.

$$\det_{\mathscr{B}}(\mathscr{F}) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) f_{1,\sigma(1)} \cdots x_{n,\sigma(n)}$$

Théorème.

Ⓗ E un **K**-ev de base $\mathscr{B} = (e_1, \cdots, e_n)$

Ⓒ $\det_{\mathscr{B}}$ est l'unique forme n-linéaire alternée dont l'image de $\mathscr{B}$ est 1

Proposition.

Ⓗ $\mathscr{B}, \mathscr{C}$ des bases de E

Ⓒ $\det_{\mathscr{C}} = \det_C(\mathscr{B}) \det_{\mathscr{B}}$

Définition – Proposition.

Ⓗ $\mathscr{B}$ est une base de E un **K**-ev de dimension finie, $f, g \in \mathscr{L}(E)$

Ⓒ 1. $\det f$ est l'unique scalaire tel que

$$\forall x_1, \cdots, x_n \in E, \qquad \det_{\mathscr{B}}(f(x_1), \cdots, f(x_n)) = \det f \times \det_{\mathscr{B}}(x_1, \cdots, x_n)$$

2. $\det(f \circ g) = \det f \times \det g$
3. $f \in \mathrm{GL}_n(\mathbf{K}) \iff \det f \neq 0$

b) Déterminants classiques

Vandermonde Pour $(\lambda_1, \cdots, \lambda_n) \in \mathbf{K}$, on note

$$V(\lambda_1, \cdots, \lambda_n) = \begin{vmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \cdots & \lambda_2^{n-1} \\ \vdots & & & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^{n-1} \end{vmatrix}$$

On montre par récurrence que

$$V(\lambda_1, \cdots, \lambda_n) = \prod_{i<j} (\lambda_j - \lambda_i)$$

- Initialisation claire
- On se place dans le cas où les λ_i sont deux à deux distincts (car sinon deux lignes sont identiques, le déterminant et nulle et la formule reste vraie). On pose

$$P(X) = V(\lambda_1, \cdots, \lambda_n, X) = \begin{vmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-1} & \lambda_1^n \\ 1 & \lambda_2 & \cdots & \lambda_2^{n-1} & \lambda_2^n \\ \vdots & & & & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^{n-1} & \lambda_n^n \\ 1 & X & \cdots & X^{n-1} & X^n \end{vmatrix}$$

P est un polynôme de degré n, qui admet $\lambda_1, \cdots, \lambda_n$ pour racines distinctes donc il s'écrit

$$P(X) = \mu(X - \lambda_1) \cdots (X - \lambda_n)$$

et en développant par rapport à la dernière colonne, on identifie

$$\mu = V(\lambda_1, \cdots, \lambda_n)$$

donc

$$V(\lambda_1, \cdots, \lambda_{n+1}) = P(\lambda_{n+1}) = \prod_{i<j} (\lambda_j - \lambda_i)$$

Déterminant tridiagonal

$$D_n = \begin{vmatrix} a & c & 0 & \dots & 0 \\ b & a & c & \ddots & 0 \\ 0 & b & a & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a \end{vmatrix}$$

On trouve facilement

$$D_{n+2} = aD_{n+1} - bcD_n$$

C'est une suite qui satisfait une relation de récurrence linéaire d'ordre 2, on connait $D_1 = a, D_0 = 1$ donc sait en trouver une forme close.

Déterminant circulant On appelle **déterminant circulant** le déterminant de la matrice suivante :

$$D = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}.$$

On va montrer que

$$\det D = \prod_{k=0}^{n-1} P(\omega^k)$$

où ω est une racine primitive n-ième de l'unité et $P = \sum_{k=0}^{n-1} a_k X^k$.

Pour $i \in [\![0, n-1]\!]$, on pose

$$V_i = \begin{pmatrix} 1 \\ \omega^i \\ \vdots \\ \omega^{i(n-1)} \end{pmatrix}.$$

Remarquons alors que $DV_i = P(\omega^i)V_i$. En posant la matrice $Q = (V_0, V_1, \dots, V_{n-1})$ il vient $DQ = Q \times \operatorname{diag}(P(1), P(\omega), \dots, P(\omega^{n-1})$ donc nous avons

$$\det(D)\det(Q) = \det(Q) \prod_{i=0}^{n-1} P(\omega^i).$$

Et le déterminant de Q est non nul ($\det Q = V(1, \omega, \dots, \omega^{n-1})$ avec V le déterminant de Vandermonde et les ω^i sont deux à deux distincts) ce qui conclut la preuve.

c) Comatrice

Définition.

Le **mineur** d'indice i, j de $A \in \mathscr{M}_n(\mathbf{K})$ est $\det(A')$ où A' est la matrice A privée de la ligne i et de la colonne j . Si $i = j$, on dit que c'est un mineur principale. On note $\Delta_{i,j}(A)$ les mineurs de A.
On appelle **comatrice** de A la matrice $\operatorname{Com}(A) = ((-1)^{i+j}\Delta_{i,j}(A))$. Les coefficients de cette matrice sont appelés **cofacteurs**.

Théorème.

(H) $A \in \mathscr{M}_n(\mathbf{K})$

(C)

1. $\forall i \in [\![1, n]\!], \qquad \det A = \sum_{j=1}^{n} (-1)^{i+j} \Delta_{i,j}(A)$
2. $\forall j \in [\![1, n]\!], \qquad \det A = \sum_{i=1}^{n} (-1)^{i+j} \Delta_{i,j}(A)$
3. $A\,\mathrm{Com}(A)^\top = \mathrm{Com}(A)^\top A = \det A I_n$

11 Système d'équation linéaire

On appelle système linéaire d'inconnues $x_1, \cdots, x_p$ un système du type

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,p}x_p = b_1 \\ \vdots \\ a_{n,1}x_1 + \cdots + a_{n,p}x_p = b_p \end{cases}$$

a) Interprétation matricielle

On pose $A = (a_{i,j})_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant p}}$, $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ et $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$. $(x_1, \cdots, x_p)$ est solution si et seulement si $AX = B$.

Il y a une unique solution si A est inversible, c'est à dire $n = p$ et $A \in \mathrm{GL}_n(\mathbf{K})$. On dit alors que c'est un système de Cramer et $X = A^{-1}B$ est l'unique solution.

Dans le cas général, il y a une solution si et seulement si $B \in \mathrm{Im}(A)$. Dans ce cas là, pour X_0 solution, l'ensemble des solutions est

$$\{X \in \mathscr{M}_{p,1}, \qquad X - X_0 \in \mathrm{Ker}(A)\}$$

b) Interprétation géométrique

On note $\varphi_i : x \longmapsto a_{i,1}x_1 + \cdots + a_{i,p}x_p$ des formes linéaires. Les équations $\varphi_i(x) = b_i$ sont des équations d'hyperplans affines. Ainsi, x est solution si et seulement si x dans l'intersection des hyperplans d'équations $\varphi_i(x) = b_i$

c) Interprétation vectorielle

Si $C_1, \cdots, C_p$ sont les colonnes de A, alors

$$x \text{ solution} \iff x_1C_1 + \cdots + x_pC_p = B$$

Dans le cas d'un système de Cramer, pour x solution,

$$\det(B, C_2, \cdots, C_n) = \det(x_1C_1 + \cdots + x_nC_n, C_2, \cdots, C_n) = x_1 \det A$$

donc

$$x_1 = \frac{\det(B, C_2, \cdots, C_n)}{\det A}.$$

De même,

$$x_j = \frac{\det(C_1, \cdots, C_{j-1}, B, C_{j+1}, \cdots, C_n)}{\det A}$$

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre IX

Réduction des endomorphismes

Sommaire

Dans tout le chapitre, on note $\mathbf{K}$ un corps.

1 Rappels sur les polynômes

Théorème.

(H) $A, B \in \mathbf{K}[X]$, $B \neq 0$

(C) Il existe un unique couple de polynômes (Q, R) dans $\mathbf{K}[X]$ tels que

$$A = QB + R$$

et $\deg R < \deg B$

Théorème – Définition.

$a \in \mathbf{K}$ est une racine de P si et seulement si

$$P(a) = 0 \iff (X - a) \mid P$$

et a est racine de multiplicité $\alpha \geqslant 1$ si et seulement si

$$\begin{cases} P(a) = P'(a) = \cdots = P^{(\alpha-1)}(a) = 0 \\ P^{(\alpha)}(a) \neq 0 \end{cases} \iff \begin{cases} (X - a)^{\alpha} \mid P \\ (X - a)^{\alpha+1} \nmid P \end{cases}$$

Si a n'est pas racine de P, on convient que a est racine de multiplicité 0.

Théorème (Interpolation de Lagrange).

Pour $a_1, \cdots, a_n \in \mathbf{R}$ des abscisses distinctes et $b_1, \cdots, b_n \in \mathbf{R}$ des ordonnées distinctes, il existe un unique polynôme de degré au plus $n - 1$ tel que

$$\forall i \in [\![1, n]\!], \qquad P(a_i) = b_i$$

Démonstration.

$$\varphi : P \in \mathbf{K}_{n-1}[X] \longmapsto (P(a_1), \cdots, P(a_n)) \in \mathbf{R}^n$$

est un isomorphisme. □

2 Idéaux de $\mathbf{K}[X]$ et arithmétique

Théorème.

$\mathbf{K}[X]$ est principal

Démonstration. C'est un anneau euclidien donc principal (cf. chapitre **Algèbre générale**) □

Théorème – Définition.

1. Il existe un unique polynôme unitaire Q tel que $P\mathbf{K}[X] + Q\mathbf{K}[X] = Q\mathbf{K}[X]$. C'est le PGCD de A et B. Deux polynômes sont premiers entre eux si leur PGCD vaut 1.
2. Il existe un unique polynôme unitaire Q tel que $P\mathbf{K}[X] \cap Q\mathbf{K}[X] = Q\mathbf{K}[X]$. C'est le PPCM de A et B.
3. (Gauss) Si A et B sont premiers entre eux et $A \mid BC$ alors $A \mid C$
4. (Bézout) A et B sont premiers entre eux si et seulement si il existe U, V tels que $AU + BV = 1$.

Exemple. $(X^n - 1) \wedge (X^m - 1) = X^{n \wedge m} - 1$

3 Décomposition en facteurs irréductibles

Définition.

Un anneau A est factoriel si

1. Pour tout $a \in A$, il existe des éléments irréductibles $p_1, \cdots, p_n$ tels que $a = p_1 \cdots p_n$
2. Cette décomposition est unique à l'ordre des facteurs près et à association près (deux éléments a et b sont associés si il existe un inversible u tel que $a = ub$)

Théorème.

$\mathbf{K}[X]$ est un anneau factoriel

Exemple. Dans $\mathbf{C}[X]$,

- $$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega)$$
- $$X^{2m} - 1 = (X + 1)(X - 1) \prod_{k=1}^{n-1} \left(X - \exp\left(\frac{ik\pi}{n}\right) \right) \left(X - \exp\left(-\frac{ik\pi}{n}\right) \right)$$

Exercice.

Montrer que

- $P(\mathbf{R}) \subset \mathbf{R}_+ \iff \exists A, B \in \mathbf{R}[X], P = A^2 + B^2$
- $P(\mathbf{R}_+) \subset \mathbf{R}_+ \iff \exists A, B \in \mathbf{R}[X], P = A^2 + XB^2$

Résolution. Éléments de résolution pour le premier point : l'ensemble des $A^2 + B^2$ est stable par produit, et en décomposant $P \geqslant 0$ en facteurs irréductibles, chacun des facteurs est somme de deux carrés. □

Exercice.

P unitaire de degré n dans $\mathbf{R}[X]$. Montrer

$$P \text{ scindé dans } \mathbf{R}[X] \iff \forall z \in \mathbf{C}, \quad |P(z)| \geqslant |\mathfrak{Im}(z)|^n$$

Démonstration.

- ($\Longleftarrow$) P scindé dans $\mathbf{C}$ de racines (a_i). $0 = |P(a_i)| \geqslant |\mathfrak{Im}(z)|^n$ donc $a_i \in \mathbf{R}$
- ($\Longrightarrow$)

$$|P(x+iy)| = \left|\prod_{j=1}^{n}(x - a_j + iy)\right| = \prod_{j=1}^{n} |x - a_j + iy| \geqslant \||\mathfrak{Im}(z)|^n$$

□

4 Polynômes d'endomorphismes

Définition – Proposition.

(H) On note E un $\mathbf{K}$-e.v., $u \in \mathscr{L}(E)$ et

$$P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbf{K}[X]$$

(C) 1.

$$P(u) \underset{\text{def}}{=} \sum_{k=0}^{+\infty} a_k u^k$$

2. $\varphi : P \in \mathbf{K}[X] \longmapsto P(u) \in \mathscr{L}(E)$ est un morphisme d'algèbres.

Démonstration. On justifie $(PQ)(u) = P(u) \circ Q(u)$. On considère

$$\psi : (P, Q) \in \mathbf{K}[X]^2 \longmapsto (PQ)(u) - P(u) \circ Q(u) \in \mathscr{L}(u)$$

- ψ est bilinéaire
- À Q fixé, $P \longmapsto \psi(P, Q)$ AL nulle si et seulement si $\forall j \in \mathbf{N}, \psi(X^j, Q) = 0$
- Pour chaque j, $Q \longmapsto \psi(X^j, Q)$ nulle si et seulement si $\forall k \in \mathbf{N}, \psi(X^j, X^k) = 0$ qui est vrai.

□

Définition.

Un polynôme P est dit **polynôme annulateur** de $u \in \mathscr{L}(E)$ si $P(u)$ est l'application nulle

Exemple. p est un projecteur si et seulement si $X^2 - X$ est annulateur. s est une symétrie si et seulement si $X^2 - 1$ est annulateur

Définition – Proposition.

L'ensemble des polynômes annulateurs d'un endomorphisme u est un idéal. Il possède un unique générateur unitaire, qu'on appelle **polynôme minimal**, qu'on notera μ_u ou Π_u

Démonstration. $(\mathrm{id}, u, \cdots, u^{n^2})$ famille liée de $\mathscr{L}(E)$ donc l'idéal n'est pas trivial □

Proposition.
$\mathbf{K}[u] \underset{\text{def}}{=} \{P(u), P \in \mathbf{K}[X]\}$ est une $\mathbf{K}$-algèbre de dimension $\deg \mu_u$ de base $(1, u, \cdots, u^{\deg \mu_u - 1})$

Exemple. $P = X^2 - 3X + 2$ polynôme minimal

$$A = \begin{pmatrix} -2 & -6 \\ 2 & 5 \end{pmatrix}$$

Puis $X^n = \mu_A \times Q + \alpha_n X + \beta_n$. En injectant 1 et 2 (les racines de μ_A) on peut exprimer α_n et β_n et $A^n = \alpha_n A + \beta_n$

5 Théorème de décomposition des noyaux

Théorème (Décomposition des noyaux).

(H) E un $\mathbf{K}$-e.v., $u \in \mathscr{L}(E)$

(C)
1. Si $P, Q \in \mathbf{K}[X]$ sont premiers entre eux, alors $\operatorname{Ker}(PQ)(u) = \operatorname{Ker} P(u) \oplus \operatorname{Ker} Q(u)$. En particulier, si PQ est annulateur alors $\operatorname{Ker}(PQ)(u) = E$
2. Si $P_1, \cdots, P_q \in \mathbf{K}[X]$ deux à deux premiers entre eux et si $P = P_1 \cdots P_q$ alors
$$\operatorname{Ker} P(u) = \operatorname{Ker} P_1(u) \oplus \cdots \oplus \operatorname{Ker} P_q(u)$$
3. Dans ce cas, si $Q_i = \frac{P}{P_i}$,
   (a) Il existe $U_1, \cdots, U_q$ tels que $U_1 Q_1 + \cdots + U_q Q_q = 1$
   (b) $(U_i Q_i)(u)$ est la projection sur $\operatorname{Ker} P_i(u)$ associée à la décomposition

Démonstration.
1. On écrit $UP + QV = 1$ et si $x \in \operatorname{Ker} P(u) \cap \operatorname{Ker} Q(u)$ alors $(UP + QV)(u)(x) = 0 = \operatorname{id}(x) = x$ donc la somme est directe
   Puis, la valeur de la somme est la bonne car $\operatorname{Ker} P(u), \operatorname{Ker} Q(u) \subseteq \operatorname{Ker} PQ(u)$ et pour $x \in \operatorname{Ker} PQ(u)$, $x = UP(u)(x) + VQ(u)(x) \in \operatorname{Ker} Q(u) + \operatorname{Ker} P(u)$
2. Par récurrence, c'est vrai
3. Les Q_i sont premiers entre eux dans leur ensemble, donc Bézout donne (a). Puis, pour x dans $\operatorname{Ker} P(u)$,
$$x = \underbrace{U_1 Q_1(u)(x)}_{\in \operatorname{Ker} P_1(u)} + \cdots + \underbrace{U_q Q_q(u)(x)}_{\in \operatorname{Ker} P_q(u)}$$
   et la somme est directe ce qui conclut.

□

Exemple. Si $u^3 + u = 0$, alors $E = \operatorname{Ker} u \oplus \operatorname{Ker}(u^2 + \operatorname{id})$ or $\operatorname{Ker}(u^2 + \operatorname{id}) \subset \operatorname{Im} u$ donc $E = \operatorname{Ker} u + \operatorname{Im} u$

Exemple. E de dimension finie, u un endomorphisme de E tel que $u \in \operatorname{Vect}(u^k, k \geqslant 2)$. Il y a donc un polynôme annulateur pour u. De même que précédemment,

$$E = \operatorname{Ker} u \oplus \operatorname{Im} u$$

Exemple. On note E l'ensemble des suites (u_n) telles que $\forall n \in \mathbf{N}, u_{n+3} = 4u_{n+2} - 5u_{n+1} + 2u_n$. On note T l'endomorphisme $(u_n)_n \longmapsto (u_{n+1})_n$ de sorte que

$$E = \operatorname{Ker}(T^3 - 4T^2 + 5T - 2\operatorname{id}) = \operatorname{Ker}((T - \operatorname{id})^2) \oplus \operatorname{Ker}(T - 2\operatorname{id})$$

et $\operatorname{Ker}(T - 2\operatorname{id}) = \{\lambda(2^n)_n, \lambda \in \mathbf{R}\}$, $\operatorname{Ker}(T - \operatorname{id}) = \{(\lambda)_n, \lambda \in \mathbf{R}\}$ puis

$$u \in \operatorname{Ker}((T - \operatorname{id})^2) \iff T(u) - u \in \operatorname{Ker}(T - \operatorname{id}) \iff (u_{n+1} - u_n)_n = (\lambda)_n$$

donc $\operatorname{Ker}((T - \operatorname{id})^2) = \{(\nu + n\mu)_n, \nu, \mu \in \mathbf{R}\}$

6 Valeurs propres, vecteurs propres

Définition.

Pour E un $\mathbf{K}$-e.v. et u endomorphisme de E,

1. On dira que $\lambda \in \mathbf{K}$ est **valeur propre** de u si $\operatorname{Ker}(u - \lambda \operatorname{id}) \neq \{0\}$
2. On dira que $x \in E$ est un **vecteur propre** associé à la valeur propre λ si $x \in \operatorname{Ker}(u - \lambda \operatorname{id}) \setminus \{0\}$
3. L'ensemble des valeurs propres (appelé **spectre**) est noté $\operatorname{Sp}_{\mathbf{K}}(u)$ ou simplement $\operatorname{Sp}(u)$.
4. L'ensemble des vecteurs propres pour la valeur propre λ (on compte le vecteur nul pour garder la structure d'e.v.) est noté $E_\lambda = \operatorname{Ker}(u - \lambda \operatorname{id})$ et s'appelle **sous-espace propre** de u pour λ.

a) Étude du spectre

Proposition.

(H) $u, v \in \mathscr{L}(E)$, $P \in \mathbf{K}[X]$ et $\lambda \in \mathbf{K}$

(C)
1. Si u et v commutent, alors $\operatorname{Ker} u$ et $\operatorname{Im} u$ sont stables par v. De même, $E_\lambda(u)$ est stable par v.
2. Si $x \in E_\lambda(u)$, $P(u)(x) = P(\lambda)x$
3. $P(\lambda) \in \operatorname{Sp}_{\mathbf{K}}(P(u))$ pour $\lambda \in \operatorname{Sp}_{\mathbf{K}}(u)$
4. Si P est annulateur alors $\operatorname{Sp}_{\mathbf{K}}(u) \subseteq \mathscr{Z}_{\mathbf{K}}(P)$
5. $\operatorname{Sp}_{\mathbf{K}}(u) = \mathscr{Z}_{\mathbf{K}}(\mu_u)$

Démonstration.

1. 2. 3. Ok
4. $P(u)(x) = P(\lambda)x$ pour x vecteur propre $\implies P(\lambda) = 0$ pour P annulateur
5. On a une inclusion par 4.
   Si λ racine de μ_u dans $\mathbf{K}$ alors
   $$\lambda \notin \operatorname{Sp}(u) \implies u - \lambda \operatorname{id} \in \operatorname{GL}(E)$$
   donc dans ce cas $\mu_u = (X - \lambda)Q$ et $Q(u) = 0$ absurde par minimalité de μ_u. Donc $\lambda \in \operatorname{Sp}(u)$

□

b) Polynôme caractéristique

Théorème – Définition.

(H) $u \in \mathscr{L}(E)$ avec E un $\mathbf{K}$-e.v. de dimension n, muni d'une base $\mathscr{B}$. $\mathscr{M}_{\mathscr{B}}(u) \underset{\text{def}}{=} A$

(C)
1. Il y a équivalence entre
   (a) $\lambda \in \operatorname{Sp}_{\mathbf{K}}(u)$
   (b) $\det(\lambda \operatorname{id} - u) = 0$
   (c) $\det(\lambda I_n - A) = 0$
2. Le polynôme $\chi_A = \chi_u$ donné par $\det(X \operatorname{id} - u) = \det(XI_n - A)$ est appelé **polynôme caractéristique** de A (ou de u)
3. χ_A est unitaire de degré n et
   $$\chi_A = X^n - \operatorname{Tr}(A)X^{n-1} + \cdots + (-1)^n \det A$$
4. $\operatorname{Sp}_{\mathbf{K}}(u) = \mathscr{Z}_{\mathbf{K}}(\chi_u)$

Démonstration. 1. 2. Ok

3. Le polynôme est unitaire de degré n car la seule permutation qui donne un coefficient de degré n dans la formule du déterminant est l'identité, et ce coefficient vaut 1. Toutes les autres permutations ne donnent que des coefficients de degré $< n-1$ donc le coefficient de X^{n-1} ne peut venir que du développement du produit de la diagonale ($\sigma = \mathrm{id}$), dont le coefficient en X^{n-1} vaut bien la trace. Pour le terme constant, on injecte 0 et par définition on obtient $\det(-A) = (-1)^n \det A$
4. $$\lambda \in \mathrm{Sp}(u) \iff \det(\lambda \,\mathrm{id} - u) = 0 \iff \lambda \in \mathscr{Z}_{\mathbf{K}}(\chi_u)$$

□

Exemple (Cas d'une matrice compagnon)**.** On note

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_p \end{pmatrix} \in \mathscr{M}_{p+1}(\mathbf{K})$$

Le calcul de $\det(XI_n - A)$ donne $\chi_A = X^{p+1} + P(X)$ avec $P(X) = a_p X^p + \cdots + a_0$

c) Théorème de Cayley-Hamilton

Théorème (Cayley-Hamilton).

> (H) E de dimension finie n et $u \in \mathscr{L}(E)$
>
> (C) χ_u est annulateur de u.

Démonstration. (Hors-Programme)

On note A canoniquement associée à u, et $B = XI_n - A$. On a

$$B\,\mathrm{Com}(B)^\top = \det(B) I_n = \chi_A(X) I_n$$

$\mathrm{Com}(B)^\top$ a des coefficients dans $\mathbf{K}_{n-1}[X]$ donc il existe des matrices $B_0, \cdots, B_{n-1}$ telles que

$$\mathrm{Com}(B)^\top = X^{n-1}B_{n-1} + \cdots + B_0.$$

Alors,

$$\begin{aligned} B\,\mathrm{Com}(B)^\top &= (XI_n - A)(X^{n-1}B_{n-1} + \cdots + B_0) \\ &= X^n B_{n-1} + X^{n-1}(B_{n-2} - AB_{n-1}) + \cdots + X(B_0 - AB_1) - AB_0 \\ &= \chi_A(X) I_n \end{aligned}$$

On identifie :

$$B_{n-1} = I_n \qquad \text{et les autres } B_{i+1} - AB_i \text{ sont de la forme } \alpha_i I_n, \alpha_i \in \mathbf{R}$$

Si on note $\chi_A = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, on a

$$B_{n-2} - AB_{n-1} = a_{n-1} I_n \quad , \quad \cdots \quad , \quad B_0 - AB_1 = a_1 I_n \quad , \quad -AB_0 = a_0 I_n$$

En remplaçant dans $\chi_A(A)$ tous les termes s'annulent. □

Conséquence.

- Pour A dans $\mathscr{M}_n(\mathbf{K})$, $\mu_A \mid \chi_A$ donc $\deg \mu_A \leqslant n$
- Si
$$\chi_A = \prod_{i=1}^{r} (X - \lambda_i)^{\alpha_i}$$
avec des λ_i deux à deux distincts, alors
$$\mathscr{M}_n(\mathbf{K}) = \bigoplus_{i=1}^{r} \mathrm{Ker}\left((A - \lambda_i I_n)^{\alpha_i}\right)$$

- Si A est nilpotente alors $A^n = 0$ car $\deg \mu_A \leqslant n$

Exercice.

> $A \in \mathcal{M}_n(\mathbf{C})$ non inversible. Montrer qu'il existe $B \in \mathcal{M}_n(\mathbf{C})$ non nulle telle que $\forall p \geqslant 1, (A+B)^p = A^p + B^p$

Éléments de résolution. $\mu_A = XP(X)$, $P(A) \neq 0$ par minimalité de μ_A et $P(A)$ convient. □

Exercice.

> Montrer que $A^3 + A^2 + A + I_n = 0 \implies \operatorname{Tr} A \leqslant 0$

Éléments de résolution. $P(X) = (X+1)(X^2+1)$ est annulateur donc $\mathrm{Sp}_{\mathbf{C}}(A) \subseteq \{-1, i, -i\}$ et $\chi_A = (X+1)^\alpha (X+i)^\beta (X-i)^\gamma$ polynôme réel donc $\beta = \gamma$ et la trace est le coeff en X^{n-1} □

Exercice.

> On note A une matrice de $\mathcal{M}_n(\mathbf{C})$. Montrer que si $P \in \mathbf{C}[X]$, alors $P(A)$ est inversible si et sulement si $P \wedge \chi_A = 1$ si et seulement si $P \wedge \mu_A = 1$

Résolution.

- Si Q annulateur tel que $P \wedge Q = 1$, il existe $\exists U, V, \quad UP + QV = 1$ donc $U(A)P(A) = I_n$ et $P(A)$ inversible
- Si $P(A)$ inversible alors on suppose $\Delta = P \wedge \chi_A$ non constant divisible par $X - \lambda$ et $P(X) = (X-\lambda)Q(X)$ donc

$$P(A) = \underbrace{(A - \lambda I_n)}_{\text{non-inversible car } \chi_A(\lambda)=0} Q(A)$$

  donc $P(A)$ n'est pas inversible, c'est absurde.

□

Exercice.

> $A \in \mathrm{GL}_5(\mathbf{R}), \operatorname{Tr} A = 2, A^3 + A^2 - 2A = 0$. Trouver χ_A

Élément de résolution. A inversible donc $X^2 + X - 2$ annulateur. $\mathrm{Sp}(A) \subset \{1, -2\}$ donc

$$\chi_A = (X-1)^\alpha (X+2)^\beta,$$

$\alpha + \beta = 5$, $\operatorname{Tr} A = \alpha - 2\beta = 2$ donc $\alpha = 4, \beta = 1$ □

Exercice.

> Pour $A, B \in \mathcal{M}_n(\mathbf{R})$. Montrer que $\chi_{AB} = \chi_{BA}$

Résolution (Première méthode).

$$\begin{pmatrix} A & -XI_n \\ I_n & 0 \end{pmatrix} \begin{pmatrix} B & -XI_n \\ I_n & -A \end{pmatrix} = \begin{pmatrix} AB - XI_n & 0 \\ B & -XI_n \end{pmatrix}$$

et

$$\begin{pmatrix} B & -XI_n \\ I_n & -A \end{pmatrix} \begin{pmatrix} A & -XI_n \\ I_n & 0 \end{pmatrix} = \begin{pmatrix} BA - XI_n & -XB \\ 0 & -XI_n \end{pmatrix}$$

donc $\chi_{AB} = \chi_{BA}$ □

Résolution (Deuxième méthode). Si A inversible, $AB = A(BA)A^{-1}$ donc $\chi_{AB} = \chi_{BA}$. Puis, dans le cas général on se place dans $\mathbf{K}(T)$ (le corps des fractions rationnelles sur $\mathbf{K}$) et $A - TI_n$ est inversible, d'où

$$\chi_{B(A-TI_n)} = \chi_{(A-TI_n)B}$$

et on prend T=0. □

7 Étude des sous-espaces propres

Proposition.

(H) E un **K**-e.v. et u un endomorphisme de E. On note $\lambda_1, \cdots, \lambda_p$ des valeurs propres de u deux à deux distinctes

(C) Les sous-espaces propres E_λ sont en somme directe

Démonstration. C'est le théorème de décomposition des noyaux sur $P = (X - \lambda_1) \cdots (X - \lambda_p)$ □

Proposition.

(H) E un **K**-e.v. et F un s.e.v. de E stable par un endomorphisme u de E.

(C) $\chi_{u_{|F}}$ divise χ_u et $\mu_{u_{|F}}$ divise μ_u

Démonstration. $\mu_u(u) = 0$ donc $\mu_u(u)_{|F} = \mu_u(u_{|F}) = 0$ donc $\mu_{u_{|F}} \mid \mu_u$. On note $\mathscr{F} = (e_1, \cdots, e_p)$ une base de F qu'on complète en base $\mathscr{B}$ de E. On note $A = \mathscr{M}_{\mathbb{F}}(u_{|F})$. On a

$$\mathscr{M}_{\mathscr{B}}(u) = \left(\begin{array}{c|c} A & * \\ \hline 0 & B \end{array}\right)$$

donc $\chi_u = \chi_A \chi_B$ □

Théorème – Définition.

(H) u endomorphisme en dimension finie

(C)
1. Si $\lambda \in \mathrm{Sp}_{\mathbf{K}}(u)$ alors on appelle **multiplicité algébrique** de λ la multiplicité de λ dans χ_u, notée $m_\lambda(u)$
2. Si $\lambda \in \mathrm{Sp}_{\mathbf{K}}(u)$ alors $1 \leqslant \dim E_\lambda(u) \leqslant m_\lambda(u)$

Démonstration.

$$x \in \mathrm{Ker}(u - \lambda\,\mathrm{id}) \implies (u - \lambda\,\mathrm{id})^r(x) = (u - \lambda\,\mathrm{id})^{r-1} \circ (u - \lambda\,\mathrm{id})(x) = 0 \implies x \in \mathrm{Ker}((u - \lambda\,\mathrm{id})^r)$$

puis théorème de décomposition des noyaux □

8 Endomorphismes diagonalisables

Définition – Proposition.

On note E un **K**-e.v., u un endomorphisme de E. On dira qu'il est **diagonalisable** s'il satisfait l'une des propriétés équivalentes suivantes :

1. Il existe une base de E constituée de vecteurs propres pour u
2. Il existe une base de E dans laquelle u a une matrice diagonale
3. Il existe une base de E dans laquelle la matrice de u est semblable à une matrice diagonale

Théorème.

(H) E un **K**-e.v. de dimension finie, u un endomorphisme, $\lambda_1, \cdots, \lambda_p$ les valeurs propres distinctes de u

(C) Il y a équivalence entre

(a) u est diagonalisable

(b) $E_{\lambda_1}(u) \oplus \cdots \oplus E_{\lambda_p}(u) = E$

(c)

$$\sum_{i=1}^{p} \dim E_{\lambda_i}(u) = \dim E$$

(d) χ_u est scindé sur $\mathbf{K}$ et $m_\lambda(u) = \dim E_\lambda(u)$ pour $\lambda \in \mathrm{Sp}_{\mathbf{K}}(u)$

(e) μ_u scindé à racines simples dans $\mathbf{K}$

(f) Il existe P annulateur scindé à racines simples. Dans ce cas,

$$\mu_u = \prod_{\lambda \in \mathrm{Sp}_{\mathbf{K}}(u)} (X - \lambda)$$

Démonstration.

- $(a \implies b)$ Il existe une base de vecteurs propres, on les regroupe par valeurs propres et on a le résultat.
- $(b \implies c)$ Clair
- $(c \implies d)$ $\chi_u = (X-\lambda_1)^{\alpha_1} \cdots (X-\lambda_p)^{\alpha_p} P(X)$ et

$$\dim E = \sum_{i=1}^{p} \dim E_{\lambda_i} \leqslant \sum_{i=1}^{p} m_{\lambda_i}(u) \leqslant \dim E$$

  donc $P = 1$ et (C)
- $(d \implies e)$ On a $(d \implies b)$ puis $(b \implies a)$ donc dans $\mathscr{B}$ adaptée,

$$A \underset{\text{def}}{=} \mathscr{M}_{\mathscr{B}}(u) = \begin{pmatrix} \lambda_1 I_{r_1} & & (0) \\ & \ddots & \\ (0) & & \lambda_p I_{r_p} \end{pmatrix}$$

  et

$$(A - \lambda_1 I_n) \cdots (A - \lambda_p I_n) = \begin{pmatrix} 0 & & & (0) \\ & * & & \\ & & \ddots & \\ (0) & & & * \end{pmatrix} \begin{pmatrix} * & & & (0) \\ & 0 & & \\ & & \ddots & \\ (0) & & & * \end{pmatrix} \cdots \begin{pmatrix} * & & & (0) \\ & \ddots & & \\ & & * & \\ (0) & & & 0 \end{pmatrix}$$

  donc $(X-\lambda_1)\cdots(X-\lambda_p)$ annulateur scindé à racines simples
- $(e \implies f)$ Clair
- $(f \implies a)$ TDN sur P puis on enlève les $E_{\lambda_i}(u) = \{0\}$ dans la décomposition

□

Exercice.

On note

$$A = \begin{pmatrix} -3 & 4 & 0 \\ 1 & 3 & 3 \\ 1 & -2 & 0 \end{pmatrix}$$

Calculer χ_A. A est-elle diagonalisable ? Si oui, diagonaliser A.

Résolution (partielle). $\chi_A(X) = (X+3)(X-1)(X-2)$ annulateur scindé à racines simples donc A diagonalisable. Les trois vecteurs

$$\begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \qquad \begin{pmatrix} 4 \\ 5 \\ -3 \end{pmatrix} \qquad \begin{pmatrix} -3 \\ 0 \\ 1 \end{pmatrix}$$

sont des vecteurs propres. ☐

Exercice.

$A \in \mathrm{GL}(\mathbf{C})$. Montrer que A^2 est diagonalisable si et seulement si A l'est.

Éléments de résolution. Le sens réciproque est immédiat, on ne montre que le sens direct. Si A^2 est diagonalisable de valeurs propres $\lambda_1, \cdots, \lambda_p$, on écrit $\delta_i^2 = \lambda_i$ et $X^2 - \delta_i^2 = (X - \delta_i)(X + \delta_i)$ donc TDN et $\mathrm{Ker}(A^2 - \lambda_i I_n) = \mathrm{Ker}(A - \delta_i I_n) \oplus \mathrm{Ker}(A + \delta_i I_n)$ ☐

Exercice.

Donner une CNS de diagonalisabilité pour une matrice diagonale par blocs

Réponse. Une matrice $A = \mathrm{diag}(A_1, \cdots, A_p)$ est diagonalisable ssi les A_i le sont. ☐

9 Sous-espaces stables

a) Restriction

Proposition.

(H) u endomorphisme diagonalisable (dimension finie), V s.e.v. stable par u.

(C) $u_{|V}$ est diagonalisable et

$$V = \bigoplus_{\lambda \in \mathrm{Sp}_{\mathbf{K}}(u)} E_\lambda(u) \cap V$$

Démonstration. μ_u scindé annulateur à racines simples et $E_\lambda(u_{|V}) = E_\lambda(u) \cap V$ ☐

b) Décomposition de Dunford (HP)

Résultat.

Soit u un endomorphisme en dimension finie n dont le polynôme caractéristique est scindé, A sa matrice dans une base $\mathscr{B}$. Il existe une matrice diagonalisable D et une matrice nilpotente N qui commutent et telles que $A = D + N$. Cette écriture est unique.

Démonstration. On suppose $\chi_A = (X - \lambda_1)^{\alpha_1} \cdots (X - \lambda_r)^{\alpha_r}$ avec les λ_i deux à deux distincts et les $\alpha_i \geqslant 1$.

Le théorème de décomposition des noyaux donne

$$\mathscr{M}_{n,1}(\mathbf{K}) = \underbrace{\mathrm{Ker}(A - \lambda_1 I_n)^{\alpha_1}}_{\underset{\mathrm{def}}{=} \Gamma_1(A)} \oplus \cdots \oplus \Gamma_r(A).$$

A et $(A - \lambda I_n)^{\alpha_i}$ commutent donc $\Gamma_i(A)$ est stable par A et

$$(A - \lambda_i I_n)^{\alpha_i}_{|\Gamma_i(A)} = 0 = (A_{|\Gamma_i(A)} - \lambda_i I_{n|\Gamma_i(A)})^{\alpha_i}$$

d'où

$$A_{|\Gamma_i(A)} = \underbrace{\lambda_i I_{n|\Gamma_i(A)}}_{D_i \text{ diagonalisable}} + \underbrace{\left(A_{|\Gamma_i(A)} - \lambda_i I_{n|\Gamma_i(A)}\right)}_{N_i \text{ nilpotente}}$$

et $D_i N_i = N_i D_i$

Dans une base $\mathscr{F}$ adaptée à la décomposition, on a

$$\mathscr{M}_{\mathscr{F}}(A) = \begin{pmatrix} D_1 + N_1 & & (0) \\ & \ddots & \\ (0) & & D_r + N_r \end{pmatrix}$$

et $\chi_A = \chi_{D_1+N_1} \times \cdots \times \chi_{D_r+N_r} = (X-\lambda_1)^{r_1}\cdots(X-\lambda_r)^{r_r}$ avec $r_i = \dim \Gamma_i(R)$. On en déduit $\dim \Gamma_i(A) = \alpha_i$ et on conclut sur l'existence avec

$$D = \begin{pmatrix} D_1 & & \\ & \ddots & \\ & & D_r \end{pmatrix} \qquad N = \begin{pmatrix} N_1 & & \\ & \ddots & \\ & & N_r \end{pmatrix} \qquad DN = ND$$

Par ailleurs, si on note π_i le projecteur sur $\Gamma_i(A)$ associé à la décomposition, π_i est un polynôme en A (d'après le théorème de décomposition des noyaux) donc $D = \sum \lambda_i \pi_i$ aussi et $N = A - D$ aussi.

On suppose que D' et N' conviennent aussi. Dans ce cas, $D - D' = N - N'$. N et N' commutent car N est un polynôme en A et N' commute avec A donc $N - N'$ est nilpotente. $D - D'$ est diagonalisable nilpotente donc nulle ce qui conclut sur l'unicité. $\square$

c) Diagonalisation simultanée

On va montrer que si $(f_i)_{i\in I}$ est une famille d'endomorphismes diagonalisables qui commutent alors on peut les diagonaliser dans une base commune.

On procède par récurrence sur $n = \dim E$.

- $n = 1$ c'est trivial
- $n \geqslant 1$, on suppose que c'est vrai au rang n et on prend E tel que $\dim E = n+1$
  - — *Premier cas.* Tous les f_i sont des homothéties. Il n'y a rien à faire.
  - — *Second cas.* L'endomorphisme f_{i_0} n'est pas une homothétie.

$$E = \bigoplus_{\lambda \in \mathrm{Sp}_{\mathbf{K}}(f_{i_0})} \underbrace{E_\lambda(f_{i_0})}_{\dim \leqslant n}.$$

  Les $E_\lambda(f_{i_0})$ sont stables par tous les f_i et les $f_{i|E_\lambda(f_{i_0})}$ sont diagonalisables donc il existe une base $\mathscr{B}_\lambda$ de $E_\lambda(f_{i_0})$ qui les diagonalise (par H). Il suffit de concaténer les $\mathscr{B}_\lambda$ pour conclure.

10 Utilisation des polynômes d'interpolation

On note $A \in \mathscr{M}_n(\mathbf{K})$, $\mathrm{Sp}_{\mathbf{K}}(A) = \{\lambda_1, \cdots, \lambda_r\}$, A diagonalisable.

- $\mathscr{M}_{n,1}(\mathbf{K}) = E_{\lambda_1}(A) \oplus \cdots \oplus E_{\lambda_r}(A)$
- On note
$$\Delta_i = \prod_{j\neq i} \frac{X-\lambda_j}{\lambda_i - \lambda_j}$$
- $\Delta_1 + \cdots + \Delta_r(X) - 1$ est de degré $\leqslant r-1$ et s'annule en $\lambda_1, \cdots, \lambda_r$ donc c'est le polynôme nul et $\sum \Delta_i = 1$
- On a $\mu_A = (X-\lambda_1)\cdots(X-\lambda_r)$ donc $(X-\lambda_i)\Delta_i$ est divisible par μ_A de sorte que $\forall X, \quad \Delta_i(A)X \in E_{\lambda_1}(A)$

  Puis, $\forall X, \Delta_1(A)X + \cdots \Delta_r(A) = X$ donc $\Delta_i(A)$ est le projecteur sur $E_{\lambda_i}(A)$ associé à la décomposition. De plus, en appliquant A,
$$\lambda_1\Delta_1(A)X + \cdots + \lambda_r\Delta_r(A) = AX$$
  qui est vrai pour tout X donc
$$A = \lambda_1\Delta_1(A) + \cdots + \lambda_r\Delta_r(A)$$
  Pour $i \neq j$, $\Delta_i(A)\Delta_j(A) = 0$ (le polynôme est divisible par μ_A) donc par récurrence (presque) immédiate,
$$\forall k \geqslant 0, \qquad A^k = \lambda_1^k\Delta_1(A) + \cdots + \lambda_r^k\Delta_r(A)$$

Exemple. On note
$$A = \begin{pmatrix} 3 & -3 & 2 \\ -1 & 5 & -2 \\ -1 & 3 & 0 \end{pmatrix}$$
et $\chi_A = (X-4)(X-2)^2$ diagonalisable car $\mu_A = (X-4)(X-2)$ est annulateur scindé à racines simples Les projecteurs spectraux sont $\Delta_4 = \frac{X-2}{4-2}$, $\Delta_2 = \frac{X-4}{2-4}$, donc
$$\forall n \geqslant 0, A^n = 4^n \Delta_4(A) + 2^n \Delta_2(A)$$

11 Trigonalisation

Théorème – Définition.

(H) u endomorphisme en dimension finie n

(C)
1. On dit que u est trigonalisable s'il existe une base $\mathscr{B}$ de E telle que $\mathscr{M}_{\mathscr{B}}(u)$ est triangulaire
2. Il y a équivalence entre
   (a) u est trigonalisable
   (b) χ_u est scindé sur $\mathbf{K}$
   En particulier, Si $\mathbf{K} = \mathbf{C}$, tous les endomorphismes sont trigonalisables

Démonstration. ($a \implies b$) Si $\mathscr{M}_{\mathscr{B}}(u) = (a_{i,j})$ alors $\chi_u = \prod_{i=1}^{n}(X - a_{i,i})$ scindé sur $\mathbf{K}$.

($b \implies a$) Par récurrence sur n :
- $n = 1$ clair
- $n \geqslant 1$, on suppose la propriété vraie au rang n et on note E tel que $\dim E = n+1$, $u \in \mathscr{L}(E)$ et χ_u scindé. On note e_1 un vecteur propre associé à la valeur propre $\lambda \in \mathrm{Sp}(u)$, et on complète (e_1) en une base $\mathscr{B}$ de E.
$$\mathscr{M}_{\mathscr{B}}(u) = \left(\begin{array}{c|c} \lambda & * \\ \hline 0 & \\ \vdots & A \\ 0 & \end{array}\right)$$
et on applique HR sur A.

□

Remarque.

Si $A \in \mathscr{M}_n(\mathbf{C})$ alors il existe $P \in \mathrm{GL}_n(\mathbf{C})$ telle que
$$PAP^{-1} = \begin{pmatrix} d_1 & & * \\ & \ddots & \\ (0) & & d_n \end{pmatrix}.$$
- $\chi_A = (X-d_1)\cdots(X-d_n)$ donc $\mathrm{Sp}_{\mathbf{C}}(A) = \{d_1, \cdots, d_n\}$
- On note $\mathrm{Sp}_{\mathbf{C}}(A)^{\mathrm{comp}}$ le multi-ensemble des valeurs-propres (c'est-à-dire l'ensemble des valeurs propres répétées avec leur multiplicité). On a
$$\mathrm{Tr}(A) = \sum_{\lambda \in \mathrm{Sp}_{\mathbf{C}}(A)^{\mathrm{comp}}} \lambda \qquad \mathrm{Tr}(A^k) = \sum_{\lambda \in \mathrm{Sp}_{\mathbf{C}}(A)^{\mathrm{comp}}} \lambda^k$$
et
$$\det A = \prod_{\lambda \in \mathrm{Sp}_{\mathbf{C}}(A)^{\mathrm{comp}}} \lambda$$

a) Trigonalisation simultanée

On note $(A_i)_i$ des matrices trigonalisables qui commutent deux à deux. Il existe $P \in \mathrm{GL}_n(\mathbf{K})$ telle que pour tout i, PA_iP^{-1} est triangulaire supérieure.

La démonstration est identique à celle de la diagonalisation simultanée.

b) Trigonalisation effective

On note

$$A = \begin{pmatrix} 0 & 1 & 0 & 2 \\ -3 & 0 & 4 & 0 \\ 0 & 1 & 0 & 3 \\ -1 & 0 & 1 & 0 \end{pmatrix}$$

On a

$$\chi_A = \begin{vmatrix} X & -1 & 0 & -2 \\ 3 & X & -4 & 0 \\ 0 & -1 & X & -3 \\ 1 & 0 & -1 & X \end{vmatrix} = X^4 - 2X^2 + 1 = (X+1)^2(X-1)^2$$

La matrice est diagonalisable ssi $\mu_A = (X+1)(X-1)$ ce qui est faux. Le TDN donne

$$\mathbf{R}^4 = \mathrm{Ker}(A - I_4)^2 \oplus \mathrm{Ker}(A + I_4)^2$$

et

$$(A - I_4)^2 = \begin{pmatrix} -4 & -2 & 6 & -4 \\ 6 & 2 & -8 & 6 \\ -6 & -2 & 8 & -6 \\ 2 & 0 & -2 & 2 \end{pmatrix}$$

d'où

$$\begin{aligned} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \in \mathrm{Vect}(A - I_4)^2 &\iff \begin{cases} 4x + 2y - 6z + 4t = 0 \\ 6x + 2y - 8z + 6t = 0 \\ 6x + 2y - 8z + 6t = 0 \\ 2x \qquad - 2z + 2t = 0 \end{cases} \\ &\iff \begin{cases} y = z \\ x = z - t \end{cases} \\ &\iff \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \in \mathrm{Vect}\left(\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \underbrace{\begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}}_{\notin \mathrm{Ker}(A - I_4)} \right) \end{aligned}$$

On note

$$(e_1, e_2) \underset{\text{def}}{=} \left((A - I_4) \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right)$$

de sorte que $e_1, e_2 \in \mathrm{Ker}(A - I_4)^2$, $(A - I_4)e_1 = 0$ donc $Ae_1 = e_1$ et $Ae_2 = e_1 + e_2$ donc (e_1, e_2) base de $\mathrm{Ker}(A - I_4)^2$ et

$$\mathscr{M}_{(e_1, e_2)}(A_{| \mathrm{Ker}(A - I_4)^2}) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

et on fait pareil sur l'autre noyau.

c) Endomorphisme nilpotent

Définition – Proposition.

