

# Agrégation 2024

Développements

Document intégralement écrit par Hugo Delaunay.  
Visitez [agreg.skyost.eu](http://agreg.skyost.eu) pour plus de ressources et d'informations.

*Une coquille? Une correction à apporter?* Rendez-vous sur le dépôt Github “Skyost/Agregation” ou contactez-moi  
via mon site web personnel [skyost.eu](http://skyost.eu).

# Table des matières

1	Caractérisation réelle de la fonction $\Gamma$ . . . . .	1
2	Connexité des valeurs d'adhérence d'une suite dans un compact . . . . .	4
3	Critère d'Eisenstein . . . . .	7
4	Décomposition de Dunford . . . . .	10
5	Décomposition polaire . . . . .	12
6	Densité des polynômes orthogonaux . . . . .	15
7	Développement asymptotique de la série harmonique . . . . .	18
8	Dimension du commutant . . . . .	22
9	Dual de $L_p$ . . . . .	25
10	Équation de Sylvester . . . . .	28
11	Équivalence des normes en dimension finie et théorème de Riesz . . . . .	30
12	Formes de Hankel . . . . .	33
13	Formule de Stirling . . . . .	35
14	Formule sommatoire de Poisson . . . . .	38
15	$\exp : \mathcal{S}_n(\mathbb{R}) \rightarrow \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme . . . . .	40
16	Intégrale de Dirichlet . . . . .	43
17	Lemme de Morse . . . . .	46
18	Loi d'inertie de Sylvester . . . . .	49
19	Méthode de Newton . . . . .	51
20	Nombres de Bell . . . . .	54
21	Projection sur un convexe fermé . . . . .	56
22	Simplicité de $A_n$ pour $n \geq 5$ . . . . .	60
23	Suite de polygones . . . . .	63
24	$\exp : \mathcal{M}_n(\mathbb{R}) \rightarrow \text{GL}_n(\mathbb{R})$ est surjective . . . . .	66
25	Théorème central limite . . . . .	69
26	Théorème chinois . . . . .	72
27	Théorème d'Abel angulaire . . . . .	75
28	Théorème de Cauchy-Lipschitz linéaire . . . . .	78
29	Théorème de Dirichlet faible . . . . .	82
30	Théorème de Fejér . . . . .	84
31	Théorème de Frobenius-Zolotarev . . . . .	87
32	Théorème de Kronecker . . . . .	90
33	Premier théorème de Sylow . . . . .	93
34	Théorème de Wantzel . . . . .	96
35	Théorème de Wedderburn . . . . .	101
36	Théorème de Weierstrass (par la convolution) . . . . .	104

37	Théorème de Weierstrass (par les probabilités) . . . . .	107
38	Théorème des deux carrés de Fermat . . . . .	109
39	Théorème des événements rares de Poisson . . . . .	112
40	Transformée de Fourier d'une gaussienne . . . . .	115
41	Trigonalisation simultanée . . . . .	118

# 1 Caractérisation réelle de la fonction $\Gamma$

On montre que la fonction  $\Gamma$  d'Euler est la seule fonction log-convexe sur  $\mathbb{R}^+$  prenant la valeur 1 en 1 et vérifiant  $\Gamma(x+1) = x\Gamma(x)$  pour tout  $x > 0$ .

**Lemme 1.** La fonction  $\Gamma$  définie pour tout  $x > 0$  par  $\Gamma(x) = \int_0^{+\infty} t^{x-1} e^{-t} dt$  vérifie :

- (i)  $\forall x \in \mathbb{R}_*^+, \Gamma(x+1) = x\Gamma(x)$ .
- (ii)  $\Gamma(1) = 1$ .
- (iii)  $\Gamma$  est log-convexe sur  $\mathbb{R}_*^+$ .

[ROM19-1]  
p. 364

*Démonstration.* (i) Soit  $x \in \mathbb{R}_*^+$ . Alors :

$$\begin{aligned}\Gamma(x+1) &= \int_0^{+\infty} t^x e^{-t} dt \\ &= \left[ -e^{-t} t^x \right]_0^{+\infty} + x \int_0^{+\infty} t^{x-1} e^{-t} dt \\ &= x\Gamma(x)\end{aligned}$$

- (ii) Comme  $t \mapsto e^{-t} \mathbb{1}_{\mathbb{R}^+}(t)$  est la densité de probabilité d'une loi exponentielle de paramètre 1, on a

$$\underbrace{\int_0^{+\infty} e^{-t} dt}_{=\Gamma(1)} = 1$$

- (iii) Soient  $x, y \in \mathbb{R}_*^+$  et  $\lambda \in ]0, 1[$ . On applique l'inégalité de Hölder en posant  $\lambda = \frac{1}{p}$  et  $1 - \lambda = \frac{1}{q}$  :

$$\begin{aligned}\Gamma(\lambda x + (1-\lambda)y) &= \int_0^{+\infty} e^{-t} t^{\lambda x} t^{(1-\lambda)y} dt \\ &= \int_0^{+\infty} (e^{-t} t^{x-1})^{\frac{1}{p}} (e^{-t} t^{y-1})^{\frac{1}{q}} dt \\ &\leq \left( \int_0^{+\infty} e^{-t} t^{x-1} \right)^{\frac{1}{p}} \left( \int_0^{+\infty} e^{-t} t^{y-1} \right)^{\frac{1}{q}} \\ &= \Gamma(x)^\lambda \Gamma(y)^{1-\lambda}\end{aligned}$$

Donc  $\ln \circ \Gamma$  vérifie bien l'inégalité de convexité sur  $\mathbb{R}_*^+$  et ainsi,  $\Gamma$  est log-convexe. □

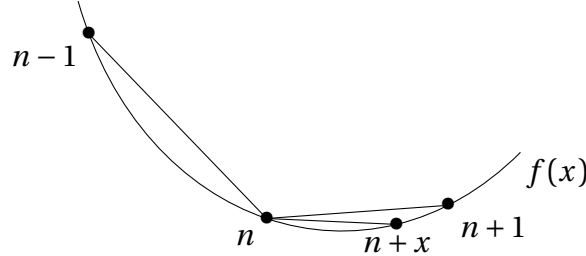
**Théorème 2** (Bohr-Mollerup). Soit  $f : \mathbb{R}_*^+ \rightarrow \mathbb{R}^+$  vérifiant le Point (i), le Point (ii) et le Point (iii) du Théorème 1. Alors  $f = \Gamma$ .

*Démonstration.* Par récurrence, on a d'après le Point (i) :

$$\forall n \in \mathbb{N}^*, \forall x \in ]0, 1], f(x+n) = (x+n-1) \dots (x+1) x f(x) \quad (*)$$

Donc les valeurs prises par  $f$  sur  $\mathbb{R}_*^+$  sont entièrement déterminées par ses valeurs prises sur  $]0, 1]$ . Ainsi, pour démontrer le théorème, il suffit de vérifier  $\forall x \in ]0, 1], f(x) = \Gamma(x)$ .

Soient donc  $x \in ]0, 1]$  et  $n \in \mathbb{N}^*$  ; on applique le lemme des trois pentes à la fonction convexe  $\ln \circ f$  (d'après le Point (iii)) appliqué aux points  $n-1, n, n+x$  et  $n+1$  :



$$\frac{(\ln \circ f)(n) - (\ln \circ f)(n-1)}{n - (n-1)} \leq \frac{(\ln \circ f)(n+x) - (\ln \circ f)(n)}{n+x - n} \leq \frac{(\ln \circ f)(n+1) - (\ln \circ f)(n)}{n+1 - n}$$

Mais, d'après (\*) et le Point (ii), on a  $f(n) = (n-1)!$ . D'où :

$$\begin{aligned} \ln(n-1) &\leq \frac{(\ln \circ f)(n+x) - \ln((n-1)!)}{x} \leq \ln(n) \\ \Rightarrow \ln((n-1)^x) &\leq (\ln \circ f)(n+x) - \ln((n-1)!) \leq \ln(n^x) \\ \Rightarrow \ln((n-1)^x (n-1)!) &\leq (\ln \circ f)(n+x) \leq \ln(n^x (n-1)!) \end{aligned}$$

Par croissance de la fonction  $\ln$ , cela donne :

$$(n-1)^x (n-1)! \leq f(n+x) \leq n^x (n-1)!$$

Et en appliquant (\*), on obtient :

$$\frac{(n-1)^x (n-1)!}{(x+n-1) \dots (x+1)x} \leq f(x) \leq \frac{n^x (n-1)!}{(x+n-1) \dots (x+1)x}$$

En ne considérant que la première inégalité, on peut remplacer  $n$  par  $n+1$  (car les deux inégalités sont vraies pour tout  $n \in \mathbb{N}^*$ ) :

$$\frac{n^x n!}{(x+n) \dots (x+1)x} \leq f(x)$$

Or,  $\frac{n^x (n-1)!}{(x+n-1) \dots (x+1)x} = \frac{n^x n!}{(x+n) \dots (x+1)x} \frac{x+n}{n}$ , donc :

$$\begin{aligned} \frac{n^x n!}{(x+n) \dots (x+1)x} &\leq f(x) \leq \frac{n^x n!}{(x+n) \dots (x+1)x} \frac{x+n}{n} \\ \Rightarrow f(x) \frac{n}{x+n} &\leq \frac{n^x n!}{(x+n) \dots (x+1)x} \leq f(x) \\ \Rightarrow f(x) &= \lim_{n \rightarrow +\infty} \frac{n^x n!}{(x+n) \dots (x+1)x} \end{aligned}$$

en faisant  $n \rightarrow +\infty$  dans la deuxième implication. Comme  $\Gamma$  vérifie le Point (i), le Point (ii), et le

Point (iii); le raisonnement précédent est a fortiori vrai aussi pour  $\Gamma$ . Donc

$$\Gamma(x) = \lim_{n \rightarrow +\infty} \frac{n^x n!}{(x+n) \dots (x+1)x} = f(x)$$

ie.  $f$  et  $\Gamma$  coïncident bien sur  $]0, 1]$ . □

*Remarque 3.* À la fin de la preuve, on obtient une formule due à Gauss :

$$\forall x \in ]0, 1], \Gamma(x) = \lim_{n \rightarrow +\infty} \frac{n^x n!}{(x+n) \dots (x+1)x}$$

que l'on peut aisément étendre à  $\mathbb{R}_*^+$  entier.

La preuve, telle qu'elle est écrite ici, est issue d'un livre de Walter Rudin. Elle est également disponible (sous une forme un peu différente) comme l'indique la référence, dans **[ROM19-1]**.

## 2 Connexité des valeurs d'adhérence d'une suite dans un compact

On montre que l'ensemble des valeurs d'adhérence d'une suite d'un espace métrique compact est connexe en raisonnant par l'absurde, puis on utilise ce résultat pour démontrer le lemme des grenouilles.

Soit  $(E, d)$  un espace métrique.

[I-P]  
p. 116

**Théorème 1.** On suppose  $E$  compact. Soit  $(u_n)$  une suite de  $E$  telle que  $d(u_n, u_{n-1}) \rightarrow 0$ . Alors l'ensemble  $\Gamma$  des valeurs d'adhérence de  $(u_n)$  est connexe.

*Démonstration.* Pour tout  $p \in \mathbb{N}$ , on note  $A_p = \{u_n \mid n \geq p\}$ . On a  $\Gamma = \bigcap_{p \in \mathbb{N}} \overline{A_p}$ .  $\Gamma$  est fermé (en tant qu'intersection de fermés) dans  $E$  qui est compact, donc  $\Gamma$  est compact. Supposons que  $\Gamma$  soit non connexe; on peut alors écrire  $\Gamma = A \sqcup B$ , où  $A$  et  $B$  sont deux fermés disjoints de  $\Gamma$ . Comme  $\Gamma$  est compact,  $A$  et  $B$  le sont aussi. Notons  $\alpha = d(A, B) > 0$  (car  $A \cap B = \emptyset$ ). Posons :

$$A' = \left\{ x \in E \mid d(x, A) < \frac{\alpha}{3} \right\} \text{ et } B' = \left\{ x \in E \mid d(x, B) < \frac{\alpha}{3} \right\}$$

$A'$  et  $B'$  sont ouverts (en tant qu'images réciproques d'ouverts par des application continues), donc  $K = E \setminus (A' \cup B')$  est fermé dans  $E$ , donc compact.

Montrons que  $(u_n)$  admet une valeur d'adhérence dans  $K$ , ce qui serait absurde car  $\Gamma \cap K = \emptyset$ . Comme  $\lim_{n \rightarrow +\infty} d(u_n, u_{n-1}) = 0$ ,

$$\exists N_0 \in \mathbb{N} \text{ tel que } \forall n \geq N_0, d(u_n, u_{n-1}) < \frac{\alpha}{3} \quad (*)$$

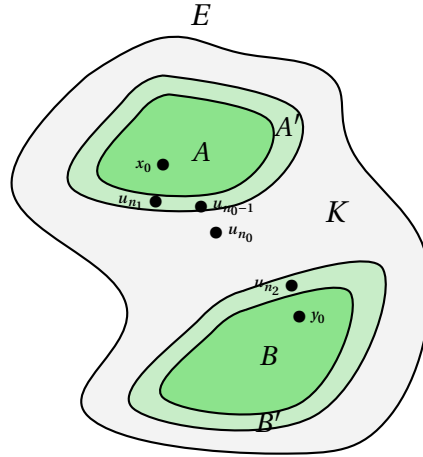
Soit  $N \geq N_0$ .

— Soit  $x_0 \in A$ . Comme  $x_0$  est valeur d'adhérence de  $(u_n)$ ,  $\exists n_1 > N$  tel que  $d(x_0, u_{n_1}) < \frac{\alpha}{3}$ . Donc  $u_{n_1} \in A'$ .

— Soit  $y_0 \in B$ . De même,  $\exists n_2 > n_1$  tel que  $d(y_0, u_{n_2}) < \frac{\alpha}{3}$ . Donc  $u_{n_2} \in B'$ .

Soit maintenant  $n_0$  le premier entier supérieur à  $n_1$  tel que  $u_{n_0} \notin A'$  (un tel entier existe car  $u_{n_2} \notin A'$ ). On a alors  $u_{n_0-1} \in A'$ .





D'après (\*), en appliquant l'inégalité triangulaire,

$$\begin{aligned}
 d(u_{n_0}, B) &\geq d(u_{n_0-1}, B) - d(u_{n_0-1}, u_{n_0}) \\
 &\geq d(A, B) - d(u_{n_0-1}, A) - d(u_{n_0-1}, u_{n_0}) \\
 &> \frac{\alpha}{3}
 \end{aligned}$$

ce qui prouve que  $u_{n_0} \notin B'$ . Comme  $u_{n_0} \notin A'$ , on a  $u_{n_0} \in K$ . On vient de montrer que,

$$\forall N \geq N_0, \exists n_0 \geq N \text{ tel que } u_{n_0} \in K$$

On peut créer comme cela une sous-suite de  $(u_n)$  dans  $K$ . Or  $K$  est compact, donc  $(u_n)$  admet une valeur d'adhérence dans  $K$ .  $\square$

**Application 2** (Lemme de la grenouille). Soient  $f : [0, 1] \rightarrow [0, 1]$  continue et  $(x_n)$  une suite de  $[0, 1]$  telle que

$$\begin{cases} x_0 \in [0, 1] \\ x_{n+1} = f(x_n) \end{cases}$$

Alors  $(x_n)$  converge si et seulement si  $\lim_{n \rightarrow +\infty} x_{n+1} - x_n = 0$ .

*Démonstration.* Le sens direct est évident. Montrons la réciproque. On suppose donc que  $\lim_{n \rightarrow +\infty} x_{n+1} - x_n = 0$  et on note  $\Gamma$  l'ensemble des valeurs d'adhérence de  $(x_n)$ .  $\Gamma$  est non vide (car  $(x_n)$  est bornée, donc admet une valeur d'adhérence par le théorème de Bolzano-Weierstrass) et est un connexe de  $\mathbb{R}$  (par le Théorème 1), donc  $\Gamma$  est un intervalle non vide.

Soit  $a \in \Gamma$ . Il existe  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  strictement croissante (on dit que  $\varphi$  est une extractrice) telle que  $x_{\varphi(n)} \rightarrow a$ . Mais alors,

$$x_{\varphi(n)+1} - x_{\varphi(n)} = f(x_{\varphi(n)}) - x_{\varphi(n)} \rightarrow f(a) - a$$

et par hypothèse, le membre de gauche converge vers 0. Donc  $f(a) - a = 0$  ie.  $a$  est un point fixe de  $f$ .

Supposons par l'absurde que  $(x_n)$  diverge. Alors  $\Gamma$  n'est pas un singleton, donc est un intervalle

d'intérieur non vide : on peut trouver  $c \in \Gamma$  et  $h > 0$  tel que  $[c - h, c + h] \subseteq \Gamma$ .

Or,  $c \in \Gamma$ , donc

$$\exists N \geq 0 \text{ tel que } |x_N - c| \leq \frac{h}{2} \implies x_N \in \Gamma$$

et en particulier,  $x_N$  est un point fixe de  $f$ . Ainsi,  $x_{n+1} = f(x_n) = x_n$  pour tout  $n \geq N$  : absurde.  $\square$

### 3 Critère d'Eisenstein

Ici, nous démontrons le célèbre critère d'Eisenstein que l'on utilise énormément en pratique pour montrer qu'un polynôme est irréductible.

Soit  $A$  un anneau commutatif et unitaire.

**Notation 1.** Soit  $P \in A[X]$ . On note  $\gamma(P)$  le contenu du polynôme  $P$ .

**Lemme 2.** Soit  $p \in A$  tel que  $(p)$  est premier. Alors  $A/(p)$  est intègre.

[ULM18]  
p. 32

*Démonstration.* Soient  $\bar{a}, \bar{b} \in A/(p)$ . On suppose  $\bar{a}\bar{b} = 0$ . Comme  $\bar{a}\bar{b} = \overline{ab}$ , on a  $ab \in (p)$ . Donc par hypothèse,

$$\begin{aligned} a \in (p) \text{ ou } b \in (p) \\ \implies \bar{a} = 0 \text{ ou } \bar{b} = 0 \end{aligned}$$

et ainsi  $A/(p)$  est bien intègre.  $\square$

**Lemme 3.** Si  $A$  est intègre, alors  $A[X]$  l'est aussi.

p. 22

*Démonstration.* Soient  $P, Q \in A[X]$  non nuls, de degrés respectifs  $n$  et  $m$  que l'on écrit  $P = \sum_{i=0}^n a_i X^i$  et  $Q = \sum_{j=0}^m b_j X^j$ . Alors, le coefficient de  $X^{n+m}$  dans le produit  $PQ$  est  $a_n b_m$ . Comme  $a_n \neq 0$ ,  $b_m \neq 0$  et  $A$  est intègre, ce coefficient est non nul. Donc en particulier, le produit  $PQ$  est non nul.  $\square$

**Lemme 4.** On suppose  $A$  factoriel. Soit  $a \in A$  irréductible. Alors  $(a)$  est premier.

p. 64

*Démonstration.* On suppose que  $a \mid bc$  avec  $b, c \in A$ . Alors, il existe  $d \in A$  tel que

$$ad = bc \quad (*)$$

Si  $b$  est inversible, alors  $a \mid c$ . De même, si  $c$  est inversible, alors  $a \mid b$ . Supposons donc que  $b$  et  $c$  ne sont pas inversibles. Comme  $a$  est irréductible, on en déduit que  $d$  est un élément non nul et non inversible de  $A$ . Il existe donc des décompositions en irréductibles

$$b = \beta_1 \dots \beta_n, \quad c = \gamma_1 \dots \gamma_m \quad \text{et} \quad d = \delta_1 \dots \delta_k$$

avec  $n, m, k \in \mathbb{N}^*$ . Par conséquent, en injectant dans  $(*)$  :

$$a\delta_1 \dots \delta_k = \beta_1 \dots \beta_n \gamma_1 \dots \gamma_m$$

Comme la factorisation en irréductibles est unique à l'ordre près, il existe  $\beta_i$  ou  $\gamma_j$  qui est associé à  $a$ . Si bien que  $a$  divise  $b$  ou  $c$  ; c'est ce que l'on voulait démontrer.  $\square$

**Lemme 5** (Gauss). On suppose  $A$  factoriel. Alors :

- (i) Le produit de deux polynômes primitifs est primitif.
- (ii)  $\forall P, Q \in A[X] \setminus \{0\}, \gamma(PQ) = \gamma(P)\gamma(Q)$ .

*Démonstration.* (i) Soient  $P, Q \in A[X]$  tels que  $\gamma(P) = \gamma(Q) = 1$ . Supposons  $\gamma(PQ) \neq 1$ . Alors, il existe  $p \in A$  irréductible tel que  $p$  divise tous les coefficients de  $PQ$ . Donc, dans  $A/(p)$ ,  $\overline{PQ} = \overline{P}\overline{Q} = 0$ .

Mais, par le Théorème 4,  $(p)$  est premier. Donc par le Théorème 2  $A/(p)$  est intègre, et en particulier,  $A/(p)[X]$  l'est aussi par le Théorème 3. Ainsi,  $\overline{P} = 0$  ou  $\overline{Q} = 0$  : absurde.

- (ii) En factorisant, on écrit  $P = \gamma(P)R$  et  $Q = \gamma(Q)S$  où  $R, S \in A[X]$  avec  $\gamma(R) = \gamma(S) = 1$ . D'où  $PQ = \gamma(P)\gamma(Q)RS$  avec  $\gamma(RS) = 1$  par le Point (i). Ainsi,  $\gamma(PQ) = \gamma(P)\gamma(Q)$ .

□

**Théorème 6** (Critère d'Eisenstein). Soient  $\mathbb{K}$  le corps des fractions de  $A$  et  $P = \sum_{i=0}^n a_i X^i \in A[X]$  de degré  $n \geq 1$ . On suppose que  $A$  est factoriel et qu'il existe  $p \in A$  irréductible tel que :

- (i)  $p \mid a_i, \forall i \in \llbracket 0, n-1 \rrbracket$ .
- (ii)  $p \nmid a_n$ .
- (iii)  $p^2 \nmid a_0$ .

Alors  $P$  est irréductible dans  $\mathbb{K}[X]$ .

*Démonstration.* Par l'absurde, on suppose  $P = UV$  avec  $U, V \in \mathbb{K}[X]$  de degré supérieur ou égal à 1. Soit  $a$  un multiple commun à tous les dénominateurs des coefficients non nuls de  $U$  et  $V$ . On a

$$a^2 P = \underbrace{aU}_{=U_1 \in A[X]} \underbrace{aV}_{=V_1 \in A[X]}$$

On applique le Théorème 5 pour obtenir :

$$a^2 \gamma(P) = \gamma(U_1) \gamma(V_1) \quad (*)$$

En factorisant, on écrit  $U_1 = \gamma(U_1)U_2$  et  $V_1 = \gamma(V_1)V_2$  avec  $U_2, V_2 \in A[X]$ . Il vient :

$$a^2 P = \gamma(U_1) \gamma(V_1) U_2 V_2 \stackrel{(*)}{=} a^2 \gamma(P) U_2 V_2$$

Et comme  $a \in A \setminus \{0\}$  et que  $A$  est intègre, on a  $P = \gamma(P)U_2 V_2 = U_3 V_3$  avec  $U_3 = \gamma(P)U_2 \in A[X]$  et  $V_3 = V_2 \in A[X]$  (dans un souci de symétrie des notations) qui sont de degré supérieur ou égal à 1.

On pose  $U_3 = \sum_{i=0}^r b_i X^i$  et  $V_3 = \sum_{j=0}^s c_j X^j$  avec  $b_r c_s = a_n \neq 0$  par définition de  $P$ . Dans  $A/(p)$ , on a

$$\overline{\overline{P}}_{=a_n X^n} = \overline{U_3 V_3} = \overline{U_3} \overline{V_3}$$

et en particulier, le terme de degré 0,  $\overline{b_0 c_0} = \overline{b_0} \overline{c_0}$  est nul. Mais,  $p$  est irréductible et  $A$  est factoriel, donc au vu du Théorème 4,  $(p)$  est premier et  $A/(p)$  est intègre par le Théorème 2. Donc par le Théorème 3,  $A/(p)[X]$  est aussi intègre. D'où  $\overline{b_0} = 0$  ou  $\overline{c_0} = 0$  (mais pas les deux car sinon  $p^2 \mid b_0 c_0 = a_0$ , ce qui serait en contradiction avec le Point (iii)).

On suppose donc  $\overline{b_0} = 0$  et  $\overline{c_0} \neq 0$ . Si on avait  $\forall i \in \llbracket 0, r \rrbracket$ ,  $\overline{b_i} = 0$ , on aurait en particulier  $\overline{b_r} = 0$ , et donc  $\overline{b_r c_s} = \overline{a_n} = 0$  (exclu par le Point (ii)). Donc,

$$\exists i \in \llbracket 0, r-1 \rrbracket \text{ tel que } \overline{b_0} = \cdots = \overline{b_i} = 0 \text{ et } b_{i+1} \neq 0$$

Ainsi,

$$\overline{a_{i+1}} = \sum_{k=0}^{i+1} \overline{b_k c_{i+1-k}} = \underbrace{\overline{b_{i+1}}}_{\neq 0} \underbrace{\overline{c_0}}_{\neq 0} \neq 0$$

ce qui est absurde au vu du Point (i) car  $i \in \llbracket 0, r-1 \rrbracket$  avec  $r-1 \leq n-1$ . □

**Application 7.** Soit  $n \in \mathbb{N}^*$ . Il existe des polynômes irréductibles de degré  $n$  sur  $\mathbb{Z}$ .

[PER]  
p. 67

*Démonstration.* On applique le Théorème 6 au polynôme  $P = X^n - 2$  avec le premier  $p = 2$  qui nous donne l'irréductibilité du polynôme sur  $\mathbb{Q}$ . Reste à montrer qu'il est irréductible sur  $\mathbb{Z}$ .

Or, en supposant  $P$  réductible sur  $\mathbb{Z}$ , on peut écrire  $P = QR$  avec  $Q, R \in \mathbb{Z}[X]$  de degré supérieur ou égal à 1 car  $P$  est primitif. Mais à fortiori,  $Q, R \in \mathbb{Q}[X]$  et ne sont pas inversibles donc  $P$  est réductible sur  $\mathbb{Q}$  : absurde. □

## 4 Décomposition de Dunford

On démontre l'existence et l'unicité de la décomposition de Dunford pour tout endomorphisme d'un espace vectoriel de dimension finie.

Soit  $E$  un espace vectoriel de dimension finie sur un corps commutatif  $\mathbb{K}$ .

[GOU21]  
p. 203

**Théorème 1** (Décomposition de Dunford). Soit  $f \in E$  un endomorphisme tel que son polynôme minimal  $\pi_f$  soit scindé sur  $\mathbb{K}$ . Alors il existe un unique couple d'endomorphismes  $(d, n)$  tel que :

- $f = d + n$ .
- $d$  est diagonalisable et  $n$  est nilpotent.
- $d \circ n = n \circ d$ .

*Démonstration.* On écrit  $\pi_f = (-1)^n \prod_{i=1}^s (X - \lambda_i)^{\alpha_i}$  et pour tout  $i$ , on note  $N_i = \text{Ker}((f - \lambda_i \text{id}_E)^{\alpha_i})$  le  $i$ -ième sous-espace caractéristique de  $f$ .

Construction : Comme  $E = N_1 \oplus \cdots \oplus N_s$ , il suffit de définir  $d$  et  $n$  sur chaque  $N_i$ . On les définit pour tout  $i$  et pour tout  $x \in N_i$  comme tels :

- $d(x) = \lambda_i x \implies d|_{N_i} = \lambda_i \text{id}_{N_i}$
- $n(x) = f(x) - \lambda_i x = f(x) - d(x) \implies n = f - d$ .

Vérification :

- Les restrictions de  $d$  et  $n$  à  $N_i$  sont bien des endomorphismes car les espaces  $N_i$  sont stables par  $f$  et par  $d$  (cf. définition de  $d$ ), donc aussi par  $n = f - d$ .
- $d$  est diagonalisable et pour tout  $i$ ,  $n|_{N_i}^{\alpha_i} = 0$  (car  $\forall x \in N_i$ ,  $(f - \lambda_i \text{id}_E)^{\alpha_i}(x) = 0$  par définition de  $N_i$ ). On pose donc  $\alpha = \max_i \{\alpha_i\}$  et on a  $n|_{N_i}^\alpha = 0$  pour tout  $i$ , donc  $n^\alpha = 0$  par somme directe. Ainsi,  $n$  est nilpotent.
- Pour tout  $i$ , on a  $d|_{N_i} = \lambda_i \text{id}_E$ , donc  $n|_{N_i} \circ d|_{N_i} = d|_{N_i} \circ n|_{N_i}$  i.e.  $d$  et  $n$  commutent sur chaque  $N_i$  donc sur  $E$  tout entier.

Unicité : Soit  $(d', n')$  un autre couple d'endomorphismes de  $E$  vérifiant les hypothèses. On remarque d'abord que  $d'$  et  $f$  commutent (car  $d'$  commute avec  $d'$  et  $n'$ , donc avec  $f = d' + n'$  aussi). Pour tout  $i$ ,  $N_i$  est stable par  $d'$  (car  $\forall x \in N_i$ ,  $(f - \lambda_i \text{id}_E)^{\alpha_i}(d'(x)) = d' \circ (f - \lambda_i \text{id}_E)^{\alpha_i}(x) = 0$ ). Comme  $d|_{N_i} = \lambda_i \text{id}_{N_i}$ , on en déduit que  $d \circ d' = d' \circ d$  sur  $N_i$ . Donc c'est également vrai sur  $E$  tout entier. Ainsi,  $d$  et  $d'$  sont diagonalisables dans une même base, donc  $d - d'$  est diagonalisable.

D'autre part, comme  $n = f - d$ ,  $n' = f - d'$  et que  $d$  et  $d'$  commutent,  $n$  et  $n'$  commutent. Si on choisit  $p$  et  $q$  tels que  $n^p = n'^q = 0$ , alors :

$$(n - n')^{p+q} = \sum_{i=0}^{p+q} \binom{p+q}{i} n^i (-1)^{p+q-i} n'^{p+q-i} = 0$$

(dans chaque terme de la somme, soit  $i \geq p$ , soit  $p+q-i \geq q$ ). Donc  $n - n' = d' - d$  est nilpotent. Or nous avons montré que  $d' - d$  est diagonalisable, donc  $d' - d = 0$ . Finalement, on a  $d = d'$  et  $n = n'$ .  $\square$

*Remarque 2.* On peut démontrer que les endomorphismes  $d$  et  $n$  sont des polynômes en  $f$ . En effet, si on note  $p_i$  la projection sur  $N_i$  parallèlement à  $\bigoplus_{\substack{j=1 \\ j \neq i}}^s N_j$ , alors, le lemme des noyaux nous indique que  $p_i$  est la restriction à  $N_i$  d'un endomorphisme en  $f$ . Comme  $d = \sum_{i=1}^s \lambda_i p_i$ ,  $d$  est également un polynôme en  $f$ ; et  $n = f - d$  aussi.

## 5 Décomposition polaire

On montre que toute matrice  $M \in \text{GL}_n(\mathbb{R})$  peut s'écrire de manière unique  $M = OS$  avec  $O \in \mathcal{O}_n(\mathbb{R})$  et  $S \in \mathcal{S}_n^{++}(\mathbb{R})$ , et que l'application  $(O, S) \mapsto M$  est un homéomorphisme.

**Lemme 1.** Soit  $S \in \mathcal{S}_n(\mathbb{R})$ . Alors  $S \in \mathcal{S}_n^{++}(\mathbb{R})$  si et seulement si toutes ses valeurs propres sont strictement positives.

*Démonstration.* Par le théorème spectral, on peut écrire  $S = {}^t P \text{Diag}(\lambda_1, \dots, \lambda_n) P$  avec  $P \in \mathcal{O}_n(\mathbb{R})$ . Si on suppose  $\lambda_1, \dots, \lambda_n > 0$ , on a  $\forall x \neq 0$ ,

$${}^t x S x = {}^t (P x) \text{Diag}(\lambda_1, \dots, \lambda_n) (P x) > 0 \text{ car } \text{Diag}(\lambda_1, \dots, \lambda_n) \in \mathcal{S}_n^{++}(\mathbb{R})$$

d'où le résultat.

Réciproquement, on suppose  $\forall x \neq 0, {}^t x S x > 0$ . Avec  $x = {}^t P e_1$  (où  $e_1$  désigne le vecteur dont la première coordonnée vaut 1 et les autres sont nulles),

$${}^t x S x = {}^t (P x) \text{Diag}(\lambda_1, \dots, \lambda_n) (P x) = {}^t e_1 D e_1 = \lambda_1 > 0$$

Et on peut faire de même pour montrer que  $\forall i \in \llbracket 1, n \rrbracket, \lambda_i > 0$ . □

**Lemme 2.**  $\mathcal{S}_n^+(\mathbb{R})$  est un fermé de  $\mathcal{M}_n(\mathbb{R})$  et  $\text{GL}_n(\mathbb{R}) \cap \mathcal{S}_n^+(\mathbb{R}) \subseteq \mathcal{S}_n^{++}(\mathbb{R})$ .

*Démonstration.* Pour la première assertion, il suffit de constater que

$$\mathcal{S}_n^+(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid {}^t M = M\} \cap \left( \bigcap_{x \in \mathbb{R}^n} \{M \in \mathcal{M}_n(\mathbb{R}) \mid {}^t x M x \geq 0\} \right)$$

qui est une intersection de fermés (par image réciproque). Maintenant, si  $M \in \text{GL}_n(\mathbb{R}) \cap \mathcal{S}_n^+(\mathbb{R})$ , alors  $M$  est diagonalisable avec des valeurs propres positives ou nulles (par le théorème spectral). Mais comme  $\det(M) \neq 0$ , toutes les valeurs propres de  $M$  sont strictement positives. Donc par le Théorème 1,  $M \in \mathcal{S}_n^{++}(\mathbb{R})$ . □

**Théorème 3** (Décomposition polaire). L'application

$$\mu : \begin{array}{ccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \rightarrow & \text{GL}_n(\mathbb{R}) \\ (O, S) & \mapsto & OS \end{array}$$

est un homéomorphisme.

*Démonstration.* Montrer qu'une application est un homéomorphisme se fait en 4 étapes : on montre qu'elle est continue, injective, surjective, et que la réciproque est elle aussi continue.

- L'application est bien définie et continue : Si  $O \in \mathcal{O}_n(\mathbb{R})$  et  $S \in \mathcal{S}_n^{++}(\mathbb{R})$ , alors  $OS \in \text{GL}_n(\mathbb{R})$ . De plus,  $\mu$  est continue en tant que restriction de la multiplication matricielle.



— L'application est surjective : Soit  $M \in \text{GL}_n(\mathbb{R})$ . Si  $x \neq 0$ , on a

$${}^t x({}^t M M)x = {}^t (Mx)(Mx) = \|Mx\|_2^2 > 0$$

En particulier,  ${}^t M M \in \mathcal{S}_n^{++}(\mathbb{R})$ . Par le théorème spectral, il existe  $P \in \mathcal{O}_n(\mathbb{R})$  et  $\lambda_1, \dots, \lambda_n > 0$  tels que  ${}^t M M = P \text{Diag}(\lambda_1, \dots, \lambda_n) P^{-1}$ . On pose alors

$$D = \text{Diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n}) \text{ et } S = P D P^{-1}$$

de sorte que  $S^2 = {}^t M M$ . Mais de plus,

$${}^t S = {}^t P^{-1} {}^t D {}^t P = S \implies S \in \mathcal{S}_n(\mathbb{R})$$

et par le Théorème 1,

$$\forall i \in \llbracket 1, n \rrbracket, \sqrt{\lambda_i} > 0 \implies S \in \mathcal{S}_n^{++}(\mathbb{R})$$

On pose donc  $O = M S^{-1}$  (ie.  $M = OS$ ), et on a

$${}^t O O = {}^t (M S^{-1}) M S^{-1} = {}^t S^{-1} {}^t M M S^{-1} = S^{-1} S^2 S^{-1} = I_n \implies O \in \mathcal{O}_n(\mathbb{R})$$

Donc  $\mu(O, S) = M$  et  $\mu$  est surjective.

— L'application est injective : Soit  $M = OS \in \text{GL}_n(\mathbb{R})$  (avec  $O$  et  $S$  comme précédemment). Soit  $M = O' S'$  une autre décomposition polaire de  $M$ . Alors il vient,

$$S^2 = {}^t M M = {}^t (O' S') O' S' = {}^t S'^t O' O' S' = S'^2$$

Soit  $Q$  un polynôme tel que  $\forall i \in \llbracket 1, n \rrbracket, Q(\lambda_i) = \sqrt{\lambda_i}$  (les polynômes d'interpolation de Lagrange conviennent parfaitement). Alors,

$$S = P D^t P = P Q(D^2) {}^t P = Q(P D^2 {}^t P) = Q({}^t M M) = Q(S^2) = Q(S'^2)$$

Mais  $S'$  commute avec  $S'^2$ , donc avec  $S = Q(S'^2)$ . En particulier,  $S$  et  $S'$  sont codiagonalisables, il existe  $P_0 \in \text{GL}_n(\mathbb{R})$  et  $\mu_1, \dots, \mu_n, \mu'_1, \dots, \mu'_n \in \mathbb{R}$  tels que

$$S = P_0 \text{Diag}(\mu_1, \dots, \mu_n) P_0^{-1} \text{ et } S' = P_0 \text{Diag}(\mu'_1, \dots, \mu'_n) P_0^{-1}$$

d'où :

$$\begin{aligned} S^2 = S'^2 &\implies P_0 \text{Diag}(\mu_1^2, \dots, \mu_n^2) P_0^{-1} = P_0 \text{Diag}(\mu_1'^2, \dots, \mu_n'^2) P_0^{-1} \\ &\implies \mu_i^2 = \mu_i'^2 \quad \forall i \in \llbracket 1, n \rrbracket \\ &\implies \mu_i = \mu_i' \quad \forall i \in \llbracket 1, n \rrbracket \text{ car } \forall i \in \llbracket 1, n \rrbracket, \mu_i > 0 \\ &\implies S = S' \end{aligned}$$

Ainsi,  $O = M S^{-1} = M S'^{-1} = O'$ . Donc  $\mu$  est injective.

— L'application inverse est continue : Soit  $(M_p) \in \text{GL}_n(\mathbb{R})^{\mathbb{N}}$  qui converge vers  $M \in \text{GL}_n(\mathbb{R})$ . Il

s'agit de montrer que la suite  $(\mu^{-1}(M_p)) = (O_p, S_p)$  converge vers  $\mu^{-1}(M) = (O, S)$ . Comme  $\mathcal{O}_n(\mathbb{R})$  est compact, il existe  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  strictement croissante telle que la suite extraite  $(O_{\varphi(p)})$  converge vers une valeur d'adhérence  $\bar{O} \in \mathcal{O}_n(\mathbb{R})$ . Ainsi, la suite  $(S_{\varphi(p)})$  converge vers  $\bar{S} = \bar{O}^{-1}M$ .

Mais,  $\bar{S} = \bar{O}^{-1}M \in \mathrm{GL}_n(\mathbb{R}) \cap \overline{\mathcal{S}_n^{++}(\mathbb{R})}$ . Donc par le Théorème 1,

$$\bar{S} \in \mathrm{GL}_n(\mathbb{R}) \cap \mathcal{S}_n^+(\mathbb{R})$$

et par le Théorème 2,

$$\bar{S} \in \mathcal{S}_n^{++}(\mathbb{R})$$

On a  $M = \bar{O}\bar{S}$ , d'où, par unicité de la décomposition polaire,  $\bar{O} = O$  et  $\bar{S} = S$ .

□

*Remarque 4.* La preuve vaut encore dans le cas complexe (pour le groupe unitaire et les matrices hermitiennes).

## 6 Densité des polynômes orthogonaux

On montre que la famille des polynômes orthogonaux associée à une fonction poids  $\rho$  vérifiant certaines hypothèses forme une base hilbertienne de  $L_2(I, \rho)$  (où  $I$  est un intervalle de  $\mathbb{R}$ ).

Soient  $I$  un intervalle de  $\mathbb{R}$  et  $\rho$  une fonction poids. On considère  $(P_n)$  la famille des polynômes orthogonaux associée à  $\rho$  sur  $I$ .

[BMP]  
p. 140

**Lemme 1.** On suppose que  $\forall n \in \mathbb{N}, g_n : x \mapsto x^n \in L_1(I, \rho)$ . Alors  $\forall n \in \mathbb{N}, g_n \in L_2(I, \rho)$ . En particulier, l'algorithme de Gram-Schmidt a bien du sens et  $(P_n)$  est bien définie.

*Démonstration.* On a  $\forall n \in \mathbb{N}$ ,

$$\int_I |x^n|^2 \rho(x) dx = \int_I |x^{2n}| \rho(x) dx = \|g_{2n}\|_1 < +\infty$$

□

**Théorème 2.** On suppose qu'il existe  $a > 0$  tel que

$$\int_I e^{a|x|} \rho(x) dx < +\infty$$

alors  $(P_n)$  est une base hilbertienne de  $L_2(I, \rho)$  pour la norme  $\|\cdot\|_2$ .

*Démonstration.* Soit  $f \in \text{Vect}(g_n)^\perp = \text{Vect}(P_n)^\perp$ . On définit

$$\forall x \in \mathbb{R}, \quad \varphi(x) = \begin{cases} f(x)\rho(x) & \text{si } x \in I \\ 0 & \text{sinon} \end{cases}$$

Montrons que  $\varphi \in L_1(\mathbb{R})$ . Remarquons tout d'abord que  $\forall t \geq 0, t \leq \frac{1+t^2}{2}$ . Ainsi, on a

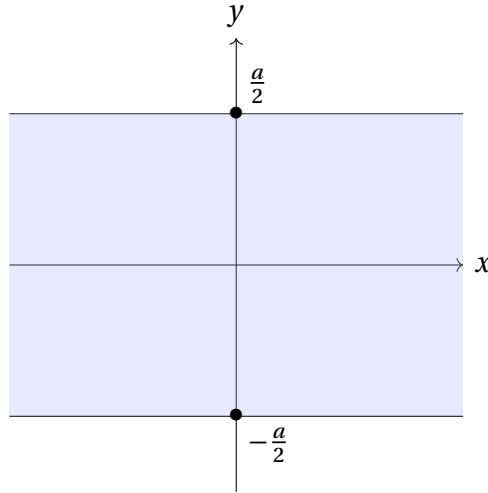
$$\forall x \in I, \quad |f(x)|\rho(x) \leq \frac{1+|f(x)|^2}{2}\rho(x)$$

Comme  $\rho$  et  $\rho f^2$  sont intégrables sur  $I$ , on en déduit que  $\varphi \in L_1(\mathbb{R})$ . On peut donc considérer sa transformée de Fourier

$$\hat{\varphi} : \xi \mapsto \int_I f(x) e^{-i\xi x} \rho(x) dx$$

Montrons que  $\hat{\varphi}$  se prolonge en une fonction  $F$  holomorphe sur

$$B_a = \left\{ z \in \mathbb{C} \mid |\text{Im}(z)| < \frac{a}{2} \right\}$$



Définissons à présent  $g : (z, x) \mapsto e^{-izx} f(x) \rho(x)$ . Pour  $z \in B_a$ , on a

$$\int_I |g(z, x)| dx \leq \int_I e^{\frac{a|x|}{2}} |f(x)| \rho(x) dx$$

En utilisant l'inégalité de Cauchy-Schwarz pour  $\|\cdot\|_2$ , on obtient de plus

$$\int_I e^{\frac{a|x|}{2}} |f(x)| \rho(x) dx \leq \left( \int_I e^{a|x|} \rho(x) dx \right)^{\frac{1}{2}} \left( \int_I |f(x)|^2 \rho(x) dx \right)^{\frac{1}{2}} < +\infty \quad (*)$$

On définit la fonction  $F$  par

$$\forall z \in B_a, \quad F(z) = \int_I e^{-izx} f(x) \rho(x) dx = \int_I g(z, x) dx$$

L'inégalité (\*) montre que cette fonction est bien définie. De plus :

- $\forall z \in B_a, x \mapsto g(z, x)$  est mesurable.
- pp. en  $x \in I, z \mapsto g(z, x)$  est holomorphe.
- $\forall z \in B_a, \forall x \in I,$

$$|g(z, x)| \leq h(x) = e^{\frac{a|x|}{2}} |f(x)| \rho(x)$$

et l'inégalité (\*) montre que  $h \in L_1(I)$ .