Ⓗ E un $\mathbf{K}$-e.v. de dimension n

Ⓒ 1. On dira que f est nilpotent s'il existe un $p \geqslant 1$ tel que $f^p = 0$.

2. Il y a équivalence entre
   (a) f nilpotent
   (b) $\chi_f = X^n$
   (c) f trigonalisable de spectre $\{0\}$

   Dans ce cas, l'indice de nilpotence est le degré de μ_f

Démonstration.

- ($b \implies a$) Cayley-Hamilton
- ($a \implies c$) X^p scindé annulateur, $\mathrm{Sp}(f) \subset \{0\}$ et $E_0(f) = \operatorname{Ker} f \neq \{0\}$
- ($c \implies b$) Ok

□

Remarque.

Si $f \in \mathscr{L}(E)$ et si P est annulateur scindé sur $\mathbf{K}$ alors μ_f est scindé et $\mathscr{Z}_{\mathbf{K}}(\mu_f) = \mathrm{Sp}_{\mathbf{K}}(f) = \mathscr{Z}_{\mathbf{K}}(\chi_f)$
Donc, $\chi_f = (X-\lambda_1)^{\alpha_1} \cdots (X-\lambda_p)^{\alpha_p} Q$ avec Q premier avec μ_f. Si Q non constant alors $Q(f)$ inversible.
Si Q a des racines dans $\widehat{\mathbf{K}}$, $Q(X) = (X-\lambda)\tilde{Q}(X)$ dans $\widehat{\mathbf{K}}[X]$ et $f - \lambda\,\mathrm{id}_E$ non inversible donc $\det Q(f) = \det(f-\lambda\,\mathrm{id}_E)\det\tilde{Q}(f) = 0$ absurde donc $Q = 1$

d) Caractérisation des matrices nilpotentes

Exercice.

Montrer que $A \in \mathscr{M}_n(\mathbf{C})$ est nilpotente ssi $\operatorname{Tr} A = \operatorname{Tr} A^2 = \cdots = \operatorname{Tr} A^n = 0$

Résolution.

- ($\implies$) Facile
- ($\impliedby$) On note $\lambda_1, \cdots, \lambda_p$ les valeurs propres distinctes non nulles de A, et on suppose qu'il y en a. Il existe des $n_1, \cdots, n_p \geqslant 1$ tels que

$$\begin{cases} n_1\lambda_1 + \cdots + n_p\lambda_p = \operatorname{Tr} A = 0 \\ n_1\lambda_1^2 + \cdots + n_p\lambda_p^2 = \operatorname{Tr} A^2 = 0 \\ \qquad\qquad \vdots \end{cases}$$

or

$$\begin{pmatrix} \lambda_1 & \cdots & \lambda_p \\ \vdots & \vdots & \vdots \\ \lambda_1^p & \cdots & \lambda_p^p \end{pmatrix}$$

est inversible (Vandermonde non nul) donc $(n_1, \cdots, n_p)^\top = (0, \cdots, 0)^\top$ absurde, donc il n'y a pas de valeur propre non nulle, d'où Ⓒ .

□

12 Autour du crochet de Lie

Définition (Hors-Programme).

On appelle **crochet de Lie** tout loi de composition interne $[\cdot,\cdot] : E^2 \to E$ bilinéaire alternée qui satisfait la relation de Jacobi

$$\forall x, y, z \in E, \qquad [x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$$

On dira alors que $(E, +, [\cdot,\cdot])$ est une **algèbre de Lie**.

Remarque.

On n'aborde ici que le cas où le crochet de Lie est le **commutateur** dans l'espace des endomorphismes d'un espace vectoriel :

$$\forall f, g \in \mathscr{L}(E), \qquad [f,g] = f \circ g - g \circ f$$

ou bien matriciellement :

$$\forall A, B \in \mathscr{M}_n(\mathbf{K}), \qquad [A,B] = AB - BA$$

a) Nilpotence de $\varphi : B \longmapsto [A,B]$ pour A nilpotente

On note $A \in \mathscr{M}_n(\mathbf{K})$ nilpotente, $\varphi : B \longmapsto [A,B]$. On introduit $T_G : B \longmapsto AB$ et $T_D : B \longmapsto BA$. Ces deux endomorphismes commutent et $\varphi = T_G - T_D$. Les deux endomorphismes sont nilpotents (car A nilpotente) donc φ aussi

b) Diagonalisabilité de $\varphi : B \longmapsto [A,B]$ pour A diagonale ou diagonalisable

- Si $A = \mathrm{diag}(\lambda_1, \cdots, \lambda_n)$ alors $\varphi(E_{i,j}) = (\lambda_i - \lambda_j)E_{i,j}$ donc φ diagonalisable (on a trouvé une base de vecteurs propres)
- Si A diagonalisable, on écrit $D = P^{-1}AP$ (notations évidentes) et

$$\varphi(B) = AB - BA \implies P^{-1}APP^{-1}BP - P^{-1}BPP^{-1}AP = P^{-1}\varphi(B)P = [P^{-1}AP, P^{-1}BP]$$

  On note $\psi : B \longmapsto PBP^{-1}$ et $\psi^{-1} \circ \varphi \circ \psi = B \longmapsto [D,B]$ diagonalisable.

13 Commutant d'un endomorphisme diagonalisable

Définition (Hors-Programme).

On appelle **commutant** d'un endomorphisme u l'ensemble des endomorphismes qui commutent avec u

On note $u \in \mathscr{L}(E)$, E un **K**-e.v. de dimension n. On suppose u diagonalisable. On note

$$C(u) = \{v \in \mathscr{L}(E), \quad u \circ v = v \circ u\}$$

le commutant de u.

- Si $\lambda_1, \cdots, \lambda_p$ sont les valeurs propres deux à deux distinctes de u alors

$$E = E_{\lambda_1}(u) \oplus \cdots \oplus E_{\lambda_p}(u)$$

- Si $v \in C(u)$ alors chaque s.e.p. est stable par v. On note

$$\begin{array}{rccc} \psi : & C(u) & \longrightarrow & \mathscr{L}(E_{\lambda_1}(u)) \times \cdots \times \mathscr{L}(E_{\lambda_p}(u)) \\ & v & \longmapsto & \left(v_{|E_{\lambda_1}(u)}, \cdots, v_{|E_{\lambda_p}(u)}\right) \end{array}$$

- ψ est une application linéaire injective
- Soit $(v_1, \cdots, v_p) \in \mathscr{L}(E_{\lambda_1}(u)) \times \cdots \times \mathscr{L}(E_{\lambda_p}(u))$. Il y a un antécédent correspondant, donc ψ est un isomorphisme et

$$\dim C(u) = \sum_{i=1}^{p} \dim(E_{\lambda_i}(u))^2$$

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre X

Espaces vectoriels normés

Sommaire

Dans tout le chapitre, E désigne un $\mathbf{K}$-espace vectoriel, avec $\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$, et I est un intervalle.

1 Normes

Définition.

$N : E \to \mathbf{R}$ est une norme si

- $\forall x \in E, N(x) = 0 \implies x = 0$
- $\forall x \in E, N(x) \geqslant 0$
- $\forall x \in E, \forall \lambda \in \mathbf{K}, N(\lambda x) = |\lambda| N(x)$
- $\forall x, y \in E, N(x+y) \leqslant N(x) + N(y)$

On dira alors que (E, N) est un espace vectoriel normé (e.v.n).

Remarque.

Si (E, N) est un e.v.n, alors

- $\forall x \in E, N(-x) = N(x)$
- $\forall x, y \in E, |N(x) - N(y)| \leqslant N(x-y)$

2 Normes usuelles

a) Dans $\mathbf{K}^n$

Pour $(x_1, \cdots, x_n) \in \mathbf{K}^n$, on pose

$$\|x\|_p = \left(\sum_{k=1}^{n} |x_k|^p \right)^{1/p}$$

et similairement

$$\|x\|_\infty = \max(|x_1|, \cdots, |x_n|)$$

Ce sont bien des normes (c'est facile pour $p = 1, 2, \infty$ en exploitant Cauchy-Schwarz, on verra avec l'**inégalité de Minkowski** que c'est vrai pour tout p)

On a les inégalités suivantes, pour tout $x \in \mathbf{K}^n$

- $\|x\|_1 \leqslant n\|x\|_\infty$
- $\|x\|_1 \leqslant \sqrt{n}\|x\|_2$ (C-S)
- $\|x\|_2 \leqslant \|x\|_1$
- $\|x\|_\infty \leqslant \|x\|_1$
- $\|x\|_2 \leqslant \sqrt{n}\|x\|_\infty$
- $\|x\|_\infty \leqslant \|x\|_2$

Il y a à chaque fois des cas d'égalité non nuls.

b) Norme de la convergence uniforme

Proposition.

H $E = \mathscr{C}_b^0(I, \mathbf{K})$ (espaces des continues bornées)

C
1. Pour $f \in E$, on pose $\|f\|_\infty = \sup_I |f|$. C'est une norme sur E
2. Il y a équivalence entre
   (a) $f_n \xrightarrow[I]{\text{CVU}} f$
   (b) $\|f_n - f\| \xrightarrow[n \to +\infty]{} 0$

Remarque.

Si I est un segment, $E = \mathscr{C}^0(I, \mathbf{K})$

c) Norme sur les fonctions intégrables

Dans $\mathscr{L}_c^1(I, \mathbf{K})$, on peut poser

$$\|f\|_1 = \int_I |f|.$$

C'est une norme.

d) Norme sur les fonctions de carré intégrable

Dans $\mathscr{L}_c^2(I, \mathbf{K})$, on peut poser

$$\|f\|_2 = \left(\int_I |f|^2\right)^{1/2}.$$

C'est une norme. Pour voir l'inégalité triangulaire :

$$\begin{aligned}
\|f+g\|_\infty \leqslant \|f\|_\infty + \|g\|_\infty &\iff \int_I |f+g|^2 \leqslant \|f\|_1 + \|g\|_1 + 2\sqrt{\left(\int_I |f|^2\right)\left(\int_I |g|^2\right)} \\
&\iff \int_I (f\overline{g} + \overline{f}g) = \mathfrak{Re}\left(2\int_I f\overline{g}\right) \leqslant 2\sqrt{\left(\int_I |f|^2\right)\left(\int_I |g|^2\right)}
\end{aligned}$$

et cette dernière inégalité correspond à Cauchy-Schwarz.

e) Normes sur les fonction continues sur un segment

3 Inégalités de Holder et Minkowski

Chapitre XI

Compacité – Connexité

Sommaire

1 Définitions

Définition.

On note E un $\mathbf{K}$-e.v.n.

1. On dira que $(x_n) \in E^{\mathbf{N}}$ possède une **valeur d'adhérence** ℓ s'il y a une suite extraite de (x_n) qui tend vers ℓ
2. Pour $x = (x_n)$, on notera $V(x)$ l'ensemble des valeurs d'adhérence.

Exemple.

1. $E = \mathbf{R}$, $\quad x = ((-1)^n)$, $\quad V(x) = \{-1, 1\}$
2. $E = \mathbf{R}$, $\quad x_n \xrightarrow[n\to+\infty]{} \ell$, $\quad V(x) = \{\ell\}$
3. $E = \mathbf{R}$, $\quad (r_n)$ une énumération de $\mathbf{Q}$. $V(r) = \mathbf{R}$ (par densité)

2 Compacité

Définition.

On dira que $A \subset E$ est une partie compact si $A = \varnothing$ ou si toute suite d'éléments de A possède une valeur d'adhérence dans A

a) Propriétés topologiques

Proposition.

Ⓗ $A \subset E$

Ⓒ 1. Si A est compacte, alors c'est une partie fermée bornée
2. Un fermé inclus dans A est compact

Démonstration. 1. Soit $(x_n) \in A^{\mathbf{N}}$ qui converge vers ℓ. C'est la seule valeur d'adhérence de x donc elle est dans A et A est fermé. Si A n'est pas bornée, la suite (x_n) définie par

$$\forall n \in \mathbf{N}, \qquad x_n \in A \setminus \mathscr{B}_f(0, n)$$

est bien définie et n'a aucune VA, ce qui est absurde.

2. C'est évident avec les définitions

□

Proposition.

Ⓗ K compact de E, u une suite de $K^{\mathbf{N}}$

Ⓒ Il y a équivalence entre
1. u converge
2. u a une seule valeur d'adhérence

Démonstration.

$(1 \implies 2)$ évident

$(2 \implies 1)$ On note ℓ la VA de u, et on suppose par l'absurde

$$x_n \underset{n\to+\infty}{\not\longrightarrow} \ell$$

Alors $\exists \varepsilon > 0, \forall N \in \mathbf{N}, \exists n \geqslant N, |u_n - \ell| \geqslant \varepsilon$. Pour un tel ε, on construit la suite extraite suivante

- $N = 1$, il existe $n_1 \geqslant 1$ tel que $|u_{n_1} - \ell| \geqslant \ell$
- $\vdots$
- $N = n_{N-1} + 1$, on construit n_N

On a ainsi construit une suite extraite qui n'admet pas ℓ comme VA, donc elle admet une autre VA ℓ' dans K ce qui est absurde. □

Exercice.

On note u une suite bornée réelle telle que

$$u_n + \frac{1}{2} u_{2n} \xrightarrow[n\to+\infty]{} 0$$

Montrer que u converge.

Remarque.

Soit $u \in E^{\mathbf{N}}$. On va montrer que
$$V(u) = \bigcap_{n \geqslant 0} \overline{\{u_k, \quad k \geqslant n\}}$$
On note $U_n = \{u_k, k \geqslant n\}, F_n = \overline{U_n}$ et F l'intersection des F_n. Si $\ell \in V(u)$ alors il existe une extractrice φ telle que $u_{\varphi(k)} \xrightarrow[n \to +\infty]{} \ell$ donc $\ell \in \overline{U_n} = F_n$ pour tout n, donc $\ell \in F$.
Si $\ell \in F$, alors on construit (k_n) de la manière suivante :

- $\mathscr{B}_o(\ell, 1) \cap U_1$ est non vide ($\ell \in F_1$) donc $\exists k_1 \geqslant 1, \quad |u_{k_1} - \ell| \leqslant 1$
- $\mathscr{B}_o(\ell, \frac{1}{2}) \cap U_{k_1+1}$ est non vide ($\ell \in F_{k_1+1}$) donc $\exists k_2 > k_1, \quad |u_{k_2} - \ell| \leqslant \frac{1}{2}$
- $\cdots$

Et on a ainsi construit une suite extraite qui tend vers ℓ, ce qui conclut.

b) Produit cartésien

Proposition.

(H) $(E_1, \| \ \|_1), \cdots, (E_p, \| \ \|_p)$ des evn, $A_1 \subset E_1, \cdots, A_p \subset E_p$ des compacts, et $\| \ \| = \sum_i \| \ \|_i$

(C) $A_1 \times \cdots \times A_p$ est un compact de $E = E_1 \times \cdots \times E_p$ pour la norme $\| \ \|$

Démonstration. On note $(X_n) = (x_{n,1}, \cdots, x_{n,p}) \in (A_1 \times \cdots \times A_p)^{\mathbf{N}}$. Alors

- $(x_{n,1})$ est une suite d'éléments de A_1 qui est un compact donc il existe une extractrice φ_1 qui fait converger la suite extraite vers $\ell_1 \in A_1$ pour $\| \ \|_1$
- $(x_{\varphi_1(n),2})$ est une suite du compact A_2, on fait pareil.
- $\cdots$

Et ainsi $(X_{\varphi_p \circ \cdots \circ \varphi_1(n)})$ converge vers $(l_1, \cdots, l_p) \in A_1 \times \cdots \times A_p$. □

Remarque.

$\mathbf{R}^p = \mathbf{R} \times \cdots \times \mathbf{R}$ munit de $\| \ \|_1$ (c'est la norme produit avec $| \ |$ sur $\mathbf{R}$), $[-1,1]^p$ est compact pour $\| \ \|_1$ donc pour $\| \ \|_\infty$ (équivalence des normes en dimension finie) et $\mathscr{B}_f^\infty(0,1)$ est un fermé inclus dans $[-1,1]^p$ donc c'est un compact.
Plus généralement, $\mathscr{B}_f^\infty(0,r)$ est compact donc toute partie finie bornée pour $\| \ \|_\infty$ est compacte.

c) Théorème des bornes atteintes

Théorème.

(H) $(E, \| \ \|)$ un $\mathbf{K}$-evn, $A \subset E$ un compact et $f : A \to \mathbf{R}$ continue.

(C)
1. $f(A)$ est un compact de $\mathbf{R}$
2. $\exists a, b \in A, \qquad f(a) = \sup_A f$ et $f(b) = \inf_A f$

Démonstration.

1. On note (y_n) une suite de $f(A)^{\mathbf{N}}$, et $(x_n) \in A^{\mathbf{N}}$ une suite d'antécédents de (y_n) par f. La suite x a une valeur d'adhérence $\ell \in A$ donc on peut en extraire une suite convergente
$$x_{\varphi(n)} \xrightarrow[n \to +\infty]{} \ell \in A.$$
On a alors
$$y_{\varphi(n)} \xrightarrow[n \to +\infty]{} f(\ell) \in f(A)$$
donc A est un compact.
2. Il existe $(x_n) \in A^{\mathbf{N}}$ telle que $f(x_n) \xrightarrow[n \to +\infty]{} \sum_A f$, vu la compacité de A on peut supposer que (x_n) converge (quitte à extraire) vers $\ell \in A$ de sorte que $f(\ell)$ est la borne supérieure cherchée.

□

Proposition.

(H) $A \subset E$ compact, E, F des **K**-evn. On note $f : A \to F$ continue.

(C) $f(A)$ compact

Démonstration. Même démo que dans **R**. □

Exemple (Compacité d'une enveloppe convexe)**.** On pose

$$f : \begin{array}{ccc} \mathbf{R}_+^n & \longrightarrow & \mathbf{R} \\ (\lambda_1, \cdots, \lambda_n) & \longmapsto & \lambda_1 + \cdots + \lambda_n \end{array}$$

et pour $x_1, \cdots, x_n \in E$,

$$\varphi : \begin{array}{ccc} \mathbf{R}^n & \longrightarrow & E \\ (\lambda_1, \cdots, \lambda_n) & \longmapsto & \lambda_1 x_1 + \cdots + \lambda_n x_n \end{array}$$

L'ensemble $f^{-1}(\{1\})$ est un compact (fermé inclus dans $[0,1]^n$ compact) pour $\| \|_\infty$, les deux fonctions sont continues donc

$$\operatorname{Conv}(x_1, \cdots, x_n) = \left\{ \lambda_1 x_1 + \cdots + \lambda_n, x_n, \qquad \lambda_i \geqslant 0, \sum \lambda_i = 1 \right\} = \varphi(f^{-1}(\{1\}))$$

est compact

Théorème (Heine).

(H) $A \subset E$ compact, $f : A \to F$ continue

(C) f est uniformément continue

Démonstration. Supposons que f n'est pas uniformément continue :

$$\exists \varepsilon > 0, \forall \delta > 0, \exists x, y \in A, \|x - y\|_E \leqslant \delta \text{ et } \|f(x) - f(y)\|_F \geqslant \varepsilon$$

Pour un tel ε, on prend $\delta_n = \dfrac{1}{n}$ et il existe $x_n, y_n \in A$ tels que

$$\|x_n - y_n\|_E \leqslant \delta \qquad \text{et} \qquad \|f(x_n) - f(y_n)\|_F \geqslant \varepsilon$$

On note φ une extractrice de (x_n) telle que $(x_{\varphi(n)})$ converge vers $\alpha \in A$ (existe par compacité), donc $y_{\varphi(n)} \xrightarrow[n \to +\infty]{} \alpha$ donc

$$\underbrace{\|f(x_n) - f(y_n)\|}_{\geqslant \varepsilon} \xrightarrow[n \to +\infty]{} 0$$

et c'est absurde □

3 Équivalence des normes en dimension finie

Théorème.

1. Toutes les normes sur $\mathbf{K}^n$ sont équivalentes.
2. En dimension finie, toutes les normes sont équivalentes.

Démonstration.

1. On va montrer que toutes les normes sont équivalents à la norme infinie. On se donne une norme $\| \|$. Si $(e_1, \cdots, e_n)$ désigne la base canonique de $\mathbf{K}^n$, et si $x = x_1 e_1 + \cdots + x_n e_n$, alors

$$\|x\| \leqslant |x_1| \|e_1\| + \cdots + |x_n| \|e_n\| \leqslant \|x\|_\infty \underbrace{\|e_1\| + \cdots + \|e_n\|}_{C}$$

Puis

$$\forall x, y \in E, \qquad |\|x\| - \|y\|| \leqslant \|x - y\| \leqslant C \|x - y\|_\infty$$

donc
$$\begin{array}{rccc} \phi : & \mathbf{R}^n & \longrightarrow & \mathbf{R} \\ & x & \longmapsto & \|x\| \end{array}$$
est continue de $(\mathbf{R}^n, \|\ \|_\infty)$ dans $(\mathbf{R}, |\ |)$. On note $S = \{x \in \mathbf{R}^n, \quad \|x\| = 1\}$ qui est un compact de $(\mathbf{R}^n, \|\ \|_\infty)$. Ainsi, φ atteint ses bornes sur S et on note c le minimum de ϕ de sorte que
$$\forall x \in E \setminus \{0\}, \qquad \frac{x}{\|x\|_\infty} \in S$$
donc
$$c \leqslant \phi\left(\frac{x}{\|x\|_\infty}\right) = \frac{\|x\|}{\|x\|_\infty}$$
ce qui donne finalement,
$$\forall x \in E, \qquad c\|x\|_\infty \leqslant \|x\| \leqslant C\|x\|_\infty$$
donc toutes les normes sont équivalentes.

2. On note $(e_1, \cdots, e_n)$ une base de E un $\mathbf{K}$-evn de dimension finie, $\|\ \|_1$ et $\|\ \|_2$ deux normes. Pour $i = 1$ et $i = 2$, on définit
$$\begin{array}{rccc} N_i : & \mathbf{K}^n & \longrightarrow & \mathbf{R}_+ \\ & (x_1, \cdots, x_n) & \longmapsto & \|x_1 e_1 + \cdots + x_n e_n\|_i \end{array}$$
qui sont deux normes équivalentes, donc les deux normes de départ sont équivalentes.

□

Théorème.

(H) $A \subset E$, E un $\mathbf{K}$-evn de dimension finie

(C) Il y a équivalence entre
1. A est une partie compacte
2. A est fermée bornée

Démonstration.

$(1 \implies 2)$ déjà fait

$(2 \implies 1)$ On note $\mathscr{B} = (e_1, \cdots, e_n)$ une base de E et $x_1, \cdots, x_n$ les coordonnées de x dans cette base. On note
$$\|x\| \underset{\text{def}}{=} \max_{1 \leqslant i \leqslant n} |x_i|$$
Par équivalence des normes, A est fermée bornée pour toutes les normes. On note $(X_p)_p$ une suite de $A^{\mathbf{N}}$ de coordonnées $x_{1,p}, \cdots, x_{n,p}$. Chacune des suites $(x_{i,p})_p$ est bornée dans $\mathbf{K}$ donc admet une suite extraite convergente, donc on peut extraire une suite de (X_p) qui converge, et la limite de cette suite extraite est bien dans A car c'est une partie fermée. □

Remarque.

En dimension finie, si A est une partie bornée, alors $\overline{A}$ est un compact. Cela généralise le théorème de **Bolzano-Weierstrass**

Proposition.

(H) $(E, \|\ \|)$ un $\mathbf{K}$-evn de dimension finie et $x = (x_n)$ une suite bornée

(C) Il y a équivalence entre
1. x converge
2. x a une unique valeur d'adhérence

Démonstration. Si $A = \{x_n, \quad n \in \mathbf{N}\}$, alors $\overline{A}$ est un compact ce qui conclut (propriété de début de cours). □

4 Algèbre linéaire et compacité

Théorème.

(H) E un **K**-evn de norme $\| \ \|$

(C) Si F est un sev de dimension finie de E alors c'est un fermé

Démonstration. On note $\mathscr{B} = (e_1, \cdots, e_n)$ une base de F, $\| \ \|_\infty$ la norme usuelle associée. Sur F, cette norme est équivalente à la norme $\| \ \|$. On note $(x_n) \in F^{\mathbf{N}}$ une suite convergente pour $\| \ \|$ vers ℓ. On doit montrer que $\ell \in F$. La suite (x_n) est bornée pour $\| \ \|$ donc pour $\| \ \|_\infty$ donc il existe $(x_{\varphi(n)})$ convergente vers $\ell' \in F$ pour $\| \ \|$ donc pour $\| \ \|$ d'où

$$x_{\varphi(n)} \xrightarrow[n\to+\infty]{\| \ \|} \ell'$$

d'où finalement $\ell = \ell' \in F$ □

Théorème.

(H) E, F des **K**-evn, E de dimension finie

(C) Toute application linéaire $f : E \to F$ est continue

Démonstration. On note $\mathscr{B} = (e_1, \cdots, e_p)$ une base de E muni de $\| \ \|_\infty$ associée. On note $x_1, \cdots, x_n$ les coordonnées de x dans cette base et on a

$$\begin{aligned}\|f(x)\|_F &= \|x_1 f(e_1) + \cdots + x_p f(e_p)\|_F \\ &\leqslant \|x\|_\infty (\|f(e_1)\|_F + \cdots + \|f(e_p)\|_F) = \|x\|_\infty M \\ &\leqslant CM\|x\|_E\end{aligned}$$

par équivalence des normes, pour un $C > 0$. □

Théorème.

(H) $(E_1, \| \ \|_1), \cdots, (E_p, \| \ \|_p)$ des evn de dimension finie, $(F, \| \ \|_F)$ un **K**-evn. $B : E_1 \times \cdots \times E_p \to F$ multilinéaire.

(C)
1. B est continue
2. $$\exists k > 0, \quad \forall u = (u_1, \cdots, u_p) \in E_1 \times \cdots \times E_p, \qquad \|B(u)\|_F \leqslant k\|u_1\|_1 \cdots \|u_p\|_p$$

Démonstration. On se donne $\mathscr{B}_j = (e_{1,j}, \cdots, e_{r_j,j})$ une base de E_j, de sorte que

$$B(u) = \sum_{k_1=1}^{r_1} \cdots \sum_{k_p=1}^{r_p} t_{k_1,1} \cdots t_{k_p,p} B(e_{k_1,1}, \cdots, e_{k_p,p})$$

donc

$$\begin{aligned}\|B(u)\| &\leqslant \sum_{k_1=1}^{r_1} \cdots \sum_{k_p=1}^{r_p} |t_{k_1,1} \cdots t_{k_p,p}| \underbrace{\|B(e_{k_1,1}, \cdots, e_{k_p,p})\|}_{\text{majoré par un } M} \\ &\leqslant M \left(\sum_{k_1=1}^{r_1} |t_{k_1,1}|\right) \times \cdots \times \left(\sum_{k_p=1}^{r_p} |t_{k_p,p}|\right) \\ &\leqslant kM\|u_1\|_1 \cdots \|u_p\|_p\end{aligned}$$

par équivalence des normes.

Puis si $u_n \to a$, alors

$$\begin{aligned}B(u_n) - B(a) = B(u_{n,1} - a_1, \cdots, u_{n,p}) &+ B(a_1, u_{n,2} - a_2, u_{n,3}, \cdots, u_{n,p}) + \cdots \\ &+ B(a_1, ..., a_{p-1}, u_{n,p} - a_p)\end{aligned}$$

donc

$$\|B(u_n) - B(a)\|_F \leqslant k \underbrace{\|u_{n,1} - a_1\|_1}_{\to 0} \underbrace{\|u_{n,2}\|_2 \cdots \|u_{n,p}\|_p}_{\text{borné}} + \cdots \xrightarrow[n\to+\infty]{} 0$$

d'où la continuité. □

5 Propriété de Heine-Borel-Lebesgue

On note $(E, \| \|)$ un **K**-evn. On va montrer l'équivalence entre

1. $A \subset E$ compact de E
2. Si $(O_i)_{i\in I}$ est une famille d'ouverts de E dont l'union contient A (on appelle alors cette famille un recouvrement de A par des ouverts), alors il existe $i_1, \cdots, i_p$ tels que

$$A \subset \bigcup_{k=1}^{p} O_{i_k}$$

(1 ⟹ 2)

Première étape. On montre l'existence de $\varepsilon_0 > 0$ tel que $\forall x \in A, \exists i \in I, \mathscr{B}_o(x, \varepsilon_0) \subset O_i$. Par l'absurde, on suppose que pour $n \in \mathbf{N}^\star$, il existe $x_n \in A$ tel que $\forall i \in I, \mathscr{B}_o(x_n, \frac{1}{n}) \not\subset O_i$. Il existe une extractrice φ telle que $(x_{\varphi(n)})$ converge vers $a \in A$. On note $i_0 \in I$ tel que $a \in O_i$, donc il existe $r_0 > 0$ tel que $\mathscr{B}_o(a, r_0) \subset O_{i_0}$. Or, APCR,

$$\|x_{\varphi(n)} - a\| + \frac{1}{\varphi(n)} \leqslant \frac{r_0}{2}$$

donc $\mathscr{B}_o(x_{\varphi(n)}, \frac{1}{\varphi(n)}) \subset \mathscr{B}_o(a, r_0) \subset O_{i_0}$, c'est absurde.

Deuxième étape. On se donne $\varepsilon > 0$ et on va montrer qu'on peut recouvrir A avec un nombre fini de boules de rayon ε

On raisonne par l'absurde et on construit la suite $(x_n) \in A^{\mathbf{N}}$ de la manière suivante :

- $\exists x_0 \in A$ et on a $A \not\subset \mathscr{B}_o(x_0, \varepsilon)$
- $\exists x_1 \in A \setminus \mathscr{B}_o(x_0, \varepsilon)$ et $A \not\subset \mathscr{B}_o(x_0, \varepsilon) \cup \mathscr{B}_o(x_1, \varepsilon)$
- $\cdots$

Par construction, on a

$$p \neq q \implies \|x_p - x_q\| \geqslant \varepsilon$$

donc toutes les suites extraites ne sont pas de Cauchy donc ne sont pas convergentes, ce qui est absurde car c'est une suite d'un compact.

Troisième étape. On applique la deuxième étape avec le ε_0 de la première étape. Cela conclut immédiatement.

(2 ⟹ 1)

Première étape. On va montrer que si (F_n) est une suite décroissante de fermés relatifs de A non vides, alors $\cap F_n \neq \varnothing$.

On suppose que $\cap F_n = \varnothing$, de sorte que $(A \setminus F_n)_n$ est un recouvrement d'ouverts de A. On en extrait un recouvrement fini :

$$\exists i_1, \cdots, i_p, \qquad A \subseteq (A \setminus F_{i_1}) \cup \cdots \cup (A \setminus F_{i_p}) = A \setminus \underbrace{(F_{i_1} \cap \cdots \cap F_{i_p})}_{\neq \varnothing} \subsetneq A$$

absurde.

Deuxième étape. $(x_n) \in A^{\mathbf{N}}$. Pour $p \in \mathbf{N}$, $F_p = \overline{\{x_p, n \geqslant p\}}$ est une suite décroissante de fermés non vides relatifs de A, donc (x_n) a une valeur d'adhérence dans A.

6 Théorème de Riesz

On note $(E, \| \ \|)$ un $\mathbf{K}$-evn. On va montrer que E est de dimension finie si et seulement si $\mathscr{B}_f(0,1)$ est compact

Le sens direct est immédiat. On suppose que E est de dimension infinie et on va montrer que la boule fermée $\mathscr{B}$ unité n'est pas compacte. On la suppose compacte par l'absurde, et Heine-Borel-Lebesgue donne

$$\exists a_1, \cdots, a_p, \qquad \mathscr{B} \subset \mathscr{B}_o(a_1, \frac{1}{2}) \cup \cdots \cup \mathscr{B}_o(a_p, \frac{1}{2})$$

On note $F = \mathrm{Vect}(a_1, \cdots, a_p) \neq E$. Il existe $x \in E \backslash F$ et $d(x, F) > 0$ car F est un fermé (sev en dimension finie). Il existe $(x_n) \in F^{\mathbf{N}}$ telle que $d(x, x_n) \longrightarrow d(x, F)$ et

$$\frac{x - x_n}{\|x - x_n\|} \in \mathscr{B}$$

donc il existe φ extractrice telle que

$$\frac{x - x_{\varphi(n)}}{\|x - x_{\varphi(n)}\|} \xrightarrow[n \to +\infty]{} \ell \in \mathscr{B}$$

Il existe $i \in [\![1, p]\!]$ tel que $\|\ell - a_i\| < \dfrac{1}{2}$. On pose $y_n = x_n + \|x - x_n\| a_i \in F$ de sorte que

$$y_n - x = x_n - x + \|x - x_n\| a_i = \|x - x_n\| \left(a_i - \frac{x - x_n}{\|x - x_n\|} \right) \xrightarrow[n \to +\infty]{} d(x, F)(a_i - \ell)$$

d'où

$$\|y_n - x\| \xrightarrow[n \to +\infty]{} d(x, F)\|a_i - \ell\| < \frac{d(x, F)}{2}$$

et donc APCR, $\|y_n - x\| < d(x, F)$ absurde.

7 Connexité par arcs

On note $(E, \| \ \|)$ un $\mathbf{K}$-evn, $A \subset E$ et $a, b \in A$. On appelle **chemin** de a à b une application continue $\gamma : [0, 1] \to E$ telle que $\gamma(0) = a$ et $\gamma(b) = b$. On écrira

$$a \underset{A}{\longrightarrow} b \qquad \text{ou} \qquad a \underset{A}{\xrightarrow{\gamma}} b$$

Définition.

On dira que A est connexe par arcs (abrégé c.p.a.) si chaque paire de points est connectée par un chemin de A.

Exemple. Les convexes sont connexes par arcs.

Proposition.

Les connexes par arcs de $\mathbf{R}$ sont les intervalles (i.e. les convexes)

Démonstration. Si $A \subset R$ est convexe, alors $]\inf A, \sup A[\subset A$ par connexité et TVI, et $\overline{A} \subset [\inf A, \sup A]$ ce qui conclut. □

8 Image des connexes par arcs

Théorème.

(H) $f : E \to F$ continue et $A \subset E$

(C)
1. Si A est connexe par arcs alors $f(A)$ aussi
2. Si A est connexe par arcs et $F = \mathbf{R}$, alors $f(A)$ est un intervalle.

Démonstration.

1. On note $\alpha = f(a)$, $\beta = f(b)$. L'application $f \circ \gamma$ avec $a \xrightarrow[A]{\gamma}$ convient.
2. Clair.

$\square$

Exercice.

Montrer que $\mathbf{R}^2 \setminus \mathbf{Q}^2$ est connexe par arcs.

9 Composantes connexes par arcs

Définition – Proposition.

(H) $A \subset E$

(C) On note $\mathscr{R}$ la relation sur A $a\mathscr{R}y \iff \exists\gamma, a \xrightarrow[A]{\gamma} b$. C'est une relation d'équivalence dont les classes d'équivalences sont appelées composantes connexes par arcs.

Exercice.

Montrer qu'un $\mathbf{R}$-evn de dimension finie privé d'un hyperplan a deux composantes connexes et les décrire.

Esquisse de réslution. Les deux composantes sont $\varphi^{-1}(\mathbf{R}_+^\star)$ et $\varphi^{-1}(\mathbf{R}_-^\star)$ avec φ une FL telle que $H = \operatorname{Ker}\varphi$ $\square$

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre XII

Séries entières

Sommaire

1 Définitions

Définition.

Soit $(a_n)_n$ une suite complexe. La série de fonctions de terme général $(a_n z^n)_n$ est appelée série entière et se note $\sum a_n z^n$. Lorsqu'elle converge, on note sa somme

$$\sum_{n=0}^{+\infty} a_n z^n$$

Exemple. Le domaine de convergence de $\sum z^n$ est $\mathscr{D}_0(0,1)$.

Le somaine de convergence $\mathscr{D}$ de $\sum \frac{z^n}{n}$ vérifie $\mathscr{D}_o(0,1) \subsetneq \mathscr{D} \subsetneq \mathscr{D}_f(0,1)$

2 Rayon de convergence

Théorème – Définition.

(H) $(a_n)_{n\in\mathbf{N}} \in \mathbf{C}^{\mathbf{N}}$

(C) 1. Les cinq nombres suivants sont égaux

$$
\begin{aligned}
R_1 &= \sup\{|z|, \quad z \in \mathbf{C}, (a_n z^n)_n \text{ bornée }\}\\
R_2 &= \sup\{|z|, \quad z \in \mathbf{C}, a_n z^n \longrightarrow 0\}\\
R_3 &= \sup\{|z|, \quad z \in \mathbf{C}, \sum a_n z^n \text{ converge }\}\\
R_4 &= \sup\{|z|, \quad z \in \mathbf{C}, \sum a_n z^n \text{ converge absolument }\}\\
R_5 &= \inf\{|z|, \quad z \in \mathbf{C}, (a_n z^n)_n \text{ non bornée}\}
\end{aligned}
$$

avec la convention $\inf \varnothing = +\infty$. On appelle ce nomber *rayon de convergence* de $\sum a_n z^n$ et on le note $R(a_n z^n)$

2. Si $\sum a_n z^n$ admet pour rayon de convergence R, alors le domaine de convergence est tel que

$$\mathscr{D}_0(0,R) \subseteq \mathscr{D} \subseteq \mathscr{D}_f(0,R)$$

Démonstration. 1. $R_1 \geqslant R_2 \geqslant R_3 \geqslant R_4$. Par l'absurde, on suppose $R_4 < R_5$. Alors, on prend $z \in \mathbf{C}$ tel que $R_5 > |z| > R_4$. $(a_n z^n)_n$ est bornée donc si on note z' tel que $|z| > |z'| > R_4$, alors

$$a_n z'^n = \underbrace{a_n z^n}_{\text{borné}} \underbrace{\left(\frac{z'}{z}\right)^n}_{|\ |<1} \text{ tg série ACV absurde car } |z'| > R_4$$

Donc $R_4 \geqslant R_5$. Par l'absurde, $R_1 > R_5$. On se donne $z \in \mathbf{C}$ tel que $R_1 > |z| > R_5$ et il existe $z', z'' \in \mathbf{C}$ tel que $R_1 \geqslant |z''| > |z| > |z'| \geqslant R_5$, $(a_n z'^n)$ non bornée et $(a_n z''^n)$ bornée.

$$\underbrace{a_n z'^n}_{\neg\text{ borné}} = a_n z''^n \left(\frac{z'}{z''}\right)^n \to_{n\to+\infty} 0$$

absurde donc $R_1 = R_2 = R_3 = R_4 = R_5$.

2. Immédiat vu 1.

□

Remarque (Lemme d'Abel).

Si $a \in \mathbf{C}^{\mathbf{N}}$ et $z_0 \in \mathbf{C}^\star$. Si la suite $(a_n z_0^n)$ est bornée alors $\forall z \in \mathscr{D}_o(0,|z_0|), \sum a_n z^n$ ACV

3 Opération algébrique sur les séries entières

Proposition.

(H) $\sum a_n z^n$ de rayon R_a et $\sum b_n z^n$ de rayon R_b

(C) 1. Pour $\lambda \in \mathbf{C}^\star$, $R(\sum \lambda a_n z^n) = R_a$
2. Pour $\lambda \in \mathbf{C}^\star$, $R(\sum (\lambda a_n + b_n) z^n) \geqslant \min(R_a, R_b)$ et si $R_a \neq R_b$, il y a égalité.
3. Le produit de Cauchy des séries $\sum a_n z^n$ et $\sum b_n z^n$ est la série $\sum c_n z^n$ avec

$$c_n = \sum_{p+q=n} a_p b_q$$

et $R(\sum c_n z^n) \geqslant \min(R_a, R_b)$.

Démonstration. 1. "Trivial"

2. $\geqslant 0$ OK et $R_a \neq R_b \implies =$ OK
3. Si $|z| < \min(R_a, R_b)$ alors $\sum a_n z^n, \sum b_n z^n$ ACV donc produit de Cauchy ie C

□

4 Régularité des séries entières

Proposition.

H $\sum a_n z^n$ de RCV $R > 0$ (ou $+\infty$)

C 1. $\forall a \in]0, R[, \quad \sum a_n z^n$ CVN sur $\mathscr{D}_f(0, a)$.

2. $z \in \mathscr{D}_o(0, R) \longmapsto \displaystyle\sum_{k=0}^{+\infty} a_n z^n$ est continue

Démonstration. $a \in]0, R[$.

$$\sum_{z \in \mathscr{D}_f(0,a)} |a_n z^n| = |a_n a^n| \text{ tg série CV car } a < R \text{ donc il y a CVN sur } \mathscr{D}_f(0, a)$$

d'où la continuité sur tous les $\mathscr{D}_f(0, a)$ donc sur $\mathscr{D}_o(0, a)$. □

Théorème.

H $f(z) = \sum_{n \geqslant 0} a_n z^n$ série entière de rayon $R > 0$

C 1. On appelle série dérivée la série $\sum_{n \geqslant 1} n a_n z^{n-1}$
   (a) Cette série a le même rayon de convergence que f
   (b) f est dérivable sur $]-R, R[$ et $\forall t \in]-R, R[$,

$$f'(t) = \sum_{n \geqslant 1} a_n n t^{n-1}$$

2. La série $\sum_{n \geqslant 0} \frac{a_n}{n+1} z^{n+1}$ a même rayon de convergence que f et pour $t \in]-R, R[$,

$$\sum_{n \geqslant 0} \frac{a_n}{n+1} z^{n+1} = \int_0^t f(u)\,\mathrm{d}u$$

Démonstration. 1. $|n a_n z^{n-1}| = |a_n a^n| \times \left|\left(\frac{z}{a}\right)^{n-1}\right| \times \frac{n}{a} \to 0$ si $|z| < a < R$. Puis, $(a_n z^n)$ non bornée entraîne $(n a_n z^{n-1})$ non bornée. On a donc $R(\sum n a_n z^{n-1}) = R$.
On vérifie les hypothèses du théorème de dérivation terme à terme :
- $\forall n \in \mathbf{N}, \quad t \in]-R, R[\longmapsto a_n t^n$ est $\mathscr{C}^1$
- $\sum a_n t^n$ converge simplement sur $]-R, R[$
- $\sum (a_n z^n)' = \sum n a_n z^{n-1}$ converge normalement donc univormément sur tout segment de $]-R, R[$.

Ainsi, le théorème donne bien C

2. Il y a égalité des rayons de convergence (vu 1) et pour tout $t \in]-R, R[$, la série $\sum a_n z^n$ converge normalement donc uniformément sur $[0, t]$, donc le théorème d'intégration terme à terme donne

$$\int_0^t f(u)\,\mathrm{d}u = \sum a_n \int_0^t u^n\,\mathrm{d}u = \sum \frac{a_n}{n+1} t^{n+1}$$

□

Exemple. On note $f(t) = -\ln(1-t)$ de sorte que

$$\forall t \in]-1,1[, \qquad f(t) = \sum_{n\geqslant 0} \frac{t^{n+1}}{n+1}.$$

Alors,

$$f(-t) = \sum_{n\geqslant 0} (-1)^{n+1} \frac{t^{n+1}}{n+1}$$

et (théorème des séries alternées)

$$\forall t \in [0,1[, \forall n \in \mathbf{N}, \qquad \left| f(-t) - \sum_{k=0}^{n} (-1)^{k+1} \frac{t^{k+1}}{k+1} \right| \leqslant \frac{1}{n+2} \xrightarrow[n\to+\infty]{} 0$$

donc le reste CVU vers 0, puis le théorème de la double limite donne

$$f(-t) \xrightarrow[\substack{t\to 1\\ t<1}]{} \sum_{n\geqslant 0} \frac{(-1)^{n+1}}{n+1} = -\ln 2$$

Remarque.

Pour $f : \mathbf{C} \longrightarrow \mathbf{C}$, on peut définir la dérivabilité au sens complexe par

$$f \text{ dérivable en } a \iff \lim_{\substack{h\to 0\\ h\neq 0}} \frac{f(a+h)-f(a)}{h} \text{ existe}$$

On note $f(z) = \sum a_n z^n$ une série entière de rayon de convergence $R > 0$ et $a \in \mathscr{D}_o(0,R)$. On va montrer que f est dérivable au sens complexe en a et que

$$f'(a) = \sum_{n\geqslant 0} n a_n a^{n-1}$$

Pour $h \neq 0$ assez petit en module :

$$\begin{aligned} \frac{f(a+h)-f(a)}{h} &= \sum_{n\geqslant 0} a_n \frac{(a+h)^n - a^n}{h} \\ &= \sum_{n\geqslant 0} a_n \underbrace{\left(\binom{n}{1} a^{n-1} + \binom{n}{2} a^{n-2} h + \cdots + h^{n-1} \right)}_{\xrightarrow[\substack{h\to 0\\ h\neq 0}]{} n a^{n-1}} \end{aligned}$$

Puis si on pose $\varphi : t \longmapsto (a+th)^n$, on a (Taylor-Lagrange)

$$|\varphi(1) - \varphi(0) - \varphi'(0)| \leqslant \frac{1}{2!} \sup_{[0,1]} |\varphi''| \leqslant \frac{n(n-1)}{2} |h|^2 (|a|+|h|)^{n-2}$$

donc si b est tel que $|a| < b < R$, il existe un voisinage V de 0 tel que $\forall h \in V, |a|+|h| < |b|$ et dans ce cas

$$\begin{aligned} \left| \frac{f(a+h)-f(a)}{h} - \sum_{n\geqslant 0} n a_n a^{n-1} \right| &\leqslant \left| \sum_{n\geqslant 0} a_n \left(\frac{(a+h)^n - a^n}{h} - n a^{n-1} \right) \right| \\ &\leqslant \sum_{n\geqslant 0} |a_n| \frac{n(n-1)}{2} |h| (|a|+|h|)^{n-2} \\ &\leqslant |h| \underbrace{\sum_{n\geqslant 0} |a_n| \frac{n(n-1)}{2} b^{n-2}}_{\text{CV car } b<R, \text{ série dérivée } 2^{\text{nde}}} \xrightarrow[\substack{h\to 0\\ h\neq 0}]{} 0 \end{aligned}$$

Exemple. Calcul de $I = \displaystyle\int_0^1 \ln(1-x)\ln x \,\mathrm{d}x$.

- $x \longmapsto \ln(1-x)\ln x$ est intégrable car continue par prolongement
- $\forall x \in]0,1[$, $\ln(1-x) = -\sum_{n\geqslant 0} \frac{x^{n+1}}{n+1}$ donc

$$I = -\int_0^1 \sum_{n\geqslant 0} \frac{x^{n+1}}{n+1} \ln x \,\mathrm{d}x$$

- $\sum \frac{x^{n+1}}{n+1} \ln x$ converge simplement sur $]0,1[$
- Les $x \longmapsto \frac{x^{n+1}}{n+1} \ln x$ sont continues intégrables sur $]0,1[$ et

$$\int_0^1 \left| \frac{x^{n+1}}{n+1} \ln x \right| \mathrm{d}x = -\int_0^1 \frac{x^{n+1}}{n+1} \ln x \,\mathrm{d}x = \frac{1}{(n+2)^2(n+1)} \quad \text{tg série CV}$$

Donc le théorème d'interversion série-intégrale (version convergence dominée) donne

$$I = \sum_{n\geqslant 0} \int_0^1 \frac{-x^{n+1}}{n+1} \ln x \,\mathrm{d}x = \sum_{n\geqslant 0} \frac{1}{(n+2)^2(n+1)}$$

et

$$\frac{1}{X(X+1)^2} = \frac{-1}{(X+1)^2} + \frac{-1}{X+1} + \frac{1}{X}$$

d'où finalement $I = 2 - \dfrac{\pi^2}{6}$

Théorème.

H $f(z) = \sum_{n\geqslant 0} a_n z^n$ avec le RCV $R > 0$

C 1. $f \in \mathscr{C}^\infty(]-R,R[, \mathbf{C})$ et

$$\forall n \in \mathbf{N}, \quad \frac{f^{(n)}(0)}{n!} = a_n$$

2.

$$\forall t \in]-R,R[, \qquad f(t) = \sum_{n\geqslant 0} \frac{f^{(n)}(0)}{n!} t^n$$

3. Si $\sum a_n z^n = \sum b_n z^n$ au voisinage de 0 alors $\forall n, a_n = b_n$

Démonstration. Facile. □

Remarque.

On peut faire des DSE ailleurs qu'en 0. Soit $f(z) = \sum_{n \geqslant 0} a_n z^n$ DSE avec un rayon de convergence non nul, et $a \in \mathscr{D}_o(0, R)$. On va montrer que pour $z \in \mathscr{D}_o(a, R - |a|)$,

$$f(z) = \sum_{n \geqslant 0} \frac{f^{(n)}(a)}{n!}(z-a)^n$$

On a :

$$\forall z \in \mathscr{D}_o(0, R), \qquad f(z) = \sum_{n \geqslant 0} a_n z^n$$

donc

$$\forall k \geqslant 0, \qquad f^{(k)}(a) = \sum_{n \geqslant k} a_n \frac{n!}{(n+k)!} a^{n-k}.$$

On va montrer que la famille

$$\left(a_n \frac{n!}{(n+k)!} a^{n-k} \frac{(z-a)^k}{k!} \right)_{n \geqslant k \geqslant 0}$$

est sommable. Pour $n \in \mathbf{N}$,

$$\sum_{k=0}^{n} \left| a_n \frac{n!}{(n+k)!} a^{n-k} \frac{(z-a)^k}{k!} \right| = |a_n|(|a| + |z-a|)^n$$

et si $z \in \mathscr{D}_o(a, R - |a|)$, on a $|a| + |z-a| < R$ donc c'est le terme général d'une série convergente. Le théorème de Fubini donne alors

$$\sum_{n \geqslant 0} \sum_{k=0}^{n} a_n \frac{n!}{(n+k)!} a^{n-k} \frac{(z-a)^k}{k!} = \sum_{n \geqslant 0} a_n z^n = f(z) = \sum_{k \geqslant 0} \sum_{n \geqslant k} a_n \frac{n!}{(n+k)!} a^{n-k} \frac{(z-a)^k}{k!} = \sum_{k \geqslant 0} \frac{f^{(k)}(a)}{k!}(z-a)^k$$

5 DSE usuels

Remarque.

On note $f \in \mathscr{C}^\infty(]-R, R[, \mathbf{C})$. Pour $n \in \mathbf{N}$ et $x \in]-R, R[$,

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} x^k + \underbrace{\int_0^x \frac{(x-t)^n}{n!} f^{(n+1)}(t) \, \mathrm{d}t}_{\underset{\text{def}}{=} R_n(x)}$$

Si $R_n(x) \xrightarrow[n \to +\infty]{\text{CVS}} 0$ sur $]-R, R[$ alors la série

$$\sum \frac{f^{(k)}(0)}{k!} x^k$$

converge et on a

$$f(x) = \sum_{n \geqslant 0} \frac{f^{(k)}(0)}{k!} x^k$$

On en déduit que si $|z| < R$,

$$\frac{f^{(k)}(0)}{k!} z^k \xrightarrow{k \to +\infty} 0$$

et

$$\sum_{k \geqslant 0} \frac{f^{(k)}(0)}{k!} z^k$$

a un rayon de convergence $\geqslant R$. La fonction f se prolonge alors naturellement sur $\mathscr{D}_o(0, R)$ avec son DSE.

Exemple. Pour la fonction exp sur **R**,

$$|R_n(x)| \leqslant \frac{|x|^{n+1}}{(n+1)!}\max(1,e^x) \xrightarrow[n\to+\infty]{} 0$$

donc la fonction exp est DSE sur **R** et admet un prolongement $\mathscr{C}^\infty$ sur **C** donné par ce DSE.

Théorème.

Expression	Terme général du DSE	Rayon de Convergence
$\exp(x)$	$\dfrac{x^k}{k!}$	$+\infty$
$\mathrm{ch}(x)$	$\dfrac{x^{2k}}{(2k)!}$	$+\infty$
$\mathrm{sh}(x)$	$\dfrac{x^{2k+1}}{(2k+1)!}$	$+\infty$
$\sin(x)$	$\dfrac{(-1)x^{2k+1}}{(2k+1)!}$	$+\infty$
$\cos(x)$	$\dfrac{(-1)^k x^{2k}}{(2k)!}$	$+\infty$
$\dfrac{1}{1-x}$	x^k	1
$\ln(1-x)$	$\dfrac{x^k}{k}$	1
$(1+x)^\alpha$	$\dbinom{\alpha}{k}x^k$	1 si $\alpha\notin\mathbf{N}$, $+\infty$ sinon

Démonstration. On ne fait la preuve que pour le dernier cas. On pose

$$f : x \longmapsto (1+x)^\alpha$$

et

$$g : x \longmapsto \sum_{k\geqslant 0}\binom{\alpha}{k}x^k.$$

La fonction f vérifie $f^{(k)}(0) = \alpha(\alpha-1)\cdots(\alpha-k+1)$, et la règle de D'Alembert montre que dans le cas $\alpha\notin\mathbf{N}$, $R(g)=1$. On a $g(0)=1$ et

$$g'(x) = \sum_{k\geqslant 1} k\binom{\alpha}{k}x^{k-1} = \alpha\sum_{k\geqslant 1}\binom{\alpha-1}{k-1}x^{k-1}$$

donc

$$(1+x)g'(x) = \alpha\left(\sum_{k\geqslant 1}\left(\binom{\alpha-1}{k}+\binom{\alpha-1}{k-1}\right)x^k+1\right) = \alpha g(x)$$

C'est un problème de Cauchy dont f et g sont solutions, donc $f=g$. □

Exemple. $f=\arctan$.

- $f'(x) = \dfrac{1}{1+x^2}$ sur **R**
- Sur $]-1,1[$,

$$\frac{1}{1+x^2} = \sum_{k\geqslant 0}(-1)^k x^{2k}$$

Donc,

$$f(x) = \arctan x = \sum_{k\geqslant 0}\frac{(-1)^k x^{2k+1}}{2k+1}$$

Exemple. $f : x \longmapsto \sqrt{1+x}$. On a (RCV 1)

$$\sqrt{1+x} = \sum_{k \geqslant 0} \binom{\frac{1}{2}}{k} x^k$$

et après calculs, on a l'expression suivante du binôme généralisé :

$$\binom{\frac{1}{2}}{k} = \frac{(-1)^{k-1}}{2^{2k-1}} \cdot \frac{1}{2k-1} \cdot \binom{2k-1}{k}$$

6 Méthodes pour obtenir un DSE

a) Utilisation d'une équation différentielle

À faire: Récupérer cette partie

b) Utilisation d'une primitive

On se donne $a \in \mathbf{R}$ et on pose

$$\forall x \in]-1,1[, \qquad S(x) = \sum_{k \geqslant 1} \frac{\sin(ka)}{k} x^k$$

On peut observer que $S(x) = \mathfrak{Im}(H(x))$ où

$$H(x) = \sum_{k \geqslant 1} (e^{ix})^k \frac{x^k}{k}.$$

H est dérivable sur $]-1,1[$ et

$$H'(x) = \sum_{k \geqslant 1} (e^{ix})^k x^{k-1} = \frac{e^{ia}}{1 - e^{ia}x}$$

d'où

$$\mathfrak{Im}(H'(x)) = \frac{x \sin a \cos a + \sin a - x \sin a \cos a}{1 + x^2 - 2x \cos a} = \frac{\sin a}{(x - \cos a)^2 + \sin^2 a}$$

Il y a deux cas :

- $a \in \pi\mathbf{Z}$. Dans ce cas, $S \equiv 0$.
- $\sin a \neq 0$ et une primitive de $\mathfrak{Im}(H'(x))$ est

$$\arctan\left(\frac{x - \cos a}{\sin a}\right)$$

et $S(0) = 0$ permet d'avoir

$$S(x) = \arctan\left(\frac{x - \cos a}{\sin a}\right) + \arctan\left(\tan\left(\frac{\pi}{2} - a\right)\right)$$

Exercice.
Application à

$$S(x) = \sum_{k \geqslant 1} \frac{\cos(ka)}{k} x^k$$

7 Utilisation des DSE

a) Pour la régularité

On pose

$$f : t \longmapsto \begin{cases} \mathrm{ch}(\sqrt{t}) & \text{si } t \geqslant 0 \\ \cos(\sqrt{-t}) & \text{sinon} \end{cases}$$

On veut savoir si f est $\mathscr{C}^\infty$. On a

$$\forall x \in \mathbf{R}, \qquad f(t) = \sum_{k \geqslant 0} \frac{t^k}{(2k)!}$$

donc f est DSE sur $\mathbf{R}$ et donc bien $\mathscr{C}^\infty$

b) Utilisation combinatoire

On note a_n le nombre d'involutions de $\mathfrak{S}_n$. On convient que $a_0 = 0$. On va montrer que $a_{n+1} = a_n + na_{n-1}$, puis on va calculer

$$\sum_{n\geqslant 0} \frac{a_n}{n!} x^n$$

et montrer

$$\frac{a_n}{n!} \xrightarrow[n\to+\infty]{} 0$$

Soit $\sigma \in \mathfrak{S}_{n+1}$ une involution. Il y a deux cas :

- $\sigma(n+1) = n+1$, on a a_n choix possibles
- $\sigma(n+1) \neq n+1$. On a n choix pour $\sigma(n+1)$ et $\sigma_{|[\![1,n]\!]\setminus\{\sigma(n+1)\}}$ est une involution, donc on a au total na_{n-1} choix.

On sait que $\frac{a_n}{n!}$ donc la série a un RCV $\geqslant 1$. On note

$$f : x \in]-1,1[\longmapsto \sum_{n\geqslant 0} \frac{a_n}{n!} x^n$$

On a alors

$$f'(x) = \sum_{n\geqslant 1} \frac{na_n}{n!} x^{n-1} = \sum_{n\geqslant 0} \frac{a_{n+1}}{n!} x^n = 1 + x + (1+x) f(x)$$

Puis $f'(0) = 0$ donc f est solution d'un problème de Cauchy. Par unicité :

$$f(x) = e^x e^{\frac{x^2}{2}} - 1$$

et cette fonction est DSE avec un RCV infini, et la convergence en 1 conclut.

8 Étude au bord

a) Continuité radiale

On note $f(z) = \sum_{n\geqslant 1} a_n z^n$ de rayon de convergence $R > 0$. On suppose qu'il existe z_0 tel que

$$\sum_{n\geqslant 0} a_n z_0^n$$

converge et $|z_0| = R$. On va montrer que

$$\lim_{\substack{t\to 1\\ t<1}} f(tz_0) = f(z_0).$$

On note

$$R_q \underset{\text{def}}{=} \sum_{k=q+1}^{+\infty} a_k z_0^k \xrightarrow[q\to+\infty]{} 0.$$

On a

$$\begin{aligned}\sum_{k=n}^{m} a_k t^k z_0^k &= \sum_{k=n}^{m} t^k (R_{k-1} - R_k) \\ &= R_{n-1} t^n + R_n (t^{n+1} - t^n) + \cdots + R_{m-1}(t^m - t^{m-1}) + R_m t^m\end{aligned}$$

Soit $\varepsilon > 0$. Alors, $\exists N \in \mathbf{N}, \forall n \geqslant N, \quad |R_n| \leqslant \varepsilon' = \frac{\varepsilon}{5}$. Pour $m > n \geqslant N+1$ et $t \in [0,1]$,

$$\left|\sum_{k=n}^{m} a_k t^k z_0^k\right| \leqslant 2\varepsilon' + \varepsilon'(t^n - t^{n+1} + \cdots t^{m-1} - t^m) \leqslant 3\varepsilon'$$

On fait $m \longrightarrow +\infty$ de sorte que

$$f(tz_0) - f(z_0) = \sum_{k=0}^{n-1} (a_k t^k z_0^k - a_k z_0^k) + \sum_{k=n}^{+\infty} (a_n t^k z_0^k - a_k t_0^k)$$

et avec $n = N$,

$$|f(tz_0) - f(z_0)| \leqslant \underbrace{\left|\sum_{k=0}^{N-1}(a_k t^k z_0^k - a_k z_0^k)\right|}_{\xrightarrow[t\to 1]{} 0} + 4\varepsilon'$$

Donc il existe $\delta > 0$ tel que $\forall t \in]1-\delta, 1[$, $|f(tz_0) - f(z_0)| \leqslant 5\varepsilon' = \varepsilon$ ce qui conclut.

b) Formule utile

On note

$$f : t \longmapsto \sum_{n\geqslant 0} a_n t^n$$

avec un RCV $R \geqslant 1$.

Pour $|t| < 1$, si on note $S_n = a_0 + \cdots + a_n$, on a

$$\frac{f(t)}{1-t} = \sum_{n\geqslant 0} S_n t^n \qquad \text{(Produit de Cauchy)}$$

Si $f(1)$ converge, alors en notant $R_n = \sum_{k\geqslant n+1} a_k$,

$$(t-1)\sum_{n\geqslant 0} R_n t^n = -R_0 + \sum_{n\geqslant 1}(R_{n-1} - R_n)t^n = -R_0 + f(t) - a_0 = f(t) - f(1)$$

donc pour $t \neq 1$,

$$\frac{f(t) - f(1)}{t-1} = \sum_{n\geqslant 0} R_n t^n$$

Exemple.

$$\sum_{n\geqslant 1} \frac{t^n}{n} = -\ln(1-t) \implies \sum_{k\geqslant 1} H_k t^k = \frac{-\ln(1-t)}{1-t}$$

Exemple. On note

$$f : t \longmapsto \sum_{n\geqslant 2} \frac{(-1)^n}{\ln n} t^n$$

avec le rayon de convergence 1 (facile). Cette fonction est continue en 1 (on peut le voir avec le TSA uniforme ou la continuité radiale). On va vérifier qu'elle est dérivable en 1. On a

$$\frac{f(t) - f(1)}{t-1} = \sum_{n\geqslant 0} R_n t^n \qquad \text{où} \quad R_n \underset{\text{def}}{=} \sum_{k=n+1}^{+\infty} \frac{(-1)^k}{\ln k}$$

Le TSA donne la convergence de $\sum R_n$, de sorte que la continuité radiale donne l'existence de la limite du taux d'accroissement en 1^-, ce qui conclut.

c) Recherche d'équivalents

Limite en un point non-convergent du bord

On se donne $f(t) = \sum_{n\geqslant 0} a_n t^n$ avec $a_n \geqslant 0$ et le RCV 1, et on suppose que $\sum a_n$ diverge. On va montrer que

$$f(t) \xrightarrow[t\to 1^-]{} +\infty$$

Soit $A > 0$. Il existe un rang N tel que

$$\sum_{k=0}^{N} a_k > A + 1.$$

Puis, pour $t \in [0,1[$,

$$f(t) \geqslant \sum_{k=0}^{N} a_k t^k \xrightarrow[t\to 1^-]{} \sum_{k=0}^{N} a_k$$

donc il existe $\delta > 0$ tel que $\forall t \in]1-\delta, 1[$,

$$f(t) \geqslant \sum_{k=0}^{N} t^k \geqslant A$$

donc $\boxed{\text{C}}$.

Sommation de relation de comparaison pour les séries entières

On se donne $f(t) = \sum_{n\geqslant 0} a_n t^n$ et $g(t) = \sum_{n\geqslant 0} b_n t^n$ de rayons de convergence 1 et de termes généraux positifs et équivalents ($a_n, b_n \geqslant 0$ et $a_n \sim b_n$). On suppose que $\sum b_n$ diverge, et on va montrer que

$$f(t) \underset{1^-}{\sim} g(t)$$

Déjà, $g(t) \xrightarrow[t\to 1^-]{} +\infty$ (vu i). Puis, pour $\varepsilon > 0$, il existe $N \in \mathbf{N}$ tel que pour $n \geqslant N$,

$$(1-\varepsilon')b_n \leqslant a_n \leqslant (1+\varepsilon')b_n \implies (1-\varepsilon')\sum_{n\geqslant N} b_n t^n \leqslant \sum_{n\geqslant N} a_n t^n \leqslant (1+\varepsilon')\sum_{n\geqslant N} b_n t^n$$

D'où

$$(1-\varepsilon')g(t) - (1-\varepsilon')\sum_{k=0}^{N-1} b_k t^k \leqslant f(t) - \sum_{k=0}^{N-1} a_k t^k \leqslant (1+\varepsilon')g(t) - (1+\varepsilon')\sum_{k=0}^{N-1} b_k t^k$$

En divisant par $g(t)$ et pour un $\delta > 0$, $1-\delta < t < 1$,

$$1 - 2\varepsilon' \leqslant \frac{f}{g}(t) \leqslant 1 + 2\varepsilon'$$

d'où $\boxed{\text{C}}$.

Exercice.

> Même exercice mais avec un rayon de convergence infini et l'équivalent en $+\infty$. En déduire un équivalent en $+\infty$ de
>
> $$\sum_{n=1}^{+\infty} \left(1+\frac{1}{n}\right)^{n^2} \frac{x^n}{n!}$$

9 Résultats théoriques sur les DSE

a) La formule de Cauchy

Soit f DSE avec $R(f) = R > 0$. On va montrer que pour $z \in \mathscr{D}_o(0,R)$ et pour r tel que $|z| < r < R$,

$$f(z) = \frac{1}{2\pi}\int_0^{2\pi} \frac{f(re^{it})re^{it}}{re^{it}-z}\,\mathrm{d}t$$

On écrit

$$f(z) = \sum_{n=0}^{+\infty} a_n z^n$$

donc

$$\forall t \in [0,2\pi], \qquad \frac{f(re^{it})re^{it}}{re^{it}-z} = \frac{f(re^{it})}{1-\left(\frac{z}{re^{it}}\right)} = f(re^{it})\sum_{n=0}^{+\infty}\left(\frac{z}{re^{it}}\right)^k = \sum_{n,m\geqslant 0} \frac{a_n r^n z^m}{r^m} e^{i(n-m)t}$$

où la dernière somme est celle d'une famille sommable. Donc la convergence normale sur $\mathcal{D}_f(0,r)$ donne

$$\int_0^{2\pi} \frac{f(re^{it})re^{it}}{re^{it}-z}\,\mathrm{d}t = \sum_{n,m\geqslant 0} a_n r^{n-m} z^m \int_0^{2\pi} e^{i(n-m)t}\,\mathrm{d}t = \sum_{n\geqslant 0} 2\pi a_n z^n = 2\pi f(z)$$

Remarque.

Pour $0<r<R$,

$$\int_0^{2\pi} f(re^{it})e^{-int}\,\mathrm{d}t = \int_0^{2\pi}\left(\sum_{k=0}^{+\infty} a_k r^k e^{ikt}\right) e^{-int}\,\mathrm{d}t = a_n r^n 2\pi$$

donc

$$a_n = \frac{1}{2\pi r^n}\int_0^{2\pi} f(re^{it})e^{-int}\,\mathrm{d}t$$

b) Théorème de Liouville

On suppose f DSE avec un rayon de convergence infini, f bornée. On a

$$\forall r>0, \forall n\in\mathbf{N}, \qquad a_n = \frac{1}{2\pi r^n}\int_0^{2\pi} f(re^{it})e^{-int}\,\mathrm{d}t$$

Pour $n\geqslant 1$,

$$|a_n| \leqslant \frac{1}{2\pi r^n}\int_0^{2\pi} \underbrace{|f(re^{it})e^{-int}|}_{\leqslant \sup_{\mathbf{C}}|f|}\,\mathrm{d}t \leqslant \frac{2\pi\sup_{\mathbf{C}}|f|}{2\pi r^n} \xrightarrow[r\to+\infty]{} 0$$

On a donc $f=a_0$ constante.

c) Principe des zéros isolés

On note R le rayon de convergence de f DSE en 0, et on suppose $R>0$.

$$\forall z\in\mathcal{D}_o(0,R), \qquad f(z) = \sum_{k=0}^{+\infty}\frac{f^{(k)}(0)}{k!}z^k$$

Si $f(0)=0$ et $f\not\equiv 0$ alors on note $p=\min\{k\in\mathbf{N}, f^{(k)}(0)\neq 0\}$. Pour z non nul au voisinage de 0,

$$f(z) = z^p\left(\frac{f^{(p)}(0)}{p!} + z\frac{f^{(p+1)}(0)}{(p+1)!}+\cdots\right)\neq 0$$

Donc 0 est un zéro isolé. On va montrer que s'il existe une suite (z_n) de racines deux à deux distinctes de f qui converge vers $a\in\mathcal{D}_o(0,R)$, alors f est nulle.

Par continuité, a est une racine de f. Cette racine n'est pas isolée donc f est nulle sur un voisinage de a (par le raisonnement qui précède).

On note

$$\mathcal{E} = \{z\in\mathcal{D}_o(0,R), \quad f\equiv 0 \text{ au voisinage de } z\}$$

Si $z_0\in\mathcal{E}$, alors on note $r_0>0$ le rayon d'un disque ouvert tel que $f(\mathcal{D}_o(z_0,r_0))=\{0\}$. Pour tout $z\in\mathcal{D}_o(z_0,r_0)$, il existe $r_z>0$ tel que $\mathcal{D}_o(z,r_z)\subset\mathcal{D}_o(z_0,r_0)$ et f s'annule sur ce disque, donc $\mathcal{D}_o(z_0,r_0)\subset\mathcal{E}$. Ainsi, $\mathcal{E}$ est un ouvert.

Si $(x_n)\in\mathcal{E}^{\mathbf{N}}$ converge vers $a\in\mathcal{D}_o(0,R)$, alors a n'est pas isolée, f s'annule sur un voisinage de a (déjà vu) donc $a\in\mathcal{E}$. L'ensemble $\mathcal{E}$ est donc un fermé relatif du disque ouvert de convergence.

C'est un ouvert fermé relatif, donc $\mathcal{E}=\mathcal{D}_o(0,R)$ et f est nulle.

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre XIII

Variables aléatoires discrètes

Sommaire

1 Tribu

a) Définition

Dans tout le chapitre, Ω désigne un ensemble non vide.

Définition.

Un ensemble $\mathscr{A}$ de parties de Ω est une **tribu** si

- $\mathscr{A}$ est stable par passage au complémentaire
- $\varnothing \in \mathscr{A}$
- $\mathscr{A}$ est stable par union dénombrable

On dit alors que $(\Omega, \mathscr{A})$ est un **espace probabilisable** et les éléments de $\mathscr{A}$ sont appelés **événements**

b) Propriétés ensemblistes

Proposition.

Soit $(\Omega, \mathscr{A})$ un espace probabilisable. Si $(A_n) \in \mathscr{A}^{\mathbf{N}}$ alors

$$\bigcap_{n \in \mathbf{N}} A_n \in \mathscr{A}$$

Démonstration. C'est une union dénombrable de complémentaires $\square$

Notation (HP).

$$\underline{\lim} A_n = \bigcup_{n\in\mathbf{N}} \left(\bigcap_{m\geqslant n} A_m \right) \qquad \overline{\lim} A_n = \bigcap_{n\in\mathbf{N}} \left(\bigcup_{m\geqslant n} A_m \right)$$

c) Opérations sur les tribus

Soit $(\mathscr{A}_i)_{i\in I}$ une famille de tribus. L'ensemble

$$\bigcap_{i\in I} \mathscr{A}_i$$

est une tribu (facile).

Remarque.

On définit ainsi la notion de tribu engendrée : la tribu engendrée par $\mathscr{E} \subset \mathscr{P}(\Omega)$ est l'intersection de toutes les tribus contenant $\mathscr{E}$.

Définition.

Soit $(\Omega, \mathscr{A})$ un espace probabilisable.

- $A, B \in \mathscr{A}$ sont **incompatible** si $A \cap B = \varnothing$
- Pour $A \in \mathscr{A}$, on appelle **événement contraire** l'événement A^c
- On dit que $(A_i)_{i\in I} \in \mathscr{A}^I$ est un **système complet d'événements** si et seulement si $(A_i)_{i\in I}$ partitionne Ω.

2 Espace probabilisé

Définition.

Soit $(\Omega, \mathscr{A})$ un espace probabilisable. On appelle **probabilité** sur $(\Omega, \mathscr{A})$ une application $\mathbf{P} : \mathscr{A} \to [0, 1]$ telle que

- $\mathbf{P}(\Omega) = 1$
- $\mathbf{P}$ est σ-additive, c'est-à-dire que pour toute suite (A_i) d'événements deux à deux incompatibles,

$$\mathbf{P}\left(\bigcup_{n\in\mathbf{N}} A_n \right) = \sum_{n\geqslant 0} \mathbf{P}(A_n)$$

Si $\mathbf{P}$ convient, on dira que $(\Omega, \mathscr{A}, \mathbf{P})$ est un **espace probabilisé**.

Remarque.

- La suite constante égale à $\varnothing$ donne $\mathbf{P}(\varnothing) = 0$.
- Si A et B sont incompatibles, alors $\mathbf{P}(A \cup B) = \mathbf{P}(A) + \mathbf{P}(B)$
- $\mathbf{P}(A^c) = \mathbf{P}(A \cup A^c) - \mathbf{P}(A) = 1 - \mathbf{P}(A)$
- $A \subset B \implies \mathbf{P}(B) = \mathbf{P}(A) + \mathbf{P}(B \setminus A) \geqslant \mathbf{P}(A)$

Exercice (Inégalité d'Edith Kosmanek).

Soit $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé, A, B des événements. Montrer que

$$|\mathbf{P}(A \cap B) - \mathbf{P}(A)\mathbf{P}(B)| \leqslant \frac{1}{4}$$

Résolution. $(A \cap B, A \cap B^c, A^c \cap B, A^c \cap B^c)$ est un SCE et un peu de calcul donne

$$\mathbf{P}(A \cap B) - \mathbf{P}(A)\mathbf{P}(B) = \mathbf{P}(A \cap B)\mathbf{P}(A^c \cap B^c) - \mathbf{P}(A^c \cap B)\mathbf{P}(A \cap B^c)$$

Puis si $a, b \geqslant 0$ sont tels que $a + b \leqslant 1$, on a $ab = \sqrt{ab}^2 \leqslant \left(\frac{a+b}{2}\right)^2 \leqslant \frac{1}{4}$ donc les deux produits sont $\leqslant \frac{1}{4}$, ce qui conclut. □

Exercice.

$(\Omega, \mathscr{A}, \mathbf{P})$ probabilisé, $A, B \in \mathscr{A}$. Montrer que $|\mathbf{P}(A) - \mathbf{P}(B)| \leqslant \mathbf{P}(A \Delta B)$

3 Propriétés élémentaires des probabilités

Théorème (Continuité croissante).

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ probabilisé, $(A_n)_{n\in\mathbf{N}}$ suite croissante d'événements

(C)

$$\mathbf{P}\left(\bigcup_{n\in\mathbf{N}} A_n\right) = \lim_{n\to\infty} \mathbf{P}(A_n).$$

Démonstration. Par σ-additivité, en posant $A_{-1} = \varnothing$, on a

$$\mathbf{P}\left(\bigcup_{n\in N} A_n\right) = \sum_{n\geqslant 0} \mathbf{P}(A_n \setminus A_{n-1}) = \lim_{n\to\infty} \sum_{k=0}^{n} \underbrace{\mathbf{P}(A_k \setminus A_{k-1})}_{=\mathbf{P}(A_k)-\mathbf{P}(A_{k-1})} = \lim_{n\to\infty} \mathbf{P}(A_n).$$

□

Théorème (Continuité décroissante).

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ probabilisé, $(A_n)_{n\in\mathbf{N}}$ suite décroissante d'événements

(C)

$$\mathbf{P}\left(\bigcap_{n\in\mathbf{N}} A_n\right) = \lim_{n\to\infty} \mathbf{P}(A_n).$$

Démonstration. C'est la continuité croissante en passant au complémentaire. □

Théorème (Sous-additivité).

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ espace probabilisé, (A_n) suite d'événements

(C) Avec la convention qu'une somme de série divergente à terme général positif vaut $+\infty$,

$$\mathbf{P}\left(\bigcup_{n\in\mathbf{N}} A_n\right) \leqslant \sum_{n=0}^{+\infty} \mathbf{P}(A_n).$$

Démonstration. On note

$$X_n = \bigcup_{k\in\mathbf{N}} A_k$$

de sorte que (X_n) est une suite croissante d'événements. Pour deux événements $A \subset B$, on a

$$\mathbf{P}(A \cup B) = \mathbf{P}(A \cup (B \setminus A)) = \mathbf{P}(A) + \mathbf{P}(B \setminus A) \leqslant \mathbf{P}(A) + \mathbf{P}(B)$$

et en itérant, on trouve

$$\forall n \in \mathbf{N}, \qquad \mathbf{P}(X_n) \leqslant \sum_{k=0}^{n} \mathbf{P}(A_i)$$

donc

$$\lim_{n\to\infty} \mathbf{P}(X_n) = \mathbf{P}\left(\bigcup_{n\in\mathbf{N}} A_n\right) \leqslant \sum_{n=0}^{+\infty} \mathbf{P}(A_n)$$

□

Remarque.

Un événement $A \in \mathscr{A}$ est dit **négligeable** si $\mathbf{P}(A) = 0$. Si (A_n) est une suite d'événements négligeables, alors

$$\mathbf{P}(\bigcup_{n\in\mathbf{N}} A_n) \leqslant \sum_{n=0}^{+\infty} \mathbf{P}(A_n) = 0$$

a) Formule de Poincaré

Soit $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé, $A_1, \cdots, A_n \in \mathscr{A}$. On va montrer que

$$\mathbf{P}(A_1 \cup \cdots \cup A_n) = \sum_{1 \leqslant i_1 \leqslant n} \mathbf{P}(A_{i_1}) - \sum_{1 \leqslant i_1 < i_2 \leqslant n} \mathbf{P}(A_{i_1} \cap A_{i_2}) + \cdots + (-1)^{n-1} \sum_{1 \leqslant i_1 < \cdots < i_n \leqslant n} \mathbf{P}(A_{i_1} \cap \cdots \cap A_{i_n})$$

On remarque pour cela

$$\mathbb{1}_{(A_1 \cup \cdots \cup A_n)^c} = 1 - \mathbb{1}_{A_1 \cup \cdots \cup A_n} = \mathbb{1}_{A_1^c \cap \cdots \cap A_n^c} = \mathbb{1}_{A_1^c} \times \cdots \times \mathbb{1}_{A_n^c} = (1 - \mathbb{1}_{A_1}) \times \cdots \times (1 - \mathbb{1}_{A_n})$$

donc en développant,

$$\mathbb{1}_{(A_1 \cup \cdots \cup A_n)^c} = 1 - \sum_{i=1}^{n} \mathbb{1}_{A_i} - \sum_{i_1 < i_2} \mathbb{1}_{A_{i_1} \cap A_{i_2}} + \cdots + (-1)^{n-1} \sum_{i_1 < \cdots < i_n} \mathbb{1}_{A_{i_1} \cap \cdots \cap A_{i_n}}$$

Or (on le verra), $\mathbf{E}(\mathbb{1}_A) = \mathbf{P}(A)$ et $\mathbf{E}$ est linéaire, ce qui conclut.

Exemple. On place r boules dans n cases. Calculer la probabilité qu'aucune case ne soit vide. On note A_i l'événement "La case n°i est vide" et $B = A_1^c \cap \cdots \cap A_n^c$. On cherche $\mathbf{P}(B)$. On a

$$\forall k \in [\![1, n]\!], \qquad \mathbf{P}(A_{i_1} \cap \cdots \cap A_{i_k}) = \left(1 - \frac{k}{n}\right)^r.$$

Puis,

$$\begin{aligned}\mathbf{P}(B^c) = 1 - \mathbf{P}(B) &= \sum_{1 \leqslant i_1 \leqslant n} \left(1 - \frac{1}{n}\right)^r - \sum_{i_1 < i_2} \left(1 - \frac{2}{n}\right)^r + \cdots + (-1)^{n-1} \sum_{i_1 < \cdots < i_n} \left(1 - \frac{n}{n}\right)^r \\ &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} \left(1 - \frac{k}{n}\right)^r\end{aligned}$$

4 Probabilité conditionnelle

Définition.

Soit $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé et $B \in \mathscr{A}$ tel que $\mathbf{P}(B) > 0$. On appelle probabilité de $A \in \mathscr{A}$ sachant B le nombre

$$\mathbf{P}_B(A) = \mathbf{P}(A|B) \underset{\text{def}}{=} \frac{\mathbf{P}(A \cap B)}{\mathbf{P}(B)}$$

Proposition.

H $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé, $A_1, \cdots, A_n \in \mathscr{A}$ tels que $\mathbf{P}(A_1 \cap \cdots \cap A_n) > 0$

C
$$\mathbf{P}(A_1 \cap \cdots \cap A_n) = \mathbf{P}(A_1)\mathbf{P}(A_2|A_1)\mathbf{P}(A_3|A_1 \cap A_2) \cdots \mathbf{P}(A_n|A_1 \cap \cdots \cap A_{n-1})$$

Démonstration. La seule difficulté est de montrer que les probabilités utilisées existent. C'est le cas car

$$\forall i \leqslant n, \qquad 0 < \mathbf{P}(A_1 \cap \cdots \cap A_n) \leqslant \mathbf{P}(A_1 \cap \cdots \cap A_i)$$

□

Exemple. On se donne un sac dans lequel il y a une boule blanche et une boule noire. À chaque tour, on tire une boule et on en remet deux de la même couleur dans le sac. Quelle est la probabilité de tirer n boules blanches lors des n premiers tirages ?

On note A_n l'événement cherché et :

- $\mathbf{P}(A_1) = \frac{1}{2}$
- $\mathbf{P}(A_n|A_{n-1}) = \dfrac{n}{n+1}$

•

$$\begin{aligned}\mathbf{P}(A_n) &= \mathbf{P}(A_1 \cap \cdots \cap A_n)\\ &= \mathbf{P}(A_1)\cdot\mathbf{P}(A_2|A_1)\cdots\mathbf{P}(A_n|A_1\cap\cdots\cap A_{n-1})\\ &= \mathbf{P}(A_1)\mathbf{P}(A_2|A_1)\cdots\mathbf{P}(A_n|A_{n-1})\\ &= \frac{1}{2}\times\frac{2}{3}\times\cdots\times\frac{n}{n+1}\\ &= \frac{1}{n+1}\end{aligned}$$

Exemple (Monty Hall)**.** Dans le jeu télévisé *Let's make a deal*, un candidat doit choisir une porte parmi trois. Derrière deux d'entre elles, il y a une chèvre, et derrière la troisième il y a une voiture. On note X la variable aléatoire qui correspond au premier choix. Une fois le choix effectué, le présentateur révèle une chèvre parmi les portes non choisies, et le candidat a l'occasion de changer son choix. On note alors Y la variable aléatoire qui vaut 0 si le candidat ne change pas son choix et 1 s'il le change. Le candidat a-t-il intérêt à changer son choix ?

On suppose que la porte gagnante est la porte numéro 1 et on note A l'événement qui correspond à une victoire du candidat. On a

- $\mathbf{P}(A|X=1, Y=1) = 1$
- $\mathbf{P}(A|X=2, Y=1) = 0$
- $\mathbf{P}(A|X=3, Y=1) = 0$
- $\mathbf{P}(A|X=1, Y=0) = 0$
- $\mathbf{P}(A|X=2, Y=0) = 1$
- $\mathbf{P}(A|X=3, Y=0) = 1$

Donc

$$\mathbf{P}(A|Y=1) = \mathbf{P}(A|X=1, Y=1) + \mathbf{P}(A|X=2, Y=1)\mathbf{P}(X=2) + \mathbf{P}(A|X=3, Y=1)\mathbf{P}(X=3) = \frac{2}{3}$$

Donc le candidat a intérêt à changer son choix.

Définition – Proposition (Trace).

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ est un espace probabilisé, $A \in \mathscr{A}$ un événement tel que $\mathbf{P}(A) > 0$

(C) 1. $\mathscr{A}_A \underset{\text{def}}{=} \{A \cap B, \quad B \in \mathscr{A}\}$ est une tribu de A

2. $(A, \mathscr{A}_A, \mathbf{P}_A)$ est un espace probabilisé, avec

$$\begin{aligned}\mathbf{P}_A : \mathscr{A}_A &\longrightarrow [0,1]\\ B &\longmapsto \frac{\mathbf{P}(B)}{\mathbf{P}(A)}\end{aligned}$$

Proposition.

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ est un espace probabilisé, $A \in \mathscr{A}$ un événement tel que $\mathbf{P}(A) > 0$

(C) $(\Omega, \mathscr{A}, \mathbf{P}_A)$ est un espace probabilisé avec

$$\begin{aligned}\mathbf{P}_A : \mathscr{A} &\longrightarrow [0,1]\\ B &\longmapsto \frac{\mathbf{P}(A\cap B)}{\mathbf{P}(A)}\end{aligned}$$

Théorème – Définition.

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ espace probabilisé

(C) 1. On dira que $(A_n) \in \mathscr{A}^{\mathbf{N}}$ est un **système complet d'événements** si
   - $\forall n \in \mathbf{N}, \quad A_n \neq \varnothing$
   - Les A_i sont deux à deux incompatibles
   - $\bigcup_{i \in \mathbf{N}} A_i = \Omega$

2. Pour tout $A \in \mathscr{A}$ on a dans ce cas

$$\mathbf{P}(A) = \sum_{n \in \mathbf{N}} \mathbf{P}(A \cap A_n) = \sum_{n \in \mathbf{N}} \mathbf{P}_{A_n}(A)\mathbf{P}(A_n)$$

en convenant que si $\mathbf{P}(A_n) = 0$ alors $\mathbf{P}(A_n)\mathbf{P}_{A_n}(A) = 0$

Démonstration. C'est la σ-additivité. □

Remarque.

On peut se dispenser de l'hypothèse $A_i \neq \varnothing$, et on peut se contenter de $\mathbf{P}(\bigcup A_n) = 1$ au lieu de $\bigcup A_n = \Omega$. On parle alors de système pseudo-complet ou presque-complet.

5 Formule de Bayes

Théorème (Bayes).

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ espace probabilisé

(C) 1. Si $A, B \in \mathscr{A}$ sont tels que $\mathbf{P}(A), \mathbf{P}(B) > 0$, alors

$$\mathbf{P}(B|A) = \frac{\mathbf{P}(A|B)\mathbf{P}(B)}{\mathbf{P}(A)}$$

2. Si $(A_n) \in \mathscr{A}^{\mathbf{N}}$ est un SCE, $B \in \mathscr{A}$ est tel que $\mathbf{P}(B) > 0$, alors

$$\mathbf{P}_B(A_i) = \frac{\mathbf{P}_{A_i}(B)\mathbf{P}(A_i)}{\sum_{n=0}^{+\infty} \mathbf{P}_{A_n}(B)\mathbf{P}(A_n)}$$

6 Germes de probabilités

Proposition (Germe de probabilité).

(H) $\Omega = \{x_i, \quad i \in \mathbf{N}\}$, $\mathscr{A} = \mathscr{P}(\Omega)$ et $(p_i)_{i \in \mathbf{N}} \in (\mathbf{R}^+)^{\mathbf{N}}$ telle que $\sum p_i = 1$

(C) Il existe une unique probabilité $\mathbf{P}$ sur $(\Omega, \mathscr{A})$ telle que $\forall i \in \mathbf{N}, \quad \mathbf{P}(\{x_i\}) = p_i$, et elle est donnée par

$$\forall X \in \mathscr{A}, \quad \mathbf{P}(X) = \sum_{\substack{i \in \mathbf{N} \\ x_i \in X}} p_i$$

Démonstration. Unicité facile, existence facile. □

7 Variables aléatoires discrètes

Définition.

Soit $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé et E un ensemble. On appelle **variable aléatoire discrète** à valeurs dans E une application $X : \Omega \to E$ telle que
- $X(\Omega)$ est fini ou dénombrable
- $\forall x \in E, \quad X^{-1}(\{x\}) \in \mathscr{A}$

Exemple. $A \in \mathscr{A}, \quad \mathbb{1}_A$ est une v.a.d

Remarque.

Si E est dénombrable, alors E s'écri t $\{x_n, \quad n \in \mathbf{N}\}$ avec les x_n deux à deux distincts. Si $X : \Omega \to E$ est une v.a.d alors

- $A_n = X^{-1}(\{x_n\})$. Les $(A_n)_n$ forment un SCE (ou un quasi-SCE)
- $p_n = \mathbf{P}(A_n)$ définit un germe de probabilité
- Une probabilité sur $(E, \mathscr{P}(E))$ est donnée par

$$\forall B \subset E, \quad \sum_{\substack{n \geqslant 0 \\ x_n \in B}} p_n$$

et on a

$$[X \in B] = \bigcup_{\substack{n \geqslant 0 \\ x_n \in B}} X^{-1}(\{x_n\}) \in \mathscr{A}$$

donc

$$\mathbf{P}(X \in B) = \sum_{\substack{n \geqslant 0 \\ x_n \in B}} \mathbf{P}(A_n) = \mathbf{P}_\star(B)$$

On a ainsi une probabilité sur $(E, \mathscr{P}(E))$ à partir de $(\Omega, \mathscr{A}, \mathbf{P})$ sans connaître Ω. On a seulement besoin de connaître les p_n (la loi de X)

Théorème.

(H) $E = \{x_n, \quad n \in \mathbf{N}\}$, les x_n deux à deux distincts, $(p_n)_{n\in\mathbf{N}} \in (\mathbf{R}^+)^{\mathbf{N}}, \quad \sum p_n = 1$

(C) Il existe Ω, une tribu $\mathscr{A}$ de Ω, $\mathbf{P}$ une probabilité telle que $(\Omega, \mathscr{A}, \mathbf{P})$ est un espace probabilisé et $X : \Omega \to E$ est une v.a.d satisfaisant $\mathbf{P}(X = x_n) = p_n$

Démonstration. Admis(e) mais facile $(\Omega = E, \mathscr{A} = \mathscr{P}(E))$ □

8 Indépendance

a) Indépendance d'événements

Définition.

$(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé. Deux événements $A, B \in \mathscr{A}$ sont dits **indépendants** si et seulement si $\mathbf{P}(A \cap B) = \mathbf{P}(A)\mathbf{P}(B)$. Si $\mathbf{P}(B) \neq 0$, c'est équivalent à $\mathbf{P}(A|B) = \mathbf{P}(A)$

b) Indépendance de variables aléatoires

Définition.

Soit $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé.

- Si $X_1, \cdots, X_n$ sont des v.a.d sur Ω, $E_i = X_i(\Omega)$, on dira que $X_1, \cdots, X_n$ sont **mutuellement indépendantes** si

$$\forall (A_1, \cdots, A_n) \in \mathscr{P}(E_1) \times \cdots \times \mathscr{P}(E_n), \qquad \mathbf{P}(X_1 \in A_1, \cdots, X_n \in A_n) = \mathbf{P}(X_1 \in A_1) \cdots \mathbf{P}(X_n \in A_n)$$

ou de manière équivalente

$$\forall (x_1, \cdots, x_n) \in E_1 \times \cdots \times E_n, \qquad \mathbf{P}(X_1 = x_1, \cdots, X_n = x_n) = \mathbf{P}(X_1 = x_1) \cdots \mathbf{P}(X_n = x_n)$$

- Si X, Y sont des v.a.d indépendantes, on note $X \perp\!\!\!\perp Y$

Remarque.

En général, l'indépendance mutuelle implique l'indépendance des variables deux à deux, mais la réciproque est fausse.

c) Coalitions

On note $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé, $X, Y, Z : \Omega \to \mathbf{N}$ mutuellement indépendantes. On note $U = X + Y$. $U(\Omega)$ est fini ou dénombrable. Pour $n \in \mathbf{N}$,

$$[U = n] = \bigcup_{k=0}^{n} [X = k, Y = n - k] \in \mathscr{A}$$

donc U est une variable aléatoire discrète. A-t-on $U \perp\!\!\!\perp Z$? On a

$$[U = n, Z = m] = \bigcup_{k=0}^{n} [X = k, Y = n - k, Z = m]$$

donc

$$\mathbf{P}(U = n, Z = m) = \mathbf{P}(Z = m) \sum_{k=0}^{n} \mathbf{P}(X = k)\mathbf{P}(Y = n - k) = \mathbf{P}(U = n)\mathbf{P}(Z = m)$$

donc $U \perp\!\!\!\perp Z$

Lemme (Coalitions).

> (H) $X_1, \cdots, X_n$ des v.a.d mutuellement indépendantes à valeurs dans $\mathbf{R}$, $d \in [\![1, n]\!]$, $f : \mathbf{R}^d \to E, \quad g : \mathbf{R}^{n-d} \to F$
>
> (C) $f(X_1, \cdots, X_d) \perp\!\!\!\perp g(X_{d+1}, \cdots, X_n)$

Démonstration. $X = f(X_1, \cdots, X_d), Y = g(X_{d+1}, \cdots, X_n)$ sont des v.a.d car pour $x \in X(\Omega)$,

$$X^{-1}(\{x\}) = \bigcup_{(x_1, \cdots, x_n) \in f^{-1}(\{x\})} [X_1 = x_1, \cdots, X_n = x_n] \in \mathscr{A}$$

car $f^{-1}(\{x\}) \subset E_1 \times \cdots \times E_d$. Soient $x \in X(\Omega), y \in Y(\Omega)$.

$$[X = x, Y = y] = \bigcup_{\substack{(x_1, \cdots, x_d) \in E_1 \times \cdots \times E_d \\ (y_{d+1}, \cdots, y_n) \in E_{d+1} \times \cdots \times E_n \\ f(x_1, \cdots, x_n) = x \\ g(y_{d+1}, \cdots, y_n) = y}} [X_1 = x_1, \cdots, X_d = x_d, Y_{d+1}, \cdots, X_n = y_n]$$

donc

$$\begin{aligned}
\mathbf{P}(X = x, Y = y) &= \sum_{\substack{(x_1, \cdots, x_d) \in E_1 \times \cdots \times E_d \\ (y_{d+1}, \cdots, y_n) \in E_{d+1} \times \cdots \times E_n \\ f(x_1, \cdots, x_n) = x \\ g(y_{d+1}, \cdots, y_n) = y}} \mathbf{P}(X_1 = x_1)\mathbf{P}(X_2 = x_2) \cdots \mathbf{P}(X_d = x_d)\mathbf{P}(X_{d+1} = y_{d+1}) \cdots \mathbf{P}(X_n = y_n) \\
&= \sum_{\substack{(x_1, \cdots, x_d) \in E_1 \times \cdots \times E_d \\ f(x_1, \cdots, x_n) = x}} \sum_{\substack{(y_{d+1}, \cdots, y_n) \in E_{d+1} \times \cdots \times E_n \\ g(y_{d+1}, \cdots, y_n) = y}} \mathbf{P}(X_1 = x_1) \cdots \mathbf{P}(X_n = y_n) \\
&= \mathbf{P}(X = x)\mathbf{P}(Y = y)
\end{aligned}$$

ce qui conclut. □

Remarque.

> Le fait que les X_i soient à valeur dans $\mathbf{R}$ est sans importance. Par ailleurs, on peut généraliser le résultat en
>
> $$f_1(X_1, \cdots, X_{d_1}), \cdots, f_p(X_{d_{p-1}+1}, \cdots, X_n)$$
>
> mutuellement indépendantes.

Définition.

> Soit $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé et $(X_n)_{n \in \mathbf{N}}$ une suite de variables aléatoires discrètes. On dira que la famille $(X_n)_{n \in \mathbf{N}}$ est est mutuellement indépendante si pour toute partie finie $I \subset \mathbf{N}$, les $(X_i)_{i \in I}$ sont mutuellement indépendantes

Théorème.

(H) $(E_n)_{n\in\mathbf{N}}$ une suite d'ensembles dénombrables, $(\mathbf{P}_n)_{n\in\mathbf{N}}$ une suite de probabilités sur $(E_n, \mathscr{P}(E_n))$.