Donc par le théorème d'holomorphie sous l'intégrale, la fonction  $F$  est holomorphe sur  $B_a$ , et coïncide sur  $\mathbb{R}$  avec  $\hat{\varphi}$ . Ce théorème nous dit de plus que

$$\forall n \in \mathbb{N}, \forall z \in B_a, F^{(n)}(z) = (-i)^n \int_I x^n e^{-izx} f(x) \rho(x) dx$$

Ce qui donne, une fois évalué en 0 :

$$\forall n \in \mathbb{N}, F^{(n)}(0) = (-i)^n \int_I x^n f(x) \rho(x) dx = (-i)^n \langle g_n, f \rangle = 0$$

L'unicité du développement en série entière d'une fonction holomorphe montre que  $F = 0$  sur un voisinage de 0. Le théorème du prolongement analytique implique alors que  $F = 0$  sur le connexe  $B_a$  tout entier, et donc en particulier, sur  $\mathbb{R}$ . Ainsi,  $\hat{\varphi} = 0$ . Comme  $\varphi$  est une fonction

intégrable, l'injectivité de la transformée de Fourier implique que  $\varphi = 0$ . Comme  $\rho(x) > 0$ , on en déduit que  $f(x) = 0$  pp. en  $x \in I$ . On vient donc de montrer qu'une fonction orthogonale à tous les polynômes est nulle i.e.  $\text{Vect}(g_n)^\perp = \{0\}$ . En ajoutant le Théorème 1 à ceci, on a bien que les polynômes orthogonaux forment une base hilbertienne de  $L_2(I, \rho)$ .  $\square$

**Contre-exemple 3.** On considère, sur  $I = \mathbb{R}_*^+$ , la fonction poids  $\rho : x \mapsto x^{-\ln(x)}$ . On pose  $\forall x \in I, f(x) = \sin(2\pi \ln(x))$ . On calcule

$$\begin{aligned} \langle f, g_n \rangle &= \int_I x^n \sin(2\pi \ln(x)) x^{-\ln(x)} dx \\ &\stackrel{y=\ln(x)}{=} \int_{\mathbb{R}} e^{(n+1)y} \sin(2\pi y) e^{-y^2} dy \\ &= e^{\frac{(n+1)^2}{4}} \int_{\mathbb{R}} e^{-\left(y - \frac{n+1}{2}\right)^2} \sin(2\pi y) dy \\ &= (-1)^{n+1} e^{\frac{(n+1)^2}{4}} \int_{\mathbb{R}} \sin(2\pi t) e^{-t^2} dt, \text{ avec } t = y - \frac{n+1}{2} \\ &\stackrel{f \text{ impaire}}{=} 0 \end{aligned}$$

Ainsi, la famille des  $g_n$  n'est pas totale. La famille des polynômes orthogonaux associée à ce poids particulier n'est donc pas totale non plus : ce n'est pas une base hilbertienne.

## 7 Développement asymptotique de la série harmonique

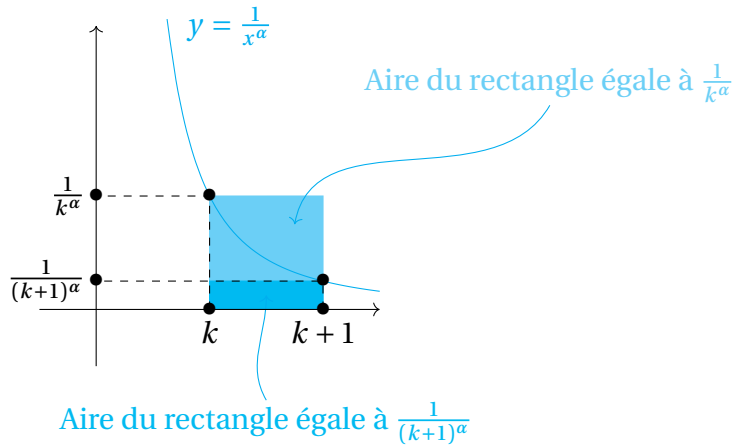
On effectue un développement asymptotique à l'ordre 2 de la série harmonique  $\sum \frac{1}{n}$ .

**Lemme 1.** Soit  $\alpha > 1$ . Lorsque  $n$  tend vers  $+\infty$ , on a

$$\sum_{k=n+1}^{+\infty} \frac{1}{k^\alpha} \sim \frac{1}{\alpha-1} \frac{1}{n^{\alpha-1}}$$

[I-P]  
p. 380

*Démonstration.* La fonction  $x \mapsto \frac{1}{x^\alpha}$  est décroissante sur  $\mathbb{R}_*^+$ , nous allons faire une comparaison série / intégrale.



On a

$$\forall k \geq 1, \frac{1}{(k+1)^\alpha} \leq \int_k^{k+1} \frac{1}{x^\alpha} dx \leq \frac{1}{k^\alpha}$$

D'où :

$$\forall k \geq 2, \int_k^{k+1} \frac{1}{x^\alpha} dx \leq \frac{1}{k^\alpha} \leq \int_{k-1}^k \frac{1}{x^\alpha} dx$$

Soit  $N \geq 2$ . Pour tout  $n \in \llbracket 2, N \rrbracket$ ,

$$\begin{aligned} \int_n^{N+1} \frac{1}{x^\alpha} dx &\leq \sum_{k=n}^N \frac{1}{k^\alpha} \leq \int_{n-1}^N \frac{1}{x^\alpha} dx \\ \Leftrightarrow \left[ \frac{-1}{\alpha-1} \frac{1}{x^{\alpha-1}} \right]_n^{N+1} &\leq \sum_{k=n}^N \frac{1}{k^\alpha} \leq \left[ \frac{-1}{\alpha-1} \frac{1}{x^{\alpha-1}} \right]_{n-1}^N \\ \Leftrightarrow \frac{1}{\alpha-1} \left( \frac{1}{n^{\alpha-1}} - \frac{1}{(N+1)^{\alpha-1}} \right) &\leq \sum_{k=n}^N \frac{1}{k^\alpha} \leq \frac{1}{\alpha-1} \left( \frac{1}{(n-1)^{\alpha-1}} - \frac{1}{N^{\alpha-1}} \right) \end{aligned}$$

La suite  $(\sum_{k=n}^N \frac{1}{k^\alpha})$  est donc convergente, car elle est croissante et majorée par  $\frac{1}{\alpha-1} \left( \frac{1}{(n-1)^{\alpha-1}} \right)$ . Lorsque  $N$  tend vers  $+\infty$ , on a donc

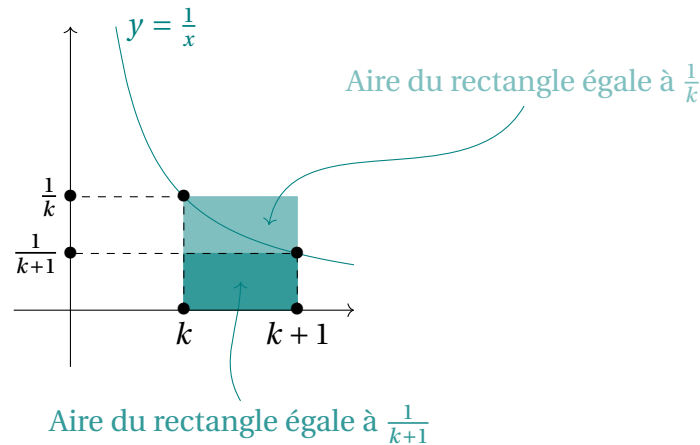
$$\frac{1}{\alpha-1} \left( \frac{1}{n^{\alpha-1}} \right) \leq \sum_{k=n}^{+\infty} \frac{1}{k^\alpha} \leq \frac{1}{\alpha-1} \left( \frac{1}{(n-1)^{\alpha-1}} \right)$$

Or, comme  $n^{\alpha-1} \sim (n-1)^{\alpha-1}$  quand  $n$  tend vers  $+\infty$ , on en conclut l'équivalent annoncé.  $\square$

**Théorème 2** (Développement asymptotique de la série harmonique). On note  $\forall n \in \mathbb{N}^*$ ,  $H_n = \sum_{k=1}^n \frac{1}{k}$ . Alors, quand  $n$  tend vers  $+\infty$ ,

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

*Démonstration.* La fonction  $x \mapsto \frac{1}{x}$  est décroissante sur  $\mathbb{R}_*^+$ , cela invite à faire une comparaison série / intégrale.



On a

$$\forall k \geq 1, \frac{1}{k+1} \leq \int_k^{k+1} \frac{1}{x} dx \leq \frac{1}{k}$$

Traitons les deux morceaux séparément.

—  $\forall k \geq 1, \int_k^{k+1} \frac{1}{x} dx \leq \frac{1}{k}$  par l'inégalité de droite. Donc, en sommant entre 1 et  $n \in \mathbb{N}^*$  :

$$\ln(n+1) = \int_1^{n+1} \frac{1}{x} dx \leq H_n$$

—  $\forall k \geq 2, \frac{1}{k} \leq \int_{k-1}^k \frac{1}{x} dx$  par l'inégalité de gauche avec un changement de variable. Donc, en sommant entre 2 et  $n \in \mathbb{N}^*$  :

$$\sum_{k=2}^n \frac{1}{k} \leq \int_1^n \frac{1}{x} dx = \ln(n)$$

et en ajoutant 1 :

$$H_n \leq \ln(n) + 1$$

On peut tout regrouper pour obtenir les inégalités suivantes :

$$\ln(n+1) \leq H_n \leq \ln(n) + 1$$

et donc, quand  $n$  tend vers  $+\infty$ ,

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

Pour la suite, on pose pour tout  $n \geq 1$ ,  $u_n = H_n - \ln(n)$  et pour tout  $n \geq 2$ ,  $v_n = H_{n-1} - \ln(n)$ . On a :

- $\forall n \geq 2, u_n - v_n = \frac{1}{n} \geq 0$  et converge vers 0 quand  $n$  tend vers  $+\infty$ .
- $\forall n \geq 1,$

$$\begin{aligned} u_n - u_{n+1} &= -\frac{1}{n+1} - \ln(n) + \ln(n+1) \\ &= -\frac{1}{n+1} - \ln\left(1 + \frac{1}{n}\right) \\ &\geq 0 \end{aligned}$$

car  $\ln(1+x) \leq x$  pour  $x \in ]-1, +\infty[$ .

- $\forall n \geq 2,$

$$\begin{aligned} v_{n+1} - v_n &= \frac{1}{n} + \ln(n) - \ln(n+1) \\ &= \frac{1}{n} - \ln\left(1 + \frac{1}{n}\right) \\ &\geq 0 \end{aligned}$$

les suites  $(u_n)$  et  $(v_n)$  sont adjacentes, elles convergent donc vers un réel  $\gamma \in \mathbb{R}$ . Posons maintenant

$$\forall n \geq 1, t_n = u_n - \gamma = H_n - \ln(n) - \gamma$$

Nous allons utiliser le lien entre séries et suites : cherchons un équivalent de la suite  $(t_n - t_{n-1})$  pour obtenir un équivalent de la somme partielle de la série de terme général  $(t_n - t_{n-1})$  qui n'est autre que la suite  $(t_n)$ . À l'aide du développement limité de  $\ln(1+x)$  en 0 on obtient

$$\begin{aligned} t_n - t_{n-1} &= \ln(n-1) - \ln(n) + \frac{1}{n} \\ &= \ln\left(1 - \frac{1}{n}\right) + \frac{1}{n} \\ &\sim -\frac{1}{2n^2} \end{aligned}$$

D'après le critère de Riemann, la série de terme général  $t_k - t_{k-1}$  converge. Le théorème de sommation des équivalents donne l'équivalence des restes. Or, un équivalent du reste de la série de Riemann  $\sum \frac{1}{n^2}$  est donné par le Théorème 1 et vaut  $\frac{1}{n}$  :

$$\sum_{k=n+1}^{+\infty} t_k - t_{k-1} = -t_n \sim \sum_{k=n+1}^{+\infty} -\frac{1}{2k^2} \sim -\frac{1}{2n}$$

D'où  $t_n \sim \frac{1}{2n}$  et  $H_n = \ln(n) + \gamma + \frac{1}{2n} + o\left(\frac{1}{n}\right)$ . On pose alors  $\forall n \geq 1, w_n = t_n - \frac{1}{2n}$  et on procède de



manière similaire pour obtenir, pour tout  $n \geq 2$  :

$$\begin{aligned}
 w_n - w_{n-1} &= \frac{1}{n} + \ln\left(1 - \frac{1}{n}\right) + \frac{1}{2n-2} - \frac{1}{2n} \\
 &= \frac{1}{n} - \frac{1}{n} - \frac{1}{2n^2} - \frac{1}{3n^3} + \frac{1}{2n} \frac{1}{1 - \frac{1}{n}} - \frac{1}{2n} + o\left(\frac{1}{n^3}\right) \\
 &= -\frac{1}{2n^2} + \frac{1}{2n} \left(1 + \frac{1}{n} + \frac{1}{n^2}\right) - \frac{1}{2n} + o\left(\frac{1}{n^3}\right) \\
 &= \frac{1}{6n^3} + o\left(\frac{1}{n^3}\right)
 \end{aligned}$$

On a donc

$$\sum_{k=n+1}^{+\infty} w_k - w_{k-1} = -w_n \sim \frac{1}{2} \frac{1}{6n^2} = \frac{1}{12n^2}$$

d'où le résultat. □

## 8 Dimension du commutant

Dans ce développement, on montre en se ramenant à la résolution d'un système d'équations linéaires homogène que la dimension du commutant d'une matrice est plus grande que celle de l'espace de départ. On applique ensuite ce résultat pour donner une condition nécessaire et suffisante qui permettant de calculer le commutant de cette matrice.

Soient  $\mathbb{K}$  un corps,  $n \geq 1$  et  $A \in \mathcal{M}_n(\mathbb{K})$ .

**Notation 1.** — On note  $\mathcal{T}_n(\mathbb{K})$  l'ensemble des matrices carrées triangulaires supérieures d'ordre  $n$  à coefficients dans le corps  $\mathbb{K}$ .

— On note  $\mathcal{C}(A)$  le commutant de  $A$ .

*Remarque 2.* On considère acquis le fait que si  $\pi_A = \chi_A$ , alors  $A$  est cyclique :

$$\exists x \in \mathbb{K}^n \setminus \{0\} \text{ tel que } (x, Ax, \dots, A^{n-1}x) \text{ est une base de } \mathbb{K}^n$$

[GOU21]  
p. 289

**Lemme 3.**

$$\dim_{\mathbb{K}}(\mathcal{C}(A)) \geq n$$

[FGN2]  
p. 160

*Démonstration.* Commençons par poser le système d'équations linéaires homogène

$$AX - XA = 0$$

d'inconnue  $X = (x_{i,j})_{i,j \in \llbracket 1, n \rrbracket} \in \mathcal{M}_n(\mathbb{K})$ . On note  $\mathcal{S}$  l'espace des solutions de ce système.

Plaçons-nous d'abord dans le cas où  $A = (a_{i,j})_{i,j \in \llbracket 1, n \rrbracket} \in \mathcal{T}_n(\mathbb{K})$ . Considérons ce système d'équations pour  $X \in \mathcal{T}_n(\mathbb{K})$ ; on a alors  $\frac{n(n+1)}{2}$  inconnues dans  $\mathbb{K}$ . Comme  $AX - XA$  est triangulaire supérieure, dire que  $X$  est solution revient à écrire  $\frac{n(n+1)}{2}$  équations correspondant à la nullité des coefficients de  $AX - XA$  dans la partie supérieure. Mais, de ces équations, on peut en retirer  $n$  qui sont triviales (celles situées sur la diagonale, de la forme  $a_{i,i}x_{i,i} - x_{i,i}a_{i,i}$ ). Ce système a donc  $\frac{n(n+1)}{2} - n$  équations pour seulement  $\frac{n(n+1)}{2}$  inconnues. Ainsi,

$$\dim_{\mathbb{K}}(\mathcal{C}(A)) = \dim_{\mathbb{K}}(\mathcal{S}) \geq \dim_{\mathbb{K}}(\mathcal{S} \cap \mathcal{T}_n(\mathbb{K})) \geq \frac{n(n+1)}{2} - \left( \frac{n(n+1)}{2} - n \right) = n$$

Si  $A$  n'est pas triangulaire mais est tout de même trigonalisable, il existe  $P \in \text{GL}_n(\mathbb{K})$  et  $T \in \mathcal{T}_n(\mathbb{K})$  telles que  $A = PTP^{-1}$ . Ainsi,

$$\begin{aligned} X \in \mathcal{C}(A) &\iff AX = XA \\ &\iff (PTP^{-1})X = X(PTP^{-1}) \\ &\iff T(P^{-1}XP) = (P^{-1}XP)T \\ &\iff P^{-1}XP \in \mathcal{C}(T) \end{aligned}$$

et puisque  $X \mapsto P^{-1}XP$  est un isomorphisme de  $\mathcal{M}_n(\mathbb{K})$ , on a

$$\dim_{\mathbb{K}}(\mathcal{C}(A)) = \dim_{\mathbb{K}}(\mathcal{C}(T))$$

donc on peut tout à fait se ramener au cas où  $A$  est triangulaire supérieure.

Enfin, si  $A$  n'est pas trigonalisable, on considère  $\mathbb{L}$  une extension de  $\mathbb{K}$  sur laquelle  $\chi_A$  est scindé. L'application

$$\varphi : \begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \rightarrow & \mathcal{M}_n(\mathbb{K}) \\ X & \mapsto & AX - XA \end{array}$$

est linéaire, donc on peut considérer sa matrice  $B \in \mathcal{M}_{n^2}(\mathbb{K})$  dans la base canonique de  $\mathcal{M}_n(\mathbb{K})$  (il s'agit de la matrice associée au système d'équations linéaires). Alors  $\mathcal{S} = \text{Ker}(B)$ . Le rang est invariant par extension de corps, donc

$$\text{rang}_{\mathbb{K}}(B) = \text{rang}_{\mathbb{L}}(B)$$

d'où

$$\begin{aligned} \dim_{\mathbb{K}}(\mathcal{S}) &= \dim_{\mathbb{K}}(\text{Ker}(B)) \\ &= n^2 - \text{rang}_{\mathbb{K}}(B) \\ &= n^2 - \text{rang}_{\mathbb{L}}(B) \\ &= \dim_{\mathbb{L}}(\text{Ker}(B)) \\ &\geq n \end{aligned}$$

car  $A$  est trigonalisable dans  $\mathbb{L}$ . D'où le résultat. □

#### Théorème 4.

$$\mathbb{K}[A] = \mathcal{C}(A) \iff \pi_A = \chi_A$$

*Démonstration.* Sens direct : Supposons  $\mathbb{K}[A] = \mathcal{C}(A)$ . Le Théorème 3 entraîne que

$$\deg(\pi_A) = \dim(\mathbb{K}[A]) \geq n$$

Mais comme  $\deg(\pi_A) \leq n$ , on a  $\deg(\pi_A) = n$ . Par le théorème de Cayley-Hamilton, on conclut

$$\pi_A = \chi_A$$

Réciproque : On suppose  $\pi_A = \chi_A$ . Par la Théorème 2, on peut trouver  $x \in \mathbb{K}^n \setminus \{0\}$  tel que  $(x, Ax, \dots, A^{n-1}x)$  est une base de  $\mathbb{K}^n$ . Ainsi, l'application

$$\varphi : \begin{array}{ccc} \mathcal{C}(A) & \rightarrow & \mathbb{K}^n \\ B & \mapsto & Bx \end{array}$$

est linéaire injective. En effet, si  $B \in \text{Ker}(\varphi)$ , alors

$$\forall k \in \llbracket 0, n-1 \rrbracket, BA^k x = A^k Bx = 0 \implies B = 0$$

car  $B$  s'annule sur une base de  $\mathbb{K}^n$ . D'où  $\dim(\mathcal{C}(A)) \leq \dim(\mathbb{K}^n) = n$ . On déduit à l'aide du Théorème 3 que

$$\dim(\mathcal{C}(A)) = n$$

Notons de plus que

$$\dim(\mathbb{K}[A]) = \deg(\pi_A) = \deg(\chi_A) = n$$

et comme  $\mathbb{K}[A] \subseteq \mathcal{C}(A)$  (car tout polynôme en  $A$  commute avec  $A$ ), on a bien le résultat.  $\square$

## 9 Dual de $L_p$

Avec les propriétés hilbertiennes de  $L_2$  couplées à certaines propriétés des espaces  $L_p$ , on montre que le dual d'un espace  $L_p$  est  $L_q$  pour  $\frac{1}{p} + \frac{1}{q} = 1$ , dans le cas où  $p \in ]1, 2[$  et où l'espace est de mesure finie.

Soit  $(X, \mathcal{A}, \mu)$  un espace mesuré de mesure finie.

**Notation 1.** On note  $\forall p \in ]1, 2[, L_p = L_p(X, \mathcal{A}, \mu)$ .

**Lemme 2.** Soient  $p \in ]1, 2[$  et  $f \in L_2$ . Alors  $f \in L_p$  telle que  $\|f\|_p \leq M \|f\|_2$  où  $M \geq 0$ .

*Démonstration.* Comme  $p \in ]1, 2[$ , on a  $\frac{2}{p} > 1$ . Soit  $r$  tel que  $\frac{p}{2} + \frac{1}{r} = 1$ . On applique l'inégalité de Hölder à  $g = |f|^p \mathbb{1}_X$  de sorte que

$$\int_X |f|^p d\mu = \| |f|^p \mathbb{1}_X \|_1 \leq \| |f|^p \|_{\frac{2}{p}} \| \mathbb{1}_X \|_r \leq \mu(X)^{\frac{1}{r}} \|f\|_2^p$$

d'où le résultat. □

**Lemme 3.** Soit  $p \in ]1, 2[$ . Alors  $L_2$  est dense dans  $L_p$  pour la norme  $\|\cdot\|_p$ .

*Démonstration.* Soit  $f \in L_p$ . On considère la suite de fonction  $(f_n)$  définie par

$$\forall n \in \mathbb{N}, f_n = f \mathbb{1}_{|f| \leq n}$$

Clairement,  $(f_n)$  est une suite de  $L_2$ . On va chercher à appliquer le théorème de convergence dominée à la suite de fonctions  $(g_n)$  définie pour tout  $n \in \mathbb{N}$  par  $g_n = |f_n - f|^p$  :

- $\forall n \in \mathbb{N}, g_n$  est mesurable.
- $(g_n)$  converge presque partout vers la fonction nulle.
- Par convexité de la fonction  $x \mapsto x^p$ , on a

$$|f_n - f|^p = 2^p \left| \frac{f_n}{2} - \frac{f}{2} \right|^p \leq 2^{p-1} (|f|^p + |f_n|^p) \leq 2^p |f|^p \in L_1$$

On peut donc conclure

$$\|f - f_n\|_p^p = \int_X |f - f_n|^p d\mu \rightarrow 0$$

ce qu'il fallait démontrer. □

**Théorème 4.** L'application

$$\varphi : \begin{array}{ll} L_q & \rightarrow (L_p)' \\ g & \mapsto \left( \varphi_g : f \mapsto \int_X f \overline{g} d\mu \right) \end{array} \quad \text{où } \frac{1}{p} + \frac{1}{q} = 1$$

est une isométrie linéaire surjective. C'est donc un isomorphisme isométrique.