(C) Il existe un espace probabilisé $(\Omega, \mathscr{A}, \mathbf{P})$ et une suite (X_n) de variables aléatoires discrètes avec $X_n : \Omega \to E_n$ telles que

- $\forall n \in \mathbf{N}, \forall x \in E_n, \quad \mathbf{P}(X_n = x) = \mathbf{P}_n(\{x\})$
- $(X_n)_{n\in\mathbf{N}}$ sont mutuellement indépendantes.

Démonstration. Admise. □

9 Exemples de lois

Définition.

Soit $p \in]0,1[$ et $(\Omega, \mathscr{A}, \mathbf{P})$ probabilisé. On dira que $X : \Omega \to \mathbf{N}^\star$ suit une loi géométrique de paramètre p si

- X est une v.a.r.d
- $\mathbf{P}(X = n) = q^{n-1}p$ où $q = p - 1$.

On écrira $X \hookrightarrow G(p)$

Remarque.

$(q^{n-1}p)_n$ est un germe de probabilité donc il existe des v.a.d qui suivent cette loi.

Théorème.

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ espace probabilisé, $X \hookrightarrow G(p)$

(C)
1. Pour $n, k \in \mathbf{N}, \quad \mathbf{P}(X > n + k | X > n) = \mathbf{P}(X > k)$. On dit que X est sans mémoire
2. Si X est une v.a.r.d à valeurs dans $\mathbf{N}^\star$ et si $\forall n, k \in \mathbf{N}, \quad \mathbf{P}(X > n+k|X > n) = \mathbf{P}(X > k)$ alors $X \hookrightarrow G(\mathbf{P}(X = 1))$

Démonstration.

1. $$\mathbf{P}(X > n) = \sum_{k\geqslant 1} \mathbf{P}(X = n + k) = \sum_{k\geqslant 1} q^{m+k-1}p = \frac{q^m p}{1-q} = q^m \neq 0$$

   et
   $$\mathbf{P}(X > n + k|X > k) = \frac{\mathbf{P}(X > n + k, X > n)}{\mathbf{P}(X > m)} = \frac{q^{n+k}}{q^m} = q^k = \mathbf{P}(X > k)$$

2. On pose $F(n) = \mathbf{P}(X > n)$. L'hypothèse donne $\forall n, k \in \mathbf{N}, F(n + k) = F(n)F(k)$. Avec $q = F(1)$, on a $\forall n \in \mathbf{N}^\star, F(n) = q^n$ et $F(0) = \mathbf{P}(X > 0) = 1 = q^0$. Ainsi,
   $$\forall n \in \mathbf{N}, \quad \mathbf{P}(X = n) = F(n - 1) - F(n) = q^{n-1}(1 - q)$$
   et $p \underset{\text{def}}{=} 1 - q$. La suite des $[X > n]$ est décroissante donc par continuité,
   $$\mathbf{P}(\varnothing) = 0 = \mathbf{P}\left(\bigcap_{n\in\mathbf{N}} [X > n]\right) = \lim_{n\to+\infty} q^n \implies p, q \in]0, 1[$$

□

Remarque.

On prend $(X_n)_n$ une suite de variables aléatoires discrètes indépendantes de loi $\mathscr{B}(p)$ sur $(\Omega, \mathscr{A}, \mathbf{P})$ espace probabilisé. Pour $\omega \in \Omega$, on pose (avec la convention $\min \varnothing = +\infty$)

$$T(\omega) = \min\{n \in \mathbf{N}^\star, \quad X_n(\omega) = 1\}$$

- $T(\Omega) = \mathbf{N}^\star \cup \{+\infty\}$ est dénombrable
- On a
$$[T = n] = [X_1 = 0, \cdots, X_{n-1} = 0, X_n = 1] \in \mathscr{A}$$
et
$$[T = +\infty] = \left(\bigcup_{n \in \mathbf{N}^\star} [T = n] \right)^c \in \mathscr{A}.$$

Ainsi, T est une v.a.d. Pour $n \in \mathbf{N}$,

$$\mathbf{P}(T = n) = \mathbf{P}(X_1 = 0, \cdots, X_{n-1} = 0, X_n = 1) = q^{n-1}p$$

et

$$\mathbf{P}(T = +\infty) = 1 - \sum_{n \geqslant 0} \mathbf{P}(T = n) = 1 - \frac{p}{1-q} = 0$$

Par abus, on dit que $T \hookrightarrow G(p)$ même si T est à valeurs dans $\mathbf{N}^\star \cup \{+\infty\}$

Exercice.

Avec les mêmes notations, on note

$$T_n = \min\{i \in \mathbf{N}^\star, \quad (X_1 + \cdots + X_n)(\omega) = n\}$$

Trouver la loi de T_n

Résolution. C'est bien une v.a.d et

$$\mathbf{P}(T_n = j) = \sum_{\substack{\varepsilon_1 + \cdots + \varepsilon_{j-1} = n-1 \\ \varepsilon_i \in \{0,1\}}} \underbrace{\mathbf{P}(X_1 = \varepsilon_1) \cdots \mathbf{P}(X_{j-1} = \varepsilon_{j-1}) \mathbf{P}(X_j = 1)}_{(1-q)^{n-1} q^{j-n} (1-q)} = \binom{j-1}{n-1} (1-p)^n q^{j-n}$$

et puis

$$1 - \mathbf{P}(T_n = +\infty) = \mathbf{P}\left(\bigcup_{j \geqslant n} [T_n = j] \right) = \sum_{j \geqslant n} \binom{j-1}{n-1} q^{j-n} p^n = \sum_{j \geqslant n} \frac{(j-1) \cdots (j-n+1)}{(n-1)!} q^{j-1} p^n$$

Or en posant $f : z \in]-1,1[\longmapsto \frac{1}{1-z}$,

$$f^{(n-1)}(q) = \sum_{j \geqslant n} (j-1) \cdots (j-n+1) q^{j-n} = \frac{(n-1)!}{(1-q)^n}$$

d'où

$$\mathbf{P}(T_n = +\infty) = 1 - \frac{p^n}{(1-q)^n} = 0$$

□

Définition.

Soit $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé. On dira que $X : \Omega \to \mathbf{N}$ suit une loi de Poisson de paramètre $\lambda > 0$ si pour $n \in \mathbf{N}$, $\mathbf{P}(X = n) = e^{-\lambda} \frac{\lambda^n}{n!}$. On écrira $X \hookrightarrow \mathbf{P}(\lambda)$

Remarque.

Il existe bien des v.a.r.d qui suivent cette loi car $\left(e^{-\lambda} \dfrac{\lambda^n}{n!} \right)$ est un germe de probabilité.

Remarque.

On va montrer que si $X_1 \hookrightarrow \mathscr{P}(\lambda_1), X_2 \hookrightarrow \mathbf{P}(\lambda_2)$ avec $X_1 \perp\!\!\!\perp X_2$, alors $X_1 + X_2 \hookrightarrow \mathbf{P}(\lambda_1 + \lambda_2)$. On note $X = X_1 + X_2$. On a

- $X(\Omega) \subset \mathbf{N}$
- $[X = n] = \bigcup_{k=0}^{n} [X_1 = k, X_2 = n - k]$

Donc

$$\begin{aligned}
\mathbf{P}(X = n) &= \sum_{k=0}^{n} \mathbf{P}(X_1 = k, X_2 = n - k) \\
&= \sum_{k=0}^{n} e^{-\lambda_1} \frac{\lambda_1^k}{k!} e^{-\lambda_2} \frac{\lambda_2^{n-k}}{(n-k)!} \\
&= \frac{e^{-\lambda_1 - \lambda_2}}{n!} \sum_{k=0}^{n} \binom{n}{k} \lambda_1^k \lambda_2^{n-k} \\
&= e^{-\lambda_1 - \lambda_2} \frac{(\lambda_1 + \lambda_2)^n}{n!}
\end{aligned}$$

Donc $X \hookrightarrow \mathbf{P}(\lambda_1 + \lambda_2)$

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre XIV

Espérance – Variance

Sommaire

1 Espérance

Définition.

On note $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé, X une variable aléatoire **réelle** discrète. On dira que X est d'**espérance fini** si $(x\mathbf{P}(X=x))_{x\in X(\Omega)}$ est sommable. Dans ce cas, on appelle **espérance** la quantité

$$\mathbf{E}(X) = \sum_{x\in X(\Omega)} x\mathbf{P}(X=x)$$

Remarque (Rappel).

Si $X(\Omega) = \{x_n, \quad n\in\mathbf{N}\}$, les x_n deux à deux distincts, alors

$$\sum_{n\in\mathbf{N}} |x_n|\mathbf{P}(X=x_n) \text{ CV} \iff (x_n\mathbf{P}(X=x_n))_{n\in\mathbf{N}} \text{ sommable}$$

Exemple.

- $X \hookrightarrow G(p)$ est d'espérance finie car $(nq^{n-1}p)_n$ est sommable, et
$$\mathbf{E}(X) = \sum_{n\geqslant 0} nq^{n-1}p = \frac{1}{p}$$
- $X \hookrightarrow \mathscr{P}(\lambda)$ pour $\lambda > 0$, on a $n\mathbf{P}(X=n) = e^{-\lambda}\frac{n\lambda^n}{n!}$ et $\mathbf{E}(X) = \lambda$
- $X = \mathbb{1}_A$ pour $A \in \mathscr{A}$, $\mathbf{E}(X) = \mathbf{P}(X=1) = \mathbf{P}(A)$

2 Formule de transfert

Théorème.

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé, X une v.a.r.d et $f : X(\Omega) \to \mathbf{R}$

(C) 1. $f(X)$ est une v.a.r.d
2. $f(X)$ est d'espérance finie si et seulement si $(f(x)\mathbf{P}(X = x))_{x \in X(\Omega)}$ et dans ce cas,

$$\mathbf{E}(f(X)) = \sum_{x \in X(\Omega)} f(x)\mathbf{P}(X = x)$$

Démonstration.

1. Lemme des coalitions
2. Pour $y \in f(X(\Omega))$, on note $I_y = f^{-1}(\{y\})$. On a

$$[f(X) = y] = \bigcup_{x \in I_y} [X = x]$$

et cette union est disjointe donc

$$\mathbf{P}(f(X) = y) = \sum_{x \in I_y} \mathbf{P}(X = x).$$

La famille $(I_y)_{y \in f(X(\Omega))}$ forme une partition de $X(\Omega)$. Puis

$$\sum_{x \in I_y} \mathbf{P}(X = x)f(x) = y \sum_{x \in I_y} \mathbf{P}(f(X) = y) = y\mathbf{P}(f(X) = y).$$

Si la famille $(f(x)\mathbf{P}(X = x))_{x \in X(\Omega)}$ est sommable, alors pour tout $y \in f(X(\Omega))$, $(f(x)\mathbf{P}(X = x))_{x \in I_y}$ est sommable et (I_y) est une partition donc la famille

$$\left(\sum_{x \in I_y} P(X = x)f(x) \right)_{y \in f(X(\Omega))}$$

est sommable et

$$\sum_{x \in X(\Omega)} f(x)\mathbf{P}(X = x) = \sum_{y \in f(X(\Omega))} \sum_{x \in I_y} f(x)\mathbf{P}(X = x) = \sum_{y \in f(X(\Omega))} y\mathbf{P}(f(X) = y) = \mathbf{E}(f(X)).$$

Si $f(X)$ est d'espérance finie, alors $(|y|\mathbf{P}(f(X) = y))_{y \in f(X(\Omega))}$ est sommable et

$$|y|\mathbf{P}(f(X) = y) = \sum_{x \in I_y} |f(x)|\mathbf{P}(X = x)$$

donc $(|f(x)|P(X = x))_{x \in X(\Omega)}$ est sommable.

□

Exemple. $X \hookrightarrow G(p)$, $Y = X^2$. La variable Y est-elle d'espérance finie ? La famille $(n^2 q^{n-1} p)_n$ est sommable donc Y a une espérance finie et

$$\mathbf{E}(Y) = \sum_{n \geqslant 1} n^2 q^{n-1} p = \frac{2 - p}{p^2}$$

On peut faire de même avec $Y = \exp(-X)$, ou encore si $X \hookrightarrow \mathscr{P}(\lambda)$, $Y = \cos X$

3 Conséquences du théorème de transfert

Proposition.

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé, X, Y deux v.a.r.d, Y d'espérance finie

(C) Si $|X| \leqslant Y$, alors X est d'espérance finie et $\mathbf{E}(|X|) \leqslant \mathbf{E}(Y)$

Démonstration. On note $Z = (X, Y)$ qui est une v.a.d et $f : \mathbf{R}^2 \to \mathbf{R}, (x, y) \longmapsto x$ de sorte que $X = f(Z)$. Alors

$$\begin{aligned} X \text{ d'espérance finie} &\iff (f(x,y)\mathbf{P}(X = x, Y = y))_{(x,y)\in X(\Omega)\times Y(\Omega)} \text{ sommable} \\ &\iff (x\mathbf{P}(X = x, Y = y))_{(x,y)\in X(\Omega)\times Y(\Omega)} \text{ sommable} \end{aligned}$$

On a

$$|x\mathbf{P}(X = x, Y = y)| \leqslant y\mathbf{P}(X = x, Y = y) \tag{$\star$}$$

Or

$$[Y = y] = \bigcup_{x\in X(\Omega)} [X = x, Y = y]$$

ce qui donne

$$\mathbf{P}(Y = y) = \sum_{x\in X(\Omega)} \mathbf{P}(X = x, Y = y)$$

donc $(y\mathbf{P}(X = x, Y = y))_{x\in X(\Omega)}$ est sommable. Y est d'espérance finie donc

$$(y\mathbf{P}(Y = y))_{y\in Y(\Omega)} = \left(\sum_{x\in X(\Omega)} y\mathbf{P}(X = x, Y = y)\right)_{y\in Y(\Omega)}$$

est sommable, donc $(y\mathbf{P}(X = x, Y = y))_{(x,y)\in X(\Omega)\times Y(\Omega)}$ est sommable et $(\star)$ conclut sur la sommabilité. Puis

$$\begin{aligned} \mathbf{E}(|X|) = \mathbf{E}(|f(Z)|) &= \sum_{\substack{x\in X(\Omega)\\ y\in Y(\Omega)}} |x|\mathbf{P}(X = x, Y = y) \\ &\leqslant \sum_{\substack{x\in X(\Omega)\\ y\in Y(\Omega)}} y\mathbf{P}(X = x, Y = y) \\ &\leqslant \sum_{y\in Y(\Omega)} \sum_{x\in X(\Omega)} y\mathbf{P}(X = x, Y = y) = \mathbf{E}(Y) \end{aligned}$$

□

Théorème.

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ espace probabilisé, $\lambda \in \mathbf{R}$ est X, Y des v.a.r.d. d'espérance finie.

(C)
1. $X + Y$ et λX sont des v.a.r.d d'espérance finie et $\mathbf{E}(X + Y) = \mathbf{E}(X) + \mathbf{E}(Y)$ et $\mathbf{E}(\lambda X) = \lambda\mathbf{E}(X)$
2. $X \geqslant 0 \implies \mathbf{E}(X) \geqslant 0$
3. $X \geqslant Y \implies \mathbf{E}(X) \geqslant \mathbf{E}(Y)$
4. Si X et Y sont indépendantes, $\mathbf{E}(XY) = \mathbf{E}(X)\mathbf{E}(Y)$

Démonstration.

1. L'homogénéité est évidente. On montre l'additivité. On pose $Z = (X, Y)$ et $f : (x, y) \longmapsto x + y$ de sorte que $T = f(Z)$ est une v.a.r.d par le lemme des coalitions. T est d'espérance finie si et seulement si $((x + y)\mathbf{P}(X = x, Y = y))_{x,y}$ est sommable.

La famille $(|x|\mathbf{P}(X=x,Y=y))_y$ est sommable car

$$[X=x]=\bigcup_{y\in Y(\Omega)}[X=x,Y=y]$$

et

$$\sum_{y\in Y(\Omega)}|x|\mathbf{P}(X=x,Y=y)=|x|\mathbf{P}(X=x)$$

sommable pour x donc $(|x|\mathbf{P}(X=x,Y=y))_{x,y}$ est sommable, idem pour $(|y|\mathbf{P}(X=x,Y=y))_{x,y}$ donc $X+Y$ est d'espérance finie. Finalement,

$$\mathbf{E}(T)=\sum_x\left(\sum_y x\mathbf{P}(X=x,Y=y)\right)+\sum_y\left(\sum_x y\mathbf{P}(X=x,Y=y)\right)=\mathbf{E}(X)+\mathbf{E}(Y)$$

2. On applique la définition
3. On utilise 2 et 1.
4. XY d'espérance finie si et seulement si $(xy\mathbf{P}(X=x,Y=y))_{x,y}$ est sommable soit encore si la famille $(x\mathbf{P}(X=x)y\mathbf{P}(Y=y))_{x,y}$ est sommable. Le théorème de Fubini discret donne la sommabilité et

$$\sum_{x,y}xy\mathbf{P}(X=x)\mathbf{P}(Y=y)=\mathbf{E}(X)\mathbf{E}(Y)$$

□

Exemple. On note $(E,(\ |\ ))$ un espace euclidien, $v_1,\cdots,v_n$ des vecteurs unitaires. On veut montrer qu'il existe $\varepsilon_1,\cdots,\varepsilon_n\in\{-1,1\}$ tels que

$$\|\varepsilon_1v_1+\cdots+\varepsilon_nv_n\|\leqslant\sqrt{n}$$

On se donne $X_1,\cdots,X_n\quad\perp\!\!\!\perp$ qui suivent une loi de Rademacher, c'est-à-dire $\mathbf{P}(X_i=-1)=\mathbf{P}(X_i=1)=\frac{1}{2}$. On note

$$N=\|X_1v_1+\cdots+X_nv_n\|^2$$

On a

$$\mathbf{E}(N)=\sum_{i=1}^n\underbrace{\mathbf{E}(X_i^2)\|v_i\|^2}_{=1}+\sum_{i\neq j}\underbrace{\mathbf{E}(X_iX_j)}_{=\mathbf{E}(X_i)\mathbf{E}(X_j)=0}(v_i|v_j)=n$$

Donc $\mathbf{P}(N\leqslant n)\neq0$ ce qui conclut.

4 Variance

Théorème – Définition.

(H) $(\Omega,\mathscr{A},\mathbf{P})$ un espace probabilisé, X une v.a.r.d

(C)
1. Si X^2 est d'espérance finie, alors X est d'espérance finie et $E(X)^2\leqslant E(X^2)$.
2. Dans ce cas, on appelle **variance** la quantité $V(X)=\mathbf{E}((X-\mathbf{E}(X))^2)$ et **écart-type** la quantité $\sigma(X)=\sqrt{V(X)}$
3. $V(X)=\mathbf{E}(X^2)-\mathbf{E}(X)^2$ (König-Huygens)
4. $V(aX+b)=a^2V(X)$

Démonstration.

1. $|X|\leqslant\frac{X^2+1}{2}$ et $\mathbf{E}((X+t)^2)=\mathbf{E}(X^2)+2t\mathbf{E}(X)+t^2\geqslant0$ donc $\Delta\leqslant0$ ie (C)
3. $\mathbf{E}((X-\mathbf{E}(X))^2)=\mathbf{E}(X^2-2X\mathbf{E}(X)+E(X)^2)=\mathbf{E}(X^2)-2\mathbf{E}(X)\mathbf{E}(X)+\mathbf{E}(X)^2=\mathbf{E}(X^2)-\mathbf{E}(X)^2$

□

Remarque.

On note X une vard de variance non nulle. La variable **centrée réduite**

$$Y = \frac{X - \mathbf{E}(X)}{\sigma(X)}$$

est telle que $\mathbf{E}(Y) = 0$ et $V(Y) = 1$

Remarque.

Si la quantité $\mathbf{E}(X^n)$ existe, on l'appelle **moment d'ordre n** de X

Exercice.

Pour $X \hookrightarrow G(p)$, montrer $\mathbf{E}(X) = \frac{1}{p}$ et $V(X) = \frac{q}{p^2}$. Pour $X \hookrightarrow \mathscr{P}(\lambda)$, montrer $\mathbf{E}(X) = \lambda, \quad V(X) = \lambda$

Théorème – Définition.

H $(\Omega, \mathscr{A}, \mathbf{P})$ un espace probabilisé, X, Y des vard avec variance.

C
1. X, Y sont d'espérances finies et
$$\mathbf{E}(XY)^2 \leqslant \mathbf{E}(X^2)\mathbf{E}(Y^2)$$
2. Dans ce cas, on appelle covariance de X et Y la quantité
$$\mathrm{Cov}(X, Y) = \mathbf{E}((X - \mathbf{E}(X))(Y - \mathbf{E}(Y)))$$
et on a
$$\mathrm{Cov}(X, Y) = \mathbf{E}(XY) - \mathbf{E}(X)\mathbf{E}(Y)$$
3. Lorsqu'il existe $(\sigma(X)\sigma(Y) \neq 0)$, on appelle coefficient de corrélation le réel
$$P(X, Y) = \frac{\mathrm{Cov}(X, Y)}{\sigma(X)\sigma(Y)} \in [-1, 1]$$

Démonstration.

1. $|XY| \leqslant \frac{X^2+Y^2}{2}$ d'où l'existence de l'espérance puis la négativité du discriminant dans $\mathbf{E}((X+tY)^2) \geqslant 0$ conclut, sauf si $\mathbf{E}(Y^2) = 0$, auquel cas $\mathbf{E}((X + tY)^2)$ est une constante, ce qui donne $E(XY) = 0$.
2. C'est la linéarité de l'espérance.
3. $|\mathrm{Cov}(X, Y)|^2 \leqslant \mathbf{E}((X - \mathbf{E}(X))^2)\mathbf{E}((Y - \mathbf{E}(Y))^2) = \sigma^2(X)\sigma^2(Y)$

□

Remarque.

On note $(X_i)_{1\leqslant i\leqslant n}$ une suite de v.a.r.d de $(\Omega, \mathscr{A}, \mathbf{P})$, $S_n = X_1 + \cdots + X_n$. On a

- $\mathbf{E}(S_n^2) = \sum_{i=1}^{n} \mathbf{E}(X_i^2) + 2\sum_{i<j} \mathbf{E}(X_iX_j)$
- $\mathbf{E}(S_n)^2 = \sum_{i=1}^{n} \mathbf{E}(X_i)^2 + 2\sum_{i<j} \mathbf{E}(X_i)\mathbf{E}(X_j)$
- $V(S_n) = \mathbf{E}(S_n^2) - E(S_n)^2 = \sum_{i=1}^{n} V(X_i) + 2\sum_{i<j} \mathrm{Cov}(X_i, X_j)$

Si les X_i sont deux à deux indépendants, alors $V(S_n) = V(X_1) + \cdots + V(X_n)$

Exemple. On munit $\mathfrak{S}_n$ de la probabilité uniforme. On note $S_n(\sigma)$ le nombre de points fixes de σ. Donner l'espérance et la variance de S_n.

Résolution. On introduit $X_i : \sigma \longmapsto \delta_{i,\sigma(i)}$ de sorte que $S_n(\sigma) = X_1 + \cdots + X_n$. Dans ce cas, on a

$$\mathbf{P}(X_i = 1) = \frac{(n-1)!}{n!} = \frac{1}{n}$$

donc $\mathbf{E}(X_i) = \frac{1}{n}$ (Bernoulli) et $\mathbf{E}(S_n) = 1$. Puis,

$$V(S_n) = \mathbf{E}(S_n^2) - E(S_n)^2 = \sum_{i=1}^{n} V(X_i) + 2\sum_{i<j} \operatorname{Cov}(X_i, X_j) = n\left(\frac{1}{n} - \frac{1}{n^2}\right) 2\frac{n(n-1)}{2}\left(\frac{1}{n(n-1)} - \frac{1}{n^2}\right) = 1$$

□

Définition.

Soient X, Y des v.a.d sur $(\Omega, \mathscr{A}, \mathbf{P})$ et $Z = (X, Y)$.

- On appelle **loi** de Z la donnée de $(\mathbf{P}(X = x, Y = y))_{\substack{x\in X(\Omega)\\ y\in Y(\Omega)}}$ appelée **loi conjointe** de X et Y.
- On appelle **loi marginale** de Z la loi de X et la loi de Y. Elles s'expriment à partir de la loi conjointe :

$$\mathbf{P}(X = x) = \sum_{y\in Y(\Omega)} \mathbf{P}(X = x, Y = y) \qquad \mathbf{P}(Y = y) = \sum_{x\in X(\Omega)} \mathbf{P}(X = x, Y = y)$$

Remarque.

Si $(a_{x,y})_{(x,y)\in I\times J}$ est une famille sommable de $[0, 1]$, alors il existe une v.a.r.d Z à valeurs dans $I \times J$ telle que $\forall (x, y) \in I \times J, \quad \mathbf{P}(Z = (x, y)) = a_{x,y}$ si et seulement si la somme de la famille vaut 1

5 Inégalités classiques

Théorème (Markov, Tchebychev).

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ espace probabilisé, X une v.a.r.d

(C)
1. Soit $a > 0$. Si X est d'espérance finie alors

$$\mathbf{P}(|X| \geqslant a) \leqslant \frac{\mathbf{E}(|X|)}{a} \tag{Markov}$$

2. Soit $a > 0$. Si X possède une variance alors

$$\mathbf{P}(|X - \mathbf{E}(X)| \geqslant a) \leqslant \frac{V(X)}{a^2} \tag{Tchebychev}$$

Démonstration.

1. $a\mathbb{1}_{|X|\geqslant a} \leqslant |X|$ et croissance de l'espérance
2. $\mathbf{P}(|X - \mathbf{E}(X)| \geqslant a) = \mathbf{P}((X - \mathbf{E}(X))^2 \geqslant a^2)$ puis Markov.

□

Exemple. On note $(X_i)_{i\geqslant 1}$ une suite de v.a.r.d $\perp\!\!\!\perp \hookrightarrow \mathscr{B}(\frac{1}{2})$. On note $S_n = X_1 + \cdots + X_n$ le nombre de succès en n lancés. $\mathbf{P}(S_n \geqslant \frac{3}{4}n)$?

- Markov : $\mathbf{P}(S_n \geqslant \dfrac{3}{4}n) \leqslant \dfrac{\frac{n}{2}}{\frac{3n}{4}} = \dfrac{2}{3}$
- Tchebychev : $\mathbf{P}(S_n \geqslant \dfrac{3}{4}) = \mathbf{P}(S_n - \mathbf{E}(S_n) \geqslant \dfrac{n}{4}) \leqslant \mathbf{P}(|S_n - \mathbf{E}(S_n)| \geqslant \dfrac{n}{4} \leqslant \dfrac{4}{n}$

Exemple. On note $X \hookrightarrow G(\frac{1}{4})$. On va majorer $\mathbf{P}(X \geqslant n)$.

- Markov : $\mathbf{P}(X \geqslant n) \leqslant \dfrac{\mathbf{E}(X)}{n} = \dfrac{4}{n}$
- Tchebychev $\mathbf{P}(X \geqslant n) \leqslant \dfrac{V(X)}{(n-4)^2} = \dfrac{12}{(n-4)^2}$
- En posant $Y = \left(\dfrac{5}{4}\right)^X$, on a $\mathbf{E}(Y) = 5$ donc

$$\mathbf{P}(X \geqslant n) \leqslant 5\left(\frac{4}{5}\right)^n$$

6 Variables aléatoires à valeurs entières

Définition – Proposition.

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ espace probabilisé, $X : \Omega \to \mathbf{N}$ une v.a.d

(C)
1. Pour tout $t \in [-1, 1]$, t^X est d'espérance finie
2. Pour tout $t \in [-1, 1]$, on note

$$G_X(t) = \mathbf{E}(t^X) = \sum_{n=0}^{+\infty} \mathbf{P}(X = n)t^n$$

On appelle cette fonction la **fonction génératrice** de X.
   (a) La série a un rayon de convergence $R \geqslant 1$
   (b) Il y a convergence normale sur $\mathscr{D}_f(0, 1)$

Démonstration. Pour $t \in [-1, 1]$, $|t^X| \leqslant 1$ or 1 a une espérance finie, puis la formule de transfert justifie l'expression de $\mathbf{E}(t^X)$. La série converge pour $t = 1$ donc il y a bien CVN et $R \geqslant 1$ □

Théorème.

(H) $X : \Omega \to \mathbf{N}$ une v.a.d

(C)
1. X est d'espérance finie si et seulement si $\sum \mathbf{P}(X \geqslant n)$ converge et dans ce cas

$$\mathbf{E}(X) = \sum_{n \geqslant 1} \mathbf{P}(X \geqslant n)$$

2. Il y a équivalence entre
   (a) X a une espérance finie
   (b) G_X est dérivable à gauche en 1
   Dans ce cas, $\mathbf{E}(X) = G'_X(1^-)$

Démonstration.
1. X est d'espérance finie si et seulement si $(k\mathbf{P}(X = k))_{k \in \mathbf{N}^\star}$ est sommable. On note

$$a_{i,k} \underset{\text{def}}{=} \mathbf{P}(X = k)\mathbb{1}_{[\![1,k]\!]}(i)$$

   La famille $(a_{i,k})_{i \in \mathbf{N}^\star}$ est sommable et

$$\sum_{i=1}^{+\infty} a_{i,k} = k\mathbf{P}(X = k)$$

   et c'est le terme général d'une famille sommable, donc Fubini discret conclut.
2. $(a \implies b)$ X d'espérance finie. Pour $t \in [0, 1[$,

$$\frac{G_X(t) - G_X(1)}{t - 1} = \sum_{n=0}^{+\infty} \mathbf{P}(X = n)\frac{t^n - 1}{t - 1} = \sum_{n=1}^{+\infty} \mathbf{P}(X = n)(1 + t + \cdots + t^{n-1})$$

   et le terme général de cette série est inférieur en valeur absolu à $n\mathbf{P}(X = n)$ qui est le terme général d'une série convergente. Il y a donc convergence normale et le théorème de la double limite donne

$$\lim_{t \to 1^-} \frac{G_X(t) - G_X(1)}{t - 1} = \sum_{n=1}^{+\infty} \mathbf{P}(X = n)n = \mathbf{E}(X)$$

($b \implies a$) G_X dérivable à gauche en 1. Pour $N \in \mathbf{N}^\star$ fixé,

$$\frac{G_X(t)-G_X(1)}{t-1} \geqslant \sum_{n=0}^{N} \mathbf{P}(X=n)(1+t+\cdots+t^{n-1}) \underset{t\to 1^-}{\Longrightarrow} G_X'(1) \geqslant \sum_{n=0}^{N} n\mathbf{P}(X=n)$$

Les sommes partielles sont majorées, donc X est d'espérance finie.

□

Exemple.

Loi de X	G_X	$R(G_X)$	$\mathbf{E}(X)$
$\mathscr{B}(p)$	$q+pt$	$+\infty$	p
$\mathscr{B}(n,p)$	$(q+pt)^n$	$+\infty$	np
$\mathscr{P}(\lambda)$	$\exp(\lambda(t-1))$	$+\infty$	λ
$\mathscr{G}(p)$	$\dfrac{pt}{1-qt}$	$\dfrac{1}{q}$	$\dfrac{1}{p}$
$\mathscr{U}(\llbracket 0,n-1\rrbracket)$	$\dfrac{1}{n}\dfrac{t^n-1}{t-1}$	$+\infty$	$\dfrac{n-1}{2}$

Remarque.

Si $X_1,\cdots,X_n$ sont des vard indépendantes à valeurs dans $\mathbf{N}$,

$$G_{X_1+\cdots+X_n}(t) = \mathbf{E}\left(t^{X_1+\cdots+X_n}\right) \underset{\perp\!\!\!\perp}{=} G_{X_1}(t)\times\cdots\times G_{X_n}(t)$$

Théorème.

H $(\Omega, \mathscr{A}, \mathbf{P})$ espace probabilisé, $X : \Omega \to \mathbf{N}$ une vad.

C Il y a équivalence entre

1. X a une variance
2. G_X est deux fois dérivable à gauche en 1.

Dans ce cas, $G_X''(1^-) = \mathbf{E}(X(X-1))$

Démonstration. ($1 \implies 2$) H X a une variance donc X a une espérance et

$$G_X'(1) = \sum_{n=1}^{+\infty} n\mathbf{P}(X=n)$$

donc

$$\frac{G_X'(t)-G_X'(1)}{t-1} = \sum_{n\geqslant 2} n\mathbf{P}(X=n)\frac{t^{n-1}-1}{t-1}$$

qui converge normalement (X^2 a une espérance finie car X a une variance), le théorème de la double limite conclut.

($2 \implies 1$) On a cette fois ci

$$\frac{G_X'(t)-G_X'(1)}{t-1} \geqslant \sum_{k=0}^{N} k(k-1)\mathbf{P}(X=k)(1+t+\cdots+t^{n-1})$$

donc avec $t \to 1^-$,

$$G_X''(1) \geqslant \sum_{n=0}^{N} n(n-1)\mathbf{P}(X=n) \geqslant 0$$

d'où la convergence de la série et C .

□

7 Somme aléatoire de v.a.r.d

On note $(X_n)_{n\in\mathbf{N}^\star}$ une suite de vard sur $(\Omega, \mathscr{A}, \mathbf{P})$, mutuellement indépendantes à valeurs dans $\mathbf{N}$. On note $N : \Omega \to \mathbf{N}^\star$ une vard indépendante des X_i et

$$S \underset{\text{def}}{=} X_1 + \cdots + X_N$$

On suppose que les X_i ont même loi. On a

$$[S = n] = \bigcup_{k\in\mathbf{N}^\star} [N = k, X_1 + \cdots + X_k = n]$$

donc

$$G_S(t) = \sum_{n\geqslant 0}\sum_{k\geqslant 1} \mathbf{P}(N = k)\mathbf{P}(X_1 + \cdots + X_k = n)t^n = \sum_{k\geqslant 1} \mathbf{P}(N = k)G_X(t)^k = G_N \circ G_X(t)$$

8 Résultats asymptotiques

Proposition.

(H) $(\Omega, \mathscr{A}, \mathbf{P})$ est un espace probabilisé, $X_n \hookrightarrow \mathscr{B}(n, p_n)$ avec $np_n \to \lambda > 0$

(C) Pour tout $k \in \mathbf{N}$,

$$\mathbf{P}(X_n = l) \xrightarrow[n\to+\infty]{} e^{-\lambda}\frac{\lambda^k}{k!}$$

Démonstration. Pas dur. □

Théorème.

(H) $(\Omega, \mathscr{A}, \mathbf{P})$, $X_1, \cdots, X_n$ des vard $\perp\!\!\!\perp$ de même loi avec variance (iid[1]), $S_n = X_1 + \cdots + X_n$ et $m = \mathbf{E}(X_1)$

(C)

$$\forall\varepsilon > 0, \quad \mathbf{P}\left(\left|\frac{S_n}{n} - m \geqslant \varepsilon\right|\right) \leqslant \frac{V(X_1)}{n\varepsilon^2} \xrightarrow[n\to+\infty]{} 0$$

Démonstration. Tchebychev □

9 Exemples

a) Loi du minimum

On cherche la loi de $Y = \min(X_1, \cdots, X_n)$ si $X_1, \cdots, X_n \hookrightarrow G(p)$ sont $\perp\!\!\!\perp$. On a

$$\mathbf{P}(Y > k) = \mathbf{P}(X_1 > k)^p = q^{kn}$$

et

$$\forall k \geqslant 1, \qquad \mathbf{P}(Y = k) = \mathbf{P}(Y > k - 1) - \mathbf{P}(Y > k) = q^{kn-n} - q^{kn} = q^{(k-1)n}(1 - q^n)$$

donc $Y \hookrightarrow G(1 - q^n)$

1. indépendantes et identiquement distribuées

b) Décomposabilité de la loi uniforme

On note Z une vard sur $(\Omega, \mathscr{A}, \mathbf{P})$ à valeurs dans $\mathbf{N}$. On dit que Z est décomposable s'il existe $X \perp\!\!\!\perp Y$ presque sûrement non constantes telles que $Z \sim X+Y$ (même loi). On va montrer que $Z \hookrightarrow \mathscr{U}([\![0, n-1]\!])$ est indécomposable si et seulement si n est premier.

- Si $n = uv$ avec $u, v \geqslant 2$, alors
$$G_Z(t) = \frac{1}{uv}\frac{t^{uv}-1}{t-1} = \frac{1}{v}\frac{(t^u)^v-1}{t^u-1} \cdot \frac{1}{u}\frac{t^u-1}{t-1}.$$
$\frac{1}{u}\frac{t^u-1}{t-1}$ est la fonction génératrice d'une vard qui suit une loi uniforme sur $[\![0, u-1]\!]$. Puis $\frac{1}{v}\frac{(t^u)^v-1}{t^u-1}$ est la fonction génératrice d'une vard qui suit une loi uniforme sur $u \cdot [\![0, v-1]\!]$ Il existe donc $X \perp\!\!\!\perp Y$ presque sûrement non constantes qui suivent des lois uniformes et telles que $Z \sim X+Y$
- On suppose que $n = p$ est premier et que Z est décomposable en $X+Y$, avec $X \perp\!\!\!\perp Y$ non constantes presque sûrement. On a alors
$$G_Z(t) = G_X(t)G_Y(t) = \frac{1}{p}(1+t+\cdots+t^{p-1})$$
Si G_X n'est pas polynômial, alors il y a une infinité de k tels que $\mathbf{P}(X=k)t^k \neq 0$, et si $\mathbf{P}(Y=i)t^i \neq 0$, le coef de t^{k+i} dans G_Z est non nul (produit de Cauchy avec des coefs positifs) donc G_Z n'est pas polynômial, ce qui est absurde. Donc G_X et G_Y sont des polynômes.
On suppose qu'il existe P, Q unitaires à coefficients positifs (les coefficients d'une série génératrice sont positifs) tels que $P(t)Q(t) = 1+\cdots+t^{p-1}$. Le polynôme PQ divise T^p-1 donc ses racines sont unitaires et
$$P(T) = (T-a_1)\cdots(T-a_r) = \overline{P}(T) = \left(T - \frac{1}{a_1}\right)\cdots\left(T-\frac{1}{a_r}\right) = \frac{(-1)^r}{a_1\cdots a_r}T^rP\left(\frac{1}{T}\right)$$
et vu les relations coefficients-racines, $\frac{(-1)^r}{a_1\cdots a_r} = 1$ donc $P(T) = T^rP\left(\frac{1}{T}\right)$ et P est un polynôme réciproque. Par le même raisonnement, Q aussi. On note $r = \deg P$ et $s = \deg Q$. On suppose $r \leqslant s$ et on a
$$P(t)Q(t) = (t^r + \alpha_{r-1}t^{r-1}+\cdots+1)(t^s+\beta_{s-1}t^{s-1}+\cdots+1) = 1+\cdots+t^{p-1}$$
donc (coef de t^r)
$$\sum_{i+j=r}\alpha_i\beta_j = \underbrace{\alpha_r\beta_0}_{=1} + \underbrace{\alpha_{r-1}\beta_1}_{\geqslant 0} + \cdots + \underbrace{\alpha_0\beta_r}_{\geqslant 0} = 1$$
donc $\alpha_{r-1}\beta_1 = \cdots = \alpha_0\beta_r = 0$ et $\beta_r = 0$
On va montrer que β_r ne peut pas être nul. On note $\omega = \exp(\frac{2i\pi}{p})$ et les racines de Q s'écrivent $\omega^{i_1}, \cdots, \omega^{i_s}$. Le coefficient de t^r dans Q vaut
$$(-1)^{s-r}\sum_{\substack{J\subset[\![1,s]\!]\\ \#J=s-r}}\prod_{j\in J}\omega^{i_j} = (-1)^{s-r}(a_0+a_1\omega+\cdots+a_{p-1}\omega^{p-1})$$
avec les a_i non tous nuls. On note
$$\hat{P}(X) = a_0 + a_1X+\cdots+a_{p-1}X^{p-1} \in \mathbf{Z}[X]$$
Le polynôme $1+X+\cdots+X^{p-1}$ est irréductible dans $\mathbf{Z}[X]$ (traité dans le chapitre de complément sur les polynômes), unitaire et annulateur de ω donc c'est son polynôme minimal. $\hat{P}$ est donc proportionnel à ce polynôme (car on a supposé $\beta_r = 0$) et $a_0 = \cdots = a_{p-1} \in \mathbf{N}^\star$. Puis $\hat{P}(1) = p \text{ dom } \hat{P}$ correspond aussi au nombre de termes dans la somme :
$$p \text{ dom } \hat{P} = \binom{s}{s-r}$$
ce qui est absurde car $s < p$ donne
$$v_p\left(\binom{s}{s-r}\right) = v_p(s!) - v_p((s-r)!) - v_p(r!) = 0$$

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre XV

Espaces préhilbertiens réels

Sommaire

1 Rappels

Dans tout le chapitre on ne considèrera que des $\mathbf{R}$-espaces vectoriels, sauf mention contraire.

Définition.

On appelle **produit scalaire** sur E une forme bilinéaire symétrique définie positive. Un $\mathbf{R}$-espace vectoriel E muni d'un produit scalaire $\langle \mid \rangle$ se note $(E, \langle \mid \rangle)$. Si E est de dimension finie, on dit qu'il est **euclidien**. Sinon, il est dit **préhilbertien**. On dit que x et y sont **orthogonaux** si $\langle x \mid y \rangle = 0$

Définition – Proposition.

(H) $(E, \langle \mid \rangle)$ un espace préhilbertien réel

(C)
1. Pour $x \in E$, l'application $x \longmapsto \sqrt{\langle x \mid x \rangle}$ est une norme. On l'appelle norme associée à $\langle \mid \rangle$
2. $\forall x, y \in E, \quad \|x+y\|^2 = \|x\|^2 + 2\langle x \mid y \rangle + \|y\|^2$
3. $\forall x, y \in E, \quad \langle x \mid y \rangle = \dfrac{1}{2}\left(\|x+y\|^2 - \|x\|^2 - \|y\|^2\right) = \dfrac{1}{4}(\|x+y\|^2 - \|x-y\|^2)$
4. $\forall x, y \in E, \quad \|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2)$ (identité du parallélogramme)

Démonstration. On verra une preuve du premier point plus tard. Le reste est facile. □

Définition.

Si $A \subset E$ où $(E, \langle \mid \rangle)$ est préhilbertien et $A \neq \varnothing$, on définit
1. $A^\perp = \{x \in E \mid \forall a \in A, \langle x \mid a \rangle = 0\}$
2. $A \perp B \iff \forall a \in A, \forall b \in B, \langle a \mid b \rangle = 0$

Remarque.

$\forall a \in A, \varphi_a : x \longmapsto \langle a \mid x \rangle \in E^\star$ et

$$A^\perp = \bigcap_{a \in A} \operatorname{Ker} \varphi_a$$

2 Produits scalaires usuels

a) Produits scalaires sur $\mathbf{R}^n$

On prend $x = (x_1, \cdots, x_n)$ et $y = (y_1, \cdots, y_n)$. Le produit scalaire canonique est définit par

$$\langle x \mid y \rangle = \sum_{i=1}^{n} x_i y_i$$

b) Produit scalaire à poids sur $\mathbf{R}[X]$

On se donne une fonction poids $f \in \mathscr{C}(I, \mathbf{R}_+) \setminus \{0\}$ telle que $\forall n \in \mathbf{N}, t \longmapsto t^n f(t)$ est intégrable sur l'intervalle I. Dans ce cas on peut définir

$$\langle P \mid Q \rangle = \int_I f(t) P(t) Q(t) \,\mathrm{d}t$$

c) Produit scalaire dans $\mathscr{L}_c^2(I, \mathbf{R})$

On a $\forall f, g \in \mathscr{L}_c^2(I, \mathbf{R}), \qquad |fg| \leqslant \dfrac{f^2 + g^2}{2}$ donc fg est intégrable sur I et on peut poser

$$\langle f \mid g \rangle = \int_I fg$$

Remarque.

On peut définir un produit scalaire à poids $w \in \mathscr{C}(I, \mathbf{R}_+^\star)$ sur l'ensemble

$$\mathscr{L}_{c,w}^2 = \left\{ f \in \mathscr{C}(I, \mathbf{R}) \;\middle|\; wf^2 \text{ intégrable } \right\}$$

3 Projections orthogonales

Théorème – Définition.

(H) $(E, \langle \mid \rangle)$ préhilbertien réel, F un sev de E de dimension finie et $(e_1, \cdots, e_n)$ une base orthonormée de F

(C)
1. $F^\perp$ est un sev de E
2. $E = F \oplus F^\perp$
3. On appelle **projection orthogonale** sur F l'application linéaire définie par

$$\forall x \in E, \quad \pi_F(x) = \langle e_1 \mid x \rangle e_1 + \cdots + \langle e_n \mid x \rangle e_n$$

4. $(F^\perp)^\perp$ si E est euclidien

Démonstration.
1. C'est la linéarité du produit scalaire
2. On se donne $x \in E$, et on pose $y = \langle x \mid e_1 \rangle e_1 + \cdots + \langle x \mid e_n \rangle e_n$. On a

$$\forall i \in [\![1, n]\!], \quad \langle x - y \mid e_i \rangle = \langle x \mid e_i \rangle - \sum_{i=j}^{n} \langle y \mid e_j \rangle \langle e_i \mid e_j \rangle = 0$$

donc $x-y \in F^\perp$ et $x = y+(x-y)$ d'où la somme directe. Puis la somme est directe car $F \cap F^\perp = \{0\}$

4. $F \subset (F^\perp)^\perp$ et même dimension finie.

□

Définition – Proposition.

(H) $(E, \langle \mid \rangle)$ préhilbertien, $p \in \mathscr{L}(E)$ projecteur

(C)
1. On dira que p est un **projecteur orthogonal** si $\operatorname{Ker} p \perp \operatorname{Im} p$
2. Il y a équivalence entre
   (a) p est un projecteur orthogonal
   (b) p est **autoadjoint** : $\forall x, y \in E, \quad \langle p(x) \mid y \rangle = \langle x \mid p(y) \rangle$

Démonstration.
$(a \implies b)$ $x, y \in E$

$$\langle p(x) \mid y \rangle = \langle p(x) \mid y - p(y) + p(y) \rangle = \langle p(x) \mid p(y) \rangle = \langle p(y) \mid p(x) \rangle = \langle x \mid p(y) \rangle$$

$(b \implies a)$ $x \in \operatorname{Ker} p, y \in \operatorname{Im} p$,

$$\langle x \mid y \rangle = \langle x \mid p(y) \rangle = \langle p(x) \mid y \rangle = 0$$

□

Exercice.
Montrer que dans E préhilbertien, un projecteur p tel que $\forall x \in E, \quad \|p(x)\| \leqslant \|x\|$ est orthogonal

Résolution. Soit $x \in \operatorname{Ker} p, y \in \operatorname{Im} p, t \in \mathbf{R}$.

$$\|p(y)\|^2 = \|p(y+tx)\|^2 \leqslant \|y+tx\| \iff \|p(y)\|^2 = \|y\|^2 \leqslant \|y\|^2 + 2t \langle y \mid x \rangle + \|x\|^2 t^2$$

donc

$$0 \leqslant 2t \langle y \mid x \rangle + \|x\|^2 t^2$$

d'où $\langle x \mid y \rangle = 0$ $(\Delta \leqslant 0)$ □

4 Distance d'un point à un sous-espace

Théorème – Définition.

(H) $(E, \langle \mid \rangle)$ préhilbertien réel et F sev de E

(C) 1. Soit $a \in E$. On pose
$$d(a, F) = \inf_{x \in F} \|x - a\|$$

2. En dimension finie, $d(a, F) = \|a - \pi_F(a)\| = \|\pi_{F^\perp}(a)\|$

Démonstration. 2. $\|a - x\|^2 = \|a - \pi_F(x)\|^2 + \|\pi_F - x\|^2 \geqslant \|a - \pi_F(a)\|^2$ □

Exemple. Déterminons
$$d = \inf_{a,b \in \mathbf{R}} \int_0^1 (\ln x - ax - b)^2 \,\mathrm{d}x$$
On se place sur $E = \mathscr{L}_c^1(]0,1], \mathbf{R})$ avec le produit scalaire usuel. On note $F = \mathbf{R}_1[X]$ de dimension finie, et on a
$$d = d(\ln, F)^2$$
On cherche $a, b \in \mathbf{R}$ tels que $\ln(x) - ax - b \perp F$. C'est équivalent à
$$\begin{cases} \langle \ln x - ax - b \mid 1 \rangle = 0 \\ \langle \ln x - ax - b \mid x \rangle = 0 \end{cases} \iff \int_0^1 (\ln x - ax - b) \,\mathrm{d}x = \int_0^1 x \ln x - ax^2 - bx \,\mathrm{d}x = 0$$
soit encore $a = 3$ et $b = -\dfrac{5}{2}$. On en déduit $d = \dfrac{1}{4}$

a) Méthode de Gauss.

On note $(E, \langle \mid \rangle)$ euclidien, $x = (x_1, \cdots, x_p)$ une famille de p vecteurs. On appelle **matrice de Gram** la matrice
$$G(x) = \begin{pmatrix} \langle x_1 \mid x_1 \rangle & \cdots & \langle x_1 \mid x_p \rangle \\ \vdots & \ddots & \vdots \\ \langle x_p \mid x_1 \rangle & \cdots & \langle x_p \mid x_p \rangle \end{pmatrix}$$
On note
$$T = \begin{pmatrix} t_1 \\ \cdots \\ t_p \end{pmatrix} \in \mathscr{M}_{p,1}(\mathbf{R})$$
de sorte que
$$\begin{aligned} T^\top G(x) T &= (t_1, \cdots, t_p) \begin{pmatrix} \langle x_1 \mid x_1 \rangle & \cdots & \langle x_1 \mid x_p \rangle \\ \vdots & \ddots & \vdots \\ \langle x_p \mid x_1 \rangle & \cdots & \langle x_n \mid x_p \rangle \end{pmatrix} \begin{pmatrix} t_1 \\ \cdots \\ t_p \end{pmatrix} \\ &= \|t_1 x_1 + \cdots + t_p x_p\|^2 \end{aligned}$$
Si x est libre, alors
$$G(x)T = 0 \implies T^\top G(x) T = 0 \implies \|t_1 x_1 + \cdots + t_p x_p\|^2 = 0 \implies T = 0$$
donc $G(x) \in \mathrm{GL}_n(\mathbf{R})$. On suppose $G(x)$ inversible.
$$t_1 x_1 + \cdots + t_p x_p = 0 \implies G(x)T = 0 = 0 \implies T = 0$$
donc x est libre. On a donc $\mathrm{rg}(G(x)) = p \iff \mathrm{rg}(x) = p$. Supposons que $\mathrm{rg}(x) = m$ et quitte à permutter, on suppose $(x_1, \cdots, x_m)$ libre.

Pour $k \geqslant m+1$, on écrit

$$x_k = \sum_{j=1}^{m} \alpha_{k,j} x_j$$

Avec des transvections (qui ne modifient pas le rang) on se ramène, en partant de $G(x)$, à

$$\begin{pmatrix} \langle x_1 \mid x_1 \rangle & \cdots & \langle x_1 \mid x_m \rangle & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \langle x_p \mid x_1 \rangle & \cdots & \langle x_p \mid x_m \rangle & 0 & \cdots & 0 \end{pmatrix}$$

qui est de rang m (on peut en extraire $G(x_1, \cdots, x_m)$ donc $\operatorname{rg}(G(x)) \geqslant m$ et l'autre inégalité est évidente). On a donc toujours $\operatorname{rg}(G(x)) = \operatorname{rg}(x)$.

Lien entre les déterminants de Gram et les distances. On note F un sev de E de base $(x_1, \cdots, x_p)$. On note $u \in E$ et $\pi_F(u) = \lambda_1 x_1 + \cdots + \lambda_p x_p$.

$$\det(G(x,u)) = \begin{vmatrix} \langle x_1 \mid x_1 \rangle & \cdots & \langle x_1 \mid x_p \rangle & \langle x_1 \mid u \rangle \\ \vdots & \ddots & \vdots & \vdots \\ \langle x_p \mid x_1 \rangle & \cdots & \langle x_p \mid x_p \rangle & \langle x_p \mid u \rangle \\ \langle u \mid x_1 \rangle & \cdots & \langle u \mid x_p \rangle & \langle u \mid u \rangle \end{vmatrix}$$

On fait $C_{p+1} \leftarrow C_{p+1} - \lambda C_1 - \cdots - \lambda_p C_p$ et idem sur les lignes, on obtient

$$\begin{vmatrix} \langle x_1 \mid x_1 \rangle & \cdots & \langle x_1 \mid x_p \rangle & \langle x_1 \mid u - \pi_F(u) \rangle \\ \vdots & \ddots & \vdots & \vdots \\ \langle x_p \mid x_1 \rangle & \cdots & \langle x_p \mid x_p \rangle & \langle x_p \mid u - \pi_F(u) \rangle \\ \langle u - \pi_F(u) \mid x_1 \rangle & \cdots & \langle u - \pi_F(u) \mid x_p \rangle & \langle u - \pi_F(u) \mid u - \pi_F(u) \rangle \end{vmatrix} = \|u - \pi_F(u)\|^2 \det(G(x))$$

donc

$$d(u,F)^2 = \frac{\det(G(x,u))}{\det(G(x))}$$

b) Projection sur un compact convexe

Existence et unicité du projeté. On note $(E, \langle \ \mid \ \rangle)$ euclidien, C un compact convexe. On va montrer que

$$\forall a \in F, \quad \exists! c \in C, \qquad \inf_{x \in C} \|x - a\| = \|c - a\|$$

On note Δ l'inf et $(c_n) \in C^{\mathbf{N}}$ une suite telle que

$$\|c_n - a\| \xrightarrow[n \to +\infty]{} \Delta$$

Une telle suite existe et C est compact donc on peut supposer (quitte à extraire) que c'est une suite convergente de limite $x \in C$, ce qui montre l'existence.

Si $c, c' \in C$ conviennent, on note $u = c - a$ et $v = c' - a$. L'identité du parallélogramme donne

$$\|x + y\|^2 + \|u - v\|^2 = 2(\|u\|^2 + \|v\|^2)$$

donc

$$\|c - c'\|^2 + \underbrace{4\|\frac{c + c'}{2} - a\|}_{\geqslant 4\Delta^2} = 4\Delta^2$$

et $\|c - c'\| \leqslant 0 \implies c = c'$

Remarque.

> Si on ne suppose pas que C est compact, alors l'unicité reste vraie mais pas l'existence. Mais, si $(c_n) \in C^{\mathbf{N}}$ est minimisante,
>
> $$\|c_n - c_m\|^2 = \underbrace{2(\|c_n - a\|^2 + \|c_m - a\|^2)}_{\leqslant 4\Delta^2 + \varepsilon \text{ APCR}} - \underbrace{4\|\frac{c_n + c_m}{2} - a\|}_{\geqslant 4\Delta^2} \leqslant \varepsilon \text{ PARC}$$
>
> donc (c_n) est une suite de Cauchy, qui converge (car E est un espace de Banach). Si C est fermé, (c_n) converge vers un élément $c \in C$

Notation.

On note $c = \pi_C(a)$

Caractérisation du projeté. On va maintenant montrer qu'il y a équivalence entre

1. $z = \pi_C(a)$
2. $\forall y \in C, \quad \langle\, y - z \mid a - z \,\rangle \leqslant 0$

$(1 \implies 2)$ Pour $t \in [0,1]$, on a $(1-t)z + ty \in C$ pour $y \in C$. Puis

$$\|a - z\|^2 \leqslant \|a - (1-t)z + ty\|^2 = \|a - z\|^2 + 2t\,\langle\, a - z \mid z - y \,\rangle + t^2\|z - y\|^2$$

donc

$$2\,\langle\, a - z \mid y - z \,\rangle \leqslant t\|z - y\|^2$$

et $t \to 0$ permet de conclure.

$(2 \implies 1)$ $\forall t \in [0,1], \forall y \in C$,

$$t\,\langle\, a - z \mid y - z \,\rangle \leqslant t\|y - z\|^2 \implies \|a - z\|^2 \leqslant \|a - y\|^2$$

par le raisonnement inverse, en prenant $t = 1$.

Caractère lipschitzien. Pour $x, x' \in E$,

$$\langle\, \pi_C(x') - \pi_C(x) \mid x - \pi_C(x) \,\rangle \leqslant 0 \qquad \text{et} \qquad \langle\, \pi_C(x) - \pi_C(x') \mid x' - \pi_C(x') \,\rangle \leqslant 0$$

donc en ajoutant les deux inégalités

$$\|\pi_C(x') - \pi_C(x)\|^2 \leqslant \langle\, \pi_C(x') - \pi_C(x) \mid x' - x \,\rangle \underset{\text{CS}}{\leqslant} \|\pi_C(x') - \pi_C(x)\| \times \|x' - x\|$$

d'où le caractère 1-lipschitzien (on divise par $\|\pi_C(x') - \pi_C(x)\|$ si c'est non nul, le cas nul est évident)

c) Procédé de Gram-Schmidt

On note E un espace préhilbertien réel, $(f_1, \cdots, f_n)$ une famille libre. On va montrer qu'il existe une famille $(e_1, \cdots, e_n)$ orthogonale telle que $\forall i \leqslant n, \mathrm{Vect}(e_1, \cdots, e_i) = \mathrm{Vect}(f_1, \cdots, f_i)$.

Principe :

- On pose $e_1 = f_1$
- On suppose $e_1, \cdots, e_i$ construits. On cherche e_{i+1} de la forme

$$e_{i+1} = \lambda_{i,1}e_1 + \cdots + \lambda_{i,i}e_i + f_{i+1}$$

La condition $e_{i+1} \perp e_1, \cdots, e_i$ impose

$$\langle\, e_{i+1} \mid e_1 \,\rangle = \cdots = \langle\, e_{i+1} \mid e_i \,\rangle = 0 \iff \begin{cases} 0 = \lambda_{i,1}\,\langle\, e_1 \mid e_i \,\rangle + \langle\, f_{i+1} \mid e_1 \,\rangle \\ \cdots \\ 0 = \lambda_{i,i}\,\langle\, e_i \mid e_i \,\rangle + \langle\, f_{i+1} \mid e_i \,\rangle \end{cases} \implies \lambda_{i,k} = -\frac{\langle\, f_{i+1} \mid e_k \,\rangle}{\langle\, e_k \mid e_k \,\rangle}$$

et ces valeurs conviennent.

Remarque.

La matrice de passage entre une famille libre et son orthogonalisée de Gram-Schmidt est triangulaire supérieure, et sa diagonale ne contient que la valeur propre 1.

5 Inégalité de Hadamard

On note $\mathscr{F} = (f_1, \cdots, f_p)$ une famille libre de E, et $\mathscr{E} = (e_1, \cdots, e_p)$ la famille orthonormée construite par le procédé de Gram-Schmidt.

On note $P_{\mathscr{F},\mathscr{E}} = \mathscr{M}_{\mathscr{F},\mathscr{E}}(\mathrm{id})$ de sorte que

$$f_j = \sum_{i=1}^{p} \left(P_{\mathscr{F},\mathscr{E}}\right)_{i,j} e_i \qquad \text{et} \qquad e_j = \sum_{i=1}^{p} \left(P_{\mathscr{E},\mathscr{F}}\right)_{i,j} f_i$$

On note $T = P_{\mathscr{E},\mathscr{F}}$, et on a

$$\begin{aligned}\left(T^\top G(\mathscr{F})T\right)_{i,j} &= \sum_{1\leqslant k,l\leqslant p} (T^\top)_{i,k} G(\mathscr{F})_{k,l} T_{l,j}\\ &= \sum_{1\leqslant k,l\leqslant p} T_{k,i} \langle f_k \mid f_l \rangle T_{l,j}\\ &= \left\langle \sum_{k=1}^{p} T_{k,i} f_k \,\middle|\, \sum_{l=1}^{p} T_{l,j} f_l \right\rangle = \langle e_i \mid e_j \rangle = \delta_{i,j}\end{aligned}$$

donc

$$T^\top G(\mathscr{F})T = I_p \qquad \text{et} \qquad \det(G(\mathscr{F})) = \frac{1}{(\det T)^2} = \prod_{i=1}^{p} \langle f_i \mid e_i \rangle^2 \underset{\text{CS}}{\leqslant} \prod_{i=1}^{p} \|f_i\|^2$$

Avec égalité si et seulement si $(f_1, \cdots, f_p)$ est orthogonale, i.e. si $e_i = \dfrac{f_i}{\|f_i\|^2}$

Prenons $A \in \mathscr{M}_n(\mathbf{R})$ inversible, on note $C_1, \cdots, C_n$ ses colonnes. On a

$$A^\top A = \begin{pmatrix} C_1^\top \\ \vdots \\ C_n^\top \end{pmatrix} (C_1, \cdots, C_n) = (\, \underbrace{C_i^\top C_j}_{\langle C_i \mid C_j \rangle} \,)_{i,j}$$

donc

$$\det(A^\top A) = \det(A)^2 \leqslant \prod_{i=1}^{n} \|C_i\|^2$$

ce qui reste vrai pour A non inversible. On a donc finalement toujours

$$\det(A)^2 \leqslant \prod_{n=1}^{n} \|C_i\|^2$$

6 Famille totale

Définition.

On se place dans $(E, \langle \mid \rangle)$ un espace préhilbertien réel de dimension infinie. On dira que $(e_k)_{k\in\mathbf{N}} \in E^{\mathbf{N}}$ est totale si c'est une famille orthonormale et si

$$\overline{\operatorname{Vect}\left((e_k)_{k\in\mathbf{N}}\right)} = E$$

Théorème.

H $(e_k)_{k\in\mathbf{N}}$ famille totale, $E_n = \operatorname{Vect}(e_1, \cdots, e_n)$, π_n projecteur orthogonal sur E_n

C
1. $\forall x \in E, \quad \|x - \pi_n(x)\|^2 \xrightarrow[n\to+\infty]{} 0$
2. Égalité de Parseval :

$$\forall x \in E, \|x\|^2 = \sum_{k=0}^{+\infty} \langle x \mid e_k \rangle^2$$

Démonstration.

1. $E = \overline{\operatorname{Vect}((e_k)_k)}$. On note $x \in E$, $\varepsilon > 0$. Il existe $y \in \operatorname{Vect}((e_k)_k)$ tel que $\|x - y\| \leqslant \varepsilon$ et il existe $N \in \mathbf{N}$ tel que $\forall n \geqslant N, y \in E_n$ donc $\|x - \pi_n(x)\| \leqslant \|x - y\| \leqslant \varepsilon$
2. $$\|x\|^2 = \|x - \pi_n(x)\|^2 + \|\pi_n(x)\|^2$$

   et

   $$\pi_n(x) = \sum_{k=0}^{n} \langle x \mid e_k \rangle e_k \qquad \text{donc} \qquad \|\pi_n(x)\|^2 = \sum_{k=0}^{n} \langle x \mid e_k \rangle^2 .$$

   Finalement,

   $$\|x\|^2 = \underbrace{\|x - \pi_n(x)\|^2}_{\xrightarrow[n\to+\infty]{} 0} + \|\pi_n(x)\|^2 \xrightarrow[n\to+\infty]{} \sum_{n=0}^{+\infty} \langle x \mid e_n \rangle^2$$

□

Remarque.

- On peut écrire

$$\pi_n(x) = \sum_{n=0}^{n} \langle\, x \mid e_n \,\rangle\, e_n \xrightarrow[n\to+\infty]{} x \qquad \text{donc} \qquad x = \sum_{n=0}^{+\infty} \langle\, x \mid e_n \,\rangle\, e_n$$

- On se donne (e_k) orthonormale. Pour $x \in E$, on pose $f_n : x \longmapsto \|x - \pi_n(x)\|$. Si (e_k) est totale alors pour chaque x, $f_n(x) \longrightarrow 0$. Si pour chaque x, $f_n(x) \longrightarrow 0$, alors $\pi_n(x) \longrightarrow x$ et $x \in \overline{\mathrm{Vect}((e_k)_k)}$ donc la famille est totale.

7 Les séries de Fourier

On note $f \in \mathscr{C}^0_{2\pi}(\mathbf{R}, \mathbf{C})$, et on définit

$$c_n(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-int}\,\mathrm{d}t = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)e^{-int}\,\mathrm{d}t$$

et

$$S_n(f) : x \longmapsto \sum_{k=-n}^{n} c_k(f)e_k(x) \qquad \text{où} \qquad e_k : x \longmapsto e^{ikx}$$

On introduit le produit hermitien

$$(\, f \mid g \,) = \frac{1}{4\pi}\int_0^{2\pi} \overline{f}g$$

Quelques remarques :

- $c_n(f) \xrightarrow[n\to+\infty]{} 0$ (Riemann-Lebesgue)
- $(\, e_k \mid e_l \,) = \delta_{k,l}$
- Si $k \in [\![-n, n]\!]$,

$$(\, f - S_n(f) \mid e_k \,) = (\, f \mid e_k \,) - \left(\sum_{l=-n}^{n} c_l(f)e_l \,\middle|\, e_k\right) = (\, f \mid e_k \,) - \sum_{l=-n}^{n} \overline{c_l(f)}\,(\, e_l \mid e_k \,) = 0$$

En particulier, $(\, f - S_n(f) \mid S_n(f) \,) = 0$ et

$$(\, f \mid f \,) = (\, f - S_n(f) \mid f - S_n(f) \,) + (\, S_n(f) \mid S_n(f) \,) \geqslant (\, S_n(f) \mid S_n(f) \,) = \sum_{k=-n}^{n} |c_k(f)|^2 \text{ CV}$$

a) Théorème de Féjer

On va montrer que

$$\sigma_n(f) : x \longmapsto \frac{1}{n+1}\sum_{k=0}^{n} S_k(f)(x)$$

converge uniformément vers $f \in \mathscr{C}^0_{2\pi}(\mathbf{R}, \mathbf{C})$

Un lemme. Pour $x \notin 2\pi\mathbf{Z}$,

$$S_n(x) = \sum_{k=-n}^{k=n} e^{ikx} = e^{-inx}\frac{1 - e^{i(2n+1)x}}{1 - e^{ix}} = \frac{\sin\left(\frac{2n+1}{2}x\right)}{\sin\left(\frac{x}{2}\right)}$$

et cette expression se prolonge par continuité sur $2\pi\mathbf{Z}$. On note $s_n = \sigma_n(\mathrm{id})$ de sorte que

$$s_n(x) = \frac{1}{n+1}\mathfrak{Im}\left(\frac{e^{i\frac{x}{2}}}{\sin\frac{x}{2}}\sum_{k=0}^{n} e^{ikx}\right) = \frac{1}{n+1}\frac{\sin^2(\frac{n+1}{2}x)}{\sin^2\frac{x}{2}}$$

qu'on prolonge encore sur $2\pi\mathbf{Z}$.

Preuve du théorème. On a :

$$\sigma_n(f)(x) = \frac{1}{2\pi}\int_0^{2\pi} \frac{f(t)}{n+1}\sum_{l=0}^{n}\sum_{k=-l}^{l} e^{ik(x-t)}\,\mathrm{d}t = \frac{1}{2\pi}\int_0^{2\pi} f(t)s_n(x-t)\,\mathrm{d}t$$

Pour $f \equiv 1$, on a $\sigma_n(f) \equiv 1$ donc

$$\frac{1}{2\pi}\int_0^{2\pi} s_n(x-t)\,\mathrm{d}t = 1$$

Pour $f \in \mathscr{C}^0_{2\pi}(\mathbf{R},\mathbf{C})$ quelconque, on a

$$\sigma_n(f)(x) - f(x) = \frac{1}{2\pi}\int_0^{2\pi}(f(t)-f(x))s_n(x-t)\,\mathrm{d}t$$

Soit $\varepsilon > 0$. f est continue périodique donc uniformément continue (Heine + périodicité) sur $\mathbf{R}$ et il existe $\delta > 0$ tel que $|u-v| \leqslant \delta \implies |f(u)-f(v)| \leqslant \varepsilon'$. Dans ce cas,

$$\sigma_n(f)(x) - f(x) = \frac{1}{2\pi}\int_{-\pi}^{\pi}(f(x-u)-f(x))s_n(u)\,\mathrm{d}u$$

et on peut séparer l'intégrale en trois intégrales adaptées à l'écriture $[-\pi,\pi] = [-\pi,-\delta]\cup[-\delta,\delta]\cup[\delta,\pi]$. Sur $[-\delta,\delta]$,

$$\left|\frac{1}{2\pi}\int_{-\delta}^{\delta}(f(x-u)-f(x))\underbrace{s_n(u)}_{\geqslant 0}\,\mathrm{d}u\right| \leqslant \frac{1}{2\pi}\int_{-\delta}^{\delta}\underbrace{|f(x-u)-f(x)|}_{\leqslant\varepsilon'}s_n(u)\,\mathrm{d}u \leqslant \varepsilon'$$

et sur $[\delta,\pi]$ (le troisième intervalle se traite identiquement),

$$\left|\frac{1}{2\pi}\int_{\delta}^{\pi}(f(x-u)-f(x))s_n(u)\,\mathrm{d}u\right| \leqslant \frac{2\|f\|_\infty}{2\pi}\frac{\pi-\delta}{n+1}\cdot\frac{1}{\sin^2\frac{\delta}{2}} \xrightarrow[n\to+\infty]{} 0$$

donc $\leqslant \varepsilon'$ APCR. Ainsi, APCR, $\|\sigma_n(f)-f\|_\infty \leqslant 3\varepsilon' = \varepsilon$ donc

$$\sigma_n(f) \xrightarrow[\mathbf{R}]{\text{CVU}} f$$

b) Weierstrass trigonométrique

Pour tout f, $\sigma_n(f)$ est un polynôme trigonométrique. Le théorème de Féjer permet alors de montrer le théorème de Weierstrass trigonométrique : toute fonction continue 2π-périodique est limite d'une suite de polynômes trigonométriques. Ainsi,

- dans $\mathbf{C}$, $\overline{\mathrm{Vect}(e_k, k\in\mathbf{Z})} = \mathscr{C}^0_{2\pi}(\mathbf{R},\mathbf{C})$
- dans $\mathbf{R}$, $\overline{\mathrm{Vect}(\sin\circ(k\,\mathrm{id}), \cos\circ(k\,\mathrm{id}), k\in\mathbf{Z})} = \mathscr{C}^0_{2\pi}(\mathbf{R},\mathbf{R})$

Dans les deux cas, la famille est orthogonale dénombrable. On obtient une famille totale en normalisant.

8 Théorème de Müntz-Szász

On se place dans $E = \mathscr{C}^0([0,1],\mathbf{R})$ muni du produit scalaire usuel

$$\langle f \mid g\rangle = \int_0^1 fg$$

On note $\mathscr{F} = (t \longmapsto t^{\lambda_i})_{i\in\mathbf{N}}$ pour $(\lambda_i)_{i\in\mathbf{N}}$ une suite strictement croissante qui tend vers $+\infty$ [1]

On note $E_n = \mathrm{Vect}(t\longmapsto t^{\lambda_i}, i\in[\![1,n]\!])$ et $d_n(t^k) = d(t^k, E_n)$.

On va montrer que $\overline{\mathrm{Vect}(\mathscr{F})} = \mathscr{C}^0([0,1],\mathbf{R})$ si et seulement si $\sum\frac{1}{\lambda_i}$ diverge. Puisque $\overline{\mathbf{R}[X]} = \mathscr{C}^0([0,1],\mathbf{R})$, on va en fait montrer que $\forall k\in\mathbf{N}, t^k \in \overline{\mathrm{Vect}(\mathscr{F})} \iff \sum\frac{1}{\lambda_i}$ DV.

1. Il s'agit d'une version plus faible du théorème pour lequel on ne suppose pas $\lambda_i \to +\infty$

On a $\left\langle t^{\lambda_i} \mid t^{\lambda_j} \right\rangle = \dfrac{1}{\lambda_i + \lambda_j + 1}$ donc

$$G_n \underset{\text{def}}{=} G(\mathscr{F}_n) = \begin{pmatrix} \dfrac{1}{\lambda_1+\lambda_1+1} & \cdots & \dfrac{1}{\lambda_1+\lambda_n+1} \\ \vdots & \ddots & \vdots \\ \dfrac{1}{\lambda_n+\lambda_1+1} & \cdots & \dfrac{1}{\lambda_n+\lambda_n+1} \end{pmatrix}$$

On va calculer son déterminant. On pose

$$\Delta_n(X) = \begin{vmatrix} \dfrac{1}{\lambda_1+\lambda_1+1} & \cdots & \dfrac{1}{\lambda_1+X+1} \\ \vdots & \ddots & \vdots \\ \dfrac{1}{\lambda_n+\lambda_1+1} & \cdots & \dfrac{1}{\lambda_n+X+1} \end{vmatrix} = \frac{P_n(X)}{(\lambda_1+X+1)\cdots(\lambda_n+X+1)}$$

avec $\deg P_n \leqslant n-1$. Pour $x = \lambda_1, \cdots, \lambda_{n-1}$, $P_n(x)$ est nul car deux colonnes sont identiques. On a donc $P_n(X) = A_n(X-\lambda_1)\cdots(X-\lambda_{n-1})$ où $A_n = \operatorname{dom} P_n$. Une décomposition en éléments simples donne

$$\frac{A_n(X-\lambda_1)\cdots(X-\lambda_{n-1})}{(\lambda_1+X+1)\cdots(\lambda_n+X+1)} = \frac{A_n(-\lambda_n-1-\lambda_1)\cdots(-\lambda_n-1-\lambda_{n-1})}{(\lambda_1-\lambda_n)\cdots(\lambda_{n-1}-\lambda_n)(\lambda_n+X+1)} + \text{ autres pôles}$$

or en décomposant par rapport à la dernière colonne,

$$\Delta_n(X) = \frac{\Delta_{n-1}(X)}{\lambda_n+X+1} + \text{ autres pôles}$$

donc par unicité des décompositions en éléments simples,

$$\Delta_{n-1} = \frac{A_n(-1)^{n-1}(\lambda_1+\lambda_n+1)\cdots(\lambda_{n-1}+\lambda_n+1)}{(\lambda_n-\lambda_{n-1})\cdots(\lambda_n-\lambda_1)(-1)^{n-1}}$$

soit encore

$$\Delta_n(X) = \frac{(\lambda_n-\lambda_{n-1})\cdots(\lambda_n-\lambda_1)}{(\lambda_1+\lambda_n+1)\cdots(\lambda_{n-1}+\lambda_n+1)}\Delta_{n-1}\frac{(X-\lambda_1)\cdots(X-\lambda_{n-1})}{(\lambda_1+X+1)\cdots(\lambda_n+X+1)}$$

et si on note $\delta_n = \Delta_n(\lambda_n)$, on a

$$\delta_n = \frac{(\lambda_n-\lambda_1)^2\cdots(\lambda_n-\lambda_{n-1})^2}{(\lambda_1+\lambda_n+1)^2\cdots(\lambda_{n-1}+\lambda_n+1)^2}\cdot\frac{\Delta_{n-1}}{2\lambda_n+1}$$

et d'après la formule de Gram,

$$d_n(t^k)^2 = \frac{\det(G(t^{\lambda_1},\cdots,t^{\lambda_n},t^k))}{\delta_n} = \frac{(k-\lambda_1)^2\cdots(k-\lambda_n)^2}{(k+\lambda_1+1)^2\cdots(k+\lambda_n+1)^2}\cdot\frac{1}{2k+1}$$

Il s'agit de voir si $d_n(t^k) \xrightarrow[n\to+\infty]{} 0$. On écrit

$$d_n(t^k)^2 = \frac{1}{2k+1}\left(\frac{1-\dfrac{k}{\lambda_1}}{1+\dfrac{k+1}{\lambda_1}}\right)^2\cdots\left(\frac{1-\dfrac{k}{\lambda_n}}{1+\dfrac{k+1}{\lambda_n}}\right)^2$$

de sorte que

$$\ln(d_n(t^k)^2) = \ln\left(\frac{1}{2k+1}\right) + 2\sum_{i=1}^{n}\ln\left(\frac{1-\dfrac{k}{\lambda_i}}{1+\dfrac{k+1}{\lambda_i}}\right)$$

or

$$\ln\left(\frac{1-\dfrac{k}{\lambda_i}}{1+\dfrac{k+1}{\lambda_i}}\right) = \ln\left(\left(1-\frac{k}{\lambda_i}\right)\left(1-\frac{k+1}{\lambda_i}+o\left(\frac{1}{\lambda_i}\right)\right)\right)$$
$$= \ln\left(1-\frac{2k+1}{\lambda_i}+o\left(\frac{1}{\lambda_i}\right)\right)$$
$$\underset{+\infty}{\sim} -\frac{2k+1}{\lambda_i}$$

donc

$$d_n(t^k) \xrightarrow[n\to+\infty]{} 0 \iff \sum \frac{1}{\lambda_i} \text{ DV}$$

9 Endomorphismes symétriques

Définition – Proposition.

(H) $(E, \langle \mid \rangle)$ est un espace préhilbertien réel

(C)
1. On dira que $f \in \mathscr{L}(E)$ est **symétrique** ou **autoadjoint** si $\forall x, y \in E, \langle f(x) \mid y \rangle = \langle x \mid f(y) \rangle$
2. On note $\mathrm{S}(E)$ l'ensemble des endomorphismes symétriques de E
3. $\mathrm{S}(E)$ est un sev de $\mathscr{L}(E)$

Exemple. Les projecteurs orthogonaux sont symétriques

Remarque.

Si $f \in \mathrm{S}(E)$ et $\mathscr{B} = (e_1, \cdots, e_n)$ est une base orthonormée de E, alors

$$\mathscr{M}_{\mathscr{B}}(f) = \begin{pmatrix} \langle f(e_1) \mid e_1 \rangle & \cdots & \langle f(e_n) \mid e_1 \rangle \\ \vdots & \ddots & \vdots \\ \langle f(e_1) \mid e_n \rangle & \cdots & \langle f(e_n) \mid e_n \rangle \end{pmatrix} \in \mathrm{S}_n(\mathbf{R})$$

Proposition.

(H) $f \in \mathrm{S}(E)$ en dimension finie, F un sev stable par f

(C) $F^\perp$ est stable par f

Démonstration.

$$\forall x \in F, \forall y \in F^\perp, \quad \langle x \mid f(y) \rangle = \langle f(x) \mid y \rangle = 0 \qquad \text{ie } f(y) \in F^\perp$$

□

Théorème (Spectral).

(H) E euclidien, $f \in \mathrm{S}(E)$

(C)
1. $\chi_f(X)$ est scindé sur $\mathbf{R}$
2. Les $E_\lambda(f)$ sont en somme directe orthogonale
3. $E = \displaystyle\bigoplus_{\lambda \in \mathrm{Sp}(f)} E_\lambda(f)$. En particulier, f est diagonalisable dans une base orthonormée.

Démonstration.

1. On note $\mathscr{B}$ une base orthonormée de E, $A = \mathscr{M}_{\mathscr{B}}(f) \in \S_n(\mathbf{R})$. Soit $\lambda \in \mathrm{Sp}_{\mathbf{C}}(A)$ et $X \in \mathbf{C}^n$ un vecteur propre associé. On a

$$\begin{aligned} {}^t\overline{X}AX &= \lambda {}^t\overline{X}X \\ &= {}^t\overline{X}{}^t\overline{A}X \\ &= {}^t(\overline{AX})X \\ &= \overline{\lambda}{}^t\overline{X}X \end{aligned}$$

donc $\lambda = \overline{\lambda}$ et $\lambda \in \mathbf{R}$. On a donc $\mathrm{Sp}_{\mathbf{C}}(A) \subset \mathbf{R}$. Puis, χ_A est scindé en tant que polynôme complexe, et a ses racines dans $\mathbf{R}$ et est donc scindé dans $\mathbf{R}[X]$.

2. Si $x \in E_\lambda(f), y \in E_\mu(f)$,

$$\langle f(x) \mid y \rangle = \lambda \langle x \mid y \rangle = \langle x \mid f(y) \rangle = \mu \langle x \mid y \rangle \implies \lambda = \mu \text{ ou } \langle x \mid y \rangle = 0$$

3. On note F la somme directe des espaces propres, et on suppose $F \neq E$. F est stable par f donc $F^\perp$ aussi, $E = F \oplus F^\perp$, et $f_{|F^\perp}$ est un endomorphisme symétrique en dimension finie. Son polynôme caractéristique est scindé, donc admet une racine et cette racine est une valeur propre, ce qui est absurde car $F^\perp$ ne contient aucun espace propre. Donc, $F = E$, ce qui conclut.

□

Remarque.

Cela montre que les matrices réelles symétriques sont diagonalisables dans une base orthonormée pour le produit scalaire usuel de $\mathscr{M}_{n,1}(\mathbf{R})$.

10 Groupe orthogonal

On se place dans E un espace euclidien.

Théorème – Définition.

1. $f \in \mathscr{L}(E)$ est un automorphisme **orthogonal** si il satisfait l'une des deux deux propriétés équivalentes suivantes
   (a) $\forall x, y \in E, \quad \langle f(x) \mid f(y) \rangle = \langle x \mid y \rangle$
   (b) $\forall x \in E, \quad \|f(x)\| = \|x\|$
2. On note $\mathrm{O}(E)$ l'ensemble des automorphisme orthogonaux. C'est un sous-groupe de $(\mathrm{GL}(E), \circ)$

Démonstration. 1. Le sens direct est évident avec $x = y$, et dans l'autre on applique la formule de polarisation

2. L'injectivité est directe avec (b) donc $\mathrm{O}(E) \subset \mathrm{GL}(E)$. Si f, g sont orthogonaux alors

$$\forall x \in E, \quad \|f^{-1} \circ g(x)\| = \|f \circ f^{-1} \circ g(x)\| = \|g(x)\| = \|x\|$$

donc $f^{-1} \circ g \in \mathrm{O}(E)$. L'identité est dans $\mathrm{O}(E)$.

□

Théorème.

(H) $f \in \mathscr{L}(E)$

(C) Il y a équivalence entre
1. $f \in \mathrm{O}(E)$
2. $\forall\, \mathscr{B}$ ON , $\quad f(\mathscr{B})$ ON
3. $\exists\, \mathscr{B}$ ON , $\quad f(\mathscr{B})$ ON

Démonstration.
(1 $\implies$ 2) $\langle f(e_i) \mid f(e_j) \rangle = \langle e_i \mid e_j \rangle = \delta_{i,j}$
(2 $\implies$ 3) direct car il existe des bases ON
(3 $\implies$ 1) En décomposant sur $\mathscr{B}$, on trouve bien $\langle f(x) \mid f(y) \rangle = \langle x \mid y \rangle$ □

Théorème – Définition.

1. $A \in \mathscr{M}_n(\mathbf{R})$ est dite orthogonale si $A^\top A = AA^\top = I_n$. On note $\mathrm{O}_n(\mathbf{R})$ l'ensemble des matrices orthogonales.
2. $\mathrm{O}_n(\mathbf{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$
3. Si $f \in \mathscr{L}(E)$, il y a équivalence
   (a) $f \in \mathrm{O}(E)$
   (b) $\forall\, \mathscr{B}$ ON , $\quad \mathscr{M}_{\mathscr{B}}(f) \in \mathrm{O}_n(\mathbf{R})$
   (c) $\exists\, \mathscr{B}$ ON , $\quad \mathscr{M}_{\mathscr{B}}(f) \in \mathrm{O}_n(\mathbf{R})$

Démonstration.
($a \implies b$) Si $A = \mathscr{M}_{\mathscr{B}}(f)$ pour $\mathscr{B}$ ON, alors on calcule

$$A^\top A = (\langle\, C_i \mid C_j \,\rangle)_{1 \leqslant i,j \leqslant n} = (\langle\, f(e_i) \mid f(e_j) \,\rangle)_{1 \leqslant 1,j \leqslant n}$$

($b \implies c$) direct
($c \implies a$) Si $A^\top A = I_n$, alors on trouve bien $\langle\, f(e_i) \mid f(e_j) \,\rangle = \delta_{i,j}$, donc $f(\mathscr{B})$ est ON. □

Remarque.

Une matrice orthogonale est telle que $\det(A)^2 = 1 \iff \det A = \pm 1$

Remarque.

Avec le produit scalaire $\langle\, M \mid N \,\rangle = \mathrm{Tr}(M^\top N)$ sur $\mathscr{M}_n(\mathbf{R})$, on a $\forall A \in \mathrm{O}_n(\mathbf{R}), \quad \langle\, A \mid A \,\rangle = \|A\|^2 = n$ donc $\mathrm{O}_n(\mathbf{R})$ est borné. Puis si

$$f : M \longmapsto M^\top M - I_n$$

alors f est continue et $\mathrm{O}_n(\mathbf{R}) = f^{-1}(\{0\})$ donc $\mathrm{O}_n(\mathbf{R})$ est compact.

11 Groupe spécial orthogonal

Théorème – Définition.

1. $f \in \mathrm{O}(E)$ est une **rotation** si $\det f = 1$. On note $\mathrm{SO}(E)$ l'ensemble des rotations de $\mathrm{O}(E)$
2. C'est un sous-groupe de $\mathrm{O}(E)$, qu'on appelle **groupe spécial orthogonal**.
3. Identiquement, $\mathrm{SO}_n(\mathbf{R})$ est le sous-groupe de $\mathrm{O}_n(\mathbf{R})$ constitué des matrices orthogonales de déterminant 1

Démonstration. $\mathrm{SO}(E) = \ker f$ où $f : A \longmapsto \det A$ donc c'est un groupe. □

a) Orientation

Si $\mathscr{B}$ et $\mathscr{B}'$ sont des bases orthonormées de E, alors $P_{\mathscr{B},\mathscr{B}'} = \mathscr{M}_{\mathscr{B}}(h)$ avec $h : e_i \longmapsto e'_i$, alors $h \in \mathrm{O}(E)$ car l'image d'une base ON est ON. On a donc $\det P_{\mathscr{B},\mathscr{B}'} = \det h = \pm 1$ et $P_{\mathscr{B},\mathscr{B}'} \in O_n(\mathbf{R})$

Définition.

1. Deux bases orthonormées ont même **orientation** si la matrice de passage de l'une à l'autre est celle d'une rotation ($\det P = 1$)
2. La relation $\mathscr{B} \mathrel{\mathscr{R}} \mathscr{B}' \iff \det P_{\mathscr{B},\mathscr{B}'} = 1$ est une relation d'équivalence sur l'ensemble des bases orthonormées, il y a deux classes d'équivalences
3. Un espace euclidien est dit **orienté** lorsqu'on a choisi l'une de ces deux classes, qui sera alors la classe des bases orthonormées **directes**
4. Si H est un hyperplan, u un vecteur unitaire orthogonal à H, et $\mathscr{B} = (e_1, \cdots, e_{n-1})$ une base orthonormée de H, alors $\mathscr{B}$ est directe si $(e_1, \cdots, e_{n-1}, u)$ est une base directe de E. On dira que H est orienté par u.

Proposition.

(H) $(E, \langle \mid \rangle)$ euclidien orienté, $u \in \mathscr{L}(E)$

(C) Il y a équivalence entre

1. $u \in \mathrm{SO}(E)$
2. $\forall\ \mathscr{B},\quad u(\mathscr{B})$ orthonormée directe
3. $\exists\ \mathscr{B},\quad u(\mathscr{B})$ orthonormée directe
4. $\forall\ \mathscr{B}$ orthonormée directe, $\mathscr{M}_{\mathscr{B}}(u) \in \mathrm{SO}_n(\mathbf{R})$
5. $\exists\ \mathscr{B}$ orthonormée directe, $\mathscr{M}_{\mathscr{B}}(u) \in \mathrm{SO}_n(\mathbf{R})$

Démonstration. Facile □

b) Le cas du plan

On se place dans $E = \mathbf{R}^2$ muni du produit scalaire canonique et de l'orientation usuelle.

$$
\begin{aligned}
A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{O}_2(\mathbf{R}) &\iff \begin{cases} a^2 + c^2 = 1 \\ b^2 + d^2 = 1 \\ ab + cd = 0 \end{cases} \\
&\iff \exists \theta, \theta' \in \mathbf{R}, \begin{cases} a = \cos\theta \qquad c = \sin\theta \\ b = \sin\theta' \qquad d = \cos\theta' \\ ab + cd = 0 \end{cases} \\
&\iff \exists \theta, \theta' \in \mathbf{R}, \begin{cases} a = \cos\theta \qquad c = \sin\theta \\ b = \sin\theta' \qquad d = \cos\theta' \\ \theta + \theta' \equiv 0 \pmod{\pi} \end{cases} \\
&\iff \exists \theta \in \mathbf{R}, \quad A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{ou} \quad A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}
\end{aligned}
$$

et

$$
A \in \mathrm{SO}_2(\mathbf{R}) \iff A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \underset{\text{def}}{=} R_\theta
$$

On a par ailleurs $R_\theta R_{\theta'} = R_{\theta+\theta'}$ donc $\mathrm{SO}_2(\mathbf{R})$ est abélien

Proposition.

Soit $u \in \mathrm{SO}(\mathbf{R}^2)$. La matrice $\mathscr{M}_{\mathscr{B}}(u)$ est indépendante de la base orthonormée directe choisie et

$$
\exists! \theta \in [0, 2\pi[, \quad \mathscr{M}_{\mathscr{B}}(u) = R_\theta
$$

On dit alors que u est la rotation d'angle θ

Démonstration. $\mathrm{SO}_2(\mathbf{R})$ est abélien donc les matrices de passage n'ont pas d'influence. □

Remarque (Angle orienté).

Pour $x, y \in E$ (E euclidien orienté de dimension 2) et $\mathscr{B}$ orthonormée directe, on a (calculer explicitement)

$$
\langle x \mid y \rangle^2 + \det_{\mathscr{B}}(x, y)^2 = \|x\|^2 \|y\|^2
$$

donc si $x, y \neq 0$, il existe un unique $\theta \pmod{2\pi}$ tel que

$$
\begin{cases} \langle x \mid y \rangle = \|x\| \|y\| \cos\theta \\ \det_{\mathscr{B}}(x, y) = \|x\| \|y\| \sin\theta \end{cases}
$$

Ce réel θ est alors appelé angle orienté $\widehat{(x, y)}$

c) Produit vectoriel

Théorème (Théorème de représentation de Riesz).

(H) E euclidien

(C) $\forall \varphi \in E^\star, \quad \exists! a \in E, \quad \forall x \in E, \quad \varphi(x) = \langle\, a \mid x \,\rangle$

Démonstration.

$$\begin{array}{rccc} \psi : & E & \longrightarrow & E^\star \\ & a & \longmapsto & (x \longmapsto \langle\, a \mid x \,\rangle) \end{array}$$

Est une AL injective et $\dim E = \dim E^\star$ donc c'est un isomorphisme. □

Théorème – Définition.

(H) E est un espace euclidien orienté de dimension 3

(C)
1. $u, v, w \in E$. La quantité $\det_{\mathscr{B}}(u, v, w)$ ne dépend pas de $\mathscr{B}$ OND. On la note $[u, v, w]$
2. $u, v \in E. \exists! w \in E, \quad \forall x \in E, [u, v, x] = \langle\, w \mid x \,\rangle$. On note alors $w = u \wedge v$
3. $(u, v) \longmapsto u \wedge v$ est bilinéaire antisymétrique
4. $u \wedge v = 0 \iff u, v$ colinéaires
5. $u \wedge v \perp u, v$
6. Si (e_1, e_2, e_3) OND alors $e_1 \wedge e_2 = e_3, e_2 \wedge e_3 = e_1, e_3 \wedge e_1 = e_2$
7. Si (e_1, e_2, e_3) ON alors cette base est directe si et seulement si $e_1 \wedge e_2 = e_3$

Démonstration.
1. Le changement de base introduit un facteur 1.
2. C'est le Théorème de représentation de Riesz
3. Le déterminant est multilinéaire antisymétrique
4. (u, v) liée car sinon il existe x tel que (u, v, x) est une base. La réciproque est évidente.
5. $x = u, x = v$
6. Facile
7. Admis (facile)

□

Remarque.

(e_1, e_2, e_3) OND, $x \leftrightarrow (x_1, x_2, x_3), y \leftrightarrow (y_1, y_2, y_3)$. En abusant de la notation du déterminant, on peut écrire

$$\begin{aligned} x \wedge y &= (x_1 e_1 + x_2 e_2 + x_3 e_3) \wedge (y_1 e_1 + y_2 e_2 + y_3 e_3) \\ &= \cdots \\ &= \begin{vmatrix} x_1 & y_1 & e_1 \\ x_2 & y_2 & e_2 \\ x_3 & y_3 & e_3 \end{vmatrix} \end{aligned}$$

d) Rotation dans l'espace

On se place dans l'espace euclidien tridimensionnel E.

Définition.

Si e est un vecteur unitaire et $\theta \in \mathbf{R}$, on appelle rotation d'axe $\mathbf{R}e$ orienté par e d'angle θ l'application linéaire telle que $r(e) = e$, $r_{|e^\perp}$ est la rotation d'angle θ pour l'orientation de $e^\perp$ par e. L'application r se note $r_{\theta,e}$.

Remarque.

Si $\mathscr{B} = (e_1, e_2, e_3)$ OND alors $e_3^\perp = \text{Vect}(e_1, e_2)$ et (e_1, e_2) OND pour l'orientation par e_3.

$$\begin{aligned}\mathscr{M}_{\mathscr{B}}(r) = \begin{pmatrix}\cos\theta & -\sin\theta & 0\\ \sin\theta & \cos\theta & 0\\ 0 & 0 & 1\end{pmatrix} &= \cos\theta\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} + (1-\cos\theta)\begin{pmatrix}0&0&0\\0&0&0\\0&0&1\end{pmatrix} + \sin\theta\begin{pmatrix}0&-1&0\\1&0&0\\0&0&0\end{pmatrix}\\ &= \cos\theta\mathscr{M}_{\mathscr{B}}(\text{id}_E) + (1-\cos\theta)\mathscr{M}_{\mathscr{B}}(\pi_{\mathbf{R}e_3}) + \sin\theta\mathscr{M}_{\mathscr{B}}(x\longmapsto e_3\wedge x)\end{aligned}$$

donc $r(x) = \cos\theta x + (1-\cos\theta)\pi_{\mathbf{R}e_3}(x) + \sin\theta e_3\wedge x$

Soit $A \in \text{SO}_3(\mathbf{R})$. A admet une valeur propre réelle (polynôme caractéristique réel de degré impaire).

$$AX = \lambda X \implies (AX)^\top AX = \lambda^2 X^\top X = X^\top A^\top AX = X^\top X \implies \lambda = \pm 1$$

Si $\lambda = -1$ et X_3 est un vecteur propre associé, $X_3^\perp$ est stable par A donc si (X_1, X_2, X_3) OND,

$$\mathscr{M}_{\mathscr{B}}(A) = \begin{pmatrix}a & b & 0\\ c & d & 0\\ 0 & 0 & -1\end{pmatrix}$$

et $\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in O_2(\mathbf{R})$, $\det\begin{pmatrix}a & b\\ c & d\end{pmatrix} = -1$ donc il existe $\theta\in\mathbf{R}$ tel que $\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}$ et le polynôme caractéristique de A est $\chi_A(X) = (X+1)(X^2-\cos^2\theta) - \sin^2\theta = (X+1)(X^2-1)$ donc 1 est toujours une valeur propre de A.

Chapitre XVI

Calcul différentiel

Sommaire

1 Notions, Définitions

E est un $\mathbf{R}$-e.v de dimension n (donc isomorphe à $\mathbf{R}^n$), F un sev de E et Ω un ouvert de E.

Remarque.

Pour $a \in \Omega, v \in E, \exists \varepsilon > 0, \forall t \in]-\varepsilon, \varepsilon[, a + tv \in \Omega$ (par définition d'un ouvert)

Définition.