*Démonstration.* Soient  $g \in L_q$  et  $f \in L_p$ . L'inégalité de Hölder donne

$$|\varphi_g(f)| \leq \|g\|_q \|f\|_p$$

donc  $\varphi_g \in (L_p)'$  et  $\|\varphi_g\| \leq \|g\|_q$ . De plus, si  $g = 0$ , alors  $\|\varphi_g\| = \|g\|_q = 0$ . On peut donc supposer  $g \neq 0$ .

Soit  $u$  une fonction mesurable de module 1, telle que  $g = u|g|$ . On pose  $h = \overline{u}|g|^{q-1}$ . Comme  $q = p(q-1)$ , on a

$$\int_X |h|^p d\mu = \int_X |g|^{(q-1)p} d\mu = \int_X |g|^q d\mu < +\infty$$

d'où  $h \in L_p$  et  $\|h\|_p^p = \int_X |h|^p d\mu = \int_X |g|^q d\mu = \|\varphi_g(h)\|$ . Comme,  $\frac{|\varphi_g(h)|}{\|h\|_p} \leq \|\varphi_g\|$ , on a en particulier,

$$\underbrace{\int_X |g|^q d\mu}_{=|\varphi_g(h)|} \leq \|\varphi_g\| \underbrace{\left( \int_X |g|^q d\mu \right)^{\frac{1}{p}}}_{=\|h\|_p}$$

et ainsi,

$$\|\varphi_g\| \geq \left( \int_X |g|^q d\mu \right)^{1-\frac{1}{p}} = \left( \int_X |g|^q d\mu \right)^{\frac{1}{q}} = \|g\|_q$$

donc  $\|\varphi_g\| = \|g\|_q$  et  $\varphi$  est une isométrie.

Montrons qu'elle est surjective. Soit  $\ell \in (L_p)'$ . D'après le Théorème 2, on a  $L_2 \subseteq L_p$ , donc on peut considérer la restriction  $\tilde{\ell} = \ell|_{L_2}$ .

$$\forall f \in L_2, \quad |\tilde{\ell}(f)| \leq \|\ell\| \|f\|_p \leq M \|\ell\| \|f\|_2 \implies \tilde{\ell} \in (L_2)'$$

Comme  $L_2$  est un espace de Hilbert, on peut appliquer le théorème de représentation de Riesz à  $\tilde{\ell}$ . Il existe  $g \in L_2$  telle que

$$\forall f \in L_2, \quad \tilde{\ell}(f) = \int_X f \overline{g} d\mu$$

Pour conclure, il reste à montrer que  $g \in L_q$  et que l'égalité précédente est vérifiée sur  $L_p$ . Comme précédemment, on considère  $u$  de module 1 telle que  $g = u|g|$  et on pose  $f_n = \overline{u}|g|^{q-1} \mathbb{1}_{|g| \leq n} \in L_\infty \subseteq L_2$ . On a

$$\int_X |g|^q \mathbb{1}_{|g| \leq n} d\mu = |\ell(f_n)| \leq \|\ell\| \|f_n\|_p = \|\ell\| \left( \int_X |g|^q \mathbb{1}_{|g| \leq n} d\mu \right)^{\frac{1}{p}}$$

D'où

$$\left( \int_X |g|^q \mathbb{1}_{|g| \leq n} d\mu \right)^{\frac{1}{q}} = \left( \int_X |g|^q \mathbb{1}_{|g| \leq n} d\mu \right)^{1-\frac{1}{p}} \leq \|\ell\|$$

D'après le théorème de convergence monotone, on a

$$\lim_{n \rightarrow +\infty} \left( \int_X |g|^q \mathbb{1}_{|g| \leq n} d\mu \right)^{\frac{1}{q}} = \left( \int_X |g|^q d\mu \right)^{\frac{1}{q}} \leq \|\ell\|$$

Et en particulier,  $g \in L_q$  de norme inférieure ou égale à  $\|\ell\|$ . Ainsi, on a  $\forall f \in L_2, \ell(f) = \varphi_g(f)$ . Les applications  $\ell$  et  $\varphi_g$  sont continues sur  $L_p$  et  $L_2$  est dense dans  $L_p$  (par le Théorème 3), donc on a bien  $\ell = \varphi_g = \varphi(g)$ .  $\square$

*Remarque 5.* Plus généralement, si l'on identifie  $g$  et  $\varphi_g$  :

- $L_q$  est le dual topologique de  $L_p$  pour  $p \in ]1, +\infty[$ .
- $L_\infty$  est le dual topologique de  $L_1$  si  $\mu$  est  $\sigma$ -finie.

[LI]  
p. 140

## 10 Équation de Sylvester

On montre que l'équation  $AX + XB = C$  d'inconnue  $X$  admet une unique solution pour tout  $C \in \mathcal{M}_n(\mathbb{C})$  et pour tout  $A, B \in \mathcal{M}_n(\mathbb{C})$  dont les valeurs propres sont de partie réelle strictement négative.

**Lemme 1.** Soit  $\|\cdot\|$  une norme d'algèbre sur  $\mathcal{M}_n(\mathbb{C})$ , et soit  $A \in \mathcal{M}_n(\mathbb{C})$  une matrice dont les valeurs propres sont de partie réelle strictement négative. Alors il existe une fonction polynômiale  $P : \mathbb{R} \rightarrow \mathbb{R}$  et  $\lambda > 0$  tels que  $\|e^{tA}\| \leq e^{-\lambda t} P(t)$ .

[GOU21]  
p. 200

*Démonstration.* On fait la décomposition de Dunford de  $A : A = D + N$ . Comme  $D$  et  $N$  commutent, on a  $e^{tA} = e^{tD} e^{tN}$ . Soient  $P$  la matrice de passage donnée par la base de diagonalisation de  $D$  et  $\lambda_1, \dots, \lambda_n$  ses valeurs propres. En notant  $\|\cdot\|$  la norme subordonnée à  $\|\cdot\|_\infty$  sur  $\mathbb{C}^n$ , on a  $\forall t \geq 0$ ,

$$\begin{aligned} \|e^{tD}\| &= \|e^{tP \text{Diag}(\lambda_1, \dots, \lambda_n) P^{-1}}\| \\ &= \|P e^{t \text{Diag}(\lambda_1, \dots, \lambda_n)} P^{-1}\| \\ &\leq \underbrace{\|P\| \|P^{-1}\|}_{=\alpha} \sup_{\|x\|_\infty=1} \|\text{Diag}(e^{t\lambda_1}, \dots, e^{t\lambda_n})x\|_\infty \\ &\leq \alpha \sup_{i \in \llbracket 1, n \rrbracket} |e^{t\lambda_i}| \\ &\leq \alpha e^{-\lambda t} \end{aligned}$$

où  $\lambda > 0$  par hypothèse. En dimension finie, toutes les normes sont équivalentes, donc il existe  $\beta > 0$  tel que  $\|e^{tD}\| \leq \beta e^{-\lambda t}$ .

Pour conclure, en notant  $r$  l'indice de nilpotence de  $N$ ,

$$\begin{aligned} \|e^{tA}\| &\leq \|e^{tD}\| \|e^{tN}\| \\ &\leq e^{-\lambda t} \underbrace{\sum_{k=0}^{r-1} \beta \frac{\|N\|^k t^k}{k}}_{=P(t)} \end{aligned}$$

□

**Théorème 2** (Équation de Sylvester). Soient  $A$  et  $B \in \mathcal{M}_n(\mathbb{C})$  deux matrices dont les valeurs propres sont de partie réelle strictement négative. Alors pour tout  $C \in \mathcal{M}_n(\mathbb{C})$ , l'équation  $AX + XB = C$  admet une unique solution  $X$  dans  $\mathcal{M}_n(\mathbb{C})$ .

[I-P]  
p. 177

*Démonstration.* Comme l'application  $\varphi : X \mapsto AX + XB$  est un endomorphisme de  $\mathcal{M}_n(\mathbb{C})$ , qui est un espace vectoriel de dimension finie, il suffit de montrer qu'elle est surjective pour obtenir l'injectivité (et donc l'unicité de la solution). Soit  $C \in \mathcal{M}_n(\mathbb{C})$ . On considère le problème de Cauchy suivant d'inconnue  $Y : \mathbb{R} \rightarrow \mathcal{M}_n(\mathbb{C})$  :

$$\begin{cases} Y' = AY + YB \\ Y(0) = C \end{cases} \quad (E)$$



Il s'agit d'une équation différentielle linéaire à coefficients constants (on peut voir cela notamment en calculant les produits  $AY$  et  $YB$  et en effectuant la somme; l'égalité matricielle avec  $Y'$  donnant le système d'équations voulu). D'après le théorème de Cauchy-Lipschitz linéaire,  $(E)$  admet une unique solution définie sur  $\mathbb{R}$  tout entier, que l'on note  $Y$ .

On vérifie que la solution est définie  $\forall t \in \mathbb{R}$  par  $Y(t) = \exp(tA)C \exp(tB)$ . En effet pour tout  $t \in \mathbb{R}$ , on a :

$$Y'(t) = A \exp(tA)C \exp(tB) + \exp(tA)CB \exp(tB) = AY + YB$$

car toute matrice  $M$  commute avec son exponentielle (puisque  $\exp(M)$  est limite d'un polynôme en  $M$ ) et donc  $M$  commute aussi avec  $\exp(tM)$  pour tout  $t \in \mathbb{R}$ .

On va maintenant montrer que  $X = -\int_0^{+\infty} Y(s) ds$  est la solution de l'équation de Sylvester. Pour tout  $t \geq 0$ , on intègre  $Y'$  entre 0 et  $t$  pour obtenir :

$$Y(t) - C = \int_0^t Y'(s) ds = A \times \int_0^t Y(s) ds + \int_0^t Y(s) ds \times B$$

Il ne reste donc plus qu'à montrer que  $Y(t) \rightarrow 0$  et que  $Y$  est intégrable pour conclure. Par le Théorème 1, il existe  $\lambda_1, \lambda_2 > 0$  et  $P_1, P_2 : \mathbb{R} \rightarrow \mathbb{R}$  polynômiales tels que  $\|e^{tA}\| \leq e^{-\lambda_1 t} P_1(t)$  et  $\|e^{tB}\| \leq e^{-\lambda_2 t} P_2(t)$  pour tout  $t \geq 0$ . Ainsi, en posant  $\lambda = \max(\lambda_1, \lambda_2)$  et  $P = P_1 P_2$ , comme  $\|\cdot\|$  est une norme d'algèbre :

$$\|Y(t)\| = \|e^{tA} C e^{tB}\| \leq \|C\| P(t) e^{-2\lambda t}$$

En particulier, on a bien  $Y(t) \rightarrow 0$ . De plus, comme  $\|C\| P(t) e^{-2\lambda t}$  est intégrable sur  $[0, +\infty[$  et domine  $\|Y(t)\|$ , alors  $Y$  est aussi intégrable  $[0, +\infty[$ . Finalement, en faisant  $t \rightarrow +\infty$ , on obtient :

$$-C = A \times \int_0^{+\infty} Y(s) ds + \int_0^{+\infty} Y(s) ds \times B$$

Donc  $\varphi(X) = C$  :  $\varphi$  est surjective et  $X$  est bien la solution de l'équation de Sylvester.  $\square$

*Remarque 3.* Pour dire que toute matrice  $M$  commute avec  $\exp(M)$ , on aurait simplement pu dire que  $\exp(M)$  est un polynôme en  $M$  ie.  $\forall M \in \mathcal{M}_n(\mathbb{C}), \exists P \in \mathbb{C}[X]$  tel que  $\exp(M) = P(M)$ .

[GOU21]  
p. 189

*Démonstration.* Soit  $M \in \mathcal{M}_n(\mathbb{C})$ . L'ensemble  $\mathbb{C}[M] = \{P(M) \mid P \in \mathbb{C}[X]\}$  est un sous-espace vectoriel de  $\mathcal{M}_n(\mathbb{C})$  qui est de dimension finie, donc  $\mathbb{C}[M]$  l'est aussi et est en particulier fermé.

Pour tout  $n \in \mathbb{N}$ , on pose  $P_n = \sum_{k=0}^n \frac{M^k}{k!} \in \mathbb{C}[M]$  de sorte que  $P_n \xrightarrow{n \rightarrow +\infty} \exp(M)$ . Comme  $\mathbb{C}[M]$  est fermé, on en déduit que  $\exp(M) \in \mathbb{C}[M]$ . Donc  $\exists P \in \mathbb{C}[X]$  tel que  $\exp(M) = P(M)$ .  $\square$

## 11 Équivalence des normes en dimension finie et théorème de Riesz

On montre l'équivalence des normes en dimension finie ainsi que le théorème de Riesz sur la compacité de la boule unité fermée toujours en dimension finie, qui sont deux résultats fondamentaux sur les espaces vectoriels normés.

**Lemme 1.** Les compacts de  $(\mathbb{R}^n, \|\cdot\|_\infty)$  sont les fermés bornés.

[I-P]  
p. 422

*Démonstration.* Soit  $X$  une partie fermée bornée de  $\mathbb{R}^n$ . Soit  $(x_n)$  une suite de  $X$ . On note  $\forall k \in \mathbb{N}$ ,  $\forall i \in \llbracket 1, n \rrbracket$ ,  $x_k^i$  la  $i$ -ième composante du vecteur  $x_k$ . Comme  $X$  est bornée, alors  $(\|x_n\|_\infty)$  est une suite réelle bornée. Montrons par récurrence que, pour tout  $k \in \llbracket 1, n \rrbracket$ , il existe des extractrices  $\varphi_1, \dots, \varphi_i$  telle que la suite réelle  $(x_{\varphi_1 \circ \dots \circ \varphi_i(n)}^i)$  converge pour tout  $i \in \llbracket 1, k \rrbracket$ .

- Pour  $k = 1$ , c'est une réécriture du théorème de Bolzano-Weierstrass.
- Pour  $k > 1$ , supposons avoir construit  $\varphi_1, \dots, \varphi_k$  telles que  $(x_{\varphi_1 \circ \dots \circ \varphi_k(n)}^i)$  converge pour tout  $i \in \llbracket 1, k \rrbracket$ . Comme

$$|x_n^{k+1}| \leq \|x_n\|_\infty$$

$(x_{\varphi_1 \circ \dots \circ \varphi_k(n)}^{k+1})$  est une suite réelle bornée. Toujours par le théorème de Bolzano-Weierstrass, il existe une extractrice  $\varphi_{k+1}$  telle que  $(x_{\varphi_1 \circ \dots \circ \varphi_{k+1}(n)}^{k+1})$  converge. D'où l'hérédité.

La propriété est en particulier vraie pour  $k = n$ . En posant  $\varphi = \varphi_1 \circ \dots \circ \varphi_n$ , on obtient une extractrice telle que

$$\forall i \in \llbracket 1, n \rrbracket, (x_{\varphi(n)}^i) \text{ converge}$$

et on en déduit que  $(x_{\varphi(n)})$  converge vers un réel  $x \in \mathbb{R}^n$ . Comme  $X$  est fermé,  $x \in X$ .  $X$  est donc séquentiellement compact, donc compact.  $\square$

**Proposition 2.** Soient  $(E, d_E)$ ,  $(F, d_F)$  deux espaces métriques et  $f : E \rightarrow F$  continue. Si  $E$  est compact, alors  $f(E)$  est compact dans  $F$ .

*Démonstration.* Soit  $(y_n)$  une suite d'éléments de  $f(E)$ . On pose  $\forall n \in \mathbb{N}$ ,  $x_n = f(y_n)$ .  $E$  est compact, donc il existe une extractrice  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  telle que  $x_{\varphi(n)} \xrightarrow{n \rightarrow +\infty} x$  où  $x \in E$ . Par continuité,

$$y_{\varphi(n)} = f(x_{\varphi(n)}) \xrightarrow{n \rightarrow +\infty} f(x) \in f(E)$$

$f(E)$  est ainsi séquentiellement compact, donc est compact.  $\square$

**Théorème 3.** Soit  $E$  un espace vectoriel sur le corps  $\mathbb{R}$  de dimension finie  $n \in \mathbb{N}$ . Alors, toutes les normes sur  $E$  sont équivalentes.

*Démonstration.* Soient  $\mathcal{B} = (e_1, \dots, e_n)$  une base de  $E$ . On définit la norme infinie  $\mathcal{N}_\infty$  associée à

la base  $\mathcal{B}$  pour tout  $x = \sum_{i=1}^n x_i e_i \in E$  par

$$\mathcal{N}_\infty : x \mapsto \max_{i \in \llbracket 1, n \rrbracket} |x_i|$$

Si  $\mathcal{N}$  est une norme sur  $E$ , on a :

$$\mathcal{N}(x) \leq \underbrace{\left( \sum_{i=1}^n \mathcal{N}(e_i) \right)}_{=\alpha} \mathcal{N}_\infty(x)$$

Donc  $\mathcal{N}_\infty$  est plus fine que  $\mathcal{N}$ .

Définissons l'isomorphisme suivant :

$$f : \begin{array}{ll} (\mathbb{R}^n, \|\cdot\|_\infty) & \rightarrow (E, \mathcal{N}) \\ (x_1, \dots, x_n) & \mapsto \sum_{i=1}^n x_i e_i \end{array}$$

La fonction  $f$  vérifie

$$\forall x \in \mathbb{R}^n, \mathcal{N}(f(x)) \leq \alpha \|x\|_\infty$$

c'est une application linéaire bornée, qui est donc continue. On considère l'ensemble

$$S_E = f(S)$$

où  $S$  désigne la sphère unité de  $(\mathbb{R}^n, \|\cdot\|_\infty)$  qui est compacte d'après le Théorème 1. D'après le Théorème 2,  $S_E$  est compacte comme image d'un compact par une application continue.

Montrons que  $S_E$  est la sphère unité de  $(E, \mathcal{N}_\infty)$ . Déjà, si  $x \in S$ , alors  $\mathcal{N}_\infty(f(x)) = \|x\|_\infty = 1$ , d'où l'inclusion directe. Pour l'inclusion réciproque, si  $y \in S_E$ , par bijectivité de  $f$ , on peut écrire  $y = f^{-1}(x)$  avec  $x \in \mathbb{R}^n$  et ainsi  $\|x\|_\infty = \mathcal{N}_\infty(f(x)) = 1$ .

L'application  $\mathcal{N} : E \rightarrow \mathbb{R}$  est continue car lipschitzienne ( $\forall x, y \in E, |\mathcal{N}(x) - \mathcal{N}(y)| \leq \mathcal{N}(x - y)$ ), donc est bornée et atteint ses bornes sur la sphère  $S_E$ . On note  $x_0 \in E$  ce minimum :

$$\forall x \in E \text{ tel que } \mathcal{N}_\infty(x) = 1, \text{ on a } \mathcal{N}(x) \geq \underbrace{\mathcal{N}(x_0)}_{=\beta}$$

Ainsi,

$$\forall x \in E, \mathcal{N}\left(\frac{x}{\mathcal{N}_\infty(x)}\right) \geq \beta \text{ ie. } \mathcal{N}(x) \geq \beta \mathcal{N}_\infty(x)$$

Donc  $\mathcal{N}$  est plus fine que  $\mathcal{N}_\infty$  : les normes  $\mathcal{N}$  et  $\mathcal{N}_\infty$  sont équivalentes. Comme la relation d'équivalence sur les normes d'un espace vectoriel est transitive, on en déduit que toutes les normes sur  $E$  sont équivalentes.  $\square$

**Théorème 4 (Riesz).** Soit  $(E, \|\cdot\|)$  un espace vectoriel normé sur le corps  $\mathbb{R}$ . Alors,  $E$  est de dimension finie si et seulement si sa boule unité fermée est compacte.

*Démonstration.* Notons  $\bar{B}$  la boule unité fermée de  $E$  et supposons  $E$  de dimension finie  $n \in \mathbb{N}$ . Comme dans la démonstration du théorème précédent,  $\bar{B}$  est compacte comme image de la

boule unité fermée de  $(\mathbb{R}^n, \|\cdot\|_\infty)$  par l'application continue  $f$ . Réciproquement, supposons  $E$  de dimension finie et, par l'absurde, également que  $\overline{B}$  est compact. On a,

$$\overline{B} \subseteq \bigcup_{x \in E} B(x, 1)$$

où  $B(x, 1)$  désigne la boule ouverte centrée en  $x$  de rayon 1. Par la propriété de Borel-Lebesgue, il existe  $x_1, \dots, x_n \in E$  tels que

$$\overline{B} \subseteq \bigcup_{i=1}^n B(x_i, 1)$$

On définit  $F = \text{Vect}(x_1, \dots, x_n)$ . Comme  $F$  est de dimension finie et  $E$  de dimension infinie, on peut trouver  $y \in E \setminus F$ . Soit  $x_0 \in F$  le projeté de  $y$  sur  $F$  :

$$d(y, F) = \|y - x_0\| > 0$$

On pose

$$u = \frac{y - x_0}{\|y - x_0\|}$$

On a  $u$  de norme 1, donc  $u \in \overline{B}$  et il existe  $i \in \llbracket 1, n \rrbracket$  tel que  $\|u - x_i\| < 1$ . Or,

$$\begin{aligned} \|u - x_i\| &= \frac{\|y - x_0 - \|y - x_0\|x_i\|}{\|y - x_0\|} \\ &= \frac{\|y - (x_0 - \|y - x_0\|x_i)\|}{\|y - x_0\|} \\ &\geq \frac{d(y, F)}{\|y - x_0\|} \\ &= 1 \end{aligned}$$

car  $x_0 + \|y - x_0\|x_i \in F$  : absurde. □

## 12 Formes de Hankel

Le but de ce développement est de construire une forme quadratique permettant de dénombrer les racines réelles distinctes d'un polynôme en fonction de ses racines complexes.

Soit  $P \in \mathbb{R}[X]$  un polynôme de degré  $n$ .