On note $f : \Omega \longrightarrow F$. On dira que f possède une dérivée en $a \in \Omega$ selon $v \in E$ si

$$\lim_{\substack{t \to 0 \\ t \neq 0}} \frac{f(a+tv) - f(a)}{t}$$

existe. On note cette limite $D_v f(a)$.
Si $\mathscr{B} = (e_1, \cdots, e_n)$ base de E et f a une dérivée en $a \in \Omega$ selon e_{i_0} alors on appelle i_0-ième dérivée partielle $D_{e_{i_0}} f(a)$, notée

$$\frac{\partial f}{\partial x_{i_0}}(a) \qquad \text{ou} \qquad \partial_{i_0} f(a)$$

Remarque.

Pour $\mathscr{B} = (e_1, \cdots, e_n)$ on note $x \underset{\mathscr{B}}{\longleftrightarrow} (x_1, \cdots, x_n)$ et on a $f(x) = f(x_1 e_1 + \cdots + x_n e_n)$ qu'on note abusivement $f(x_1, \cdots, x_n)$.

$$\frac{f(x+te_1) - f(x)}{t} = \frac{f(x_1 + t, x_2, \cdots, x_n) - f(x_1, \cdots, x_n)}{t}$$

Pour calculer $\partial_i f(a)$, on fait comme si les autres variables étaient constantes et on dérive par rapport à x_i.

Remarque.

D_v est linéaire

Remarque.

Avoir une dérivée en a n'implique pas la continuité en a. Contre-exemple :

$$f(x,y) = \begin{cases} \frac{y^2}{x} & \text{si } x \neq 0 \\ y & \text{sinon} \end{cases}$$

2 Différentielle

Définition – Proposition.

(H) $f : \Omega \longrightarrow F$, $a \in \Omega$.

(C)
1. On dira que f est différentiable en a s'il existe $\varphi \in \mathscr{L}(E,F), \varepsilon > 0$ tels que

$$\forall h \in \mathscr{B}_o(0,\varepsilon), f(a+h) = f(a) + \varphi(h) + o_0(h)$$

   Dans ce cas φ est unique et se note $\mathrm{d}f_a$
2. Si f est différentiable en a alors f est continue en a
3. Si f est différentiable en a alors f a une dérivée en a selon tout v et

$$D_v f(a) = \mathrm{d}f_a(v)$$

Démonstration.

1. Si φ, ψ conviennent, $\varphi(tv) - \psi(tv) = o_0(tv)$ ie

$$\varphi(v) - \psi(v) = o_0(v) \xrightarrow[t \to 0]{} 0$$

   d'où $\varphi \equiv \psi$.
2. $f(a+h) = f(a) + \varphi(h) + o_0(h) \xrightarrow[h \to 0]{} f(a)$
3. $$\frac{f(a+tv) - f(a)}{t} = \mathrm{d}f_a(v) + o_0(v) \xrightarrow[\substack{t \to 0 \\ t \neq 0}]{} \mathrm{d}f_a(v)$$

□

Théorème – Définition.

1. Soit $f \in \mathscr{L}(E,F)$ et $a \in E$. La fonction f est différentiable en a et $\mathrm{d}f_a = f$.
2. Si $\mathscr{B} = (e_1, \cdots, e_n)$ est une base de E et si π_i est l'application i-ième coordonnée alors $\forall a \in E, \mathrm{d}\pi_i = \pi_i$ ne dépend pas de a. On note cette application $\mathrm{d}x_i$.
3. Si $\mathscr{B}$ est une base de E et f est différentiable en a alors

$$\mathrm{d}f_a = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a)\,\mathrm{d}x_i$$

Démonstration.

1. $f(a+h) = f(a) + f(h)$
2. Ok
3. $h = h_1 e_1 + \cdots + h_n e_n$,

$$\mathrm{d}f_a(h) = h_1\,\mathrm{d}f_a(e_1) + \cdots + h_n\,\mathrm{d}f_a(e_n) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a)\,\mathrm{d}x_i(h)$$

□

Remarque.

Pour une fonction $f : \mathbf{R} \longrightarrow F$, $f'(a) = \mathrm{d}f_a(1)$

3 Calculs de différentielles

a) Quelques exemples

Exemple. Étude en 0 de

$$f(x,y) = \begin{cases} \frac{y^2}{x} & \text{si } x \neq 0 \\ y & \text{sinon} \end{cases}$$

$$\frac{\partial f}{\partial x}(0,0) = 0 \qquad \frac{\partial f}{\partial y}(0,0) = f(0,1) = 1$$

donc

$$\frac{\partial f}{\partial x}(0,0)\,\mathrm{d}x + \frac{\partial f}{\partial y}(0,0)\,\mathrm{d}y$$

existe mais f est non différentiable car non $\mathscr{C}^0$

Exemple. Calcul de la différentielle de $f : A \in \mathscr{M}_n(\mathbf{R}) \longmapsto A^2$

$$f(A+H) = f(A) + AH + HA + H^2$$

et pour une norme sous-multiplicative, $\|H^2\| \leqslant \|H\|^2 = o_0(H)$ donc

$$\mathrm{d}f_A(H) = AH + HA$$

Exemple. Calcul de la différentielle de $f : M \in GL_n(\mathbf{R}) \longmapsto M^{-1}$

On fixe $M \in GL_n(\mathbf{R})$. Alors $\exists \varepsilon > 0 / \mathscr{B}_o(M,\varepsilon) \subset GL_n(\mathbf{R})$. Pour H dans $\mathscr{B}_o(0,\varepsilon)$,

$$M + H \in \mathscr{B}_o(M,\varepsilon)$$

et

$$\left((M+H)^{-1} - M^{-1}\right)(M+H) = I_n - M^{-1}(M+H) = -M^{-1}H$$

donc

$$\begin{aligned}(M+H)^{-1}-M^{-1} &= -M^{-1}H(M+H)^{-1}\\ &= -M^{-1}HM^{-1}+M^{-1}Ho_0(1)\\ &= \underbrace{-M^{-1}HM^{-1}}_{\mathrm{d}f_M(H)}+o_0(H)\end{aligned}$$

Exercice.

Calcul de la différentielle de $f : A \in \mathscr{M}_n(\mathbf{R}) \longmapsto A^{\intercal}A$

b) Interprétation matricielle

Théorème – Définition.

On note $f : \Omega \to \mathbf{R}^m$, $\Omega \subset \mathbf{R}^n$, on écrit $f = (f_1, \cdots, f_m)$. On suppose que f est différentiable en $a \in \Omega$ et on note $\mathscr{C}_n$ (resp. $\mathscr{C}_m$) la base canonique de $\mathbf{R}^n$ (resp. $\mathbf{R}^m$). Alors :

1. On appelle matrice jacobienne de f en a la matrice

$$J_f(a) = \left(\frac{\partial f_i}{\partial x_j}(a)\right)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}$$

2. Si $x \underset{\mathscr{C}_n}{\longleftrightarrow} X$ alors

$$\mathrm{d}f_a(x) \underset{\mathscr{C}_m}{\longleftrightarrow} J_f(a)X$$

Démonstration.

$$\mathrm{d}f_a(x) = \sum_{i=1}^{n} \underbrace{\frac{\partial f}{\partial x_i}(x)}_{\left(\frac{\partial f_1}{\partial x_i}(x),\cdots,\frac{\partial f_m}{\partial x_i}(x)\right)} \overbrace{\mathrm{d}x_i(x)}^{=x_i} \underset{\mathscr{C}_n}{\longleftrightarrow} \begin{pmatrix}\sum_{i=1}^{n}\frac{\partial f_1}{\partial x_i}(a)x_i\\ \vdots\\ \sum_{i=1}^{n}\frac{\partial f_m}{\partial x_i}(a)x_i\end{pmatrix} = J_f(a)X$$

□

4 Opérations sur les différentielles

Proposition.

Si $f, g : \omega \subset E \to F$ sont différentiables en a, alors pour $\lambda \in \mathbf{R}$, $\lambda f + g$ est différentiable en a et $\mathrm{d}(\lambda f + g)_a = \lambda df_a + \mathrm{d}g_a$

Proposition.

(H) $B : E_1 \times E_2 \to F$ bilinéaire, $f_1 : \Omega_1 \to E_1$ différentiable en a_1, $f_2 : \Omega_2 \to E_2$ différentiable en a_2.

(C) $f = B(f_1, f_2)$ est différentiable en $a = (a_1, a_2)$ et

$$\mathrm{d}f_a(h_1,h_2) = B(\mathrm{d}f_{1_{a_1}}(h_1), f_2(a_2)) + B(f_1(a_1), \mathrm{d}f_{2_{a_2}}(h_2))$$

Démonstration. On développe $f(a+h) = B(f_1(a_1+h_1), f_2(a_2+h_2))$ □

Exemple.

- $(E, (\ |\ ))$ euclidien, $\varphi : (x,y) \longmapsto (x|y)$

$$\mathrm{d}\varphi_{(x,y)}(h,k) = (h|y) + (x|k)$$

- $\varphi = \det$. On note
$$A = (C_1 \cdots C_n) \quad H = (H_1 \cdots H_n)$$
alors
$$\det(A+H) = \det(A) + \det(H_1, C_2, \cdots, C_n) + \cdots + \det(C_1, \cdots, C_{n-1}, H_n) + o_0(H)$$
On en déduit
$$\begin{aligned}\mathrm{d}\varphi_A(H) &= \sum_{j=1}^{n} \det(C_1, \cdots, H_i, \cdots, C_n) \\ &= \sum_{j=1}^{n}\sum_{i=1}^{n} (-1)^{i+j} h_{i,j} \Delta_{i,j}(A) \\ &= \mathrm{Tr}(\mathrm{Com}(A)^\intercal H)\end{aligned}$$

5 Composition des fonctions différentielles

Proposition.

(H) $f : \Omega \subset E \to F$ différentiable en a telle que $f(\Omega) \subset \Omega'$, $g : \Omega' \subset F \to G$ différentiable en $f(a)$

(C) $g \circ f$ est différentiable en a et $\mathrm{d}(g \circ f)_a = \mathrm{d}g_{f(a)} \circ \mathrm{d}f_a$

Démonstration. On a
$$g(f(a)+k) = g(f(a)) + \mathrm{d}g_{f(a)}(k) + o(k)$$
et
$$f(a+h) = f(a) + \underbrace{\mathrm{d}f_a(h) + o(h)}_{k}$$
donc
$$g \circ f(a+h) = g(f(a)) + \mathrm{d}g_{f(a)}(\mathrm{d}f_a(h) + o_0(h)) + \underbrace{o(\underbrace{\mathrm{d}f_a(h) + o_0(h)}_{o(h)})}_{o(h)}$$
d'où (C) ☐

Remarque.

$E = \mathbf{R}^n$, $F = \mathbf{R}^m$, $G = \mathbf{R}^p$, $f = (f_1, \cdots, f_m) : E \to F$, $g = (g_1, \cdots, g_p) : F \to G$, $\mathscr{C}_k$ base canonique de $\mathbf{R}^k$.

Si $x \underset{\mathscr{C}_n}{\longleftrightarrow} X$ alors $\mathrm{d}f_a(x) \underset{\mathscr{C}_m}{\longleftrightarrow} J_f(a)X$ et $\mathrm{d}(g \circ f)_a(x) \underset{\mathscr{C}_p}{\longleftrightarrow} J_{g\circ f}(a)X \underset{\mathscr{C}_p}{\longleftrightarrow} J_g(f(a))J_f(a)X$. C'est vrai pour tout X donc
$$\underbrace{J_{g\circ f}(a)}_{\in \mathscr{M}_{p,n}} = \underbrace{J_g(f(a))}_{\in \mathscr{M}_{p,m}} \underbrace{J_f(a)}_{\in \mathscr{M}_{m,n}}$$
On va identifier le coefficient i, j.
$$\begin{aligned} & [J_{g\circ f}(a)]_{i,j} = \sum_{k=1}^{m} [J_g(f(a))]_{i,k} [J_f(a)]_{k,j} \\ \iff & \frac{\partial (g_i \circ f)}{\partial x_j}(a) = \sum_{k=1}^{m} \frac{\partial g_i}{\partial y_k}(f(a)) \frac{\partial f_k}{\partial x_j}(a) \\ \iff & \boxed{\partial_j (g_i \circ f)(a) = \sum_{k=1}^{m} \partial_k g_i(f(a)) \partial_j f_k(a)} \qquad \textit{(règle de la chaîne)}\end{aligned}$$
En particulier, si $p = n = 1$, $\varphi : t \in \mathbf{R} \to g(f_1(t), \cdots, f_m(t))$ alors
$$(g \circ f)'(a) = \sum_{k=1}^{m} \frac{\partial g}{\partial y_k}(f(a)) f_k'(a)$$

Remarque.

Si $f : \Omega \subset E \to \mathbf{R}$ est différentiable en a et $f(a) \neq 0$ alors $\frac{1}{f}$ est différentiable en a car $x \longmapsto \frac{1}{x}$ est différentiable en $f(a)$

Remarque.

Si $f : \Omega \subset E \to F$ est $a \in \Omega$, $v \in E$ alors $\varphi : t \longmapsto f(a+tv)$ est définie au $\mathscr{V}(0)$ et $\varphi'(t) = \mathrm{d}f_{a+tv}(v)$

6 Applications de classe $\mathscr{C}^1$

Théorème – Définition.

(H) $f : \Omega \subset E \longrightarrow F$

(C)
1. On dira que f est $\mathscr{C}^1$ sur Ω si f est différentiable sur Ω et si $a \in \Omega \longmapsto \mathrm{d}f_a \in \mathscr{L}(E,F)$ est $\mathscr{C}^0$
2. Une fonction $\mathscr{C}^1$ est continue
3. On note $\mathscr{B} = (e_1, \cdots, e_n)$ une base de E, $\mathscr{C} = (u_1, \cdots, u_m)$ une base de F et $f = (f_1, \cdots, f_m)$. Il y a équivalence entre :
   (a) f est $\mathscr{C}^1$ sur Ω
   (b) Les f_i ont toutes leurs dérivées partielles sur Ω et les $\partial_j f_i$ sont $\mathscr{C}^0$ sur Ω
4. On note $\mathscr{C}^1(\Omega, F)$ l'ensemble de ces fonctions

Démonstration.

2. Les fonctions $\mathscr{C}^1$ sont différentiables donc continues.
3. $(a) \implies (b)$:

$$J_f(a) = \mathscr{M}_{\mathscr{B},\mathscr{C}}(\mathrm{d}f_a) = \left(\frac{\partial f_i}{\partial x_j}(a)\right)_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}$$

est continue par rapport à a par hypothèse.

$(b) \implies (a)$: Il suffit de montrer que f est différentiable sur Ω. On commence par le cas $F = \mathbf{R}$.

$$\begin{aligned} f(a+h) - f(a) = \quad & f(a_1+h_1, \cdots, a_n+h_n) - f(a_1, a_2+h_2, \cdots, a_n+h_n) \\ & + f(a_1, a_2+h_2, \cdots, a_n+h_n) - f(a_1, \cdots, a_i, a_{i+1}+h_{i+1}, \cdots, a_n+h_n) \\ & + f(a_1, \cdots, a_i, a_{i+1}+h_{i+1}, \cdots, a_n+h_n) + \cdots \\ & + f(a_1, \cdots, a_{n-1}, a_n+h_n) - f(a_1, \cdots, a_n) \end{aligned}$$

et chaque ligne est fonction d'une seule variable, donc le théorème des accroissements finis donne

$$\begin{aligned} \exists c_{i,h} \in]a_i, a_i+h_i[, \quad f(a+h) - f(a) = \quad & h_1 \frac{\partial f}{\partial x_1}(c_{1,h}, a_2+h_2, \cdots, a_n+h_n) \\ & + h_2 \frac{\partial f}{\partial x_2}(a_1, c_{2,h}, a_3+h_3, \cdots, a_n+h_n) \\ & + \qquad \vdots \\ & + \underbrace{h_n \frac{\partial f}{\partial x_n}(a_1, \cdots, a_{n-1}, c_{n,h})}_{\longrightarrow h_n \frac{\partial f}{\partial x_n}(a) \text{ donc } = h_n \frac{\partial f}{\partial x_n}(a) + o(1)} \\ = \quad & \underbrace{h_1 \frac{\partial f}{\partial x_1}(a) + \cdots + h_n \frac{\partial f}{\partial x_n}(a)}_{\text{AL}} + \underbrace{h_1 o(1) + \cdots h_n o(1)}_{o(h)} \end{aligned}$$

donc f est différentiable sur Ω. Si $F \neq \mathbf{R}$ on raisonne coordonnée par coordonnée.

□

Proposition.

1. $\mathscr{C}^1(\Omega, F)$ est un $\mathbf{R}$-e.v.
2. Si $\mathscr{C}$ base de F est $f : \Omega \longrightarrow F$ donnée par $f = (f_1, \cdots, f_n)$ (dans $\mathscr{C}$) alors il y a équivalence entre
   (a) f est $\mathscr{C}^1$
   (b) Les f_i sont toutes $\mathscr{C}^1$
3. Si $f : \Omega \longrightarrow F$ et $g : \Omega' \supset f(\Omega) \longrightarrow G$ sont $\mathscr{C}^1$ alors $g \circ f$ aussi

Démonstration. 1. et 2. sont faciles, 3. est déjà vu. □

Théorème.

H $f : \Omega \subset E \longrightarrow \mathbf{R}$, $a, b \in \Omega$ tels que $[a, b] \subset \Omega$

C 1.
$$f(b) - f(a) = \int_0^1 \mathrm{d}f_{(1-t)a+tb}(b-a)\,\mathrm{d}t$$

2. Si $|||\,\mathrm{d}f_x|||\leqslant M$ pour $x \in [a, b]$ alors $|f(b) - f(a)| \leqslant M\|b - a\|$

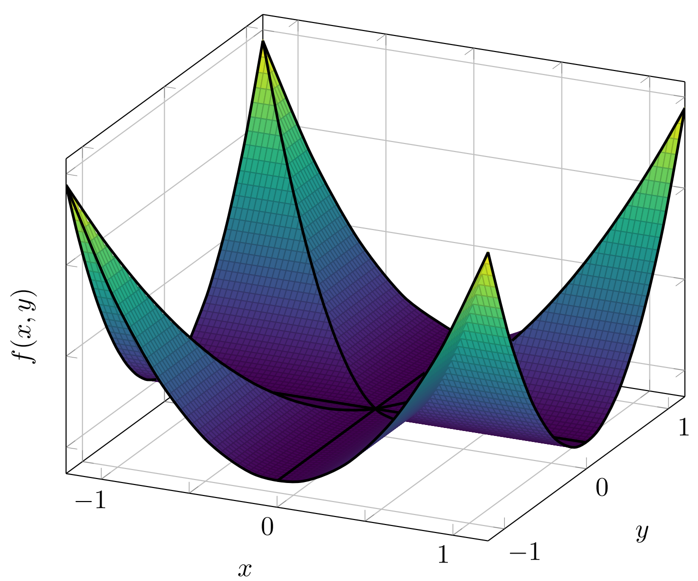
Démonstration. 1. $\varphi : t \longmapsto f(a + t(b - a))$ est telle que $\varphi'(t) = \mathrm{d}f_{(1-t)a+tb}(b - a)$ et
$$f(b) - f(a) = \varphi(1) - \varphi(0) = \int_0^1 \varphi'$$

2.
$$|f(b) - f(a)| \leqslant \int_0^1 \|\,\mathrm{d}f_{(1-t)a+tb}(b-a)\|\,\mathrm{d}t \leqslant M \int_0^1 \|b - a\|\,\mathrm{d}t$$

□

7 Étude de régularité

a) $f : (x, y) \longmapsto \min(x^2, y^2)$



D'abord,

$$f(x,y) = \frac{x^2+y^2-|x^2-y^2|}{2}$$

donc f est $\mathscr{C}^0$. On note Δ le fermé $\{(x,y)\in\mathbf{R}^2, x^2=y^2\}$, $\mathbf{R}^2\setminus\Delta$ est ouvert et $f\in\mathscr{C}^1(\mathbf{R}^2\setminus\Delta,\mathbf{R})$ comme composée de fonctions $\mathscr{C}^1$.

Il reste à savoir si f est différentiable sur Δ et si éventuellement la différentielle est continue.

$$\begin{aligned}f(x+h,x+k)-f(x,x) &= \frac{(x+h)^2+(x+k)^2-|(x+h)^2-(x+k)^2|}{2}-x^2\\ &= x(h+k)+\frac{h^2+k^2}{2}-\left|x(h+k)+\frac{h^2-k^2}{2}\right|\end{aligned}$$

Pour $k=0$,

$$\frac{f(x+h,x)-f(x,x)}{h} = x+\frac{h}{2}-\frac{\left|xh+\frac{h^2}{2}\right|}{h}\xrightarrow[h\to0\pm]{} x\pm|x|$$

Donc f n'a pas de dérivée partielle par rapport à x en (x,x) pour $x\in\Delta\setminus\{0\}\underset{\text{def}}{=}\Delta^\star$ (idem en $(x,-x)$) donc n'est pas différentiable sur les points de Δ.

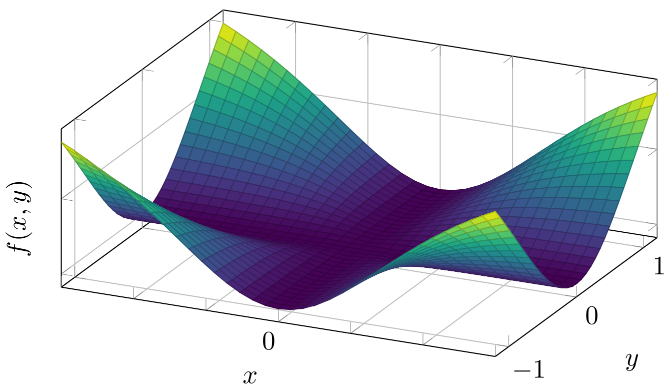
En $(0,0)$, f est différentiable car $0\leqslant f(x,y)\leqslant x^2+y^2=o(\|(x,y)\|_2)$ donc $f(x,y)=f(0,0)+0+o((x,y))$ et $\mathrm{d}f_{(0,0)}=0$

Ainsi $(x,y)\longmapsto \mathrm{d}f_{(x,y)}$ est définie sur $\mathbf{R}^2\setminus\Delta^\star$. Elle est continue sur $\mathbf{R}^2\setminus\Delta$, puis on va montrer qu'elle est continue en $(0,0)$. On note $(x_0,y_0)\in\mathbf{R}^2\setminus\Delta$ tels que $x_0^2>y_0^2$ donc au voisinage de (x_0,y_0), $f(x,y)=y^2$ et $\mathrm{d}f_{(x_0,y_0)}=2y_0\,\mathrm{d}y$ puis sinon $\mathrm{d}f_{(x_0,y_0)}=2x_0\,\mathrm{d}x$. Dans tous les cas, $\mathrm{d}f_{(x,y)}\xrightarrow[(x,y)\to0]{}0=\mathrm{d}f_{(0,0)}$ donc la différentielle est continue sur son domaine de définition.

b) Domaine de continuité

On pose

$$f:(x,y)\longmapsto\begin{cases}\dfrac{x^2y^2}{x^2+y^2} & \text{si } (x,y)\neq(0,0)\\ 0 & \text{sinon}\end{cases}$$

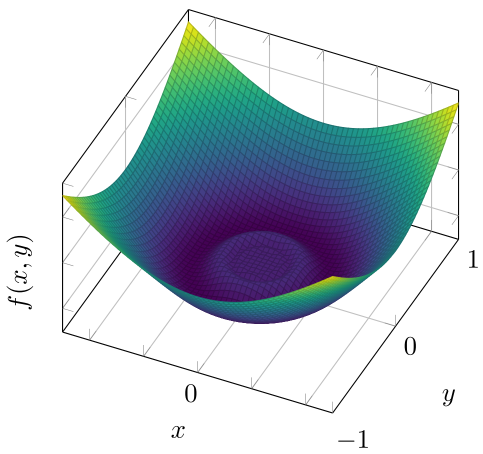


f est clairement continue sur $\mathbf{R}^2\setminus\{(0,0)\}$ puis $x^2y^2\leqslant(x^2+y^2)^2$ donc $0\leqslant f(x)\leqslant x^2+y^2=o((x,y))$ donc f continue en 0

c) Une fonction différentiable non $\mathscr{C}^1$

On pose

$$f:(x,y)\longmapsto\begin{cases}(x^2+y^2)\sin\left(\dfrac{1}{\sqrt{x^2+y^2}}\right) & \text{si } (x,y)\neq(0,0)\\ 0 & \text{sinon}\end{cases}$$



La fonction est clairement $\mathscr{C}^1$ sur $\mathbf{R}^2 \setminus \{0\}$ puis $f(x,y) = o_0((x,y))$ donc $\mathrm{d}f_0 = 0$ et f est différentiable. Il reste à voir si la différentielle est continue en $(0,0)$.

Puis,

$$\frac{\partial f}{\partial x}(x,y) = \begin{cases} 2x \sin\left(\dfrac{1}{\sqrt{x^2+y^2}}\right) - \dfrac{x}{\sqrt{x^2+y^2}} \cos\left(\dfrac{1}{\sqrt{x^2+y^2}}\right) & \text{si } (x,y) \neq (0,0) \\ 0 & \text{sinon} \end{cases}$$

et

$$\frac{\partial f}{\partial x}(x,0) \underset{x \to 0}{\not\longrightarrow} 0$$

donc f n'est pas $\mathscr{C}^1$

d) Expression intégrale

On considère $g : \mathbf{R}^2 \to \mathbf{R}$ de classe $\mathscr{C}^1$ et

$$F : x \longmapsto \int_0^x g(x,t)\,\mathrm{d}t$$

On va montrer que F est $\mathscr{C}^1$ et on va calculer F'. On a

$$F(x) \underset{t=ux}{=} \int_0^1 g(x,ux)\,\mathrm{d}u$$

On note donc $h : (x,u) \longmapsto g(x,ux)$ et F est $\mathscr{C}^1$ par théorème de dérivation sous le signe somme puis

$$\begin{aligned} F'(x) &= \int_0^1 g(x,ux)\,\mathrm{d}u + x\int_0^1 \frac{\partial g}{\partial x}(x,ux)\,\mathrm{d}u + x\int_0^1 \frac{\partial g}{\partial t}(x,ux)\,\mathrm{d}u \\ &= \int_0^1 \frac{\partial}{\partial t}(ug(x,ux)) + x\int_0^1 \frac{\partial g}{\partial x}(x,ux)\,\mathrm{d}u \\ &= g(x,x) + \int_0^x \frac{\partial g}{\partial x}(x,t)\,\mathrm{d}t \end{aligned}$$

8 Caractérisation des fonctions constantes

On se place dans E et on note Ω un ouvert connexe par arcs de E, et $f : \Omega \to F$. On note $\mathscr{B} = (e_1, \cdots, e_n)$ une base de E. On va montrer que f est constante sur Ω si et seulement si f est $\mathscr{C}^0$ et a toutes ses dérivées partielles nulles.

- ($\Longrightarrow$) Direct

- ($\Longleftarrow$) Par hypothèse, $\partial_i f = 0$ est continue donc f est $\mathscr{C}^1$ donc pour $[a,b] \subset \Omega$,

$$f(b) - f(a) = \int_0^1 \mathrm{d}f_{(1-t)a+tb}(b-a)\,\mathrm{d}t = 0 \implies f(b) = f(a)$$

  Vu ce qui précède, f est constante sur toutes les boules invertes incluses dans Ω. On prend $a \in \Omega$ et on note
$$\mathscr{E} = \{x \in \Omega, f(x) = f(a)\}.$$
  Cet ensemble est un fermé en tant que préimage par une application continue (f) par le fermé $\{f(a)\}$. C'est aussi un ouvert car pour $x_0 \in \mathscr{E}$, f est constante sur une boule ouverte centrée en x_0 donc par définition de $\mathscr{E}$, cette boule est dans $\mathscr{E}$.
  On note $h = \mathbb{1}_{\mathscr{E}}$ de sorte que $h^{-1}(\{0\}) = \Omega \setminus \mathscr{E}$, $h^{-1}(\{1\}) = \mathscr{E}$, $h^{-1}(\varnothing) = \varnothing$, $h^{-1}(\{0,1\}) = \Omega$. Ainsi, h est continue car la préimage d'un fermé est un fermé (induit). Ainsi, $h(\Omega)$ est connexe par arcs donc $h(\Omega) = \{1\}$ car $\mathscr{E}$ non vide et $\Omega = \mathscr{E}$

Autre méthode : Il suffit de montrer que Ω est connexe par arcs polygonaux. On fixe $a \in \Omega$ et on note $\mathscr{E} = \{x \in \Omega,$ il existe un arc polygonal entre a et $x\}$. C'est un ouvert (même justification que dans la méthode d'avant). Si (α_n) est une suite de $\mathscr{E}$ convergente vers $\alpha \in \Omega$, alors APCR α_n est dans une boule incluse dans Ω centrée en α, puis il suffit de relier α_n et α dans Ω pour conclure que $\alpha \in \mathscr{E}$. Ainsi c'est un ouvert fermé de Ω donc c'est Ω (déjà fait)

9 Extrema – Gradient

Dans cette partie, $f : \Omega \to \mathbf{R}$. On suppose $(E, (\ |\ ))$ euclidien.

Théorème – Définition.

(H) $f : \Omega \to \mathbf{R}$ différentiable en $a \in \Omega$

(C)
1. $\mathrm{d}f_a$ est une forme linéaire
2. Il existe un unique $w \in E$ tel que
$$\forall x \in E, \qquad \mathrm{d}f_a(x) = (w|x)$$
   Ce vecteur est appelé gradient de f en a et se note $\nabla f(a), \overrightarrow{\mathrm{grad}} f(a), \dots$
3. Si $\mathscr{B} = (e_1, \cdots, e_n)$ est une base ON de E alors
$$\nabla f(a) = \sum_{i=1}^n \partial_i f(a) e_i$$

Démonstration.

1. C'est dans la définition.
2. C'est une application du théorème de représentation de Riesz. On note
$$\varphi : x \in E \longmapsto (y \in E \longmapsto (x|y))$$
   De sorte que
$$\varphi(a) = \varphi(b) \iff \forall y \in E,\ (a-b|y) = 0 \iff a - b \in E^\perp = \{0\} \iff a = b$$
   donc φ est linéaire injective en dimension finie, et $\dim E^\star = \dim E$ donc cette application est bijective : $w = \varphi^{-1}(\mathrm{d}f_a)$ convient.
3. $$\mathrm{d}f_a(x) = \sum_{i=1}^n \partial_i f(a) \underbrace{\mathrm{d}x_i(x)}_{(e_i|x)}$$

$\square$

Remarque (Interprétation géométrique).

On note $u \in E$ unitaire.

$$f(a+tu) = f(a) + \mathrm{d}f_a(tu) + o_0(t) = f(a) + t(\nabla f(a)|u) + o_0(t).$$

Pour a fixé tel que $\nabla f(a) \neq 0$, $(\nabla f(a)|u)$ est maximal pour $u = \dfrac{\nabla f(a)}{\|\nabla f(a)\|}$ et dans ce cas $(\nabla f(a)|u) = \|\nabla f(a)\|$

Remarque (Égalité des accroissements finis).

On note $f : \Omega \to E$ différentiable, et $[a,b] \subset \Omega$. On note

$$g : t \in [0,1] \longmapsto f((1-t)a + tb) \in \mathbf{R}$$

- g est continue sur $[0,1]$, dérivable sur $]0,1[$ (car dérivable sur $[0,1]$)
- On applique l'égalité des accroissements finis à g :

$$\exists t_0 \in]0,1[, \quad g(1) - g(0) = g'(t_0)$$

soit encore

$$f(b) - f(a) = \mathrm{d}f_{(1-t_0)a+t_0b}(b-a) = (\nabla f(\underbrace{(1-t_0)a + t_0b}_{\underset{\text{def}}{=} c}) \mid b-a)$$

Ainsi, il existe $c \in]a,b[$ tel que $f(b) - f(a) = \mathrm{d}f_c(b-a)$

Théorème – Définition.

H $f : \Omega \subset E \to \mathbf{R}, a \in \Omega$, f différentiable en a.

C
1. On dira que f a un point critique en a si $\mathrm{d}f_a = 0$ (i.e. si $\nabla f(a) = 0$ avec un produit scalaire)
2. Si a est un extremum local de f alors a est un point critique de f.

Démonstration. 2. On note $u \in E$, $\varphi : t \longmapsto f(a+tu)$ est définie sur un intervalle du type $]-\varepsilon, \varepsilon[$, et φ atteint un extremum local en 0. Ainsi, $\varphi'(0) = 0 = \mathrm{d}f_a(u)$ vrai pour tout u donc $\mathrm{d}f_a = 0$

□

Exemple. On pose

$$f : (x,y) \longmapsto (x^2+y^2)\exp(x^2-y^2)$$

Cette fonction est $\mathscr{C}^1$ et si (x,y) est un extremum alors

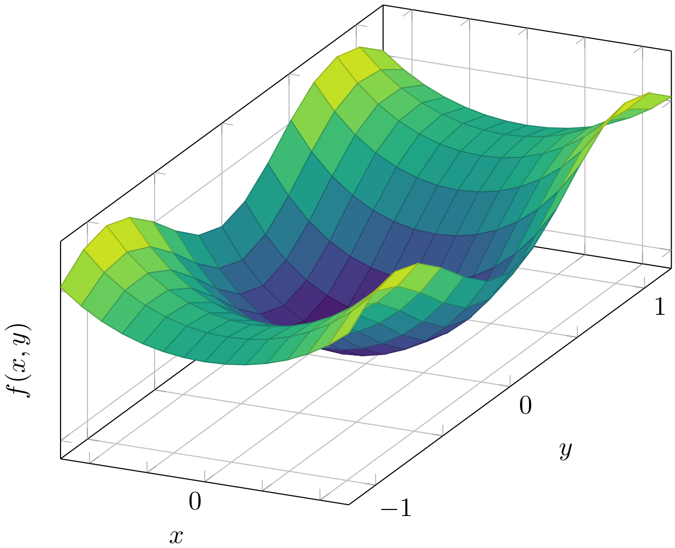
$$\begin{cases} \dfrac{\partial f}{\partial x}(x,y) = \exp(x^2-y^2)2x(1+(x^2+y^2)) = 0 \\ \dfrac{\partial f}{\partial y}(x,y) = \exp(x^2-y^2)2y(1-(x^2+y^2)) = 0 \end{cases} \iff \begin{cases} x = 0 \\ y(1-y^2) = 0 \end{cases} \iff \begin{cases} x = 0 \\ y \in [\![-1,1]\!] \end{cases}$$

Il reste à vérifier si les trois points sont bien des extrema.

- $(0,0)$ est un minimum global
- On fait l'étude en $(0,1)$.

$$\underbrace{f(h,1+k) - f(0,1)}_{\Delta(h,k)} = 2e^{-1}(h^2-k^2) + o_0(\|(h,k)\|)$$

  et $\Delta(h,0) > 0$ pour $h > 0$ assez petit, $\Delta(0,k) < 0$ pour $k > 0$ assez petit donc Δ change de signe au voisinage de $(0,1)$ donc $(0,1)$ n'est pas un extremum (c'est un point selle).
- De même, $(0,-1)$ n'est pas un extremum.



Exercice.

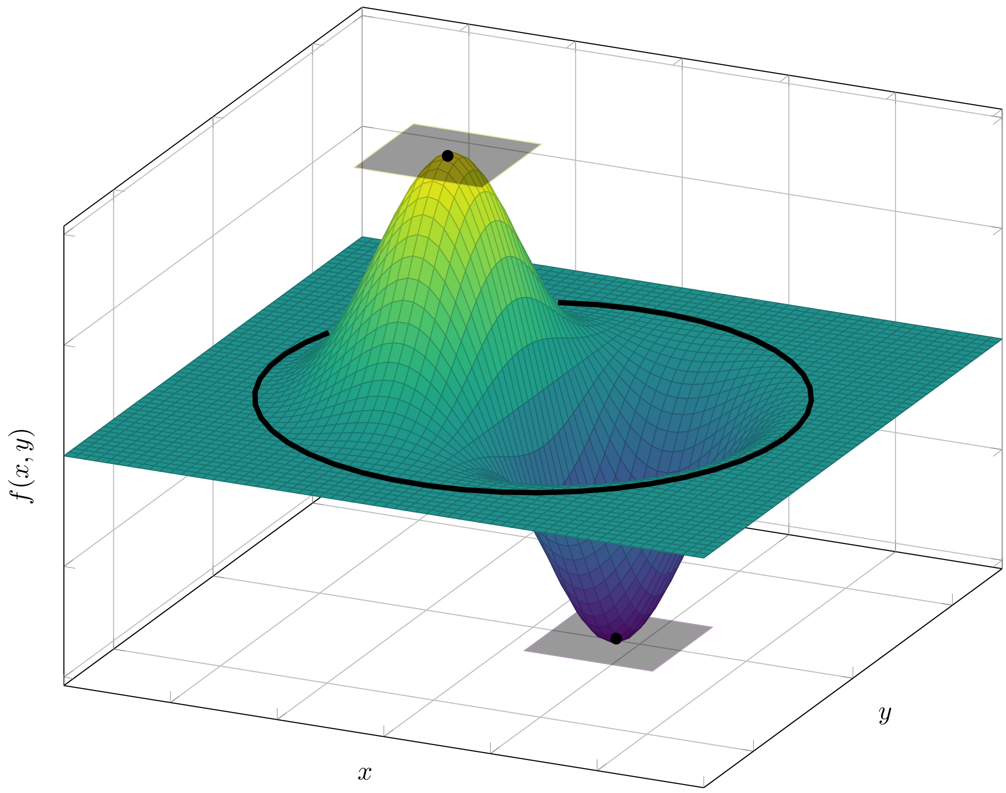
On note $S = \{x \in \mathbf{R}^n, \quad \|x\| = 1\}$ la sphère unité. On suppose $f : \mathbf{R}^n \to \mathbf{R}$ différentiable sur son domaine de définition et constante sur S. Montrer qu'il existe $x_0 \in \mathbf{R}^n$ tel que

$$\|x\| < 1 \qquad \text{et} \qquad \mathrm{d}f_{x_0} = 0$$

Résolution. $\mathscr{B}_f(0, 1)$ est un compact donc f est bornée et atteint ses bornes (son minimum en α et son maximum en β par exemple) sur cette boule.

- Si $f(\alpha) = f(\beta)$ alors f est constante et $x_0 = 0$ convient
- Si $f(\alpha) < f(\beta)$ alors α ou β n'est pas dans S et ce point convient.

□



Remarque.

C'est une généralisation possible du théorème de Rolle. Plus généralement, si K est un compact d'intérieur non vide de $\mathbf{R}^n$ tel que $f : \mathbf{R}^n \to \mathbf{R}$ différentiable est constante sur $\partial K = \overline{K} \setminus \mathring{K}$, alors il existe $x \in \mathring{K}$ tel que $\mathrm{d}f_x = 0$

10 Application à la géométrie

Définition.

On note $X \subseteq E$ non vide, $x \in X$ et $v \in E$. On dira que v est un vecteur tangent à X en x s'il existe un $\varepsilon > 0$ et $\gamma \in \mathscr{D}^1(]-\varepsilon, \varepsilon[, X)$ tel que $\gamma(0) = x$, $\gamma'(0) = v$

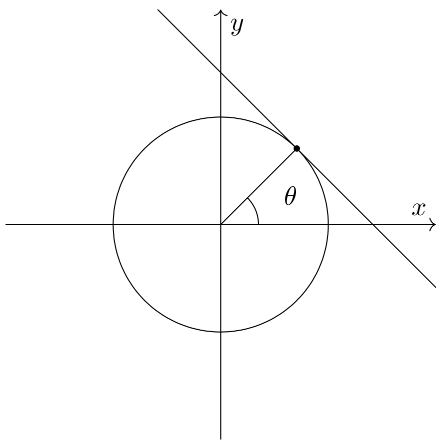
Exemple.

1. On note $\mathscr{C}$ le cercle unité (dans le plan) et $(x_0, y_0) \in \mathscr{C}$.
   - Si (α, β) tangent à $\mathscr{C}$ en (x_0, y_0) alors il existe γ dérivable telle que $\gamma(0) = (x_0, y_0)$ et en dérivant la relation $(\gamma(t) \mid \gamma(t)) = 1$ on a $2(\gamma(t) \mid \gamma'(t)) = 0$ donc $((x_0, y_0) \mid (\alpha, \beta)) = 0$
   - Si $(x_0, y_0) \perp (\alpha, \beta)$, on note $(x_0, y_0) = (\cos\theta, \sin\theta)$ et on pose

$$\begin{array}{rccc} \gamma : & [-1, 1] & \longrightarrow & \mathscr{C} \\ & t & \longmapsto & (\cos(\theta + tu), \sin(\theta + tv)) \end{array}$$

   et γ est dérivable, $\gamma(0) = (x_0, y_0)$, et $\gamma'(0) = (-uy_0, vx_0)$ colinéaire à (α, β) d'où l'équivalence.

   La droite $(x_0, y_0)^\perp$ est l'ensemble des vecteurs tangents en (x_0, y_0). L'espace tangent associé est la droite affine $\mathscr{D} = (x_0, y_0) + (x_0, y_0)^\perp$



2. $E = \mathbf{R}^3$, $f : \mathbf{R}^2 \to \mathbf{R}$ différentiable, $X = \{(x, y, f(x, y)), \quad x, y \in \mathbf{R}\}$. Le vecteur (α, β, λ) est tangent à X en $(x_0, y_0, f(x_0, y_0))$ si et seulement si

$$\lambda = \frac{\partial f}{\partial x}(x_0, y_0)\alpha + \frac{\partial f}{\partial y}(x_0, y_0)\beta \tag{$\star$}$$

En effet, si (α, β, ν) tangent alors on note γ l'arc associé et $z(t) - f(x(t), y(t)) = 0$ donc en dérivant

$$z'(t) - \frac{\partial f}{\partial x}(x(t), y(t))x'(t) - \frac{\partial f}{\partial y}(x(t), y(t))y'(t)$$

donc on a bien $(\star)$. Puis, si (α, β, λ) satisfait $(\star)$ alors

$$\gamma : t \in]-1, 1[\longmapsto (x_0 + t\alpha, y_0 + t\beta, f(x_0 + t\alpha, y_0 + t\beta))$$

convient.

3. *Cas des lignes de niveau.* On note $f : \Omega \to \mathbf{R}$, $X_a = f^{-1}(a)$. On suppose X_a non-vide et $\gamma :]-\varepsilon, \varepsilon[\to X_a$ dérivable avec $\gamma(0) = t_0$, $\gamma'(0) = v$. En dérivant la relation $f \circ gamma = a$ on a

$$\forall x \in]-\varepsilon; \varepsilon[, \quad \mathrm{d}f_{\gamma(x)} \circ \gamma'(x) = 0$$

donc pour $x = 0$, $\mathrm{d}f_{t_0}(v) = 0 = (\nabla f(t_0) \mid v)$

11 Calcul de vecteurs tangents

a) Vecteurs tangents à $O_n(\mathbf{R})$ en I_n

On veut déterminer les vecteurs tangents à $X = O_n(\mathbf{R})$ en I_n. On se donne

$$\gamma :]-\varepsilon; \varepsilon[\longrightarrow O_n(\mathbf{R})$$

dérivable telle que $\gamma(0) = I_n$.

- $\forall x \in]-\varepsilon; \varepsilon[, \qquad \gamma(t) \in O_n(\mathbf{R})$, i.e. $\gamma(t)^\top \gamma(t) = I_n$. En dérivant :

$$\gamma'(t)^\top \gamma(t) + \gamma(t)^\top \gamma'(t) = 0 \implies \gamma'(0)^\top + \gamma'(0) = 0 \implies \gamma'(0) \in \mathscr{AS}_n(\mathbf{R})$$

- On note $A \in \mathscr{M}_n(\mathbf{R})$ antisymétrique et $\gamma : t \in]-1, 1[\longmapsto e^{tA}$ de sorte que $\gamma(t) \in O_n(\mathbf{R})$ (facile à vérifier en écrivant l'exponentielle comme somme d'une série), $\gamma(0) = I_n$ et $\gamma'(0) = A$ donc A est tangent à X en I_n.

b) Vecteurs tangents à $\mathrm{GL}_n(\mathbf{R})$ en I_n

$\mathrm{GL}_n(\mathbf{R})$ est un ouvert donc tous les vecteurs sont tangents à I_n.

c) Vecteurs tangents à $\mathrm{SL}_n(\mathbf{R})$ en I_n

On note γ un chemin qui satisfait les bonnes hypothèses, $\gamma(0) = I_n$, $\det \circ \gamma = 1$ donc

$$\mathrm{d}(\det)_{\gamma(t)} \circ \gamma'(t) = \mathrm{Tr}(\mathrm{Com}(\gamma(t))^\top \gamma'(t)) = 0 \implies \mathrm{Tr}(\gamma'(0)) = 0$$

On note maintenant A une matrice de trace nulle et

$$\gamma : t \longmapsto \frac{I_n + tA}{\sqrt[n]{\det(I_n + tA)}}$$

est définie au voisinage de 0 et convient car

$$\gamma'(t) = \frac{A}{\sqrt[n]{\det(I_n + tA)}} + (I_n + tA)\left(-\frac{1}{n}\,\mathrm{Tr}(\mathrm{Com}(I_n + tA)^\top A)\det(I_n + tA)^{-\frac{n+1}{n}}\right)$$

donc $\gamma'(0) = A$.

d) Vecteurs tagents à la surface d'équation $\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1$

On cherche les vecteurs tangents à $X = \{(x, y, z),\ \frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1\}$ en $M_0 = (x_0, y_0, z_0) \in X$.

On note $\gamma :]-\varepsilon, \varepsilon[\longrightarrow X$ différentiable telle que $\gamma(0) = M_0$ On a

$$\forall |t| < \varepsilon, \qquad \frac{x(t)^2}{a^2} + \frac{y(t)^2}{b^2} + \frac{z(t)^2}{c^2} = 1$$

donc en dérivant,

$$\frac{2xx'}{a^2} + \frac{2yy'}{b^2} + \frac{2zz'}{c^2} = 0$$

donc $\gamma'(0) \perp \left(\frac{x_0}{a^2}, \frac{y_0}{b^2}, \frac{z_0}{c^2}\right)$. La réciproque est vraie : si on note (α, β, λ) perpendiculaire à $x \underset{\text{def}}{=} \left(\frac{x_0}{a^2}, \frac{y_0}{b^2}, \frac{z_0}{c^2}\right) \in X$, alors $x \neq 0$ donc par exemple $z_0 > 0$ et

$$\gamma : t \longmapsto \left(x_0 + t\alpha, y_0 + t\beta, c^2\sqrt{1 - \frac{(x_0 + t\alpha)^2}{a^2} - \frac{(y_0 + t\beta)^2}{b^2}}\right)$$

convient.

12 Espace tangent

Définition – Proposition.

(H) $X \subset E, a \in X$

(C)
1. On note $V_a(X)$ l'ensemble des vecteurs tangents à X en a.
2. L'espace tangent à X en a est $T_a(X) = a + V_a(X)$
3. Si $f : \Omega \subset E \to \mathbf{R}$ et si $a \in \Omega$ n'est pas un point critique alors $X = f^{-1}(\{f(a)\})$ vérifie
   (a) $V_a(X) = \nabla f(a)^\perp$
   (b) $T_a(X) = a + \nabla f(a)^\perp$

   En particulier, si $E = \mathbf{R}^3$ et $X = f^{-1}(\{\lambda\})$ et $a = (x_0, y_0, z_0) \in X$ point non critique de f alors $T_a(X)$ est donné par l'équation cartésienne

$$\frac{\partial f}{\partial x}(a)(x - x_0) + \frac{\partial f}{\partial y}(a)(y - y_0) + \frac{\partial f}{\partial z}(a)(z - z_0) = 0$$

Démonstration. Admise □

13 Dérivée partielle d'ordre supérieur

Définition.

On note $f : \Omega \subset E \to F$, $n \geqslant 2$, $\mathscr{B} = (e_1, \cdots, e_p)$ base de E. On définit récursivement $\mathscr{C}^n(\Omega, F)$ par

$$f \in \mathscr{C}^n(\Omega, F) \iff f \text{ différentiable sur } \Omega \text{ et } \forall i \in [\![1, p]\!],\ \partial_i f \in \mathscr{C}^{n-1}(\Omega, F)$$

Notation.

$$\frac{\partial}{\partial x_k}\left(\frac{\partial f}{\partial x_i}\right)(a) = \frac{\partial f}{\partial x_k \partial x_i} = \partial^2_{k,i} f(a)$$

et

$$\frac{\partial}{\partial x_{i_1}}\left(\frac{\partial}{\partial x_{i_2}}\left(\cdots\left(\frac{\partial f}{\partial x_{i_p}}\right)\right)\right)(a) = \partial^p_I f(a), \qquad I = (i_1, \cdots, i_p)$$

Théorème (Schwarz).

(H) $f \in \mathscr{C}^2(\Omega, F)$, $a \in \Omega$, $\mathscr{B} = (e_1, \cdots, e_p)$ base de $E \supseteq \Omega$.

(C) Pour $i, j \in [\![1, p]\!]$,

$$\frac{\partial^2 f}{\partial x_i \partial x_j}(a) = \frac{\partial^2 f}{\partial x_j \partial x_i}(a)$$

Démonstration. Admis □

14 Exemples

a) Identité d'Euler

On note $f : \mathbf{R}^n \setminus \{0\} \to \mathbf{R}$ différentiable. On dira que f est α-homogène si

$$\forall x, t \in \mathbf{R}^n \times \mathbf{R}, \quad x \neq 0 \implies f(tx) = t^\alpha f(x)$$

On va montrer que f est α-homogène si et seulement si

$$\sum_{i=1}^{n} x_i \partial_i f(x) = \alpha f(x)$$

- ($\implies$) On a $f(tx) = t^\alpha f(x)$ donc

$$\mathrm{d}d_{tx}(x) = \alpha t^{\alpha-1} f(x) \underset{t=1}{\implies} \mathrm{d}f_x(x) = \alpha f(x)$$

- ($\impliedby$) On note $h(t) = t^{-\alpha} f(tx)$ de sorte que

$$h'(t) = -\alpha t^{-\alpha-1} f(tx) + t^{-\alpha}\, \mathrm{d}f_{tx}(x) = t^{-\alpha-1}(-\alpha f(tx) + \mathrm{d}f_{tx}(tx)) = 0$$

  par hypothèse donc $h(t) = h(1) = f(x)$ ce qui conclut.

b) Calcul du laplacien en coordonnées polaires

On note $f : \mathbf{R}^2 \to \mathbf{R}$ de classe $\mathscr{C}^2$, et

$$f^\star : \begin{array}{ccc} \mathbf{R}_+ \times [0, 2\pi] & \longrightarrow & \mathbf{R} \\ (\rho, \theta) & \longmapsto & f(\rho\cos\theta, \rho\sin\theta) \end{array}$$

On appelle laplacien de f la fonction

$$\Delta f : (x, y) \longmapsto \frac{\partial^2 f}{\partial x^2}(x, y) + \frac{\partial^2 f}{\partial y^2}(x, y)$$

On veut calculer $(\Delta f)^\star$ en fonction de $f^\star$.

- $$\frac{\partial f^\star}{\partial \rho}(\rho,\theta) = \left(\frac{\partial f}{\partial x}\right)^\star(\rho,\theta)\cos\theta + \left(\frac{\partial f}{\partial y}\right)^\star(\rho,\theta)\sin\theta$$
- $$\frac{\partial f^\star}{\partial \theta}(\rho,\theta) = \left(\frac{\partial f}{\partial x}\right)^\star(\rho,\theta)(-\rho\sin\theta) + \left(\frac{\partial f}{\partial y}\right)^\star(\rho,\theta)\rho\cos\theta$$
- $$\begin{aligned}\frac{\partial^2 f^\star}{\partial \rho^2}(\rho,\theta) &= \left(\frac{\partial^2 f}{\partial x^2}\right)^\star(\rho,\theta)\cos^2\theta + \left(\frac{\partial^2 f}{\partial x\partial y}\right)^\star(\rho,\theta)\cos\theta\sin\theta\\ &+ \left(\frac{\partial^2 f}{\partial y\partial x}\right)^\star(\rho,\theta)\sin\theta\cos\theta + \left(\frac{\partial^2 f}{\partial y^2}\right)(\rho,\theta)\sin^2\theta\end{aligned}$$
- $$\begin{aligned}\frac{\partial^2 f^\star}{\partial \theta^2}(\rho,\theta) &= -\rho\left(\frac{\partial f}{\partial x}\right)^\star(\rho,\theta)\cos\theta - \rho\left(\frac{\partial f}{\partial y}\right)^\star(\rho,\theta)\sin\theta\\ &+ \left(\frac{\partial^2 f}{\partial x^2}\right)^\star(\rho,\theta)\rho^2\sin^2\theta + \left(\frac{\partial^2 f}{\partial y\partial x}\right)^\star(\rho,\theta)(-\rho^2\sin\theta\cos\theta)\\ &+ \left(\frac{\partial^2 f}{\partial x\partial y}\right)^\star(\rho,\theta)(-\rho^2\sin\theta\cos\theta) + \left(\frac{\partial^2 f}{\partial y^2}\right)^\star(\rho,\theta)\rho^2\cos^2\theta\end{aligned}$$

Donc pour $\rho \neq 0$,
$$\frac{1}{\rho^2}\frac{\partial^2 f^\star}{\partial \theta^2}(\rho,\theta) + \frac{\partial^2 f}{\partial \rho^2}(\rho,\theta) = (\Delta f)^\star(\rho,\theta) - \frac{1}{\rho}\frac{\partial f^\star}{\partial \rho}(\rho,\theta)$$
d'où
$$(\Delta f)^\star(\rho,\theta) = \frac{1}{\rho^2}\frac{\partial^2 f^\star}{\partial \theta^2}(\rho,\theta) + \frac{\partial^2 f^\star}{\partial \rho^2}(\rho,\theta) + \frac{1}{\rho}\frac{\partial f^\star}{\partial \rho}(\rho,\theta)$$

Exercice.

> Déterminer les $g \in \mathscr{C}^2(\mathbf{R}_+^\star, \mathbf{R})$ tel que $f : (x_1, \cdots, x_n) \in \mathbf{R}^n \setminus \{0\} \longmapsto g(x_1^2 + \cdots + x_n^2)$ est harmonique ($\Delta f = 0$)

Résolution. Soit g solution. Alors
$$\frac{\partial f}{\partial x_i}(x) = g'(x_1^2+\cdots+x_n^2)2x_i$$
et
$$\frac{\partial^2 f}{\partial x_i^2}(x) = g''(x_1^2+\cdots+x_n^2)4x_i^2 + 2g'(x_1^2+\cdots+x_n^2)$$
donc
$$\Delta f = 0 \iff \forall x \in \mathbf{R}^n\setminus\{0\},\quad \sum_{i=1}^n g''(\|x\|^2)4x_i^2 + 2g'(\|x\|^2) = 0 \iff 4\|x\|^2 g''(\|x\|^2) + 2g'(\|x\|^2)n = 0$$
donc
$$\Delta f = 0 \iff \forall r > 0,\quad 4rg''(r) + 2ng'(r) = 0 \iff \cdots \iff \exists A, B,\quad g : r \longmapsto B + \frac{A}{r^{n/2-1}}$$

□

15 Régression linéaire

On dispose de données expérimentales $(x_{i,1}, \cdots, x_{i,p}, y_i)$ avec $i \in [\![1, n]\!]$. On sait que les vraies valeurs $(\overline{x}_{i,1}, \cdots, \overline{x}_{i,p}, \overline{y}_i)$ vérifient une relation du type

$$\overline{y}_i = \beta_1 \overline{x}_{i,1} + \cdots + \beta_p \overline{x}_{i,p}$$

On veut connaitre les β_i à l'aide des mesures effectuées. On note :

$$X = (x_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}} \qquad \overline{X} = (\overline{x}_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}} \qquad \Gamma = \begin{pmatrix}\beta_1\\ \vdots\\ \beta_p\end{pmatrix} \qquad Y = \begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix} \qquad \overline{Y} = \begin{pmatrix}\overline{y}_1\\ \vdots\\ \overline{y}_n\end{pmatrix}$$

de sorte que $\overline{Y} = \overline{X}\Gamma$. On connait X et Y, on veut approcher Γ. On va trouver B qui minimise $\|Y - XB\|$ et on va montrer que si $\operatorname{rg} X = p$ alors il y a une unique solution minimale donnée par

$$B = (X^\top X)^{-1} X^\top Y$$

- On note $f : B \longmapsto \|Y - BX\|^2$ de sorte que

$$f(B+H) = \|Y\|^2 - 2(Y \mid XB) - 2(Y \mid XH) + \|XB\|^2 + 2(XB \mid XH) + \underbrace{\|XH\|^2}_{o_0(H)}$$

  donc

$$\mathrm{d}f_B(H) = 2(XB - Y \mid XH) = -2(X^\top Y \mid H) + 2(X^\top XB \mid H)$$

- B point critique $\iff \forall H, (-X^\top Y + X^\top XB \mid H) = 0 \iff X^\top XB = X^\top Y$
- Si $p = \operatorname{rg} X$ alors $\dim \operatorname{Ker} X = 0$ et X est une matrice injective.

$$B \in \operatorname{Ker}(X^\top X) \iff X^\top XB = 0 \implies B^\top X^\top XB = 0 \implies \|XB\|^2 = 0 \implies B = 0$$

  donc $X^\top X$ est inversible.
- B point critique $\iff B = (X^\top X)^{-1} X^\top Y$

16 Exemple d'équation aux dérivées partielles

On va déterminer les solution $f \in \mathscr{C}^1(\mathbf{R}_+^\star \times \mathbf{R}, \mathbf{R})$ telles que

$$x\frac{\partial f}{\partial y}(x,y) - y\frac{\partial f}{\partial x}(x,y) = kf(x,y)$$

Pour $r \in \mathbf{R}^\star$, $\theta \in \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$, $f^\star(r,\theta) = f(r\cos\theta, r\sin\theta)$. Donc :

$$\frac{\partial f^\star}{\partial \theta}(r,\theta) = -r\sin\theta\left(\frac{\partial f}{\partial x}\right)^\star(r,\theta) + r\cos\theta\left(\frac{\partial f}{\partial y}\right)^\star(r,\theta) = kf^\star(r,\theta)$$

d'où

$$f \text{ solution} \iff \forall r > 0, \exists a(r) \;/\; \forall \theta \in \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[, \quad f^\star(r\theta) = a(r)\exp(k\theta)$$

donc les solutions sont de la forme $f(x,y) = a\left(\sqrt{x^2+y^2}\right)\exp\left(k\arctan\left(\frac{y}{x}\right)\right)$, qui convient si elle est $\mathscr{C}^1$ (i.e. si a est $\mathscr{C}^1$)

17 Méthodes de gradient

On note $J : \mathbf{R}^n \to \mathbf{R}$ minorée $\mathscr{C}^1$ et on suppose qu'elle atteint sa borne inférieure en un point $x^\star$.

Idée : On va construire une suite (x_n) telle que $J(x_n) \to J(x^\star)$. On a

$$J(x_n + tv) = J(x_n) + t(\nabla J(x_n) \mid v) + o_0(tv)$$

et on va prendre $v = -\nabla J(x_n)$ de sorte que $x_{n+1} = x_n - t_n\nabla J(x_n)$, $t_n > 0$ à choisir

a) Méthode de gradient conjugué

On note $A \in S_p^{++}(\mathbf{R})$, $b \in \mathbf{R}^p$ et

$$J : \begin{array}{ccc} \mathbf{R}^p & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \dfrac{1}{2}(Ax \mid x) - (b \mid x) \end{array}$$

La fonction J est $\mathscr{C}^1$ et

$$J(x) \geqslant \frac{1}{2} \underbrace{\lambda_1}_{\min \mathrm{Sp}(A) > 0} \|x\|^2 - \|b\| \cdot \|x\| \implies J(x) \xrightarrow[\|x\| \to +\infty]{} +\infty$$

par conséquent, J atteint son minimum (i.e. $x^\star$ existe) car atteint sur un compact du type $\mathscr{B}_f(0, R)$.

On a

$$\mathrm{d}J_x(h) = (Ax - b \mid h)$$

et $\mathrm{d}J_{x^\star} = 0$ donc $x^\star = A^{-1}b$

On va mettre en place une méthode de descente de gradient.

$$J(x + t\nabla J(x)) = J(x) + t(Ax - b \mid \nabla J(x)) + \frac{1}{2}t^2(A\nabla J(x) \mid \nabla J(x))$$

Cette fonction de t atteint un minimum lorsque

$$(Ax - b \mid \nabla J(x)) + t(A\nabla J(x) \mid \nabla J(x)) = 0 \iff t = -\frac{(Ax - b \mid \nabla J(x))}{(A\nabla J(x) \mid \nabla J(x))}$$

Or $\mathrm{d}J_x(h) = (Ax - b \mid h) = (\nabla J(x) \mid h)$ donc $\nabla J(x) = Ax - b$. On construit alors (x_n) comme suit :

- x_0 est quelconque
- $x_{n+1} = x_n + t_n \nabla J(x)$ avec

$$t_n = \begin{cases} -\dfrac{\|Ax_n - b\|^2}{(A(Ax_n - b) \mid Ax_n - b)} & \text{si } Ax_n - b \neq 0 \\ 0 & \text{sinon} \end{cases}$$

On a

$$J(x_{n+1}) = J(x_n) + t_n \|Ax_n - b\|^2 + \frac{1}{2}t_n^2(A(Ax_n - b) \mid Ax_n - b)$$

soit encore

$$J(x_{n+1}) = J(x_n) - \frac{\|Ax_n - b\|^4}{2(A(Ax_n - b) \mid Ax_n - b)} \leqslant J(x_n)$$

si $x_n \neq x_{n+1}$. On a égalité si $x_n = x_{n+1}$. Si (x_n) ne prend pas la valeur $x^\star$ alors $(J(x_n))$ est décroissante minorée donc converge. On a alors $Ax_n - b \longrightarrow 0$ donc $x_n \longrightarrow x^\star$.

b) Méthode de gradient à pas optimal

Soit $f : \mathbf{R}^n \to \mathbf{R}$ de classe $\mathscr{C}^1$ telle que

$$\exists \alpha > 0, \forall u, v \in \mathbf{R}^n, (\nabla f(u) - \nabla f(v) \mid u - v) \geqslant \alpha \|u - v\|^2$$

1. On va établir que

$$\forall u, v \in \mathbf{R}^n, f(u) \geqslant f(v) + (\nabla f(u) \mid v - u) + \frac{\alpha}{2}\|v - u\|^2$$

et en déduire que f a un minimum global.

$$\begin{aligned}
f(v) - f(u) &= \int_0^1 \mathrm{d}f_{(1-t)v+tu}(v-u)\,\mathrm{d}t \\
&= \int_0^1 (\nabla f((1-t)v+tu) \mid v-u)\,\mathrm{d}t \\
&\geqslant \int_0^1 (\nabla f(u) \mid v-u) + \alpha(1-t)\|v-u\|^2\,\mathrm{d}t \\
&= (\nabla f(u) \mid v-u) + \frac{\alpha\|v-u\|^2}{2}
\end{aligned}$$

puis

$$f(v) \geqslant f(u) - \|\nabla f(u)\| \cdot \|v-u\| + \frac{\alpha}{2}\|v-u\|^2 \xrightarrow[\|v\|\to+\infty]{} +\infty$$

Donc f possède un minimum global (car pour une boule fermée centrée en 0 assez grande, la borne inférieure globale est la borne inférieure sur cette boule compacte donc c'est un minimum par continuité de f).

2. On va montrer l'unicité du minimum.
Si $x^\star$ et $v^\star$ sont tels que $f(x^\star) = f(v^\star) = \min f$ alors

$$\nabla f(v^\star) = \nabla f(v^\star) = 0 \implies 0 \geqslant \alpha\|x^\star - v^\star\|^2 \implies x^\star = v^\star$$

3. On souhaite approcher $x^\star$.
   (a) Soit $u \in \mathbf{R}^n \setminus \{x^\star\}$. On va montrer que $\varphi_u : t \longmapsto f(y + t\nabla f(u))$ admet un minimum global.
   On a

$$\varphi_u'(t) = \mathrm{d}f_{u+t\nabla f(u)}(\nabla f(u)) = (\nabla f(u + t\nabla f(u)) \mid \nabla f(u))$$

   et

$$\begin{aligned}
(t-s)(\varphi_u'(t) - \varphi_u'(s)) &= (\nabla f(\underbrace{u + t\nabla f(u)}_{u'}) - \nabla f(\underbrace{u + s\nabla f(u)}_{v'}) \mid \underbrace{(t-s)\nabla f(u)}_{u'-v'}) \\
&\geqslant \alpha\|v' - u'\|^2 = \alpha(t-s)^2\|\nabla f(u)\|^2 \geqslant 0
\end{aligned}$$

   donc ϕ_u' est croissante et φ_u est convexe. Puis,

$$\begin{aligned}
\varphi_u'(t) - \varphi_u'(s) \geqslant \alpha(t-s)\|\nabla f(u)\|^2 &\xrightarrow[t\to+\infty]{} +\infty \\
&\xrightarrow[s\to-\infty]{} +\infty
\end{aligned}$$

   donc ϕ_u' est croissante surjective dans $\mathbf{R}$ d'où l'unicité et l'existence du minimum de φ_u.

   (b) On considère le schéma numérique suivant :

$$\begin{cases}
u_0 \in \mathbf{R}^n & \\
u_{p+1} = u_p & \text{si } u_p = x^\star \text{ (on suppose que cela n'arrive pas)} \\
u_{p+1} = u_p + t_p\nabla f(u_p) & \text{sinon}
\end{cases}$$

   où t_p minimise φ_{u_p}. On va montrer que (u_k) converge vers $x^\star$.

$$\varphi_{u_k}'(t_k) = 0 \implies (\nabla f(u_{k+1}) \mid \nabla f(u_k)) = 0$$

   d'où

$$f(u_k) \geqslant f(u_{k+1}) + \underbrace{(\nabla f(u_{k+1}) \mid u_k - u_{k+1})}_{=0} + \frac{\alpha}{2}\|u_k - u_{k+1}\|^2$$

   donc

$$f(u_k) - f(u_{k+1}) \geqslant 0$$

   donc $(f(u_k))_k$ est décroissante minorée donc converge. Puis

$$\underbrace{f(u_k) - f(u_{k+1})}_{\longrightarrow 0} \geqslant \frac{\alpha}{2}\|u_k - u_{k+1}\|^2$$

or (u_k) bornée car sinon $(f(u_k))$ non convergente. On note R un majorant de $(\|u_k\|)$ et ∇f est uniformément continue sur $\mathscr{B}_f(0, R+)$ donc

$$\nabla f(u_{k+1}) - \nabla f(u_k) = \nabla f(u_k + u_{k+1} - u_k) - \nabla f(u_k) \xrightarrow[k\to+\infty]{} 0$$

or

$$\|\nabla f(u_{k+1}) - \nabla f(u_k)\|^2 = \|\nabla f(u_{k+1})\|^2 + \|\nabla f(u_k)\|^2 \xrightarrow[k\to+\infty]{} 0$$

donc $\|\nabla f(u_k)\| \to 0$. Enfin,

$$(\underbrace{\nabla f(u_k)}_{\to 0} - \underbrace{\nabla f(x^\star)}_{=0} \mid u_k - x^\star) \geqslant \alpha\|u_k - x^\star\|^2$$

d'où $u_k \to x^\star$

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Chapitre XVII

Compléments sur les polynômes

Tous les théorèmes ou propositions présents dans ce chapitre sont soit déjà connus (donc au programme) soit nouveaux et sont alors des compléments de cours (hors programme). Le chapitre dans sa totalité n'est pas au programme, seuls quelques rappels du programme y sont présents car pertinents et/ou utiles au développement d'autres compléments.

Sommaire

1 Rappels

$\mathbf{K}$ désigne un corps (donc commutatif). Un polynôme de $\mathbf{K}[X]$ s'écrit P ou $P(X)$, l'évaluation en $a \in \mathbf{K}$ de P se note $P(a)$. L'application

$$P \in \mathbf{K}[X] \longmapsto (a \longmapsto P(a) \in \mathbf{K})$$

est un morphisme d'algèbres qui est injectif si $\mathbf{K}$ est infini. Pour $P \in \mathbf{K}[X] \setminus \{0\}$, $a \in \mathbf{K}$ est une racine de P ssi

$$P(a) = 0 \iff (X-a) \mid P$$

et a est racine de multiplicité $\alpha \geqslant 1$ ssi

$$\begin{cases} P(a) = P'(a) = \cdots = P^{(\alpha-1)}(a) = 0 \\ P^{(\alpha)}(a) \neq 0 \end{cases} \iff \begin{cases} (X-a)^{\alpha} \mid P \\ (X-a)^{\alpha+1} \nmid P \end{cases}$$

Si a n'est pas racine de P, on convient que a est racine de multiplicité 0.

Notation.

- On note $Z_{\mathbf{K}}(P)$ l'ensemble des racines de P dans $\mathbf{K}$
- On note $\operatorname{mult}(P, a)$ la multiplicité de la racine a dans P

Théorème.

Soit $P \in \mathbf{K}[X] \setminus \{0\}$. Le polynôme P a au plus $\deg P$ racines dans $\mathbf{K}$. En particulier, le polynôme nul est le seul polynôme qui a une infinité de racines.

Théorème.

Soit $P \in \mathbf{K}[X]$.

1.
$$P(X) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(0)}{k!} X^k$$

2.
$$\forall a \in \mathbf{K}, \quad P(X) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!} (X-a)^k$$

Démonstration.

1. L'application
$$\psi : P \longmapsto P(X) - \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}(X-a)^k$$
est linéaire nulle sur les vecteurs de la base canonique.

□

Remarque.

On montre de même que
$$P(a) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(X)}{k!}(a-X)^k$$

2 Factorisation des polynômes

a) Rappels

Théorème.

Soit $P \in \mathbf{K}[X]$, $a_1, \cdots, a_p$ deux à deux distincts et $n_1, \cdots, n_p \in \mathbf{N}^\star$. Si $a_1, \cdots, a_p$ sont des racines de multiplicités $n_1, \cdots, n_p$ de P, alors
$$(X-a)^{n_1} \cdots (X-a_p)^{n_p} \mid P$$
En particulier, si $\deg P = \sum_i n_i$ alors il existe $\lambda \in \mathbf{K}^\star$ tel que
$$P(X) = \lambda(X-a_1)^{n_1} \cdots (X-a_p)^{n_p}$$

b) Théorème de d'Alembert-Gauss

Théorème (D'Alembert-Gauss).

Tout polynôme non constant de $\mathbf{C}[X]$ admet au moins une racine

Preuve de Gauss. • $P \in \mathbf{C}[X]$ non constant a même racine que $\frac{1}{\deg P}P$ donc on suppose P unitaire.

• Si $P(X) = a_0 + \cdots + a_{n-1}X^{n-1} + X^n$, et $M = \max |a_i|$, alors pour $|z| \geqslant M+2$,
$$\begin{aligned}|P(z)| &\geqslant |z|^n - M\frac{|z|^n - 1}{|z|-1} = \frac{|z|^{n+1} - |z|^n - M|z|^n + M}{|z|-1} \\ &\geqslant \frac{|z|^n}{|z|-1}(|z|-1-M) \geqslant |z|^n\left(1 - \frac{M}{M+1}\right) \geqslant \frac{(M+2)^n}{M+1} > M\end{aligned}$$

•
$$\begin{aligned}\inf_{\mathbf{C}} |P| &= \min\left(\underbrace{\inf_{|z|>M+2}|P(z)|}_{>M}, \underbrace{\inf_{|z|\leqslant M+2}|P(z)|}_{\leqslant |P(0)| \leqslant M}\right) \\ &= \inf_{|z|\leqslant M+2}|P(z)|\end{aligned}$$
Par compacité il existe $z_0 \in \mathscr{B}_f(0, M+2)$ tel que $\inf_{\mathbf{C}}|P| = |P(z_0)|$.

• Si $P(z_0) \neq 0$ alors il existe $k \geqslant 1$ tel que
$$\begin{aligned}P(z_0+h) &= P(z_0) + \frac{P^{(k)}(z_0)}{k!}h^k + o(h^k), \quad P(z_0) \neq 0 \\ &= P(z_0)\left(1 + h^k\frac{P^{(k)}(z_0)}{P(z_0)k!} + o(h^k)\right)\end{aligned}$$

- En écrivant
$$\frac{P^{(k)}(z_0)}{P(z_0)k!} = \rho e^{i\theta}, \quad h = \varepsilon e^{-i\frac{\theta+\pi}{k}}$$
on obtient
$$P(z_0 + \varepsilon e^{-i\frac{\theta}{k}}) = \underbrace{P(z_0)\underbrace{\left(1 - \varepsilon^k\rho + o(\varepsilon^k)\right)}_{|\ |<1}}_{|\ |<|P(z_0)|}$$
absurde.

$\square$

3 Polynômes sous contraintes

a) Contraintes sur les zéros

Exercice.

Si $Z_{\mathbf{C}}(P) = Z_{\mathbf{C}}(Q)$ et $Z_{\mathbf{C}}(P+1) = Z_{\mathbf{C}}(Q+1)$ pour P, Q non constants de $\mathbf{C}[X]$, alors $P = Q$

On suppose par l'absurde que $P \neq Q$ et par exemple $n = \deg P \geqslant \deg Q = m$. On note $u_1, \cdots, u_r$ les racines de P (et donc de Q), $v_1, \cdots, v_s$ les racines de $P+1$ (donc de $Q+1$). Les u_i et les v_j sont tous distincts, donc
$$\deg P = n \geqslant \deg(P - Q) \geqslant r + s \quad \text{car } P - Q \text{ s'annule en } u_i \text{ et } v_j \text{ et } P - Q \neq 0$$
On a $P' = (P+1)'$ donc P' a $n - r$ racines dans les u_i avec multiplicité, et $n - s$ dans les n_j donc
$$n - r + n - s \leqslant \deg P' = n - 1 \iff n + 1 \leqslant r + s$$
Or $r + s \leqslant n$ absurde et donc $P = Q$

b) Coefficients unitaires

Exercice.

Déterminer les $P \in \mathbf{R}[X]$ non constants avec les coefficients ± 1 et dont toutes les racines sont réelles.

Résolution. On note P un polynôme de degré $n \geqslant 2$ qui convient et quitte à changer P en $-P$, P est unitaire.

- $P(X) = X^n + p_{n-1}X^{n-1} + \cdots + p_0$
- $r_1, \cdots, r_n$ les racines (non nulles car $p_0 \neq 0$) donne
$$r_1^2 + \cdots + r_n^2 = p_{n-1}^2 - 2p_{n-2} > 0 \implies p_{n-2} = -1 \text{ et } r_1^2 + \cdots + r_n^2 = 3$$
- $$p_0 X^n P\left(\frac{1}{X}\right) = X^n + p_0p_1X^{n-1} + p_0p_2X^{n-2} + \cdots$$
vérifie les mêmes propriétés donc
$$\frac{1}{r_1^2} + \cdots + \frac{1}{r_n^2} = 3$$
- $$\sum_{i=1}^{n} \underbrace{\left(r_i^2 + \frac{1}{r_i^2}\right)}_{\geqslant 2} = 6 \implies n \leqslant 3$$

On doit étudier 12 polynômes
$$\begin{array}{lll}
\cancel{X^2 + X + 1} & \cancel{X^3 + X^2 + X + 1} & \cancel{X^3 - X^2 + X + 1} \\
X^2 + X - 1 & \cancel{X^3 + X^2 + X - 1} & \cancel{X^3 - X^2 + X - 1} \\
\cancel{X^2 - X + 1} & \cancel{X^3 + X^2 - X + 1} & X^3 - X^2 - X + 1 \\
X^2 - X - 1 & X^3 + X^2 - X - 1 & \cancel{X^3 - X^2 - X - 1}
\end{array}$$

$\square$

c) Équation fonctionnelle

Exercice.

Déterminer les polynômes $P \in \mathbf{C}[X]$ tels que $P(X)P(X+2) + P(X^2) = 0$

Résolution. -1 et 0 sont les deux polynômes constants solutions.

Soit P non constant solution et a une racine. $P(a) = 0 \implies P(a^2) = 0$ donc P admet une infinité de racines sauf si $|a| = 1$ ou $a = 0$.

Si $a = 0$ est racine alors $P(-2)P(0) + P(4) = 0$ donc 4 est racine ce qui est absurde. Donc $|a| = 1$.

Si a est racine alors $(a-2)^2$ racine donc $|a-2| = 1 = |a|$ donc $a = 1$ (intersection de deux cercles), donc 1 seule racine de P et donc pour un $k \geqslant 1$,

$$P = \lambda(X-1)^k$$

En calculant, on trouve $\lambda^2 + \lambda = 0$ et $\lambda \neq 0$ donc $\lambda = -1$ □

Exercice.

Trouver les polynômes $P \in \mathbf{R}[X]$ tels que

$$(X+1)P(X-1) - (X-1)P(X)$$

est un polynôme constant

Résolution. On suppose que P convient et $(X+1)P(X-1) - (X-1)P(X) = \lambda$.

- $2P(-1) = \lambda$ et $2P(0) = \lambda$ donc $P(0) = P(-1)$
- $Q(X) = P(X) - \frac{\lambda}{2}$ s'annule en -1 et 0 donc $Q(X) = X(X+1)A(X)$ i.e. $P(X) = X(X+1)A(X) + \frac{\lambda}{2}$.
- $$(X+1)((X-1)XA(X-1) + \frac{\lambda}{2}) - (X-1)X(X+1)A(X) - (X-1)\frac{\lambda}{2} = \lambda$$

  donc

  $$X(X-1)(X+1)(A(X-1) - A(X)) = 0 \implies A(X) = A(X-1)$$

  et donc A est un polynôme constant. Donc P est de la forme $P(X) = aX(X+1) + \mu, \quad a, \mu \in \mathbf{R}$

□

4 Liens coefficients et racines

a) Relations de Viète

Pour $x_1, \cdots, x_n \in \mathbf{C}$ on note :

$$\sigma_i(x_1, \cdots, x_n) = \sum_{\substack{I \subset [\![1,n]\!] \\ |I| = i}} \prod_{l \in I} x_l$$

Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme de degré n et $x_1, \cdots, x_n$ ses racines dans $\mathbf{C}$.

- $$P(X) = a_n(X - x_1)\cdots(X - x_n) = a_n(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \cdots (-1)^n \sigma_n X^{n-n})$$
- Ainsi,

  $$\forall i \in [\![1,n]\!], \quad (-1)^i \sigma_i = \frac{a_{n-i}}{a_n}$$

En particulier, on en déduit

$$x_1 + \cdots + x_n = -\frac{a_{n-1}}{a_n}$$

et

$$x_1 \times \cdots \times x_n = (-1)^n \frac{a_0}{a_n}$$

b) Somme de Newton

On note $P(X) = a_n X^n + \cdots + a_0$ un polynôme de $\mathbf{C}[X]$, $x_1, \cdots, x_n$ ses racines. On note $S_k = x_1^k + \cdots + x_n^k$ appelée $k-$ième somme de Newton .

Pour $k \geqslant n$,

$$\begin{aligned} a_n S_k + a_{n-1} S_{k-1} + \cdots + a_0 S_{k-n} &= a_n x_1^k + \cdots + a_0 x_1^{k-n} + \cdots + a_n x_n^k + \cdots + a_0 x_n^{k-n} \\ &= x_1^{k-n} P(x_1) + \cdots + x_n^{k-n} P(x_n) = 0 \end{aligned}$$

Avec les relations de Viète, pour $k \geqslant n$,

$$\underbrace{\sigma_0}_{= 0 \text{ convention}} \qquad S_k - \sigma_1 S_{k-1} + \cdots + (-1)^n S_{k-n} = 0$$

Il est possible de calculer $S_1, \cdots, S_{n-1}$ par des formules de récurrence.

- $S_0 = n$ clair. On va montrer que

$$k\sigma_k = \sum_{i=1}^{k} (-1)^{i-1} \sigma_{k-i} S_i$$

- On note P le polynôme $P/\operatorname{dom} P$

$$P(x) = \prod_{i=1}^{n} (x - x_i) = \frac{1}{a_n} \sum_{k=0}^{n} a_k x^k = \sum_{k=0}^{n} \sigma_{n-k} (-1)^{n-k} x^k$$

d'où

$$x^n P\left(\frac{1}{x}\right) = \underbrace{\prod_{k=1}^{n} (1 - x x_k)}_{Q(x)} = \sum_{k=0}^{n} \sigma_{n-k} (-1)^{n-k} x^{n-k} = \sum_{k=0}^{n} \sigma_k (-1)^k x^k$$

-

$$\begin{aligned} \sum_{k=0}^{n} k\sigma_k (-1)^k x^k &= x \sum_{k=1}^{n} \frac{Q(x)}{1 - xxk} (-x_k) \\ &= -\sum_{k=1}^{n} \frac{x x_k}{1 - x x_k} Q(x) \\ &= -\left(\sum_{k=1}^{n} \sum_{i \geqslant 0} (x x_k)^{i+1} \right) Q(x) \\ &= -\sum_{i \geqslant 0} x^{i+1} S_{i+1} \sum_{l=0}^{n} (-1)^k \sigma_k x^k \end{aligned}$$

En identifiant le coefficient de x^k,

$$\begin{aligned} (-1)^k k\sigma_k = -\sum_{l=0}^{k-1} (-1)^l \sigma_l S_{k-l} \iff k\sigma_k &= -\sum_{l=0}^{k-1} (-1)^{k-l} \sigma_l S_{k-l} \\ &= \sum_{l=1}^{k} (-1)^{l-1} \sigma_{k-l} S_l \end{aligned}$$

5 Polynômes scindés sur R

a) Une CNS

Exercice.

> Montrer que $P \in \mathbf{R}[X]$ de degré n est scindé sur $\mathbf{R}$ ssi
>
> $$\forall z \in \mathbf{C}, \quad |P(z)| \geqslant |\operatorname{dom}(P)| \times |\mathfrak{Im}(z)|^n$$

Résolution. *(⟹)* clair, les racines complexes de P ont une partie imaginaire nulle.

(⟹) On écrit $P(X) = \mathrm{dom}(P)(X - a_1)\cdots(X - a_n), \quad a_i \in \mathbf{R}$. En injectant $z = a + ib$,

$$|P(z)| = |\operatorname{dom} P| \times |a - a_1 + ib| \cdots |a - a_n + ib| \geqslant |\operatorname{dom} P||b|^n$$

□

b) Opérations stabilisant $\mathscr{S}$

On note $\mathscr{S}$ l'ensemble des polynômes scindés de $\mathbf{R}[X]$. On note

$$P(X) = \lambda(X - a_i)^{\alpha_1} \cdots (X - a_p)^{\alpha_p}, \quad a_1 < \cdots < a_p$$

et on a les propriétés de stabilité suivantes.

Rolle donne que P' s'annule au moins une fois sur $]a_i, a_{i+1}[$ pour $1 \geqslant i < p$. Il y a alors au total $(\alpha_1 - 1) + \cdots + (\alpha_p - 1) + p - 1 = n - 1$ racines réelles (avec multiplicité) et $\deg P' = n - 1$ donc P' est scindé et $\mathscr{S}$ est stable par dérivation.

Pour $a \in \mathbf{R}$ fixé, on note $g(x) = e^{ax}P(x)$, $g'(x) = (P'(x) + aP(x))e^{ax}$. $P' + aP$ s'annule en a_i avec multiplicité $\geqslant \alpha_i - 1$. Rolle donne que g' s'annule au moins une fois sur $]a_i, a_{i+1}[$ donc $P' + aP$ aussi. Ce polynôme a $n - 1$ racines réelles et est de degré n, donc par division la dernière racine est réelle. Donc $P' + aP \in \mathscr{S}$

Plus généralement, si D est l'opérateur de dérivation polynomiale, pour $Q \in \mathscr{S}$ alors

- $$Q(X) = \lambda(X - b_1) \cdots (X - b_p)$$
- $$Q(D) = \lambda(D - b_1\mathrm{id}) \circ \cdots \circ (D - b_p\mathrm{id})$$

et pour $P \in \mathscr{S}$, $Q(D)(P) \in \mathscr{S}$.

c) Faisceau de polynômes à racines entrelacées (ENS)

Exercice.

> On note $P, Q \in \mathbf{R}[X]$ deux polynômes scindés à racines simples distinctes tels qu'entre deux racines de l'un, il y en aie au moins une de l'autre. Montrer que $\lambda P + \mu Q$ est scindé sur $\mathbf{R}$

Résolution. On suppose que P a la plus petite racine, on note $x_1 < \cdots < x_n$ les racines de P. Sur $]x_1, x_2[$, il y a au moins une racine de Q et au plus une (sinon x_1 et x_2 ne sont pas consécutives) donc les $n - 1$ premières racines de Q satisfont

$$x_1 < y_1 < \cdots < x_{n-1} < y_{n-1} < x_n$$

Il y a lors deux cas : Q possède une racine $y_n > x_n$, ou Q a $n - 1$ racines réelles. On se place dans le premier cas (l'autre se traite similairement).

Comme $\lambda, \mu \in \mathbf{R}$ sont quelconques, on peut supposer P et Q unitaires donc

$$P(X) = (X - x_1) \cdots (X - x_n) \qquad Q(X) = (X - y_1) \cdots (X - y_n)$$

Pour $\lambda, \mu \neq 0$, les racines réelles de $\lambda P + \mu Q$ sont différentes des x_i, y_i, donc sont les mêmes que celles de $\frac{\lambda P + \mu Q}{PQ}$ sur $\mathbf{R} \setminus \{x_i, y_i\}$.

$$\varphi(x) = \frac{\lambda P(x) + \mu Q(x)}{P(x)Q(x)} = \frac{\lambda}{Q(x)} + \frac{\mu}{P(x)}$$

Si $\lambda, \mu > 0$, alors φ s'annule n fois car il y a changement de signe entre $]x_i, y_i[$ (les polynômes sont unitaires donc on connaît exactement les signes de P et Q). Si $\lambda > 0 > \mu$, on trouve $n - 1$ racines réelles de la même manière, et par division la dernière est aussi réelle. Les autres cas se traitent de la même manière. □

6 Valeurs des polynômes

a) Polynôme à valeurs entières

On va caractériser les polynômes de $\mathbf{C}[X]$ tels que $P(\mathbf{Z}) \subset \mathbf{Z}$

On définit
$$\binom{X}{0} = 1 \qquad \text{et} \qquad \forall n \geqslant 1, \quad \binom{X}{n} = \frac{1}{n!}X(X-1)\cdots(X-n+1)$$

Lemme.

Pour tout $n \in \mathbf{N}$ et pour tout $x \in \mathbf{Z}$,
$$\binom{x}{n} \in \mathbf{Z}$$

Démonstration. Pour $0 \leqslant x \leqslant n-1$, $\binom{x}{n} = 0$. Pour $x \geqslant n$, $\binom{x}{n}$ est un coef du binôme. Pour $x < 0$, $(-1)^n\binom{x}{n}$ est un coef du binôme. □

On introduit
$$\Delta : P \in \mathbf{K}[X] \longmapsto P(X+1) - P(X)$$

Pour $n \geqslant 1$,
$$\Delta\binom{X}{n} = \binom{X}{n-1} \qquad \text{et} \qquad \Delta\binom{X}{0} = 0$$

et $\left(\binom{X}{n}\right)_{n\geqslant 0}$ est une base de $\mathbf{C}[X]$ (degré échelonné). On suppose que $P \in \mathbf{C}[X]$ vérifie $P(\mathbf{Z}) \subset \mathbf{Z}$. On note $a_0, \cdots, a_n$ les coefficients de la décomposition de P dans cette base. Alors
$$P(0) = a_0 \in \mathbf{Z}, \quad a_1 = \Delta P(0) \in \mathbf{Z}, \cdots, \quad a_n = \Delta^n P(0) \in \mathbf{Z}$$

Ainsi, $a_0, \cdots, a_n \in \mathbf{Z}$ et la réciproque est évidente. On a ainsi établi
$$P(\mathbf{Z}) \subset \mathbf{Z} \iff \exists n \in \mathbf{N}, \exists, a_0, \cdots, a_n \in \mathbf{Z}, P(X) = \sum_{k=0}^{n} a_k \binom{X}{k}$$

Remarque.

On a aussi établi la formule de Gregory
$$P(X) = \sum_{k\geqslant 0} \Delta^k P(0)\binom{X}{k}$$

Exercice (ENS).

On note $P \in \mathbf{R}[X]$ un polynôme de degré n tel que $P(0), P(1), P(4), \cdots, P(n^2) \in \mathbf{Z}$. Montrer que $\forall a \in \mathbf{Z}, P(a^2) \in \mathbf{Z}$.

Résolution. $Q(X) = P((X-n)^2)$ de degré $2n$ envoie $2n+1$ valeurs de $\mathbf{Z}$ dans $\mathbf{Z}$ donc a des coefficients entiers dans la base explicitée précédemment donc est à valeurs dans $\mathbf{Z}$ ce qui conclut. □

b) Polynôme stabilisant le cercle unité

Exercice.

Déterminer les polynômes $P \in \mathbf{C}[X]$ tels que $\mathbb{U}$ est stable par P.

Résolution. Le cas des polynômes constants est immédiat. On note $P(z) = a_0 + \cdots + a_n z^n$. On a
$$P(e^{i\theta})\overline{P(e^{i\theta})} = 1 \implies P(e^{i\theta})\overline{P}(e^{-i\theta}) = 1 \implies P(e^{i\theta})\overline{P}(e^{-i\theta})e^{in\theta} = e^{in\theta}$$

Si on note $Q(X) = \overline{P}\left(\frac{1}{X}\right)X^n = \overline{a}_0 X^n + \cdots + \overline{a}_n$ alors $PQ - X^n$ s'annule sur $\mathbb{U}$ donc est nul donc $P(X) \mid X^n$, $\deg P = n$ et $P = \lambda X^n$, où $\lambda = P(1) \in \mathbb{U}$. La réciproque est claire. □

Exercice.

Variantes

- $P(\mathbf{C}) \subset \mathbf{R}$. Solution : Formule de Gregory, interpolation de Lagrange, polynôme conjugué, ...
- $P(\mathbf{Q}) \subset \mathbf{Q}$. Solution : Formule de Gregory, interpolation de lagrange.
- $P(\mathbf{Q}) \subset \mathbf{R} \setminus \mathbf{Q}$ et $P(\mathbf{R} \setminus \mathbf{Q}) \subset \mathbf{Q}$
- $P(\mathbf{Q}) = \mathbf{Q}$

Résolution. Résolution pour $P(\mathbf{Q}) = \mathbf{Q}$. Déjà $P \in \mathbf{Q}[X]$ (par la 2-ième variante), donc il existe d entier positif minimal tel que $Q = dP \in \mathbf{Z}[X]$. On se donne v premier avec les coefs a_i de P et d et v nombre premier. Il existe $\frac{a}{b}$, $a \wedge b = 1$, tel que $P(\frac{a}{b}) = \frac{d}{v}$ donc

$$v(a_n a^n + \cdots + a_0 b^n) = db^n \implies v \mid b^n \implies v \mid b$$

et si $n \geqslant 2$ alors $v^2 \mid db^n$ et donc $v | a_n a^n + \cdots$ donc $v \mid a$ absurde. Par suite, $n = 1$, et la réciproque est évidente. □

c) Polynômes positifs

On va caractériser les polynômes tq $P(\mathbf{R}_+) \subset \mathbf{R}_+$. On pose

$$\mathscr{E} = \{P \in \mathbf{R}[X] \ / \ \exists A, B \in \mathbf{R}[X], P = A^2 + XB^2\}$$

et on note $\mathscr{S}$ l'ensemble des polynômes qui conviennent. On a clairement $\mathscr{E} \subset \mathscr{S}$, puis $\mathscr{E}$ est stable par produit car

$$(A^2 + XB^2)(A_1^2 + XB_1^2) = (AA_1 + XBB_1)^2 + X(BA_1 + AB_1)^2$$

Soit $P \in \mathscr{S}$. Dans la décomposition de P en irréductibles de $\mathbf{R}[X]$, si on note $\alpha_1, \cdots, \alpha_p$ les puissances des facteurs de degré 1, on a $(X - a_i)$ change de signe si α_i impair et dans ce cas $a_i < 0$ et $X - a_i = \sqrt{-a_i}^2 + X1^2 \in \mathscr{E}$. Les autres termes sont dans $\mathscr{E}$ et donc $\mathscr{S} = \mathscr{E}$.

7 Localisation des racines

a) Théorème de Gauss-Lucas

On note $P \in \mathbf{C}[X]$ avec $n = \deg P \geqslant 2$. On va montrer que si $z_1, \cdots, z_n$ sont les racines de P (répétées avec multiplicités) alors les racines de P' sont dans l'enveloppe convexe de $z_1, \cdots, z_n$. On a :

$$\frac{P'}{P}(z) = \frac{\alpha_1}{z - z_1} + \cdots + \frac{\alpha_p}{z - z_p}$$

donc si z est une racine de P' différente des $z_1, \cdots, z_n$, alors

$$\alpha_1 \frac{z - z_1}{|z - z_1|^2} + \cdots + \alpha_p \frac{z - z_p}{|z - z_p|^2} = 0 \iff z\left(\frac{\alpha_1}{|z - z_1|^2} + \cdots + \frac{\alpha_p}{|z - z_p|^2}\right) = \frac{\alpha_1}{|z - z_1|^2} z_1 + \cdots + \frac{\alpha_p}{|z - z_p|^2} z_p$$

Donc z est bien un barycentre de $z_1, \cdots, z_n$.

b) Borne de Cauchy

On note $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0 \in \mathbf{C}[X]$ et on pose $M = \max\limits_{i \leqslant n-1} |a_i|$. On note $z \in \mathbf{C}$ tel que $|z| > M + 1$. Par l'absurde si $P(z) = 0$ alors

$$\begin{aligned} |z^n| = |a_{n-1}z^{n-1} + \cdots + a_0| \leqslant M \frac{|z|^n - 1}{|z| - 1} &\implies |z|^{n+1} - |z|^n \leqslant M|z|^n - M \\ &\implies |z||z|^n \leqslant (M+1)|z|^n \\ &\implies |z| \leqslant M + 1 \quad \text{absurde} \end{aligned}$$

Bilan les racines de P sont dans le disque $D(0, M + 1)$

c) Enestrom-Kakeya

Résultat (Cauchy).

Si $P(x) = x^n - b_{n-1}x^{n-1} - \cdots - b_0$ est un polynôme tel que les b_i sont positifs non tous nuls alors P a une seule racine a dans $\mathbf{R}_+^\star$, a est racine simple et $\mathbf{Z}_\mathbf{C}(P) \subset \mathscr{B}_f(0, a)$.

Démonstration. Pour $x > 0$, $f(x) = -\frac{P(x)}{x^n} = \frac{b_0}{x^n} + \cdots + \frac{b_{n-1}}{x} - 1$ est décroissante.

x	0	a	$+\infty$
$f(x)$	$+\infty$	$\searrow$	-1

Donc f a une unique racine $a > 0$, puis

$$f'(a) = -n\frac{b_0}{x^{n+1}} - \cdots - \frac{b_{n-1}}{x^2} < 0 \implies P'(a) \neq 0$$

donc a est racine simple de P. Si z_0 est une racine de P dans $\mathbf{C}$ alors $P(z_0) = 0$ donc

$$|z_0^n| = |b_{n-1}z_0^{n-1} \cdots b_0| \leqslant b_{n-1}|z_0^n| + b_0$$

donc $P(|z_0|) \leqslant 0$ et $f(|z_0|) \geqslant 0$ donc $|z_0| \leqslant a$ □

Résultat (Enestrom-Kakeya).