[C-G]  
p. 356

**Théorème 1** (Formes de Hankel). On note  $x_1, \dots, x_t$  les racines complexes de  $P$  de multiplis-  
cités respectives  $m_1, \dots, m_t$ . On pose

$$s_0 = n \text{ et } \forall k \geq 1, s_k = \sum_{i=1}^t m_i x_i^k$$

Alors :

- (i)  $\sigma = \sum_{i,j \in \llbracket 0, n-1 \rrbracket} s_{i+j} X_i X_j$  définit une forme quadratique sur  $\mathbb{C}^n$  ainsi qu'une forme quadratique  $\sigma_{\mathbb{R}}$  sur  $\mathbb{R}^n$ .
- (ii) Si on note  $(p, q)$  la signature de  $\sigma_{\mathbb{R}}$ , on a :
  - $t = p + q$ .
  - Le nombre de racines réelles distinctes de  $P$  est  $p - q$ .

*Démonstration.*  $\sigma$  est un polynôme homogène de degré 2 sur  $\mathbb{C}$  (car la somme des exposants est 2 pour chacun des monômes), qui définit donc une forme quadratique sur  $\mathbb{C}^n$ . De plus, on peut écrire :

$$\forall k \geq 1, s_k = \sum_{\substack{x_i \text{ racine de } P \\ x_i \in \mathbb{R}}} m_i x_i^k + \sum_{\substack{x \text{ racine de } P \\ x_i \in \mathbb{C}}} m_i (x^i + \bar{x}^k)$$

donc  $s_k = \overline{s_k}$  ie.  $s_k \in \mathbb{R}$ . Donc  $\sigma$  définit une forme quadratique  $\sigma_{\mathbb{R}}$  sur  $\mathbb{R}^n$ . D'où le premier point.

Soit  $\varphi_k$  la forme linéaire sur  $\mathbb{C}^n$  définie par le polynôme homogène de degré 1

$$P_k(X_0, \dots, X_{n-1}) = X_0 + x_k X_1 + \dots + x_k^{n-1} X_{n-1}$$

pour  $k \in \llbracket 0, t \rrbracket$ . Dans la base duale  $(e_i^*)_{i \in \llbracket 0, n-1 \rrbracket}$  de la base canonique  $(e_i)_{i \in \llbracket 0, n-1 \rrbracket}$  de  $\mathbb{C}^n$ , on a

$$\varphi_k = e_0^* + x_k e_1^* + \dots + x_k^{n-1} e_{n-1}^*$$

Et comme

$$\det((\varphi_k)_{k \in \llbracket 0, t \rrbracket}) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_0 & x_1 & \dots & x_t \\ \vdots & \ddots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \dots & x_t^{n-1} \end{vmatrix} \begin{matrix} \text{Vandermonde} \\ \neq 0 \end{matrix}$$

la famille  $(\varphi_k)_{k \in \llbracket 0, t \rrbracket}$  est de rang  $t$  sur  $\mathbb{C}$ . Or, le coefficient de  $X_i X_j$  dans  $\sum_{k=1}^t m_k P_k^2$  vaut

$$\begin{cases} \sum_{k=1}^t m_k x_k^{2i} = s_{i+j} & \text{si } i = j \\ \sum_{k=1}^t 2m_k x_k^i x_k^j = \sum_{k=1}^t 2m_k x_k^{i+j} = 2s_{i+j} & \text{sinon} \end{cases}$$

donc,  $\sigma = \sum_{k=1}^t m_k \varphi_k^2$ . En particulier,  $\text{rang}(\sigma) = t$  par indépendance des  $\varphi_k$ . On en déduit,

$$p + q = \text{rang}(\sigma_{\mathbb{R}}) = \text{rang}(\sigma) = t$$

(le rang est invariant par extension de corps).

Soit  $k \in \llbracket 0, t \rrbracket$ . Calculons la signature de la forme quadratique  $\varphi_k^2 + \overline{\varphi_k}^2$  :

- Si  $x_k \in \mathbb{R}$ , on a  $\varphi_k^2 + \overline{\varphi_k}^2 = 2\varphi_k^2$ , qui est de signature  $(1, 0)$  car  $\varphi_k \neq 0$ .
- Si  $x_k \notin \mathbb{R}$ , on a  $\varphi_k^2 + \overline{\varphi_k}^2 = 2\text{Re}(\varphi_k)^2 - 2\text{Im}(\varphi_k)^2$  qui est bien une forme quadratique réelle. Et  $x_k \neq \overline{x_k}$ , donc la matrice

$$\begin{pmatrix} 1 & 1 \\ x_k & \overline{x_k} \\ \vdots & \vdots \\ x_k^{n-1} & \overline{x_k}^{n-1} \end{pmatrix}$$

est de rang 2 (cf. le mineur correspondant aux deux premières lignes). Donc  $\varphi_k$  et  $\overline{\varphi_k}$  sont indépendantes. Ainsi,  $\text{rang}(\varphi_k^2 + \overline{\varphi_k}^2) = 2$  sur  $\mathbb{C}$ , donc sur  $\mathbb{R}$  aussi (toujours par invariance du rang par extension de corps). Donc la signature de  $\varphi_k^2 + \overline{\varphi_k}^2$  est  $(1, 1)$ .

Maintenant, regroupons les  $\varphi_k$  conjuguées entre elles lorsqu'elles ne sont pas réelles :

$$\sigma = \sum_{\substack{k=1 \\ x_k \in \mathbb{R}}}^t m_k \varphi_k^2 + \sum_{\substack{k=1 \\ x_k \notin \mathbb{R}}}^t m_k (\varphi_k^2 + \overline{\varphi_k}^2)$$

En passant à la signature, on obtient :

$$(p, q) = (r, 0) + \left( \frac{t-r}{2}, \frac{t-r}{2} \right) = \left( \frac{t+r}{2}, \frac{t-r}{2} \right)$$

où  $r$  désigne le nombre de racines réelles distinctes de  $P$ . Par unicité de la signature d'une forme quadratique réelle, on a bien  $p - q = r$ . D'où le point (ii).  $\square$

*Remarque 2.* Tout l'intérêt de ces formes quadratiques est qu'on peut calculer les  $s_k$  par récurrence en utilisant les polynômes symétriques élémentaires, sans avoir besoin des racines.

**Proposition 3** (Sommes de Newton). On pose  $P = \sum_{k=0}^n a_k X^k$ . Les sommes de Newton vérifient les relations suivantes :

- (i)  $s_0 = n$ .
- (ii)  $\forall k \in \llbracket 1, n-1 \rrbracket, s_k = -k a_{n-k} \sum_{i=1}^{k-1} s_i a_{n-k+i}$ .
- (iii)  $\forall p \in \mathbb{N}, s_{p+n} = \sum_{i=1}^n s_i a_{p+n-i}$ .

## 13 Formule de Stirling

Dans ce développement un peu technique, nous démontrons la formule de Stirling  $n! \sim \sqrt{2n\pi} \left(\frac{n}{e}\right)^n$  à l'aide du théorème central limite et de la fonction  $\Gamma$  d'Euler.

**Lemme 1.** Soit  $Y$  une variable aléatoire réelle à densité. Alors  $\forall n \geq 1$ ,  $\frac{Y-n}{\sqrt{n}}$  est à densité et,

$$f_{\frac{Y-n}{\sqrt{n}}}(x) = \sqrt{n}f_Y(n + x\sqrt{n}) \text{ pp. en } x \in \mathbb{R}$$

*Démonstration.*  $\forall x \in \mathbb{R}$ ,

$$\begin{aligned} F_{\frac{Y-n}{\sqrt{n}}}(x) &= \mathbb{P}\left(\frac{Y-n}{\sqrt{n}} \leq x\right) \\ &= \mathbb{P}(Y \leq x\sqrt{n} + n) \\ &= F_Y(x\sqrt{n} + n) \end{aligned}$$

Or, la fonction de répartition d'une variable aléatoire réelle à densité est dérivable presque partout, et sa dérivée est presque partout égale à sa densité. Donc :

$$f_{\frac{Y-n}{\sqrt{n}}}(x) = \sqrt{n}f_Y(x\sqrt{n} + n) \text{ pp. en } x \in \mathbb{R}$$

□

*Remarque 2.* Il ne s'agit ni plus ni moins qu'une version affaiblie du théorème de changement de variable.

**Lemme 3.** Soient  $X$  et  $Y$  deux variables aléatoires indépendantes telles que  $X \sim \Gamma(a, \gamma)$  et  $Y \sim \Gamma(b, \gamma)$ . Alors  $Z = X + Y \sim \Gamma(a + b, \gamma)$ .

[G-K]  
p. 180

*Démonstration.* Soit  $f_{a,\gamma} : x \mapsto \frac{\gamma^a}{\Gamma(a)} x^{a-1} e^{-\gamma x} \mathbb{1}_{\mathbb{R}^+}(x)$  la densité de la loi  $\Gamma(a, \gamma)$ .  $\forall x \geq 0$ , on a :

$$\begin{aligned} f_Z(x) &= \int_0^x f_{a,\gamma}(t) f_{b,\gamma}(x-t) dt \\ &= \int_0^x \frac{\gamma^a}{\Gamma(a)} t^{a-1} e^{-\gamma t} \frac{\gamma^b}{\Gamma(b)} (x-t)^{b-1} e^{-\gamma(x-t)} dt \\ &= \frac{\gamma^{a+b} e^{-\gamma x}}{\Gamma(a)\Gamma(b)} \int_0^x t^{a-1} (x-t)^{b-1} dt \\ &\stackrel{t=ux}{=} \frac{\gamma^{a+b} e^{-\gamma x}}{\Gamma(a)\Gamma(b)} x^{a+b-1} \int_0^1 u^{a-1} (1-u)^{b-1} du \\ &= K_{a,b} f_{a+b,\gamma}(x) \end{aligned}$$

où  $K_{a,b} = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} \int_0^1 u^{a-1} (1-u)^{b-1} du$ . Notons par ailleurs que  $f_Z$  est nulle sur  $\mathbb{R}^-$  et coïncide donc avec  $K_{a,b} f_{a+b,\gamma}$  sur  $\mathbb{R}^+$ .

Pour conclure, on utilise la condition de normalisation :

$$1 = \int_{\mathbb{R}} f_Z(x) dx = K_{a,b} \int_{\mathbb{R}} f_{a+b,\gamma}(x) dx = K_{a,b}$$

On obtient ainsi  $f_Z = f_{a+b,\gamma}$ , ce que l'on voulait.  $\square$

#### **Théorème 4** (Formule de Stirling).

$$n! \sim \sqrt{2n\pi} \left(\frac{n}{e}\right)^n$$

p. 556

*Démonstration.* Soit  $(X_n)$  une suite de variable aléatoires indépendantes de même loi  $\mathcal{E}(1)$ . On pose  $S_n = \sum_{k=0}^n X_k$ . Montrons par récurrence que  $S_n \sim \Gamma(n+1, 1)$ .

- Pour  $n = 0$  : c'est clair car  $\mathcal{E}(1) = \Gamma(1, 1)$ .
- On suppose le résultat vrai à un rang  $n \geq 0$ . Pour montrer qu'il reste vrai au rang  $n+1$ , il suffit d'appliquer le Théorème 3 à  $S_n \sim \Gamma(n, 1)$  et  $X_{n+1} \sim \Gamma(1, 1)$  (qui sont bien indépendantes).

Par le Théorème 1 appliqué à  $S_n$ , pp. en  $x \in \mathbb{R}$ ,

$$\begin{aligned} \overbrace{f_{\frac{S_n-n}{\sqrt{n}}}(x)}^{=g_n(x)} &= \sqrt{n} f_{S_n}(n + x\sqrt{n}) \\ &= \frac{\sqrt{n}}{\Gamma(n+1)} n^n \left(1 + \frac{x}{\sqrt{n}}\right)^n e^{-(n+x\sqrt{n})} \mathbb{1}_{[-\sqrt{n}, +\infty[}(x) \\ &= a_n h_n(x) \end{aligned}$$

avec :

- $a_n = \frac{n^{n+\frac{1}{2}} e^{-n} \sqrt{2\pi}}{\Gamma(n+1)}$  (ce qui nous intéresse).
- $h_n : x \mapsto \frac{e^{-\sqrt{n}x}}{\sqrt{2\pi}} \left(1 + \frac{x}{\sqrt{n}}\right)^n \mathbb{1}_{[-\sqrt{n}, +\infty[}(x)$  (ce qui nous intéresse moins).

Montrons maintenant que  $\frac{S_n-n}{\sqrt{n}}$  converge en loi vers  $\mathcal{N}(0, 1)$ . D'après le théorème central limite,

$$\frac{S_n - \mathbb{E}(S_n)}{\sqrt{\text{Var}(S_n)}} \xrightarrow{(d)} \mathcal{N}(0, 1)$$

où :

- $\mathbb{E}(S_n) = (n+1)\mathbb{E}(X_0) = n+1$ .
- $\text{Var}(S_n) = (n+1)\text{Var}(X_0) = n+1$  par indépendance.



On applique maintenant le théorème de Slutsky :

$$\frac{S_n - n}{\sqrt{n}} = \underbrace{\frac{\sqrt{n+1}}{\sqrt{n}}}_{\rightarrow 1} \left( \underbrace{\frac{S_n - (n+1)}{\sqrt{n+1}}}_{\xrightarrow{(d)} \mathcal{N}(0,1)} + \underbrace{\frac{1}{\sqrt{n+1}}}_{\rightarrow 0} \right) \xrightarrow{(d)} \mathcal{N}(0,1)$$

Tout cela pour dire que,

$$\int_0^1 g_n(x) dx = \mathbb{P} \left( \frac{S_n - n}{\sqrt{n}} \in [0, 1] \right) \rightarrow \int_0^1 \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}} dx$$

De plus :

- $\forall n \in \mathbb{N}$ ,  $h_n$  est mesurable.
- $\forall x \in \mathbb{R}$ ,  $h_n(x) = \frac{e^{-x^2 \varphi\left(\frac{x}{\sqrt{n}}\right)}}{\sqrt{2\pi}} \mathbb{1}_{]-1, +\infty[}\left(\frac{x}{\sqrt{n}}\right)$  où  $\forall x > -1$ ,  $\varphi(x) = \frac{x - \ln(1+x)}{x^2}$ . Par développement limité, on a  $\lim_{x \rightarrow 0} \varphi(x) = \frac{1}{2}$ . Donc  $\forall x \in \mathbb{R}$ ,  $h_n(x) \rightarrow \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}$ .
- Comme  $\forall x > -1$ ,  $\varphi(x) \geq 0$ , alors  $h_n$  est dominée par  $x \mapsto \frac{1}{\sqrt{2\pi}}$ .

Donc par le théorème de convergence dominée,

$$\int_0^1 h_n(x) dx \rightarrow \int_0^1 \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}} dx$$

Pour conclure, on écrit :

$$\int_0^1 g_n(x) dx = a_n \int_0^1 h_n(x) dx \Rightarrow \lim_{n \rightarrow +\infty} a_n = \frac{\lim_{n \rightarrow +\infty} \int_0^1 g_n(x) dx}{\lim_{n \rightarrow +\infty} \int_0^1 h_n(x) dx} = 1$$

et comme  $\Gamma(n+1) = n!$ , par définition de  $a_n$  :

$$1 = \lim_{n \rightarrow +\infty} a_n = \lim_{n \rightarrow +\infty} \frac{n^{n+\frac{1}{2}} e^{-n} \sqrt{2\pi}}{n!}$$

□

## 14 Formule sommatoire de Poisson

On démontre la formule sommatoire de Poisson en utilisant principalement la théorie des séries de Fourier.

**Théorème 1** (Formule sommatoire de Poisson). Soit  $f : \mathbb{R} \rightarrow \mathbb{C}$  une fonction de classe  $\mathcal{C}^1$  telle que  $f(x) = O\left(\frac{1}{x^2}\right)$  et  $f'(x) = O\left(\frac{1}{x^2}\right)$  quand  $|x| \rightarrow +\infty$ . Alors :

$$\forall x \in \mathbb{R}, \sum_{n \in \mathbb{Z}} f(x+n) = \sum_{n \in \mathbb{Z}} \hat{f}(2\pi n) e^{2i\pi n x}$$

où  $\hat{f}$  désigne la transformée de Fourier de  $f$ .

[GOU20]  
p. 284

*Démonstration.* Comme  $f(x) = O\left(\frac{1}{x^2}\right)$ , il existe  $M > 0$  et  $A > 0$  tel que

$$\forall |x| > A, |f(x)| \leq \frac{M}{x^2} \quad (*)$$

Soit  $K > 0$ . On a  $\forall x \in [-K, K], \forall n \in \mathbb{Z}$  tel que  $|n| > K + A$  :

$$|f(x+n)| \stackrel{(*)}{\leq} \frac{M}{(x+n)^2} \leq \frac{M}{(|n|-|x|)^2} \leq \frac{M}{(|n|-K)^2}$$

Donc  $\sum_{n \in \mathbb{Z}} f(x+n)$  converge normalement sur tout segment de  $\mathbb{R}$  donc converge simplement sur  $\mathbb{R}$ . On note  $F$  la limite simple en question.

On montre de même que  $\sum_{n \in \mathbb{Z}} f'(x+n)$  converge normalement sur tout segment de  $\mathbb{R}$ . Donc par le théorème de dérivation des suites de fonctions,  $F$  est de classe  $\mathcal{C}^1$  sur tout segment de  $\mathbb{R}$ , donc sur  $\mathbb{R}$  tout entier (la continuité et la dérivabilité sont des propriétés locales).

Soit  $x \in \mathbb{R}$ . On a :

$$\begin{aligned} \forall N \in \mathbb{N}, \sum_{n=-N}^N f(x+1+n) &= \sum_{n=-N-1}^{N+1} f(x+n) \\ &\xrightarrow{N \rightarrow +\infty} F(x+1) = F(x) \end{aligned}$$

ie.  $F$  est 1-périodique. On peut calculer ses coefficients de Fourier.  $\forall n \in \mathbb{Z}$ ,

$$c_n(F) = \int_0^1 F(t) e^{-2i\pi n t} dt = \int_0^1 \sum_{n=-\infty}^{+\infty} f(t+n) e^{-2i\pi n t} dt$$

Par convergence uniforme sur un segment, on peut échanger somme et intégrale :

$$c_n(F) = \sum_{n=-\infty}^{+\infty} \int_n^{n+1} f(t) e^{-2i\pi n t} dt$$

Or, la transformée de Fourier d'une fonction  $L_1$  est convergente. On peut donc écrire :

$$c_n(F) = \int_{-\infty}^{+\infty} f(t) e^{-2i\pi n t} dt = \hat{f}(2\pi n)$$

Comme  $F$  est de classe  $\mathcal{C}^1$ , sa série de Fourier converge uniformément vers  $F$ . D'où le résultat.  $\square$

**Application 2** (Identité de Jacobi).

$$\forall s > 0, \sum_{n=-\infty}^{+\infty} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n=-\infty}^{+\infty} e^{-\frac{\pi n^2}{s}}$$

*Démonstration.* Soit  $\alpha > 0$ . On définit  $G_\alpha : x \mapsto e^{-\alpha x^2}$  et on connaît sa transformée de Fourier :

$$\forall \xi \in \mathbb{R}, \widehat{G_\alpha}(\xi) = \sqrt{\frac{\pi}{\alpha}} e^{-\frac{\xi^2}{4\alpha}}$$

Soit  $s > 0$ . Appliquons le Théorème 1 à la fonction  $G_{\pi s}$  :

$$\begin{aligned} \sum_{n \in \mathbb{Z}} e^{-\pi s(x+n)^2} &= \frac{1}{\sqrt{s}} \sum_{n \in \mathbb{Z}} e^{-\frac{(2\pi n)^2}{4\pi s}} e^{2i\pi n x} \\ \xRightarrow{x=0} \sum_{n \in \mathbb{Z}} e^{-\pi s n^2} &= \frac{1}{\sqrt{s}} \sum_{n \in \mathbb{Z}} e^{-\frac{\pi n^2}{s}} \end{aligned}$$

$\square$

## 15 $\exp : \mathcal{S}_n(\mathbb{R}) \rightarrow \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme

Dans ce développement, on démontre que l'exponentielle de matrices induit un homéomorphisme de  $\mathcal{S}_n(\mathbb{R})$  sur  $\mathcal{S}_n^{++}(\mathbb{R})$ .

**Lemme 1.**  $\mathcal{S}_n(\mathbb{R})$  est un fermé de  $\mathcal{M}_n(\mathbb{R})$ .

*Démonstration.* Il suffit d'écrire

$$\mathcal{S}_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid {}^t M = M\} = f^{-1}\{0\}$$

où  $f : M \mapsto {}^t M - M$  est continue, donc  $\mathcal{S}_n(\mathbb{R})$  est fermé en tant qu'image réciproque d'un fermé par une application continue.  $\square$

**Lemme 2.** Une suite bornée d'un espace métrique qui admet une seule valeur d'adhérence converge vers cette valeur d'adhérence.

*Démonstration.* Soit  $(x_n)$  une suite bornée d'un espace métrique  $(E, d)$  qui n'admet qu'une seule valeur d'adhérence  $\ell \in E$ . On suppose par l'absurde que  $(x_n)$  ne converge pas vers  $\ell$  :

$$\exists \epsilon > 0 \text{ tel que } \forall N \in \mathbb{N}, \exists n \geq N \text{ tel que } d(x_n, \ell) > \epsilon \quad (*)$$

On va construire une sous-suite qui converge vers une valeur d'adhérence différente de  $\ell$ .

Par  $(*)$  appliqué à  $N = 0$ ,  $\exists n_0 \geq 0$  tel que  $d(x_{n_0}, \ell) > \epsilon$ . On définit donc  $\varphi(0) = n_0$ .

Supposons construite  $\varphi(i)$  jusqu'à un rang  $k$  telle que  $\forall i \leq k$ ,  $\varphi(i+1) > \varphi(i)$  (lorsque cela a un sens) et  $d(x_{\varphi(i)}, \ell) > \epsilon$ . Il suffit alors d'appliquer  $(*)$  à  $N = \varphi(k) + 1$  pour obtenir un  $n_k \geq \varphi(k) + 1 > \varphi(k)$  tel que  $d(x_{n_k}, \ell) > \epsilon$ ; on définit alors  $\varphi(k+1) = n_k$ .

Nous venons donc de construire par récurrence une application  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  strictement croissante et telle que  $\forall n \in \mathbb{N}$ ,  $d(x_{\varphi(n)}, \ell) > \epsilon$ . La suite  $(x_{\varphi(n)})$  est bornée (par hypothèse) : elle est contenue dans un compact et admet une valeur d'adhérence  $\ell'$  (par le théorème de Bolzano-Weierstrass). Soit donc  $\phi : \mathbb{N} \rightarrow \mathbb{N}$  strictement croissante telle que  $(x_{(\varphi \circ \psi)(n)})$  converge vers  $\ell'$ .