Si $P(x) = a_{n-1}x^{n-1} + \cdots + a_0$ est un polynôme à coefficients strictement positifs, alors si z est une racine complexe de P,

$$\delta = \min_{i \leqslant n-1} \frac{a_{i-1}}{a_i} \leqslant |z| \leqslant \max_{i \leqslant n-1} \frac{a_{i-1}}{a_i} = \gamma$$

Démonstration. On considère le polynôme

$$\begin{aligned} Q(x) = (x-\gamma)P(x) &= a_{n-1}x^n + (a_{n-2} - \gamma a_{n-1})x^{n-1} + \cdots + (a_0 - \gamma a_1)x - \gamma a_0 \\ &= a_{n-1} \underbrace{\left(x^n - \frac{\gamma a_{n-1} - a_{n-2}}{a_{n-1}}x^{n-1} - \cdots - \frac{\gamma a_1 - a_0}{a_{n-1}}x - \frac{\gamma a_0}{a_{n-1}}\right)}_{\text{vérifie les hypothèses du résultat précédent donc a une unique racine réelle } > 0,\ \gamma} \end{aligned}$$

d'où la seconde inégalité. La première s'obtient en remarquant que z racine de P entraîne z non nul et $\frac{1}{z}$ racine de $X^{n-1}P\left(\frac{1}{X}\right)$ auquel on applique le même raisonnement. □

d) Disques de Gershgorin

On se donne $A \in \mathscr{M}_n(\mathbf{C})$ et $\lambda \neq a_{1,1}, \cdots, a_{n,n}$. On note $D = \operatorname{diag}(a_{1,1}, \cdots, a_{n,n})$ et $E = A - D$. Si λ est valeur propre, alors

$$A_\lambda = \underbrace{A - \lambda I_n}_{\text{non inversible}} = \underbrace{D - \lambda I_n}_{\text{inversible}} + E$$

Puis $\exists X \in \mathscr{M}_{n,1}(\mathbf{C}), X \neq 0 / A_\lambda X = 0$ donc

$$\begin{aligned} (D - \lambda I_n)X + EX = 0 &\iff X = -(D - \lambda I_n)^{-1}EX \\ &\iff \forall i \in [\![1, n]\!], \quad x_i = -\frac{1}{a_{i,i} - \lambda}\sum_{k \neq i} a_{i,k}x_k \end{aligned}$$

On considère un indice i tel que $|x_i|$ est maximal et donc

$$|a_{i,i} - \lambda| = |\sum_{k \neq i} a_{i,k}\frac{x_k}{x_i} \leqslant \sum_{k \neq i} |a_{i,k}| = R_i$$

et donc

$$\lambda \in \mathscr{D}(a_{i,i}, R_i) \qquad \text{reste vrai si } \lambda = a_{i,i}$$

On a donc
$$\mathrm{Sp}_{\mathbf{C}}(A) \subset \bigcup_{i=1}^{n} \underbrace{\mathscr{D}(a_{i,i}, R_i)}_{\text{disques de Gershgorin}}$$

8 Arithmétique des polynômes

a) Division euclidienne

Exercice.

Effectuer la division euclidienne de $X^n - 1$ par $X^m - 1$, pour $n, m \geqslant 1$

Résolution. On note (u_k) la suite définie par
$$\begin{cases} u_0 = n, u_1 = m \\ u_{k+1} \quad \text{reste de la division euclidienne de } u_{k-1} \text{ par } u_k \end{cases}$$
tant que $u_k \neq 0$ et on note
$$\begin{cases} U_0 = X^n - 1, U_1 = X^m - 1 \\ U_{k+1} \quad \text{reste de la division euclidienne de } U_{k-1} \text{ par } U_k \end{cases}$$
tant que $U_k \neq 0$

On vérifie par récurrence que $U_k = X^{u_k} - 1$. Les cas $k = 0, 1$ sont immédiats. On a $u_{k+1} + au_k = u_{k-1}$ donc par HR si $U_k \neq 0$ (ie $u_k \neq 0$), alors
$$U_{k-1} = U^{u_{k+1}} X^{au_k} - 1 = \underbrace{X^{u_{k+1}} - 1}_{\deg < \deg U_k} + \underbrace{X^{u_{k+1}} \left(X^{au_k} - 1\right)}_{\text{divisible par } U_n}$$
d'où le résultat. On en déduit que les deux suites s'arrêtent en même temps et donc
$$U_0 \wedge U_1 = U_{k-1} = X^{m \wedge n} - 1$$
□

b) Théorème chinois

Exercice.

On se donne $P_1, \cdots, P_n$ deux à deux premiers entre eux et $R_1, \cdots, R_n \in \mathbf{C}[X]$. Montrer qu'il existe $Q_1, \cdots, Q_n$ tels que
$$P_1 Q_1 + R_1 = \cdots = P_n Q_n + R_n$$

Résolution. C'est une application directe du théorème chinois (dans un anneau principal) : si $d_i = \deg P_i - 1$ et $N = -1 + \sum d_i$, alors
$$\varphi : P \in \mathbf{C}_N[X] \longmapsto (P \mod P_1, \cdots, P \mod P_n) \in \mathbf{C}_{d_1}[X] \times \cdots \times \mathbf{C}_{d_n}[X]$$
est un isomorphisme d'algèbres. □

c) Théorèmes de Mason, Snyder, et Fermat

On va montrer le théorème de Mason (ou Mason-Stothers) avec une démonstration de Snyder [1]

Lemme.

Si $P \in \mathbf{C}[X]$ non nul, alors
$$\deg P = \deg (P \wedge P') + n_0(P)$$
où $n_0(P) = \# Z_{\mathbf{C}}(P)$.

1. https://doi.org/10.1007/s000170050074

Démonstration. Le cas P constant est immédiat. On suppose maintenant P non constant :

$$P(X) = c(X - a_1)^{\alpha_1} \cdots (X - a_p)^{\alpha_p}$$

donc

$$P \wedge P' = (X - a_1)^{\alpha_1 - 1} \cdots (X - a_p)^{\alpha_p - 1}$$

□

Théorème (Mason).

Si A, B, C sont des polynômes complexes deux à deux premiers entre eux avec $A + B = C$ et $(A', B', C') \neq (0, 0, 0)$, alors

$$\deg C \leqslant n_0(ABC) - 1$$

Démonstration. Comme $A = C - B$ et $B = C - A$ les rôles de A, B, C sont symétriques. On peut supposer A non constant. On a alors

$$\begin{vmatrix} A & C \\ A' & C' \end{vmatrix} = \begin{vmatrix} A & B \\ A' & B' \end{vmatrix}$$

donc $AC' - CA' = AB' - BA'$ donc

$$A \wedge A', \quad B \wedge B', \quad C \wedge C' \quad \Big| \quad AC' - A'C = AB' - BA'$$

Si $AC' - A'C = 0$ alors $AC' = A'C$ et $C \mid C'$ donc $C = 0$, et de même $B = 0$ donc $A = 0$ absurde. Les trois polynômes A, B, C sont premiers entre eux donc les trois PGCD le sont aussi et

$$A \wedge A' \quad \times \quad B \wedge B' \quad \times \quad C \wedge C' \quad \Big| \; AC' - A'C \neq 0$$

donc

$$\deg A \wedge A' + \deg B \wedge B' + \deg C \wedge C' \leqslant \deg(AC' - A'C)$$

et par le résultat précédent

$$\deg A + \deg B + \deg C \leqslant \underbrace{AB' - A'B}_{\leqslant \deg A + \deg B - 1} + \underbrace{n_0(A) + n_0(B) + n_0(C)}_{n_0(ABC)}$$

□

Théorème (Fermat).

Si $A, B, C \in \mathbf{C}[X]$ non constants, A et B premiers entre eux et $A^n + B^n = C^n$ alors $n \leqslant 2$

Démonstration. On note $p = \max(\deg A, \deg B, \deg C)$ et

$$np = \max(\deg A^n, \deg B^n, \deg C^n) < n_0(A^n B^n C^n) = n_0(ABC) \leqslant 3p \implies n < 3$$

□

d) Résultant

On note $P = a_p X^p + \cdots + a_0$, $Q = b_q X^q + \cdots + b_0$ de degrés respectifs p, q.

On considère l'application linéaire

$$\varphi : (U, V) \in \mathbf{K}_{q-1}[X] \times \mathbf{K}_{p-1}[X] \longmapsto UP + VQ$$

Si $P \wedge Q = 1$, alors pour $U, V \in \mathrm{Ker}\varphi$, on a $Q \mid U$ et $P \mid V$ donc $U = V = 0$ en comparant les degrés. Sinon, si $P \wedge Q = \Delta$ non constant, alors $\varphi(Q/\Delta, -P/\Delta) = 0$. Ainsi, φ est un isomorphisme si et seulement si $P \wedge Q = 1$

La matrice de φ dans la base $(X^{q-1},0),\cdots,(X,0),(1,0),(0,X^{p-1}),\cdots,(0,1)$ est

$$\begin{pmatrix}
a_p & 0 & \cdots & 0 & b_q & 0 & \cdots & 0 \\
a_{p-1} & a_p & \ddots & \vdots & \vdots & b_q & \ddots & \vdots \\
\vdots & a_{p-1} & \ddots & 0 & \vdots & & \ddots & 0 \\
\vdots & \vdots & \ddots & a_p & b_1 & & & b_q \\
a_0 & & & a_{p-1} & b_0 & \ddots & \vdots & \vdots \\
0 & \ddots & & \vdots & 0 & \ddots & b_1 & \vdots \\
\vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 & b_1 \\
0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0
\end{pmatrix} \underset{\text{def}}{=} R(P,Q)$$

On appelle résultant de P et Q le déterminant de cette matrice. Ainsi,

$$P \wedge Q \neq 1 \iff \det R(P,Q) = 0$$

9 Polynômes irréductibles

a) Contenu de Gauss

On note $P(X) = a_nX^n + \cdots + a_0 \in \mathbf{Z}[X]$ de degré $n \geqslant 1$. On appelle contenu de P le nombre

$$a_n \wedge \cdots \wedge a_0$$

Définition.

$P \in \mathbf{Z}[X]$ est dit primitif si $C(P) = 1$

On va montrer que si $P, Q \in \mathbf{Z}[X]$ non constants alors

$$C(PQ) = C(P)C(Q)$$

On commence par supposer que P et Q sont primitifs et on suppose par l'absurde $C(PQ) \neq 1$. On note p premier diviseur de $C(PQ)$. On note i_0 (resp j_0) le plus petit indice tel que p ne divise pas a_{i_0} (resp. b_0).

$$P(X) = a_nX^n + \cdots + a_{i_0}X^{i_0} + \underbrace{\cdots}_{\text{divisible par } p}$$

$$Q(X) = b_nX^n + \cdots + b_{j_0}X^{j_0} + \underbrace{\cdots}_{\text{divisible par } p}$$

Alors,

$$[PQ(X)]_{i_0+j_0} = a_{i_0}b_{j_0} + pk \quad \text{non divisible par } p$$

Or c'est un coef de PQ donc divisible par p, absurde.

Dans le cas général,

$$C\left(\frac{PQ}{C(P)C(Q)}\right) = 1 = \frac{C(PQ)}{C(P)C(Q)}$$

Résultat.

$P \in \mathbf{Z}[X]$ primitif est irréductible dans $\mathbf{Z}[X]$ si et seulement s'il l'est dans $\mathbf{Q}[X]$

Démonstration. Si le polynôme est irréductible dans $\mathbf{Q}[X]$ alors il l'est dans $\mathbf{Z}[X]$. On suppose P irréductible dans $\mathbf{Z}[X]$ et $P = AB$ dans $\mathbf{Q}[X]$. Il existe p, q minimaux positifs tels que $pqP = pAqB$, pA et qB dans $\mathbf{Z}[X]$ et

$$C(pqP) = pqC(P) = pq = C(pA)C(qB) \implies P = \frac{pA}{C(pA)} \times \frac{qB}{C(qB)}$$

absurde (les deux facteurs sont dans $\mathbf{Z}[X]$). □

b) Critère d'Eisenstein

Résultat (Critère d'Eisenstein).

On note $P = p_n X^n + \cdots + p_0 \in \mathbf{Z}[X]$ non constant de degré n. Si p est premier tel que

$$\begin{cases} p \mid p_0, \cdots, p_{n-1} \\ p \nmid p_n \\ p^2 \nmid p_0 \end{cases}$$

alors P est irréductible dans $\mathbf{Q}[X]$

Démonstration. On suppose par l'absurde que P n'est pas irréductible dans $\mathbf{Q}[X]$ donc dans $\mathbf{Z}[X]$. On écrit alors $P = AB$ avec A et B non constants à coefficients entiers. On a

$$p \mid p_0 = a_0 b_0$$

donc par exemple p divise a_0 mais pas b_0 (il ne peut pas diviser les deux par hypothèse). Si p divise tous les a_i, alors $p \mid \operatorname{dom} A \times \operatorname{dom} B = p_n$ absurde. On note alors i_0 le plus petit i tel que $p \nmid a_i$. B est non constant donc $i_0 < n$.

$$p \mid p_{i_0} = a_{i_0} b_0 + \underbrace{a_{i_0 - 1} b_1 + \cdots + a_0 b_{i_0}}_{\text{divisible par } p} \qquad \text{non divisible par } p$$

absurde d'où la conclusion. □

Conséquence 1. Pour p premier, on considère

$$\mu_p(X) = X^{p-1} + \cdots + X + 1$$

Alors,

$$\mu_p \text{ irréductible} \iff \mu_p(X+1) \text{ irréductible} \iff \frac{(X+1)^p - 1}{(X+1) - 1} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1} \text{ irréductible}$$

vrai par le critère d'Eisenstein

Conséquence 2. Pour tout $n \geqslant 1$, le polynôme

$$S_n(X) = 1 + X + \frac{X}{2!} + \cdots + \frac{X^n}{n!}$$

est irréductible. En effet, c'est équivalent à vérifier que

$$n! S_n(X) = X^n + n X^{n-1} + \cdots + n!$$

est irréductible dans $\mathbf{Z}[X]$.

Si $n = 2m$, alors il existe p premier tel que $m < p < 2m$ donc $p < n < 2p$ et on conclut avec Eisentein. Sinon, si $n = 2m+1$ alors il existe p premier tel que $m < p < 2m$ et $p < 2m < n$ et $2m \leqslant 2p - 1$ donc $n \leqslant 2p - 1 < 2p$ et on conclut de même.

c) $\mathbf{Z}[X]$ vs $\mathbf{Z}_p[X]$

On va montrer que $X^4 + 1$ est irréductible dans $\mathbf{Z}[X]$ et n'est jamais irréductible dans $\mathbf{Z}_p[X]$. Dans $\mathbf{C}[X]$,

$$X^4 + 1 = \left(X - e^{i\frac{\pi}{4}}\right)\left(X - ie^{i\frac{\pi}{4}}\right)\left(X + e^{i\frac{\pi}{4}}\right)\left(X + ie^{i\frac{\pi}{4}}\right)$$

Aucun des facteurs ni des produits n'est dans $\mathbf{Q}[X]$ donc $X^4 + 1$ est irréductible dans $\mathbf{Q}[X]$ donc dans $\mathbf{Z}[X]$.

Pour $p = 2$, $(X^4 + 1) = (X + 1)^4$ n'est pas irréductible. On suppose donc p premier impair et on observe que

$$\begin{aligned} X^4 + 1 &= (X^2)^2 - (-1) \\ &= (X^2 + 1)^2 - 2X^2 \\ &= (X^2 - 1)^2 - (-2X^2) \end{aligned}$$

Il est donc suffisant que $-1, 2$ ou -2 soit un carré de $\mathbf{Z}_p$. Si -1 et 2 ne sont pas des carrés, alors -2 est un carré. En effet, si on note $\mathscr{C}^\star$ l'ensemble des carrés non nuls, alors

$$\varphi : x \in \mathbf{Z}_p^\star \longmapsto x^2 \in \mathscr{C}^\star$$

est un morphisme surjectif de noyeau $\ker\varphi = \{\pm 1\}$ donc $\#\mathscr{C}^\star = \frac{p-1}{2}$.

$$X^{\frac{p-1}{2}} - 1$$

a au plus $\frac{p-1}{2}$ racines ($\mathbf{Z}_p$ est un corps) et s'annule sur $\mathscr{C}^\star$ donc $\mathscr{C}^\star$ est exactement l'ensemble des racines de ce polynôme (le petit théorème de fermat donne $x^{p-1} = 1$ pour tout x non nul). Si -1 et 2 ne sont pas carrés, alors

$$(-2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \times (2)^{\frac{p-1}{2}} = -1 \times -1 = 1$$

donc -2 carré.

10 Polynômes cyclotomiques (HP)

Définition.

Soit $n \geqslant 1$.

- On appelle racine primitive n-ième de l'unité tout générateur de $\mathbb{U}_n$. On note $\mathbb{P}_n$ ces racines.
- Il y a $\varphi(n)$ générateurs de $\mathbb{U}_n$: les w^l avec $l \wedge n = 1$ et w un générateur.
- On appelle n-ième polynôme cyclotomique le polynôme

$$\mu_n(X) = \prod_{u \in \mathbb{P}_n} (X - u)$$

Proposition.

Pour tout $n \in \mathbf{N}^\star$,

$$X^n - 1 = \prod_{d \mid n} \mu_d(X)$$

Démonstration. Pour $d \mid n$, on note $E_d = \{u \in \mathbb{U}_n, \operatorname{ord} u = d\}$, donc

$$\mathbb{U}_n = \bigsqcup_{d \mid n} E_d$$

ainsi

$$X^n - 1 = \prod_{d \mid n} \prod_{u \in E_d} (X - u) = \prod_{d \mid n} \mu_d(X)$$

car $E_d = \mathbb{P}_d$ (les éléments d'ordre d sont au nombre de $\varphi(d)$ et engendrent tous $\mathbb{U}_d$). □

Remarque.

Si $n = p$ est premier alors

$$\mu_n(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + 1$$

Proposition.

Pour tout $n \geqslant 1$, μ_n est unitaire à coefficients entiers, de degré $\varphi(n)$.

Démonstration. On raisonne par récurrence sur n pour le caractère entier, le reste est immédiat.

- $n = 1$ immédiat
- On se donne $n \geqslant 1$ et on suppose la propriété vraie jusqu'au rang n. Si $n+1$ est premier, la conclusion est immédiate. Sinon,

$$X^{n+1} - 1 = \prod_{d \mid n+1} \mu_d(X) = \mu_{n+1}(X) \times \underbrace{\prod_{\substack{d \mid n+1 \\ d \neq n+1}} \mu_d(X)}_{\in \mathbf{Z}[X],\ \text{unitaire}}$$

Donc μ_{n+1} est le quotient dans la division euclidienne de $X^{n+1} - 1$ par un polynôme **unitaire** de $\mathbf{Z}[X]$, d'où la conclusion.

□

a) Expression de μ_n

On introduit la fonction arithmétique de Möbius

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n \text{ produit de } k \text{ premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

Cette fonction est multiplicative : pour a, b premiers entre eux, $\mu(ab) = \mu(a)\mu(b)$. Puis, pour $n \geqslant 1$,

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$$

En effet, si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$,

$$\sum_{d \mid n} \mu(d) = \sum_{\substack{d \mid n \\ \mu(d) \neq 0}} = \sum_{I \subset [\![1,k]\!]} (-1)^{\# I} = \sum_{i=0}^{k} \binom{k}{i} (-1)^i = (1-1)^k = 0$$

Résultat.

$$\mu_n(X) = \prod_{d \mid n} \left(X^d - 1\right)^{\mu\left(\frac{n}{d}\right)}$$

Démonstration.

$$\begin{aligned} \prod_{d \mid n} \left(X^d - 1\right)^{\mu\left(\frac{n}{d}\right)} &= \prod_{d \mid n} \prod_{d' \mid d} \mu_{d'}(X)^{\mu\left(\frac{n}{d}\right)} \\ &= \prod_{d' \mid n} \prod_{u \mid \frac{n}{d'}} \mu_{d'}(X)^{\mu\left(\frac{n}{d'u}\right)} \\ &= \prod_{d' \mid n} \mu_{d'}(X)^{\left(\sum_{u \mid \frac{n}{d'}} \mu\left(\frac{n}{d'u}\right)\right)} \\ &= \mu_n(X) \end{aligned}$$

car

$$\sum_{u \mid \frac{n}{d'}} \mu\left(\frac{n}{d'u}\right) = \sum_{u \mid \frac{n}{d'}} \mu(u) = \begin{cases} 1 & \text{si } \frac{n}{d'} = 1 \iff d' = n \\ 0 & \text{sinon} \end{cases}$$

□

Remarque.

Cela donne une autre preuve de $\mu_n(X) \in \mathbf{Z}[X]$

b) Suites arithmétiques

On note p un nombre premier et $m \geqslant 1$ un entier non divisible par p. Supposons que a est un entier et que

$$\mu_m(a) = 0 \pmod{p}$$

On a dans ce cas

$$p \mid \mu_m(a) \mid a^m - 1 \text{ premier avec } a \implies p \not\mid a$$

Si $d = \operatorname{ord} a$ alors $d \mid m$ donc $X^d - 1 | X^m - 1$. Par l'absurde, si $d \neq n$ alors $X^d - 1 \wedge \mu_m = 1$ (aucune racine commune dans $\mathbf{C}$) donc (Gauss) $(X^d - 1) \times \mu_m(X) | X^m - 1$. On en déduit ($d$ est l'ordre de a)

$$(a^d - 1)\mu_m(a) \mid a^m - 1 \implies a^m - 1 = 0 \pmod{p^2}$$

et comme $a + p$ vérifie les mêmes hypothèses ($a + p \equiv a \pmod p$ donc $\mu_m(a + p) = 0 \pmod p$ et l'ordre est le même donc $\neq m$), on a $(a + p)^m - 1 = 0 \pmod{p^2}$, d'où

$$p^2 \mid (a + p)^m - a^m = p\left(a^{m-1} + \underbrace{\cdots}_{\text{multiple de } p}\right) \implies p \mid a$$

c'est absurde, donc $\operatorname{ord} a = m$. Puis $m = \operatorname{ord} a \mid p - 1$ donc p est un terme de la suite $(1 + km)_{k\in\mathbf{N}}$. Si cette suite n'a qu'un nombre fini de nombres premiers $p_1, \cdots, p_s$ alors pour k assez grand, $\mu_m(kp_1 \cdots p_s) > 2$. On a aussi $\mu_m(0) = \pm 1$ (entier de module 1) donc si p est un premier qui divise $\mu_m(kp_1 \cdots p_s)$ et p est parmi les p_i alors $p \mid \mu_m(0)$ absurde, donc p n'est pas parmi les p_i et la suite a une infinité de termes premiers.

c) Irréductibilité

Nous allons montrer que les polynômes cyclotomiques sont irréductibles par un argument de Landau.

On note α une racine primitive n-ième de l'unité et P son polynôme minimal. La suite $(P(\alpha^k))_{k\in\mathbf{N}}$ est n-périodique à valeurs dans $\mathbf{Z}[\alpha]$ et chacun des termes s'écrit de manière unique $Q_k(\alpha)$ pour un polynôme Q_k de degré $< \deg P$.

On note A le plus grand coefficient de tous les Q_k en valeurs absolues. Dans $\mathbf{Z}_p[X]$, $P(X^p) = P(X)^p$ (Frobenius) donc il existe $U \in \mathbf{Z}[X]$ tel que

$$P(X^p) = P(X)^p + pU(X)$$

Pour $p > A$,

$$P(\alpha^p) = P(\alpha)^p + pU(\alpha) = pU(\alpha) = pV(\alpha) \quad \text{avec } \deg V < \deg P$$

donc

$$Q_p(\alpha) = pV(\alpha) \qquad \text{et} \qquad P \mid Q_p - pV$$

et donc

$$Q_p = pV$$

d'où $p \mid$ les coefs de Q_p qui sont de module $\leqslant A < p$ donc $Q_p = 0$ et $P(\alpha^p) = 0$. Ici, on s'est seulement servis du fait que α est une racine de l'unité, donc si $p_1, \cdots, p_r$ sont $> A$ alors $P(\alpha^{p_1 \cdots p_r}) = 0$.

On note m premier avec n, N le produit des premiers $\leqslant A$. On a $m + nN = m \pmod n$ et si p divise $m + nN$ alors $p > A$ donc $P(\alpha^{m+nN}) = 0 = P(\alpha^m)$

Ainsi les (α^m) avec $m \wedge n = 1$ sont racines de P donc $\mu_n(X) \mid P(X)$. $\mu_n(\alpha) = 0$ donc P divise μ_m, donc $P = \mu_m$. C'est un polynôme minimal donc irréductible.

11 Nombres algébriques

Si $K \subset L$ sont deux corps alors on dit que $a \in L$ est algébrique sur K s'il existe $P \in \mathbf{K}[X]$ non nul tel que $P(a) = 0$.

Dans $\mathbf{C}$, on appelle nombre algébrique les nombres algébriques sur $\mathbf{Q}$ et on note A l'ensemble de ces nombres.

Remarque.

Si a est algébrique sur un corps K alors

$$I_a = \{P \in \mathbf{K}[X] \ / \ P(a) = 0\}$$

est un idéal non réduit à $\{0\}$ de $K[X]$ euclidien donc principal, donc il existe un unique polynôme unitaire $\mu_a(X)$ tel que $I_a = \mu_a K[X]$, que l'on appelle polynôme minimal de a. Dans ce cas

$$\operatorname{Vect}_K r((a^k)_{k\in\mathbf{N}}) = \operatorname{Vect}_K(1, a, \cdots, a^{\deg \mu_a - 1}) = \{P(a), P \in K[X]\}$$

a) Structure de corps

Résultat.

A est un corps

Démonstration. • $A \subset \mathbf{C}$

- $1 \in A$ en tant que racine de $X - 1$
- Soient $x, y \in A$, $p = \deg \mu_x, q = \deg \mu_y$. Pour tout $n \in \mathbf{N}$,

$$\begin{cases} x^n \in \mathrm{Vect}_{\mathbf{Q}}(1, x, \cdots, x^{p-1}) \\ y^n \in \mathrm{Vect}_{\mathbf{Q}}(1, y, \cdots, y^{q-1}) \end{cases} \qquad \text{donc} \qquad x^n y^n, (x+y)^n \in \mathrm{Vect}_{\mathbf{Q}}(x^i y^j, i < q, j < q)$$

  Les familles $((x-y)^n)_n$ et $((xy)^n)_n$ sont liées donc $x - y, xy \in A$.
- Si $x \in A$ non nul et si on note $E = \mathrm{Vect}_{\mathbf{Q}}(1, x, \cdots, x^{p-1})$ alors

$$\varphi : z \in E \longmapsto xz \in E$$

  est un endomorphisme injectif en dimension finie donc c'est un isomorphisme et $\varphi^{-1}(1)$ donne $x^{-1} \in E \subset A$

□

b) Règle de multiplicativité des degrés

On note a algébrique sur $\mathbf{K}$ de degré d.

$$\varphi : P \in \mathbf{K}[X] \longmapsto P(a)$$

est un morphisme de $\mathbf{K}$-algèbres donc $\mathrm{Im}\,\varphi = \mathrm{Vect}_{\mathbf{K}}(1, \cdots, a^{p-1})$ est une $\mathbf{K}$-algèbre, notée $\mathbf{K}[a]$.

$\mathbf{K}[d]$ est une algèbre de dimension finie d sur $\mathbf{K}$ et pour $x \in \mathbf{K}[a] \setminus \{0\}$,

$$\psi : y \in \mathbf{K}[a] \longmapsto xy \in \mathbf{K}[a]$$

est un endomorphisme injectif en dimension finie donc c'est un automorphisme et x a un inverse dans $\mathbf{K}[a]$, qui est donc un corps.

Définition.

Si $K \subset L$ alors L est un K-ev et si L est de dimension finie sur K alors on note

$$[L : K] = \dim_K(L)$$

Proposition.

1. Soit $K \subset L \subset N$ trois corps. Si $\dim_L N, \dim_K L < +\infty$ alors $\dim_K N < +\infty$ et

$$[N : K] = [N : L] \times [L : K]$$

2. Si $a \in \mathbf{C}$ est algébrique et si $b \in K$ est algébrique sur $\mathbf{Q}[a]$ alors b est algébrique sur $\mathbf{Q}$.

Démonstration.

1. $(n_1, \cdots, n_p)$ base de N sur L, $(\ell_1, \cdots, \ell_q)$ base de L sur K. Si $n \in \mathbf{N}$ alors il existe $\lambda_1, \cdots, \lambda_p \in L$ tel que $n = \lambda_1 n_1 + \cdots + \lambda_p n_p$ et chaque $\lambda_i \in \mathrm{Vect}_{\mathbf{Q}}(\ell_1, \cdots, \ell_p)$ donc $n \in \mathrm{Vect}_{\mathbf{Q}}(\ell_i n_j)$ (famille génératrice finie) donc
$$[N : K] < +\infty$$
   Vérifions que $(\ell_i n_j)_{\substack{1 \leqslant i \leqslant q \\ 1 \leqslant j \leqslant p}}$ est libre sur $\mathbf{Q}$.
$$\sum_{i,j} \lambda_{i,j} \ell_i n_j = 0 \implies \sum_{j=1}^{p} n_j \sum_{i=1}^{q} \lambda_{i,j} \ell_i = 0 \implies \forall j \in [\![1, p]\!], \sum_{i=1}^{q} \lambda_{i,j} \ell_i = 0 \implies \forall i, j, \lambda_{i,j} = 0$$
2. C'est une conséquence directe de 1.

□

Remarque.

Si b est racine d'une équation polynômiale à coefficients dans $\mathbf{Q}[a]$, il l'est aussi d'une équation polynômiale à coefficients dans $\mathbf{Q}$.

12 Polynômes orthogonaux

On note $p : I \longrightarrow \mathbf{R}_+^\star$ continue telle que pour tout entier naturel k, $t \longmapsto t^k p(t)$ est intégrable sur I. Dans ce cas,

$$(P|Q) = \int_I p(t)P(t)Q(t)\ \mathrm{d}t$$

est bien définit et est un produit scalaire sur $\mathbf{R}[X]$

Proposition.

Il existe une unique famille $(P_k)_k$ de polynômes unitaires tels que

- $\forall k \in \mathbf{N}, \quad \deg P_k = k$
- Les P_k sont deux à deux orthogonaux

Démonstration. Le procédé de Gram-Schmidt appliqué à la base canonique donne l'existence. Si (P_k) convient alors

- $P_0 = 1$ (unitaire de degré 0)
- Si $P_0, \cdots, P_k$ conviennent, alors

$$P_{k+1} = \underbrace{X^{k+1}}_{\text{unitaire}} + \underbrace{\lambda_0 P_0 + \cdots + \lambda_k P_k}_{\deg\leqslant k \text{ se décompose sur } P_0,\cdots,P_k}$$

et l'orthogonalité détermine de manière unique les λ_i

□

a) Récurrence d'ordre 2

Proposition.

La famille des $(P_n)_n$ vérifie pour $n \geqslant 2$

$$P_n(X) = -(X + \lambda_{n-1})P_{n-1}(X) - \mu_{n-2}P_{n-2}(X) = 0$$

avec

$$\lambda_{n-1} = -\frac{(XP_{n-1}|P_{n-1})}{\|P_{n-1}\|^2}, \quad \mu_{n-2} = -\frac{\|P_{n-1}\|^2}{\|P_{n-2}\|^2}$$

Démonstration. On note $E_i = \mathbf{R}_i[X]$. Pour $Q \in \mathrm{Vect}(P_0, \cdots, P_{n-2}) = \mathbf{R}_{n-2}[X]$, $(XP_n|Q) = (P_n|XQ) = 0$ car $XQ \in \mathbf{R}_{n-1}[X]$. On a alors

$$P_n(X) - XP_{n-1}(X) \in E_{n-3}^\perp$$

or $\deg(P_n - XP_{n-1}) \leqslant n-1$ (simplification du coef dominant) donc

$$P_n(X) - XP_{n-1}(X) = \lambda_{n-1}P_{n-1}(X) + \cdots + \lambda_0 P_0(X)$$

et on a $P_n - XP_{n-1} \perp P_0, \cdots, P_{n-3}$ donc $\lambda_0 = \cdots = \lambda_{n-3} = 0$. On en déduit,

$$\lambda_{n-1}(P_{n-1}|P_{n-1}) = (P_n|P_{n-1}) - (XP_{n-1}|P_{n-1})$$

et

$$\lambda_{n-2}(P_{n-2}|P_{n-2}) = \underbrace{(P_n|P_{n-2})}_{=0} - (XP_{n-1}|P_{n-2}) = -(P_{n-1}| \underbrace{XP_{n-2}}_{P_{n-1}+\in E_{n-2}}) = -(P_{n-1}|P_{n-1})$$

d'où la conclusion avec $\mu_{n-2} = \lambda_{n-2}$ □

b) Changements de signes

On appelle changement de signe d'un polynôme un point x_0 tel que $(x-x_0)P(x)$ est de signe constant au voisinage de x_0. On note $N_I(P)$ le nombre de changements de signes de P sur l'intervalle I

Supposons $N_I(P_n)=p<n$. On note $x_1,\cdots,x_p$ les changements de signes et

$$(P_n|\underbrace{(X-x_1)\cdots(X-x_p)}_{\in E_{n-1}})=0=\int_I p(t)\underbrace{P_n(t)(t-x_1)\cdots(t-x_p)}_{\text{signe constant}}\,\mathrm{d}t$$

donc

$$\forall t\in I, p(t)P_n(t)(t-x_1)\cdots(t-x_p)=0$$

et P_n=0 absurde. Donc $N_I(P_n)=n$ et P_n est scindé à racines simples, toutes dans I.

c) Entrelacement des racines

On note

$$w_n(x)=\begin{vmatrix}P_n(x) & P_{n+1}(x)\\ P_n'(x) & P_{n+1}'(x)\end{vmatrix}=P_n(x)P_{n+1}'(x)-P_n'(x)P_{n+1}(x)$$

On a $w_0\equiv 1$ et après calcul avec la relation de récurrence,

$$w_n(x)=P_n(x)^2\underbrace{-\mu_{n-1}}_{>0}w_{n-1}(x)$$

donc comme $w_0>0$, on en déduit que pour tout x,n, $w_n(x)>0$. Notons $\alpha<\beta$ deux racines consécutives de P_{n+1}.

$$P_{n+1}'(\alpha)P_n(\alpha)>0 \qquad \text{et} \qquad P_{n+1}'(\beta)P_n(\beta)>0$$

or P_{n+1} de signe constant sur $]\alpha,\beta[$ et donc $P_{n+1}'(\alpha)P_{n+1}'(\beta)<0$ (car sinon il y aurait changement de signe). Ainsi, $P_n(\alpha)P_n(\beta)<0$ donc P_n s'annule sur $]\alpha,\beta[$. On a ainsi trouvé n racines de P_n, une entre chaque racine de P_{n+1} : il y a entrelacement des racines

13 Formules d'interpolation

a) Rappels

On considère $x_1,\cdots,x_n\in\mathbf{K}$ deux à deux distincts, et on note

$$\Delta_i(X)=\prod_{j\neq i}\frac{X-x_j}{x_i-x_j}$$

de telle manière que

$$\Delta_i(x_j)=\delta_{i,j}$$

Théorème.

On considère $x_1,\cdots,x_n,y_1,\cdots,y_n\in\mathbf{K}$, les x_i deux à deux distincts. Dans ce cas, il existe un unique polynôme $P\in\mathbf{K}_{n-1}[X]$ tel que

$$\forall i\in[\![1,n]\!],\quad P(x_i)=y_i$$

De plus,

$$P(X)=\sum_{i=1}^n y_i\Delta_i(X)$$

Démonstration. Le polynôme donné convient. Si P et Q conviennent, $P-Q$ a n racines et est de degré au plus $n-1$ donc $P=Q$. □

Remarque.

Si on note

$$\omega(x) = \prod_{j=1}^{n} (x - x_j)$$

alors

$$\prod_{j \neq i} (x_i - x_j) = \lim_{x \to x_i} \frac{\omega(x) - \omega(x_i)}{x - x_i} = w'(x_i)$$

et

$$\Delta_i(x) = \frac{\omega(x)}{\omega(x_i)(x - x_i)}$$

donc

$$P(x) = \underbrace{\left(\sum_{i=1}^{n} \frac{y_i}{\omega'(x_i)(x - x_i)} \right)}_{\text{DSE de } \frac{P(x)}{\omega(x)}} \omega(x)$$

b) Formules d'ordre supérieur

On se donne $n_1, \cdots, n_r \in \mathbf{N}^\star$, $x_1, \cdots, x_r \in \mathbf{K}$ deux à deux distincts et $n = n_1 + \cdots + n_r$.

$$\varphi : P \in \mathbf{K}_{n-1}[X] \longmapsto (P(x_1), \cdots, P^{(n_1-1)}(x_1), \cdot, P(x_r), \cdots, P^{(n_r-1)}) \in \mathbf{K}^n$$

est une application linéaire injective, il y a égalité des dimensions donc c'est un isomorphisme et on en déduit que pour $(y_{i,k})_{i \leqslant r, j \leqslant n_i}$ donné, il existe un unique polynôme de degré au plus $n - 1$ tel que

$$\forall i, k, P^{(k)}(x_i) = y_{i,k}$$

c) Analyse de l'erreur

On se donne $f \in \mathbf{C}^n([a, b], \mathbf{R}), x_1, \cdots, x_n \in [a, b]$ deux à deux distincts.

$$P(x) = \sum_{i=1}^{n} f(x_i)\Delta_i(x)$$

l'interpolation de Lagrange de f. On veut estimer $f(x) - P(x)$. On note $x \in [a, b] \setminus \{x_1, \cdots, x_r\}$ et on note

$$g(t) = f(t) - P(t) - \lambda_x \omega(t)$$

où λ_x tel que $g(x) = 0$ (ajout d'une racine supplémentaire). Rolle itéré donne :

- g s'annule en $x_1, \cdots, x_n, x$ ($n + 1$ points)
- $\cdots$
- $g^{(n)}$ s'annule au moins une fois en c_n

$$0 = f^{(n)}(c_n) - P^{(n)}(c_n) - \lambda_x n!$$

donc $\lambda_x = \dfrac{f^{(n)}(c_n)}{n!}$ et donc

$$|f(x) - P(x)| = |\lambda_x \omega(x)| \leqslant |\omega(x)| \sup_{[a,b]} \frac{|f^{(n)}|}{n!}$$

cette inégalité est encore vraie pour $x \in \{x_1, \cdots, x_n\}$

Remarque.

On constate que l'erreur est meilleure si

$$|\omega(x)| = |(x - x_1) \cdots (x - x_n)|$$

est petit. On peut donc s'intéresser aux choix des x_i minimisant $\|\omega\|_\infty$ sur $[a, b]$. C'est un problème difficile, mais le choix de $x_1, \cdots, x_n$ équirépartis est mauvais.

14 Suites de polynômes

Théorème (Weierstrass).

Si f est continue de $[a,b]$ dans $\mathbf{C}$ alors il existe une suite (P_n) de fonctions polynômiales telle que

$$P_n \xrightarrow[{[a,b]}]{CVU} f$$

Idée de la preuve. Bernstein puis convolution □

Remarque.

Le résultat est faux sur un intervalle autre qu'un segment.

a) Inégalité de Bernstein

Lemme.

Si $z_1, \cdots, z_n$ sont les racines du polynôme z^n+1 et P polynôme réel de degré n, alors pour tout $t \in \mathbf{C}$,

$$tP'(t) = \frac{n}{2}P(t) + \frac{1}{n}\sum_{k=1}^{n} P(-z_k)\frac{2z_k}{(z_k-1)^2}$$

Démonstration. On note $\varphi(z,t) = \frac{P(tz)-P(t)}{z-1}$ pour $z \neq 1$. C'est une fonction polynomiale de degré $\leqslant n-1$ pour t fixé.

D'après la formule d'interpolation de Lagrange en $z_1, \cdots, z_n$,

$$\begin{aligned}\varphi(z,t) &= \sum_{k=1}^{n} \varphi(z_k,t)\frac{z^n+1}{z-z_k} \times \underbrace{\frac{1}{(z_k-z_1)\cdots\widehat{(z_k-z_k)}\cdots(z_k-z_n)}}_{=\lim\limits_{z\to z_k}\frac{z-z_k}{z^n+1}=\frac{1}{nz_k^{n-1}}=-\frac{z_k}{n}} \\ &= \sum_{k=1}^{n} -\varphi(z_k,t) \times \frac{z^n+1}{z-z_k}\frac{z_k}{n}\end{aligned}$$

On fait tendre z vers 1.

$$tP'(t) = \sum_{k=1}^{n} \varphi(z_k,t)\frac{2}{z_k-1}\frac{z_k}{n} = \frac{1}{n}\sum_{k=1}^{n} P(-tz_k)\frac{2z_k}{(z_k-1)^2} - \frac{P(t)}{n}\sum_{k=1}^{n}\frac{2z_k}{(z_k-1)^2}$$

Il nous reste à évaluer ce dernier terme. On reprend la formule précédente avec $P(t) = t^n$.

$$nt^n = \frac{1}{n}\sum_{k=1}^{n} 2t^n\frac{z_k^{n+1}}{(z_k-1)^2} - \frac{t^n}{n}\sum_{k=1}^{n}\frac{2z_k}{(z_k-1)^2} \underset{z_k^{n+1}=-z_k}{=} -\frac{2t^n}{n}\sum_{k=1}^{n}\frac{2z_k}{(z_k-1)^2}$$

Et alors,

$$\sum_{k=1}^{n}\frac{2z_k}{(z_k-1)^2} = -\frac{n^2}{2}$$

ce qui termine la preuve de la formule. □

Résultat.

On note pour $P \in \mathbf{R}[X]$, $\|P\| = \sup\limits_{|z|=1}|P(z)|$. Si P est de degré n alors

$$\|P'\| \leqslant n\|P\|$$

Démonstration. On prend t de module 1,

$$|tP'(t)| = |P'(t)| \leqslant \frac{n}{2}|P(t)| + \frac{1}{n}\sum_{k=1}^{n}\left|\frac{2z_k}{(z_k-1)^2}\right| \times \|P\|$$

Et $z_k \in \mathbb{U}$ donc s'écrit $z = e^{i\theta}$ et donc ($\theta \in]0, 2\pi[$)

$$\frac{2z_k}{(z_k-1)^2} = \frac{2}{(e^{i\frac{\theta}{2}} - e^{-i\frac{\theta}{2}})^2} = \frac{2}{-4\sin^2\frac{\theta}{2}} < 0$$

et

$$\sum_{k=1}^{n} \left| \frac{2z_k}{(z_k-1)^2} \right| = -\sum_{k=1}^{n} \frac{2z_k}{(z_k-1)^2} = \frac{n^2}{2}$$

ce qui termine la preuve. □

b) Théorème d'oscillation de Tchebychev

On note C_n le n-ième polynôme de Tchebychev et $T_n = \dfrac{C_n}{2^{n-1}}$ de sorte que T_n est unitaire.

Résultat.

> Pour tout P unitaire de degré n,
>
> $$\frac{1}{2^{n-1}} = \max_{[-1,1]} |T_n| \leqslant \max_{[-1,1]} |P|$$

Démonstration.

$$T_n(\cos\theta) = \frac{1}{2^{n-1}}\cos(n\theta) \implies \max_{[-1,1]} |T_n| = \frac{1}{2^{n-1}}$$

Supposons par l'absurde que $\max\limits_{[-1,1]} |P| < \dfrac{1}{2^{n-1}}$ et posons

$$Q(X) = T_n(X) - P(X)$$

Pour $x_k = \cos\left(\frac{k\pi}{n}\right), k \in [\![0, n]\!]$, on a

$$T_n(x_k) = \frac{(-1)^k}{2^{n-1}}$$

d'où on tire le tableau de signes

x	x_0		x_1		x_2		$\cdots$		x_n
$Q(x)$	$+$	0	$-$	0	$+$	0	$\cdots$	0	$(-1)^n$

On en déduit que Q s'annule au moins n fois et $\deg Q \leqslant n-1$ donc $Q = 0$, donc $P = T_n$ absurde. □

15 Aspects topologiques

a) Le théorème de Baire

Résultat.

> $(E, \|\ \|)$ un e.v.n tel que toute suite de Cauchy converge (complet). Si $(O_n)_n$ est une suite d'ouverts denses de E alors $\cap O_n$ est dense.

Démonstration. On note U ouvert de E.

- $U \cap O_0$ est un ouvert non vide donc il existe $x_0 \in U \cap O_0$ et $2a_0 > 0$ tel que $\mathscr{B}_o(x_o, 2a_o) \subset U \cap O_0$ et donc $\mathscr{B}_f(x_0, a_0) \subset U \cap O_0$. On note $r_0 = \min(a_0, 1)$.
- $\mathscr{B}_o(a_0, r_0) \cap O_1$ ouvert non vide donc il existe x_1 et $a_1 > 0$ tels que $\mathscr{B}_f(x_1, a_1) \subset \mathscr{B}_0(x_0, r_0) \cap O_1$ et on note $r_1 = \min\left(a_1, \frac{1}{2}\right)$
- $\cdots$

On construit ainsi deux suites $(x_n)_n \in E^{\mathbf{N}}$, $(r_n) \in {\mathbf{R}_+^\star}^{\mathbf{N}}$ telles que

$$\begin{cases} \mathscr{B}_f(x_n, r_n) \subset \mathscr{B}_f(x_{n-1}, r_{n-1}) \subset \cdots \subset \mathscr{B}_f(x_0, r_0) \\ \mathscr{B}_f(x_n, r_n) \subset O_n, \quad r_n \leqslant \dfrac{1}{n} \end{cases}$$

Pour $m > n$, $x_m \in \mathscr{B}_f(x_m, r_m) \subset \mathscr{B}_f(x_n, r_n)$ donc

$$\|x_m - x_n\| \leqslant \frac{1}{n}$$

donc (x_n) de Cauchy donc convergente vers x.

Pour m fixé, APCR $x_n \in \mathscr{B}_f(x_m, r_m)$ fermé donc $x \in \mathscr{B}_f(x_m, r_m) \subset O_m$ donc $x \in O_m$ pour tout m. Ainsi,

$$x \in \bigcap_{n \in \mathbf{N}} O_n$$

et $x \in \mathscr{B}_f(x_0, r_0) \subset U$ donc $x \in U$ et donc

$$U \cap \left(\bigcap_{n \in \mathbf{N}} O_n \right)$$

pour tout ouvert U.

Corollaire.

Si $(F_n)_n$ est une suite de fermés d'intérieurs vides alors

$$\bigcup_{n \in \mathbf{N}} F_n$$

est d'intérieur vide.

□

b) Incomplétude de $\mathbf{R}[X]$

On supose qu'il existe une norme $\|\cdot\|$ telle que $(\mathbf{R}[X], \|\cdot\|)$ est complet (i.e. toutes les suites de Cauchy convergent)

- $E_n = \mathrm{Vect}(1, \cdots, X^n)$ est un fermé (s.e.v. de dimension finie)
- $$\forall P \in E_n, \forall \varepsilon > 0, \quad P + \frac{X^{n+1}}{k} \xrightarrow[k \to +\infty]{} P$$

  donc APCR

  $$P + \frac{X^{n+1}}{k} \in \mathscr{B}_0(P, \varepsilon)$$

  donc $\mathscr{B}_o(P, \varepsilon) \not\subset E_n$ et E_n d'intérieur vide.
- Par le théorème de Baire,

  $$\underbrace{\bigcap_{n \in \mathbf{N}} E_n}_{\text{intérieur vide}} = \underbrace{\mathbf{R}[X]}_{\text{intérieur non vide}}$$

  absurde.

Il n'existe donc aucune norme pour laquelle $\mathbf{R}[X]$ est complet.

En particulier, $(X_k)_k$ est une base qu'on peut orthonormaliser par le procédé de Gram-Schmidt en une base $(P_k)_k$ qui est totale, sans que $\mathbf{R}[X]$ soit complet.

⋆ ⋆ ⋆ ⋆

⋆ ⋆ ⋆ ⋆ ⋆

Index