On a  $\forall n \in \mathbb{N}$ ,  $d(x_{(\varphi \circ \psi)(n)}, \ell) > \epsilon$ , qui donne  $d(\ell', \ell) \geq \epsilon$  après un passage à la limite. Donc  $\ell \neq \ell'$ . Et  $\ell'$  est clairement valeur d'adhérence de  $(x_n)$  : absurde.  $\square$

**Lemme 3.** Soit  $S \in \mathcal{S}_n(\mathbb{R})$ . Alors,

$$\|S\|_2 = \rho(S)$$

où  $\rho$  est l'application qui à une matrice  $y$  associe son rayon spectral.

[I-P]  
p. 182

*Démonstration.* D'après le théorème spectral, il existe  $(e_1, \dots, e_n)$  une base orthonormée de  $\mathbb{R}^n$  formée de vecteurs propres de  $S$  associés aux valeurs propres  $\lambda_1, \dots, \lambda_n$  de  $S$ , qui sont réelles car  $S$

est symétrique. Soit  $x \in \mathbb{R}^n$  dont on note  $(x_1, \dots, x_n)$  ses coordonnées dans cette base. On a

$$\|Sx\|_2^2 = \left\| \sum_{i=1}^n \lambda_i x_i e_i \right\|_2^2 = \sum_{i=1}^n \lambda_i^2 x_i^2 \leq \rho(S)^2 \|x\|_2^2$$

D'où  $\|S\|_2 \leq \rho(S)$ . Pour obtenir l'inégalité inverse, il suffit de considérer  $\lambda \in \mathbb{R}$  une valeur propre de  $S$  telle que  $|\lambda| = \rho(S)$  et  $x \in \mathbb{R}^n$  un vecteur propre associé à  $\lambda$ . On a alors

$$\|Sx\|_2 = |\lambda| \|x\|_2$$

et on a bien  $\rho(S) \leq \|S\|_2$ . □

**Théorème 4.** L'application  $\exp : \mathcal{S}_n(\mathbb{R}) \rightarrow \mathcal{S}_n^{++}(\mathbb{R})$  est un homéomorphisme.

*Démonstration.* Montrer qu'une application est un homéomorphisme se fait en 4 étapes : on montre qu'elle est continue, injective, surjective, et que la réciproque est elle aussi continue.

— L'application est bien définie et continue : Soit  $S \in \mathcal{S}_n(\mathbb{R})$ . D'après le théorème spectral,

$$\exists P \in \mathcal{O}_n(\mathbb{R}) \text{ telle que } S = P^{-1} \underbrace{\text{Diag}(\lambda_1, \dots, \lambda_n)}_{=D} P$$

où  $\lambda_1, \dots, \lambda_n$  désignent les valeurs propres de  $S$ . On a donc

$$\begin{aligned} \exp(S) &= P^{-1} \exp(D) P \\ &= P^{-1} \text{Diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) P \end{aligned}$$

Or,  $P^{-1} = {}^t P$ , donc  ${}^t \exp(S) = \exp(S)$  et  $\exp(S) \in \mathcal{S}_n(\mathbb{R})$ . De plus,  $\forall x \in \mathbb{R}^n$ ,

$${}^t x S x = {}^t (P x) D (P x) > 0$$

car  $D \in \mathcal{S}_n^{++}(\mathbb{R})$ . Donc  $S \in \mathcal{S}_n^{++}(\mathbb{R})$ . Elle est de plus continue en tant que restriction de l'exponentielle définie sur  $\mathcal{M}_n(\mathbb{K})$  (qui est la somme d'une série normalement convergente sur toute boule ouverte de  $\mathcal{M}_n(\mathbb{K})$ ).

— L'application est surjective : Soit  $S \in \mathcal{S}_n^{++}(\mathbb{R})$ . On peut écrire

$$S = P \text{Diag}(\mu_1, \dots, \mu_n) P^{-1}$$

Il suffit alors de poser  $U = P^{-1} \text{Diag}(\ln(\mu_1), \dots, \ln(\mu_n)) P \in \mathcal{S}_n(\mathbb{R})$  pour avoir  $\exp(U) = S$ ; d'où la surjectivité.

— L'application est injective : Soient  $S, S' \in \mathcal{S}_n(\mathbb{R})$  telles que  $\exp(S) = \exp(S')$ . Montrons que  $S = S'$ . Comme avant,  $\exists P, P' \in \mathcal{O}_n(\mathbb{R})$  telles que

$$S = P \text{Diag}(\lambda_1, \dots, \lambda_n) P^{-1} \text{ et } S' = P' \text{Diag}(\lambda'_1, \dots, \lambda'_n) P'^{-1}$$

Soit  $L \in \mathbb{R}[X]$  tel que  $\forall i \in \llbracket 1, n \rrbracket$ ,  $L(e^{\lambda_i}) = \lambda_i$  et  $L(e^{\lambda'_i}) = \lambda'_i$  (les polynômes d'interpolation de Lagrange conviennent parfaitement et sont bien définis dans le cas présent car  $e^{\lambda_i} =$

$e^{\lambda_j} \Rightarrow \lambda_i = \lambda_j$  par injectivité de l'exponentielle). D'où

$$\begin{aligned} L(\exp(S)) &= L(P \text{Diag}(\lambda_1, \dots, \lambda_n) P^{-1}) \\ &= PL(\exp(\text{Diag}(\lambda_1, \dots, \lambda_n))) P^{-1} \\ &= P \text{Diag}(\lambda_1, \dots, \lambda_n) P^{-1} \\ &= S \end{aligned}$$

et de même,  $L(\exp(S')) = S'$ . D'où  $S = S'$  car on a supposé  $\exp(S) = \exp(S')$ .

- L'application inverse est continue : Soit  $(A_k)$  une suite de  $\mathcal{S}_n^{++}(\mathbb{R})$  qui converge vers  $A \in \mathcal{S}_n^{++}(\mathbb{R})$ . Il s'agit de montrer que la suite  $(B_k)$  de terme général  $B_k = \exp^{-1}(A_k)$  converge vers  $B = \exp^{-1}(A)$ . Supposons tout d'abord  $(B_k)$  non bornée. Comme sur  $\mathcal{S}_n(\mathbb{R})$ ,  $\|\cdot\|_2 = \rho(\cdot)$  (par le Théorème 3), il existe  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  strictement croissante telle que  $\rho(B_{\varphi(k)}) \rightarrow +\infty$ . On peut donc extraire une suite de valeurs propres  $(\lambda_k)$  telle que  $|\lambda_k| \rightarrow +\infty$ . Encore une fois, quitte à extraire, on peut supposer  $\lambda_k \rightarrow +\infty$  ou  $\lambda_k \rightarrow -\infty$ .
- Si  $\lambda_k \rightarrow +\infty$ ,  $e^{\lambda_k} \rightarrow +\infty$ . Mais  $\forall k \in \mathbb{N}$ ,  $e^{\lambda_k}$  est valeur propre de  $A_k$ , donc  $\rho(A_k) \rightarrow +\infty$  : absurde car  $(A_k)$  converge.
  - Si  $\lambda_k \rightarrow -\infty$ ,  $e^{-\lambda_k} \rightarrow +\infty$ . Mais  $\forall k \in \mathbb{N}$ ,  $e^{-\lambda_k}$  est valeur propre de  $A_k^{-1}$ , donc  $\rho(A_k^{-1}) \rightarrow +\infty$  : absurde car  $(A_k^{-1})$  converge par continuité de  $M \mapsto M^{-1}$ .

Donc la suite  $(B_k)$  est bornée. Par le théorème de Bolzano-Weierstrass,  $(B_k)$  admet une valeur d'adhérence  $\widetilde{B}_0$ . Comme  $\mathcal{S}_n(\mathbb{R})$  est fermé (c'est le Théorème 1),  $\widetilde{B}_0 \in \mathcal{S}_n(\mathbb{R})$ .

Soit  $\widetilde{B} \in \mathcal{S}_n(\mathbb{R})$  une valeur d'adhérence de  $(B_k)$  et soit  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  strictement croissante telle que  $B_{\varphi(k)} \rightarrow \widetilde{B}$ . Alors,

$$\exp(B) = A \longleftarrow A_{\varphi(k)} = \exp(B_{\varphi(k)}) \longrightarrow \exp(\widetilde{B})$$

ie.  $\exp(B) = \exp(\widetilde{B})$ ; donc  $B = \widetilde{B} = \widetilde{B}_0$  par injectivité de  $\exp$ . Donc par le Théorème 2,  $B_k \rightarrow B$ .

□

## 16 Intégrale de Dirichlet

Il s'agit ici de calculer l'intégrale de Dirichlet en utilisant les théorèmes classiques d'intégration.

**Lemme 1.**

$$\forall y, t \in \mathbb{R}^+, |e^{-(y-i)t}| \leq 1$$

*Démonstration.* Soient  $y, t \in \mathbb{R}^+$ . On a :

$$|e^{-(y-i)t}| = |e^{-yt} e^{it}| = |e^{-yt}| |e^{it}|$$

Or,  $e^{it}$  est un complexe de module 1 et  $yt \geq 0$ , donc  $e^{-yt} \leq 1$ . D'où le résultat.  $\square$

**Théorème 2** (Intégrale de Dirichlet). On pose  $\forall x \geq 0$ ,

$$F(x) = \int_0^{+\infty} \frac{\sin(t)}{t} e^{-xt} dt$$

alors :

- (i)  $F$  est bien définie et est continue sur  $\mathbb{R}^+$ .
- (ii)  $F$  est dérivable sur  $\mathbb{R}_*^+$  et  $\forall x \in \mathbb{R}_*^+, F'(x) = -\frac{1}{1+x^2}$ .
- (iii)  $F(0) = \int_0^{+\infty} \frac{\sin(t)}{t} dt = \frac{\pi}{2}$ .

[G-K]  
p. 107

*Démonstration.* Posons  $\forall x \in \mathbb{R}^+$  et  $\forall t \in \mathbb{R}_*^+, f(x, t) = \frac{\sin(t)}{t} e^{-xt}$  ainsi que  $\forall n \geq 1, F_n(x) = \int_0^n f(x, t) dt$ .<sup>478</sup> On a :

- $\forall x \geq 0, t \mapsto f(x, t)$  est mesurable.
- Presque partout en  $t > 0, x \mapsto f(x, t)$  est continue.
- $\forall x \geq 0$  et presque partout en  $t > 0, |f(x, t)| \leq 1$ , et  $t \mapsto 1$  est intégrable sur  $[0, n]$ .

On peut donc appliquer le théorème de continuité sous l'intégrale pour conclure que  $F_n$  est continue sur  $\mathbb{R}^+$ .

Soient  $x \geq 0$  et  $q \geq p \geq N \geq 0$ . On a :

$$\begin{aligned}
 |F_q(x) - F_p(x)| &= \left| \int_p^q f(x, t) dt \right| \\
 &= \left| \operatorname{Im} \left( \int_p^q e^{-xt} \frac{e^{it}}{t} dt \right) \right| \\
 &\leq \left| \int_p^q \frac{e^{-(x-i)t}}{t} dt \right| \\
 &= \frac{1}{|x-i|} \left| \int_p^q (x-i) \frac{e^{-(x-i)t}}{t} dt \right| \\
 &\leq \left| \int_p^q (x-i) \frac{e^{-(x-i)t}}{t} dt \right| \\
 &= \left| \int_p^q -(x-i) e^{-(x-i)t} \frac{1}{t} dt \right|
 \end{aligned}$$

Nous allons réaliser une intégration par parties. Pour cela, posons :

$$\begin{aligned}
 - u'(t) &= -(x-i)e^{-(x-i)t} \implies u(t) = e^{-(x-i)t} \\
 - v(t) &= \frac{1}{t} \implies v'(t) = -\frac{1}{t^2}
 \end{aligned}$$

Ce qui nous donne :

$$\begin{aligned}
 \left| \int_p^q (x-i) \frac{e^{-(x-i)t}}{t} dt \right| &= \left| [u(t)v(t)]_p^q - \int_p^q u(t)v'(t) dt \right| \\
 &= \left| \frac{e^{-(x-i)q}}{q} - \frac{e^{-(x-i)p}}{p} + \int_p^q \frac{e^{-(x-i)t}}{t^2} dt \right|
 \end{aligned}$$

On applique maintenant le Théorème 1 :

$$\begin{aligned}
 \left| \frac{e^{-(x-i)q}}{q} - \frac{e^{-(x-i)p}}{p} + \int_p^q \frac{e^{-(x-i)t}}{t^2} dt \right| &\leq \frac{1}{p} + \frac{1}{q} + \int_p^q \frac{1}{t^2} dt \\
 &= \frac{1}{q} + \frac{1}{p} - \left[ \frac{1}{t} \right]_p^q \\
 &\leq \frac{2}{N}
 \end{aligned}$$

D'où :

$$|F_q(x) - F_p(x)| \leq \frac{2}{N}$$

Donc la suite de fonctions continues  $(F_n)$  vérifie le critère de Cauchy uniforme, et converge ainsi vers  $F$  uniformément. En particulier,  $F$  est continue sur  $\mathbb{R}^+$ .

Soit  $a > 0$ .  $f$  est dérivable par rapport à  $x$  et pour tout  $x \in ]a, +\infty[$  et  $t \in \mathbb{R}^+$  :

$$\left| \frac{\partial f}{\partial x}(x, t) \right| = |-\sin(t)e^{-xt}| \leq e^{-at}$$



On applique le théorème de dérivation sous l'intégrale, qui donne :

$$\forall x \in ]a, +\infty[, F'(x) = \int_0^{+\infty} -\sin(t) e^{-xt} dt$$

En particulier, c'est vrai sur  $\mathbb{R}_*^+$  car la dérivabilité est une propriété locale. Or  $\forall A > 0$ , on a :

$$\begin{aligned} \int_0^A e^{-(i+x)t} dt &= \frac{1 - e^{-(i+x)A}}{i+x} \\ \Rightarrow \lim_{A \rightarrow +\infty} \int_0^A e^{-(i+x)t} dt &= \frac{1}{i+x} = \frac{-i+x}{1+x^2} \\ \Rightarrow \operatorname{Im} \left( \lim_{A \rightarrow +\infty} \int_0^A e^{-(i+x)t} dt \right) &= \operatorname{Im} \left( \frac{-i+x}{1+x^2} \right) = -\frac{1}{1+x^2} \end{aligned}$$

Or,

$$\operatorname{Im} \left( \lim_{A \rightarrow +\infty} \int_0^A e^{-(i+x)t} dt \right) = \lim_{A \rightarrow +\infty} \int_0^A \operatorname{Im} (e^{-(i+x)t}) dt = \int_0^{+\infty} -\sin(t) e^{-xt} dt = F'(x)$$

En recollant les deux morceaux :

$$F'(x) = -\frac{1}{1+x^2} \quad (*)$$

Soient  $x, y \in \mathbb{R}_*^+$ . En intégrant (\*) entre  $x$  et  $y$ , on obtient :

$$F(x) - F(y) = \arctan(x) - \arctan(y)$$

Mais,

$$\begin{aligned} |F(y)| &= \left| \int_0^{+\infty} \frac{\sin(t)}{t} e^{-yt} dt \right| \\ &\leq \int_0^{+\infty} \left| \frac{\sin(t)}{t} e^{-yt} \right| dt \\ &\leq \int_0^{+\infty} e^{-yt} dt \\ &= \frac{1}{y} \\ &\longrightarrow_{y \rightarrow +\infty} 0 \end{aligned}$$

Il suffit donc de faire tendre  $y$  vers  $+\infty$  pour obtenir :

$$\forall x > 0, F(x) = \frac{\pi}{2} - \arctan(x)$$

Ce qui, en faisant tendre  $x$  vers 0, donne :

$$F(0) = \int_0^{+\infty} \frac{\sin(t)}{t} dt = \frac{\pi}{2}$$

□

## 17 Lemme de Morse

En usant (certains diront plutôt “en abusant”) du théorème d’inversion locale, on montre le lemme de Morse et on l’applique à l’étude de la position d’une surface par rapport à son plan tangent.

**Notation 1.** Si  $f : \mathbb{R}^n \rightarrow \mathbb{R}$  est une application dont toutes les dérivées secondes existent, on note  $\text{Hess}(f)_a$  la hessienne de  $f$  au point  $a$ .

**Lemme 2.** Soit  $A_0 \in \mathcal{S}_n(\mathbb{R})$  inversible. Alors il existe un voisinage  $V$  de  $A_0$  dans  $\mathcal{S}_n(\mathbb{R})$  et une application  $\psi : V \rightarrow \text{GL}_n(\mathbb{R})$  de classe  $\mathcal{C}^1$  telle que

$$\forall A \in V, A = {}^t\psi(A)A_0\psi(A)$$

*Démonstration.* On définit l’application

$$\begin{aligned} \varphi : \mathcal{M}_n(\mathbb{R}) &\rightarrow \mathcal{S}_n(\mathbb{R}) \\ M &\mapsto {}^tMA_0M \end{aligned}$$

qui est une application polynômiale en les coefficients de  $M$ , donc de classe  $\mathcal{C}^1$ . Soit  $H \in \mathcal{M}_n(\mathbb{R})$ . On calcule :

$$\begin{aligned} \varphi(I_n + H) - \varphi(I_n) &= {}^tHA_0 + A_0H + {}^tHA_0 + H \\ &= {}^t(A_0H) + A_0H + o(\|H\|^2) \end{aligned}$$

où  $(\|\cdot\|)$  désigne une quelconque norme d’algèbre sur  $\mathcal{M}_n(\mathbb{R})$ . Ainsi, on a  $d\varphi_{I_n}(H) = {}^t(A_0H) + A_0H$ . D’où

$$\text{Ker}(d\varphi_{I_n}) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid A_0M \in \mathcal{A}_n(\mathbb{R})\} = A_0^{-1}\mathcal{A}_n(\mathbb{R})$$

On définit donc

$$F = \{M \in \mathcal{M}_n(\mathbb{R}) \mid A_0M \in \mathcal{S}_n(\mathbb{R})\} = A_0^{-1}\mathcal{S}_n(\mathbb{R})$$

et on a  $\mathcal{M}_n(\mathbb{R}) = F \oplus \text{Ker}(d\varphi_{I_n})$ . Ainsi, la différentielle  $d(\varphi|_F)_{I_n}$  est bijective (car  $\text{Ker}(d(\varphi|_F)_{I_n}) = \text{Ker}(d\varphi_{I_n}) \cap F = \{0\}$ ).

On peut donc appliquer le théorème d’inversion locale à  $\varphi|_F$  : il existe  $U$  un voisinage ouvert de  $I_n$  dans  $F$  tel que  $(\varphi|_U)$  soit  $\mathcal{C}^1$ -difféomorphisme de  $U$  sur  $V = \varphi(U)$ . De plus, on peut supposer  $U \subseteq \text{GL}_n(\mathbb{R})$  (quitte à considérer  $U \cap U'$  où  $U'$  est un voisinage ouvert de  $I_n$  dans  $\text{GL}_n(\mathbb{R})$  ; qui existe par continuité de  $\det$ ).

Ainsi,  $V$  est un voisinage ouvert de  $A_0 = \varphi(I_n)$  dans  $\mathcal{S}_n(\mathbb{R})$  vérifiant :

$$\forall A \in V, A = {}^t(\varphi|_U)^{-1}(A)A_0(\varphi|_U)^{-1}(A)$$

Il suffit alors de poser  $\psi = (\varphi|_U)^{-1}$  (qui est bien une application de classe  $\mathcal{C}^1$ ) pour avoir le résultat demandé.  $\square$

[ROU]  
p. 209

**Lemme 3** (Morse). Soit  $f : U \rightarrow \mathbb{R}$  une fonction de classe  $\mathcal{C}^3$  (où  $U$  désigne un ouvert de  $\mathbb{R}^n$  contenant l'origine). On suppose :

- $df_0 = 0$ .
- La matrice symétrique  $\text{Hess}(f)_0$  est inversible.
- La signature de  $\text{Hess}(f)_0$  est  $(p, n - p)$ .

Alors il existe un difféomorphisme  $\phi = (\phi_1, \dots, \phi_n)$  de classe  $\mathcal{C}^1$  entre deux voisinage de l'origine de  $\mathbb{R}^n$   $V \subseteq U$  et  $W$  tel que  $\phi(0) = 0$  et

$$\forall x \in U, f(x) - f(0) = \sum_{k=1}^p \phi_k^2(x) - \sum_{k=p+1}^n \phi_k^2(x)$$

*Démonstration.* On écrit la formule de Taylor à l'ordre 1 avec reste intégral au voisinage de 0, qui donne :

$$\begin{aligned} f(x) &= f(0) + df_0(x) + \int_0^1 (1-t) d^2 f_{tx}(x, x) dt \\ \Leftrightarrow f(x) - f(0) &= {}^t x Q(x) x \end{aligned} \quad (*)$$

où  $Q(x)$  est la matrice symétrique définie par  $Q(x) = \int_0^1 (1-t) \text{Hess} f_{tx} dt$  (qui est une application  $\mathcal{C}^1$  sur  $U$  car  $f$  est  $\mathcal{C}^3$  sur  $U$ ).

Par hypothèse,  $Q(0) = \frac{\text{Hess}(f)_0}{2}$  est une matrice symétrique inversible, donc en vertu du Théorème 2, il existe un voisinage  $V_1$  de  $Q(0)$  dans  $\mathcal{S}_n(\mathbb{R})$  et une application  $\psi : V_1 \rightarrow \text{GL}_n(\mathbb{R})$  de classe  $\mathcal{C}^1$  tels que :

$$\forall A \in V_1, A = {}^t \psi(A) Q(0) \psi(A)$$

Mais, l'application  $x \mapsto Q(x)$  est continue sur  $U$  (puisque  $f$  est de classe  $\mathcal{C}^3$  sur  $U$ ), donc il existe  $V_2$  voisinage de 0 dans  $U$  tel que  $\forall x \in V_2, Q(x) \in V_1$ . On peut donc définir l'application  $M = \psi \circ Q|_{V_2}$ , qui nous permet d'écrire

$$\forall x \in V_2, Q(x) = {}^t M(x) Q(0) M(x) \quad (**)$$

Or,  $Q(0)$  est de signature  $(p, n - p)$ , donc d'après la loi d'inertie de Sylvester, il existe  $P \in \text{GL}_n(\mathbb{R})$  telle que

$$Q(0) = {}^t P \underbrace{\begin{pmatrix} I_p & \\ & -I_{n-p} \end{pmatrix}}_{=D} P \quad (***)$$

Finalement en combinant (\*) avec (\*\*) et (\*\*\*), cela donne

$$\begin{aligned} \forall x \in V_2, f(x) - f(0) &= {}^t (PM(x)x) D (PM(x)x) \\ \Leftrightarrow \varphi(x) = PM(x)x \quad \forall x \in V_2, f(x) - f(0) &= {}^t \varphi(x) D \varphi(x) \end{aligned}$$

ce qui est bien l'expression voulue.

Il reste à montrer que  $\varphi$  définit bien un difféomorphisme de classe  $\mathcal{C}^1$  entre deux voisinages de

l'origine. Notons déjà que  $\varphi$  est de classe  $\mathcal{C}^1$  car  $M$  l'est. Calculons la différentielle en 0 de  $\varphi$ . Soit  $h \in V_2$ ;

$$\begin{aligned}\varphi(h) - \varphi(0) &= PM(h)h \\ &= P(M(0) + dM_0(h) + o(\|h\|))h \\ &= PM(0)h + o(\|h\|)\end{aligned}$$

d'où  $d\varphi_0(h) = PM(0)h$ . Or,  $PM(0)$  est inversible, donc en particulier,  $d\varphi_0$  l'est aussi. On peut appliquer le théorème d'inversion locale à  $\varphi$ , qui donne l'existence de deux ouverts  $V$  et  $W$  contenant l'origine (car  $\varphi(0) = 0$ ) tel que  $\phi = \varphi|_V$  soit un  $\mathcal{C}^1$ -difféomorphisme de  $V$  sur  $W$ .  $\square$

**Application 4.** Soit  $S$  la surface d'équation  $z = f(x, y)$  où  $f$  est de classe  $\mathcal{C}^3$  au voisinage de l'origine. On suppose la forme quadratique  $d^2 f_0$  non dégénérée. Alors, en notant  $P$  le plan tangent à  $S$  en 0 :

- (i) Si  $d^2 f_0$  est de signature  $(2, 0)$ , alors  $S$  est au-dessus de  $P$  au voisinage de 0.
- (ii) Si  $d^2 f_0$  est de signature  $(0, 2)$ , alors  $S$  est en-dessous de  $P$  au voisinage de 0.
- (iii) Si  $d^2 f_0$  est de signature  $(1, 1)$ , alors  $S$  traverse  $P$  selon une courbe admettant un point double en  $(0, f(0))$ .

p. 341

*Démonstration.* Une équation cartésienne de  $P$  est donnée par

$$z - 0 = f(0) + df_0(x, y)$$

La différence d'altitude entre la surface  $S$  et le plan tangent  $P$  au point  $h \in \mathbb{R}^2$  est donc donnée par

$$\delta(h) = f(h) - (f(0) + df_0(h))$$

et le Théorème 3 permet d'écrire

$$\delta(h) = \alpha \phi_1(h)^2 + \beta \phi_2(h)^2$$

où  $(\alpha, \beta)$  désigne la signature de  $d^2 f_0$  et  $\phi = (\phi_1, \phi_2)$  est un  $\mathcal{C}^1$ -difféomorphisme entre deux voisinages de l'origine dans  $\mathbb{R}^2$ . En particulier,  $\phi_1$  et  $\phi_2$  ne s'annulent simultanément qu'en 0.

- (i) Si  $d^2 f_a$  est de signature  $(2, 0)$ , on a  $\delta(h) > 0$  pour  $h$  voisin de 0 et  $h \neq 0$ .
- (ii) Si  $d^2 f_a$  est de signature  $(0, 2)$ , on a  $\delta(h) < 0$  pour  $h$  voisin de 0 et  $h \neq 0$ .
- (iii) Si  $d^2 f_a$  est de signature  $(1, 1)$ , on a  $\delta(h) = \phi_1(h)^2 - \phi_2(h)^2$  et  $S$  traverse  $P$  selon une courbe admettant un point double en  $(0, f(0))$ .

 $\square$

## 18 Loi d'inertie de Sylvester

*Le but de ce développement est de montrer la très connue loi d'inertie de Sylvester qui donne l'existence (et une forme d'unicité) de la décomposition d'une forme quadratique réelle en carrés de formes linéaires indépendantes.*

Soit  $E$  un espace vectoriel sur  $\mathbb{R}$  de dimension finie  $n \geq 1$ . Soit  $\Phi$  une forme quadratique sur  $E$ .

[GOU21]  
p. 243

**Notation 1.** — On note  $\varphi$  la forme polaire associée à  $\Phi$ .

— Si  $\Gamma$  est une partie de  $E^*$ , on note  $\Gamma^\circ$  son orthogonal (ie.  $\Gamma^\circ = \{x \in E \mid \forall f \in \Gamma, f(x) = 0\}$ ).

**Lemme 2.** Il existe une base de  $E$  qui soit  $\Phi$ -orthogonale.

*Démonstration.* On procède par récurrence sur  $n$ .

- Si  $n = 1$  : il n'y a rien à montrer, toute base est  $\Phi$ -orthogonale.
- On suppose le résultat vrai à un rang  $n \geq 1$  et montrons le au rang  $n + 1$ . Si  $\Phi = 0$ , alors toute base de  $E$  est  $\Phi$ -orthogonale. Sinon, il existe  $v \in E$  tel que  $\Phi(v) \neq 0$ . Dans ce cas, l'application  $f = \varphi(v, \cdot)$  est une forme linéaire non nulle sur  $E$ .

$H = \text{Ker}(f)$  est un hyperplan de  $E$  et comme  $v \notin H$ , on a  $E = H \oplus \text{Vect}(v)$ . Or,  $\dim(H) = n - 1$ , donc on peut appliquer l'hypothèse de récurrence à  $\Phi|_H$ , et on obtient une base  $\mathcal{B}$  de  $H$  qui est  $\Phi$ -orthogonale. En particulier,  $\mathcal{B} \cup \{v\}$  est une base  $\Phi$ -orthogonale de  $E$ .

□

**Théorème 3** (Loi d'inertie de Sylvester).

$$\exists p, q \in \mathbb{N} \text{ et } \exists f_1, \dots, f_{p+q} \in E^* \text{ tels que } \Phi = \sum_{i=1}^p |f_i|^2 - \sum_{i=p+1}^{p+q} |f_i|^2$$

où les formes linéaires  $f_i$  sont linéairement indépendantes et où  $p + q \leq n$ . De plus, ces entiers ne dépendent que de  $\Phi$  et pas de la décomposition choisie.

Le couple  $(p, q)$  est la **signature** de  $\Phi$  et le rang  $\Phi$  est égal à  $p + q$ .

*Démonstration.* Soit  $\mathcal{B} = (e_1, \dots, e_n)$  une base  $\Phi$ -orthogonale (dont l'existence est assurée par le Théorème 2). En posant  $\forall i \in \llbracket 1, n \rrbracket$ ,  $\lambda_i = \Phi(e_i)$ , on a

$$\forall x \in E \text{ que l'on écrit } x = x_1 e_1 + \dots + x_n e_n, \Phi(x) = \sum_{i=1}^n |x_i|^2 \Phi(e_i) = \sum_{i=1}^n \lambda_i |x_i|^2$$

Chaque  $\lambda_i$  est strictement positif, strictement négatif, ou nul. Quitte à les réordonner, on peut supposer

$$\lambda_1, \dots, \lambda_p > 0, \lambda_{p+1}, \dots, \lambda_{p+q} < 0, \text{ et } \lambda_{p+q+1} = \dots = \lambda_n = 0$$

Pour  $i \in \llbracket 1, p \rrbracket$ , on peut écrire  $\lambda_i = \omega_i^2$  et pour  $i \in \llbracket p+1, p+q \rrbracket$ , on peut écrire  $\lambda_i = -\omega_i^2$  où les  $\omega_i \in \mathbb{R}^*$ . On définit :

$$\forall i \in \llbracket 1, q \rrbracket, f_i = \omega_i e_i^*$$

Ainsi définies, les formes linéaires  $f_i$  sont linéairement indépendantes et on obtient bien :

$$\Phi = \sum_{i=1}^p |f_i|^2 - \sum_{i=p+1}^q |f_i|^2 \quad (*)$$

Reste maintenant à montrer l'indépendance de  $p$  et de  $q$  vis-à-vis de la décomposition choisie. Soit donc

$$\Phi = \sum_{i=1}^{p'} |g_i|^2 - \sum_{i=p'+1}^{q'} |g_i|^2 \quad (**)$$

une autre écriture en carrés de formes linéaires indépendantes. Supposons  $p' \neq p$  avec par exemple  $p' > p$ . Complétons  $g_1, \dots, g_{p'+q'}$  en une base  $g_1, \dots, g_n$  de  $E^*$ . Donc, la famille  $\Gamma = (f_1, \dots, f_p, g_{p'+1}, \dots, g_n)$  est de cardinal  $p + n - p' < n$ . Elle ne peut donc pas former une base de  $E^*$ . Donc

$$\dim(\Gamma^\circ) = \dim(E^*) - \dim(\Gamma) \geq 1$$

Par conséquent,

$$\exists x \neq 0 \text{ tel que } f_1(x) = \dots = f_p(x) = g_{p'+1}(x) = \dots = g_n(x) = 0$$

Donc  $\Phi(x) \leq 0$  par (\*). Supposons par l'absurde que

$$g_1(x) = \dots = g_{p'}(x) = 0$$

Comme  $(g_i)_{i \in \llbracket 1, n \rrbracket}$  est une base de  $E^*$  et que  $x$  s'annule sur cette base, on a  $x = 0$  : c'est absurde. Donc, il existe  $i \in \llbracket 1, p' \rrbracket$  tel que  $g_i(x) \neq 0$ . En particulier  $\Phi(x) > 0$  par (\*\*): contradiction. Ainsi,  $p = p'$ . On montre de même que  $q = q'$ .

Dans la base  $\Phi$ -orthogonale  $(e_1, \dots, e_n)$ , la matrice de  $\Phi$  est

$$\begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

d'où le rang de  $\Phi$ . □

La preuve de **[GOU21]** est un peu décousue. Il faut savoir recoller les morceaux pour bien montrer existence et "unicité" de la décomposition.

## 19 Méthode de Newton

On démontre ici la méthode de Newton qui permet de trouver numériquement une approximation précise d'un zéro d'une fonction réelle d'une variable réelle.

**Théorème 1** (Méthode de Newton). Soit  $f : [c, d] \rightarrow \mathbb{R}$  une fonction de classe  $\mathcal{C}^2$  strictement croissante sur  $[c, d]$ . On considère la fonction

$$\varphi : \begin{array}{ccc} [c, d] & \rightarrow & \mathbb{R} \\ x & \mapsto & x - \frac{f(x)}{f'(x)} \end{array}$$

(qui est bien définie car  $f' > 0$ ). Alors :

- (i)  $\exists ! a \in [c, d]$  tel que  $f(a) = 0$ .
- (ii)  $\exists \alpha > 0$  tel que  $I = [a - \alpha, a + \alpha]$  est stable par  $\varphi$ .
- (iii) La suite  $(x_n)$  des itérés (définie par récurrence par  $x_{n+1} = \varphi(x_n)$  pour tout  $n \geq 0$ ) converge quadratiquement vers  $a$  pour tout  $x_0 \in I$ .

[ROU]  
p. 152

*Démonstration.* Soit  $x \in [c, d]$ . Comme  $f(a) = 0$ , on peut écrire :

$$\begin{aligned} \varphi(x) - a &= x - a - \frac{f(x) - f(a)}{f'(x)} \\ &= \frac{f(a) - f(x) - (a - x)f'(x)}{f'(x)} \end{aligned}$$

Or, la formule de Taylor-Lagrange à l'ordre 2 donne l'existence d'un  $z \in ]a, x[$  tel que

$$\begin{aligned} f(a) &= f(x) + f'(x)(a - x) + \frac{1}{2}f''(z)(a - x)^2 \\ \iff f(a) - f(x) - f'(x)(a - x) &= \frac{1}{2}f''(z)(a - x)^2 \end{aligned}$$

D'où :

$$\varphi(x) - a = \frac{f''(z)}{2f'(x)}(x - a)^2 \quad (*)$$

Soit  $C = \frac{\max_{x \in [c, d]} |f''(x)|}{2 \min_{x \in [c, d]} |f'(x)|}$ . Par (\*), on a :

$$\forall x \in [c, d], |\varphi(x) - a| \leq C|x - a|^2$$

Soit maintenant  $\alpha > 0$  suffisamment petit pour que  $C\alpha < 1$  et que  $I = [a - \alpha, a + \alpha] \subseteq [c, d]$ . Alors :

$$x \in I \implies |\varphi(x) - a| \leq C\alpha^2 < \alpha$$

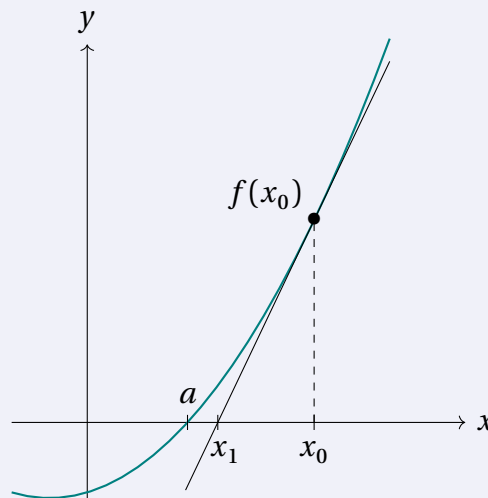
(la première inégalité se voit en faisant un dessin, et la seconde vient du fait que  $C\alpha < 1$ ). D'où

$\varphi(I) \subseteq I$ . Et si  $x_0 \in I$ , on a donc  $\forall n \in \mathbb{N}, x_n \in I$  et

$$\begin{aligned} |x_{n+1} - a| &= |\varphi(x_n) - a| \\ &\leq C|x_n - a|^2 \end{aligned}$$

D'où  $C|x_n - a| \leq (C|x_0 - a|)^{2^n} \leq (C\alpha)^{2^n}$  où  $C\alpha < 1$ . On a donc bien convergence quadratique de la suite  $(x_n)$  vers le réel  $a$ .  $\square$

**Remarque 2.** On suppose que l'on connaisse une approximation grossière du point que l'on nomme  $x_0$ .



L'idée de la méthode est de remplacer la courbe représentative de  $f$  par sa tangente au point  $x_0$  :

$$y = f'(x_0)(x - x_0) + f(x_0)$$

L'abscisse  $x_1$  du point d'intersection de cette tangente avec l'axe des abscisses est donnée par

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$$

d'où le fait d'itérer la fonction  $\varphi : x \mapsto x - \frac{f(x)}{f'(x)}$ .

[DEM]  
p. 100

**Corollaire 3.** En reprenant les hypothèses et notations du théorème précédent, et en supposant de plus  $f$  strictement convexe sur  $[c, d]$ , le résultat du théorème est vrai sur  $I = [a, d]$ . De plus :

- (i)  $(x_n)$  est strictement décroissante (ou constante).
- (ii)  $x_{n+1} - a \sim \frac{f''(a)}{2f'(a)}(x_n - a)^2$  pour  $x_0 > a$ .

[ROU]  
p. 152

**Démonstration.** La dérivée  $f'$  est strictement croissante (car  $f$  est strictement convexe) sur  $]c, d[$ . Ainsi, soit  $x \in [a, d]$ . Si  $x = a$ , on a  $\varphi(x) = x$ , et la suite  $(x_n)$  est alors constante. Supposons



maintenant  $x > a$ . On a :

$$\varphi(x) = x - \frac{\overbrace{f(x)}^{>0}}{\underbrace{f'(x)}_{>0}} < x$$

Et par (\*) (de la démonstration précédente),  $\exists z \in ]a, x[$  :

$$\varphi(x) - a = \frac{f''(z)}{2f'(z)}(x - a)^2 > 0 \iff \varphi(x) < a$$

Ainsi,  $I = [a, d]$  est stable par  $\varphi$  et pour  $x_0 \in ]a, d]$ , on a  $x_n \in ]a, d]$  pour tout  $n \in \mathbb{N}$  et la suite  $(x_n)$  est strictement décroissante. La suite  $(x_n)$  admet donc une limite  $\ell$  vérifiant  $\varphi(\ell) = \ell \iff f(\ell) = 0$  ie.  $\ell = a$  par unicité. Comme dans le théorème précédent, la convergence est quadratique :

$$0 \leq x_{n+1} - a \leq C(x_n - a)^2$$

Enfin, si  $x_0 \in ]a, d]$ , on a comme dans (\*) :

$$\forall n \in \mathbb{N}, x_n > a \text{ et } \frac{x_{n+1} - a}{(x_n - a)^2} = \frac{f''(z_n)}{2f'(x_n)}$$

où  $z_n \in ]a, x_n[$  (d'après la démarche effectuée pour obtenir (\*)). On fait tendre  $n$  vers l'infini et la fraction de droite tend vers  $\frac{f''(a)}{2f'(a)}$  ; d'où le résultat.  $\square$

*Remarque 4.* L'ajout de l'hypothèse de convexité à la méthode de Newton, nous permet de nous affranchir de l'intervalle  $I$  tout en gardant la même vitesse de convergence.

## 20 Nombres de Bell

En utilisant les propriétés des séries entières, nous calculons le nombre de partitions de l'ensemble  $\llbracket 1, n \rrbracket$ .

**Théorème 1** (Nombres de Bell). Pour tout  $n \in \mathbb{N}^*$ , on note  $B_n$  le nombre de partitions de  $\llbracket 1, n \rrbracket$ . Par convention on pose  $B_0 = 1$ . Alors,

$$\forall k \in \mathbb{N}^*, B_k = \frac{1}{e} \sum_{n=0}^{+\infty} \frac{n^k}{n!}$$

[GOU21]  
p. 314

*Démonstration.* Notons que clairement  $B_1 = 1$ . Soit  $n \in \mathbb{N}^*$ , exprimons  $B_{n+1}$  en fonction des termes précédents. Pour tout  $k \leq n$ , on note  $E_k$  l'ensemble des partitions  $P$  de  $\llbracket 1, n+1 \rrbracket$  tel que la partie de  $P$  qui contient l'entier  $n+1$  est de taille  $k+1$ . Choisir une partition dans  $E_k$ , c'est choisir  $k$  entiers de  $\llbracket 1, n \rrbracket$  (ceux de l'ensemble qui contient  $n+1$  dans la partition), puis construire une partition des  $n-k$  éléments restants. Donc  $|E_k| = \binom{n}{k} B_{n-k}$ .

Comme  $E_0, \dots, E_n$  forment une partition de l'ensemble des partitions de  $\llbracket 1, n+1 \rrbracket$ , on obtient :

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_{n-k} = \sum_{k=0}^n \binom{n}{n-k} B_k = \sum_{k=0}^n \binom{n}{k} B_k \quad (*)$$

À toute partition  $P$  de  $\llbracket 1, n \rrbracket$ , on peut associer une permutation  $\sigma_P \in S_n$ , qui est le produit des cycles de supports les éléments de  $P$ . On construit ainsi une application  $P \mapsto \sigma_P$  injective. D'où :

$$B_n \leq |S_n| = n!$$

On en déduit en particulier que  $\frac{B_n}{n!} \leq 1$ . En vertu du lemme d'Abel, le rayon de convergence  $R$  de la série entière  $\sum \frac{B_n}{n!} x^n$  est supérieur ou égal à 1. On peut donc définir

$$B: \begin{array}{ll} ]-R, R[ & \rightarrow \mathbb{R} \\ x & \mapsto \sum_{n=0}^{+\infty} \frac{B_n}{n!} x^n \end{array}$$

et en dérivant,  $\forall x \in ]-R, R[$  :

$$\begin{aligned} B'(x) &= \sum_{n=0}^{+\infty} \frac{B_{n+1}}{n!} x^n \\ &\stackrel{(*)}{=} \sum_{n=0}^{+\infty} \frac{1}{n!} \left( \sum_{k=0}^n \binom{n}{k} B_k \right) x^n \\ &= \sum_{n=0}^{+\infty} \left( \sum_{k=0}^n \frac{B_k}{k!} \frac{1}{(n-k)!} \right) x^n \end{aligned}$$

On reconnaît là le produit de Cauchy suivant :

$$B'(x) = \sum_{n=0}^{+\infty} \left( \sum_{k=0}^n \frac{B_k}{k!} \frac{1}{(n-k)!} \right) x^n = \left( \sum_{n=0}^{+\infty} \frac{B_n}{n!} x^n \right) \left( \sum_{n=0}^{+\infty} \frac{x^n}{n!} \right) = B(x) e^x$$

Reste à résoudre cette équation différentielle linéaire homogène d'ordre 1 :

$$B(x) = \lambda e^{e^x}$$

Or,  $B(0) = B_0 = 1 = \lambda e^1$ . D'où  $B(x) = \frac{1}{e} e^{e^x}$ .

La série entière définissant l'exponentielle a un rayon de convergence infini. On peut écrire, pour tout  $z \in \mathbb{C}$  :

$$e^{e^z} = \sum_{n=0}^{+\infty} \frac{e^{nz}}{n!} = \sum_{n=0}^{+\infty} \sum_{k=0}^{+\infty} \underbrace{\frac{(nz)^k}{n!k!}}_{u_{n,k}(z)}$$

On va appliquer le théorème de Fubini-Lebesgue à  $u_{n,k}(z)$  (où  $z \in \mathbb{C}$  est fixé) :

$$\sum_{n=0}^{+\infty} \sum_{k=0}^{+\infty} |u_{n,k}(z)| = \sum_{n=0}^{+\infty} \frac{e^{n|z|}}{n!} = e^{e^{|z|}} < +\infty$$

Donc on peut intervertir les signes de sommations. Pour tout  $x \in ]-R, R[$ ,

$$\begin{aligned} B(x) &= \frac{1}{e} e^{e^x} \\ &= \frac{1}{e} \sum_{n=0}^{+\infty} \sum_{k=0}^{+\infty} u_{n,k}(x) \\ &= \frac{1}{e} \sum_{k=0}^{+\infty} \sum_{n=0}^{+\infty} u_{n,k}(x) \\ &= \frac{1}{e} \sum_{k=0}^{+\infty} \left( \sum_{n=0}^{+\infty} \frac{n^k}{n!} \right) \frac{x^k}{k!} \end{aligned}$$

Par unicité du développement en série entière d'une fonction, on en déduit, par identification des coefficients :

$$\forall k \in \mathbb{N}^*, B_k = \frac{1}{e} \sum_{n=0}^{+\infty} \frac{n^k}{n!}$$

□

La partie sur le dénombrement (au début de la preuve) est un peu technique. N'hésitez pas à passer du temps dessus et à y réfléchir en faisant des exemples.

## 21 Projection sur un convexe fermé

On montre le théorème de projection sur un convexe fermé dans un espace de Hilbert réel en utilisant les suites de Cauchy et des propriétés du produit scalaire.

Soit  $H$  un espace de Hilbert réel de norme  $\|\cdot\|$  et dont on note  $\langle \cdot, \cdot \rangle$  le produit scalaire associé.

**Lemme 1** (Identité du parallélogramme). Soient  $x, y \in H$ . Alors :

$$\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2)$$

[L1]  
p. 32

*Démonstration.* D'une part,

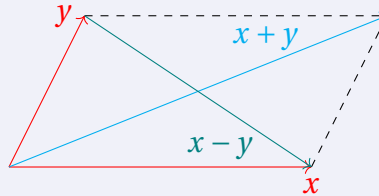
$$\|x + y\|^2 = \langle x + y, x + y \rangle = \|x\|^2 + \|y\|^2 + 2\langle x, y \rangle$$

D'autre part,

$$\|x - y\|^2 = \langle x - y, x - y \rangle = \|x\|^2 + \|y\|^2 - 2\langle x, y \rangle$$

En additionnant les deux lignes, on obtient bien l'égalité voulue.  $\square$

*Remarque 2.* L'interprétation géométrique de cette égalité est que dans le parallélogramme formé par les vecteurs  $x$  et  $y$ , la somme des carrés des diagonales est égale à la somme des carrés des côtés.

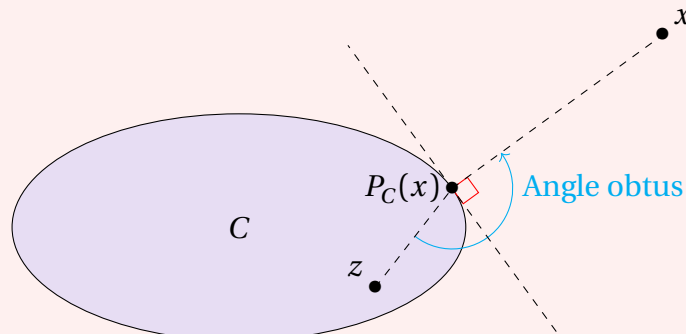


**Théorème 3** (Projection sur un convexe fermé). Soit  $C \subseteq H$  un convexe fermé non-vide. Alors :

$$\forall x \in H, \exists ! y \in C \text{ tel que } d(x, C) = \inf_{z \in C} \|x - z\| = d(x, y)$$

On peut donc noter  $y = P_C(x)$ , le **projeté orthogonal de  $x$  sur  $C$** . Il s'agit de l'unique point de  $C$  vérifiant

$$\forall z \in C, \langle x - P_C(x), z - P_C(x) \rangle \leq 0 \quad (*)$$



[GOU20]  
p. 427

*Démonstration.* Soit  $x \in H$ . Posons  $\delta = d(x, C)$ . Par la caractérisation séquentielle de la borne inférieure, il existe  $(y_n)$  une suite de  $C$  telle que  $\|x - y_n\| \rightarrow \delta$ . Montrons que  $(y_n)$  est une suite de Cauchy. On applique le Théorème 1 :

$$\forall p, q \in \mathbb{N}, \|(x - y_p) + (x - y_q)\|^2 + \|y_p - y_q\|^2 = 2(\|x - y_p\|^2 + \|x - y_q\|^2) \quad (**)$$

Or,  $C$  est convexe. Donc  $\forall p, q \in \mathbb{N}, \frac{y_p + y_q}{2} \in C$ . Par définition,

$$\begin{aligned} \left\| x - \frac{y_p + y_q}{2} \right\| &\geq \delta \\ \Leftrightarrow \frac{1}{2} \|(x - y_p) + (x - y_q)\| &\geq \delta \\ \Leftrightarrow \|(x - y_p) + (x - y_q)\|^2 &\geq 4\delta^2 \end{aligned}$$

Par (\*\*), quand  $p, q \rightarrow +\infty$  :

$$\|y_p - y_q\| \leq 2(\underbrace{(\|x - y_p\|^2 - \delta^2)}_{\rightarrow \delta^2} + \underbrace{(\|x - y_q\|^2 - \delta^2)}_{\rightarrow \delta^2}) \rightarrow 0$$

Ainsi  $(y_n)$  est une suite de Cauchy de  $H$  qui est complet, donc  $(y_n)$  converge vers  $y \in H$ . Mais,  $C$  est fermé et  $(y_n)$  est une suite de  $C$ , donc  $y \in C$ .

Montrons maintenant que  $y$  est unique. Soit  $z \in C$  tel que  $\delta = \|x - z\|$ . On définit la suite  $(z_n)$  par

$$\forall n \in \mathbb{N}, z_n = \begin{cases} y & \text{si } n \text{ est pair} \\ z & \text{si } n \text{ est impair} \end{cases}$$

Cette suite vérifie  $\forall n \in \mathbb{N}, \|x - z_n\| = \delta$  donc en particulier  $\|x - z_n\| \rightarrow \delta$ , et on peut tout-à-fait refaire le raisonnement précédent pour montrer que  $(z_n)$  converge (vers  $y = z$ , donc). Ainsi, on a bien existence et unicité du projeté.

Soit  $y \in C$  vérifiant (\*). Montrons que  $y = P_C(x)$ .  $\forall z \in C$ ,

$$\begin{aligned} \|z - x\|^2 &= \|(z - y) - (x - y)\|^2 \\ &= \|z - y\|^2 + \|x - y\|^2 - 2\langle z - y, x - y \rangle \\ &\geq \|z - y\|^2 + \|x - y\|^2 \\ &\geq \|x - y\|^2 \end{aligned}$$

ie.  $\|z - x\| \geq \|x - y\|$ . De plus,  $y \in C$ , donc  $d(y, C) = d(x, C)$ . D'où  $y = P_C(x)$ .

Montrons maintenant que  $P_C(x)$  vérifie bien (\*).  $\forall z \in C$ , on a

$$\|x - z\|^2 \geq \|x - P_C(x)\|^2$$

Or, en développant :

$$\begin{aligned}\|x - z\|^2 &= \|(x - P_C(x)) - (z - P_C(x))\|^2 \\ &= \|x - P_C(x)\|^2 + \|z - P_C(x)\|^2 - 2\langle x - P_C(x), z - P_C(x) \rangle \\ &\geq \|x - P_C(x)\|^2\end{aligned}$$

D'où, par la dernière inégalité,

$$\|z - P_C(x)\|^2 - 2\langle x - P_C(x), z - P_C(x) \rangle \geq 0 \quad (***)$$

Soit maintenant  $z_0 \in C$ . On va appliquer  $(***)$  à  $z = \lambda z_0 + (1 - \lambda)z_0 \in C$  pour  $\lambda \in ]0, 1]$  :

$$\begin{aligned}\lambda^2 \|z_0 + P_C(x)\|^2 - 2\lambda \langle x - P_C(x), z_0 - P_C(x) \rangle &\geq 0 \\ \Rightarrow \lambda \|z_0 + P_C(x)\|^2 - 2\langle x - P_C(x), z_0 - P_C(x) \rangle &\geq 0 \\ \xrightarrow{\lambda \rightarrow 0} -2\langle x - P_C(x), z_0 - P_C(x) \rangle &\geq 0\end{aligned}$$

ce que l'on voulait. □

*Remarque 4.*  $(*)$  traduit le fait géométrique que l'angle du vecteur  $\overrightarrow{P_C(x)x}$  avec  $\overrightarrow{P_C(x)z}$  est obtus pour tout  $z \in C$ . En effet, en notant cet angle  $\theta$ , on a pour  $z \in C$  :

$$\langle x - P_C(x), z - P_C(x) \rangle = \|x - P_C(x)\| \|z - P_C(x)\| \cos(\theta)$$

et si  $\theta$  est obtus, on a bien  $\cos(\theta) \leq 0$ .

**Corollaire 5.** Soit  $F$  un sous-espace vectoriel fermé de  $H$ . Alors  $F \oplus F^\perp = H$ .

*Démonstration.* Si  $x \in F \cap F^\perp$ , alors  $\|x\| = \langle x, x \rangle = 0$ , et donc  $x = 0$ . Montrons maintenant que  $F + F^\perp = H$ . Soit  $x \in H$ . Comme  $F$  est un convexe fermé de  $H$  (en tant que sous-espace vectoriel fermé), on peut appliquer le Théorème 3. Ainsi, il existe un unique  $P_F(x) \in F$  tel que  $d(x, F) = d(x, P_F(x))$  et

$$\forall z \in F, \langle x - P_F(x), z - P_F(x) \rangle \leq 0 \quad (*)$$

Soit  $z_0 \in F$ . on peut appliquer  $(*)$  à  $z = z_0$  :

$$\langle x - P_F(x), z_0 - P_F(x) \rangle \leq 0$$

On va également appliquer  $(*)$  à  $z = -z_0 + 2P_F(x) \in F$  :

$$\langle x - P_F(x), -z_0 + P_F(x) \rangle \leq 0 \iff \langle x - P_F(x), z_0 - P_F(x) \rangle \geq 0$$

Ce qui montre que l'inégalité de  $(*)$  est en fait une égalité. On en tire :

$$\forall z \in F, \langle x - P_F(x), z \rangle = \langle x - P_F(x), z - P_F(x) \rangle - \langle x - P_F(x), 0 - P_F(x) \rangle = 0$$

donc  $x - P_F(x) \in F^\perp$ . En conclusion, on a :

$$x = \underbrace{P_F(x)}_{\in F} + \underbrace{x - P_F(x)}_{\in F^\perp} \in F + F^\perp$$

et on a donc bien la somme directe  $H = F \oplus F^\perp$ . □

## 22 SimPLICITÉ de $A_n$ pour $n \geq 5$

On montre que  $A_n$  est simple pour  $n \geq 5$  en montrant dans un premier temps le cas  $n = 5$ , puis en s'y ramenant.

**Lemme 1.** Les 3-cycles sont conjugués dans  $A_n$  pour  $n \geq 5$ .

[PER]  
p. 15

*Démonstration.* Soient  $\alpha = (a_1 \ a_2 \ a_3)$  et  $\beta = (b_1 \ b_2 \ b_3)$  deux 3-cycles. Soit  $\sigma \in S_n$  telle que

$$\forall i \in \llbracket 1, 3 \rrbracket, \sigma(a_i) = b_i$$

On a deux possibilités pour  $\sigma$  :

- $\sigma$  est paire. Alors  $\sigma \in A_n$ , et le résultat est démontré pour  $\alpha$  et  $\beta$ .
- $\sigma$  est impaire. Comme  $n \geq 5$ , il existe  $c_1, c_2$  tels que  $c_1, c_2 \notin \{b_1, b_2, b_3\}$ . On pose alors  $\tau = (c_1 \ c_2)$ , et on a

$$(\tau\sigma)(a_1 \ a_2 \ a_3)(\tau\sigma)^{-1} = (b_1 \ b_2 \ b_3)$$

avec  $\tau\sigma$  paire. Le résultat est encore démontré pour  $\alpha$  et  $\beta$ .

□

**Lemme 2.**  $A_n$  est engendré par les 3-cycles pour  $n \geq 3$ .

[ROM21]  
p. 49

*Démonstration.* Montrons tout d'abord qu'un produit de deux transpositions est un produit de 3-cycles. Soient  $\alpha = (a_1 \ a_2)$  et  $\beta = (b_1 \ b_2)$  deux transpositions. Si  $\alpha = \beta$ , alors  $\alpha\beta = \text{id} = \sigma^3$  où  $\sigma$  désigne n'importe quel 3-cycle.

Si  $\alpha \neq \beta$ , on a deux possibilités :

- Leur support comporte un élément commun :  $a_1 = b_1 = c$ . Donc  $\alpha = (c \ a_2)$  et  $\beta = (c \ b_2)$  avec  $c, a_2, b_2$  distincts. Donc  $\alpha\beta = (a_2 \ c \ b_2)$ .
- Leur support n'a pas d'élément commun. Dans ce cas  $a_1, a_2, b_1, b_2$  sont distincts et  $\alpha\beta = (a_1 \ a_2 \ b_1)(a_2 \ b_1 \ b_2)$ .

Soit maintenant  $\sigma \in A_n$ . Comme  $\sigma$  est paire, on peut la décomposer en un produit d'un nombre pair  $n$  de transpositions :

$$\sigma = \prod_{i=1}^{n-1} \tau_i \tau_{i+1}$$

qui est bien un produit de 3-cycles.

□

**Lemme 3.** Les doubles transpositions sont conjuguées dans  $A_n$  pour  $n \geq 5$ .

p. 66

*Démonstration.* Soient  $\alpha = (a_1 \ b_1)(c_1 \ d_1)(e_1)$  et  $\beta = (a_2 \ b_2)(c_2 \ d_2)(e_2)$  deux doubles transpositions. Il suffit de prendre  $\sigma \in A_5$  telle que  $\sigma(a_1) = a_2$ ,  $\sigma(b_1) = b_2$  et  $\sigma(e_1) = e_2$  pour avoir  $\sigma\alpha\sigma^{-1} = \beta$ .

□



**Lemme 4.**  $A_5$  est simple.

*Démonstration.* Commençons par décrire les types possibles des permutations de  $A_5$  (le “type” d’une permutation désigne les cardinaux des supports des cycles apparaissant dans sa décomposition en cycles disjoints).

Type de permutation	Nombre de permutations
[1]	1
[3]	$\frac{5 \times 4 \times 3}{3} = 20$
[5]	$\frac{5 \times 4 \times 3 \times 2 \times 1}{5} = 24$
[2, 2]	$\frac{1}{2} \frac{5 \times 4 \times 3 \times 2}{4} = 15$

Soit  $H \triangleleft A_5$  tel que  $H \neq \{\text{id}\}$ . Montrons que  $H = A_5$ .

- Si  $H$  contient une permutation de type [2, 2], alors par le Théorème 3, il contient toutes les permutations de type [3].
- Si  $H$  contient une permutation de type [3], alors par le Théorème 1, il les contient toutes.
- Si  $H$  contient une permutation de type [5],  $\sigma = \begin{pmatrix} a & b & c & d & e \end{pmatrix}$ , il contient alors le commutateur

$$\begin{aligned}
 (a \ b \ c) \sigma (a \ b \ c)^{-1} \sigma^{-1} &= (a \ b \ c) \sigma (c \ b \ a) \sigma^{-1} \\
 &= (a \ b \ c) (\sigma(c) \ \sigma(b) \ \sigma(a)) \\
 &= (a \ b \ c) (d \ c \ b) \\
 &= (b \ d \ a)
 \end{aligned}$$

qui est un 3-cycle. Par le Théorème 1, il les contient tous.

Or,  $H$  ne peut pas vérifier qu’un seul des points précédents en vertu du théorème de Lagrange, car ni  $16 = 15 + 1$ , ni  $21 = 20 + 1$  ne divisent  $|A_5| = 60$ . Donc  $H$  vérifie au moins deux des points précédents, et ainsi  $|H| \geq 1 + 15 + 20 = 36$ . Donc  $|H| = 60$  et  $H = A_5$ .  $\square$

Si les théorèmes de Sylow sont mentionnés dans le plan, il est préférable de mentionner l’argument suivant.

[PER]  
p. 28

*Remarque 5.* Dans le raisonnement précédent, si  $H$  contient une permutation de type [5] (qui est donc d’ordre 5), alors  $H$  contient le 5-Sylow engendré par cet élément. Or, on sait par les théorèmes de Sylow que les sous-groupes de Sylow sont conjugués entre eux. Donc  $H$  contient tous les 5-Sylow et donc contient tous les éléments d’ordre 5.

**Théorème 6.**  $A_n$  est simple pour  $n \geq 5$ .

*Démonstration.* Soit  $N \triangleleft A_n$  tel que  $N \neq \{\text{id}\}$ . L'idée générale de la démonstration est de se ramener au cas  $n = 5$  à l'aide d'une permutation bien spécifique.

Soit  $\sigma \in N \setminus \{\text{id}\}$ , il existe donc  $a \in \llbracket 1, n \rrbracket$  tel que  $\sigma(a) = b \neq a$ . Soit  $c \in \llbracket 1, n \rrbracket$  différent de  $a, b$  et  $\sigma(b)$ . On pose  $\tau = \begin{pmatrix} a & c & b \end{pmatrix} \in A_n$  (on a  $\tau^{-1} = \begin{pmatrix} a & b & c \end{pmatrix}$ ). Soit  $\rho = \tau \sigma \tau^{-1} \sigma^{-1}$ . Par calcul :

$$\rho = \begin{pmatrix} a & c & b \end{pmatrix} \sigma \begin{pmatrix} a & b & c \end{pmatrix} \sigma^{-1} = \begin{pmatrix} a & c & b \end{pmatrix} \begin{pmatrix} \sigma(a) & \sigma(b) & \sigma(c) \end{pmatrix}$$

Notons bien que  $\rho \neq \text{id}$  (en tant que produit de 3-cycles, car  $\sigma(b) \neq c$ , donc  $\rho(b) \neq b$  par calcul). Or,  $\tau \sigma \tau^{-1} \in N$  car  $N$  est distingué et  $\sigma^{-1}$  aussi car  $N$  est un groupe, donc  $\rho \in N$ .

Notons  $\mathcal{F} = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ . Comme  $\sigma(a) = b$ ,  $|\mathcal{F}| \leq 5$ . Quitte à rajouter, au besoin, des éléments à  $\mathcal{F}$ , on peut supposer que  $|\mathcal{F}| = 5$ . On pose

$$A(\mathcal{F}) = \{\alpha \in A_n \mid \forall i \in \llbracket 1, n \rrbracket \setminus \mathcal{F}, \alpha(i) = i\}$$

le sous-groupe de  $A_n$  contenant les éléments qui laissent fixes  $\llbracket 1, n \rrbracket \setminus \mathcal{F}$ . Si on pose  $\mathcal{F} = \{a_1, a_2, a_3, a_4, a_5\}$ , on a une bijection entre  $\mathcal{F}$  et  $\llbracket 1, 5 \rrbracket$  :

$$\begin{aligned} \mathcal{F} &\rightarrow \llbracket 1, 5 \rrbracket \\ a_i &\mapsto i \end{aligned}$$

Donc  $A(\mathcal{F})$  et  $A_5$  sont deux groupes isomorphes (en effet, une permutation n'agissant que sur  $\mathcal{F}$  peut s'identifier à une permutation n'agissant que sur  $\llbracket 1, 5 \rrbracket$ ). De plus, par le Théorème 4, comme  $A_5$  est simple,  $A(\mathcal{F})$  l'est aussi.

Soit  $N_0 = N \cap A(\mathcal{F})$ .  $N_0 \triangleleft A(\mathcal{F})$ , en effet, soient  $\alpha \in N_0$  et  $\beta \in A(\mathcal{F})$  :

- $\beta \alpha \beta^{-1} \in A(\mathcal{F})$  car  $A(\mathcal{F})$  est un groupe.
- $\beta \alpha \beta^{-1} \in N$  car  $N \triangleleft A_5$ .

En particulier,  $N_0$  est distingué dans  $A(\mathcal{F})$  qui est simple. De plus,  $\rho \in N_0$  (car  $\text{Supp}(\rho) \subseteq \mathcal{F}$  et  $\epsilon(\rho) = (-1)^6 = 1$  donc  $\rho \in A(\mathcal{F})$ , et on avait déjà  $\rho \in N$ ). Donc  $N_0 \neq \{\text{id}\}$ , et ainsi  $N_0 = A(\mathcal{F})$ . On en déduit :

$$A(\mathcal{F}) = N \cap A(\mathcal{F}) \tag{*}$$

Finalement,  $\tau$  est un 3-cycle qui n'agit que sur  $\mathcal{F}$ , donc  $\tau \in A(\mathcal{F})$  et par (\*),  $\tau \in N$ . Or,  $\tau$  est un 3-cycle et les 3-cycles sont conjugués dans  $A_n$  (par le Théorème 1) donc  $N$  contient tous les 3-cycles. Et comme ceux-ci engendrent  $A_n$  (par le Théorème 2), on a  $N = A_n$ .  $\square$

## 23 Suite de polygones

Il s'agit ici d'étudier une suite de polygones à l'aide de déterminants classiques, et de montrer qu'elle converge vers l'isobarycentre du polygone de départ.

**Lemme 1** (Déterminant circulant). Soient  $n \in \mathbb{N}^*$  et  $a_1, \dots, a_n \in \mathbb{C}$ . On pose  $\omega = e^{\frac{2i\pi}{n}}$ . Alors

[GOU21]  
p. 153

$$\begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{vmatrix} = \prod_{j=0}^{n-1} P(\omega^j)$$

où  $P = \sum_{k=0}^{n-1} a_k X^k$ .

*Démonstration.* On définit

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{C}) \text{ et } \Omega = (\omega^{(i-1)(j-1)})_{i,j \in \llbracket 1, n \rrbracket} \in \mathcal{M}_n(\mathbb{C})$$

Pour  $i \geq 2$ , la  $i$ -ième ligne de  $A$  est

$$(a_{n-i+1} \quad \dots \quad a_{n-1} \quad a_0 \quad \dots \quad a_{n-i-2})$$

Si on multiplie cette ligne par la  $j$ -ième colonne de  $\Omega$ , on obtient le coefficient

$$\begin{aligned} & a_{n-i+1} + a_{n-i+2}\omega^{j-1} + \dots + a_0\omega^{(j-1)(i-1)} + a_1\omega^{(j-1)i} + \dots + a_{n-i-2}\omega^{(j-1)(n-1)} \\ &= \omega^{(j-1)(i-1)}(a_0 + a_1\omega^{j-1} + \dots + a_{n-1}\omega^{(j-1)(n-1)}) \\ &= \omega^{(j-1)(i-1)}P(\omega^{j-1}) \end{aligned}$$

et c'est encore vrai pour  $i = 1$  puisque  $\omega^0 = 1$ . Donc la  $j$ -ième colonne de  $A\Omega$  est égale à la  $j$ -ième colonne de  $\Omega$  multipliée par  $P(\omega^{j-1})$ . Ceci entraîne que

$$\det(A) \det(\Omega) = \det(A\Omega) = P(1)P(\omega) \dots P(\omega^{n-1}) \det(\Omega)$$

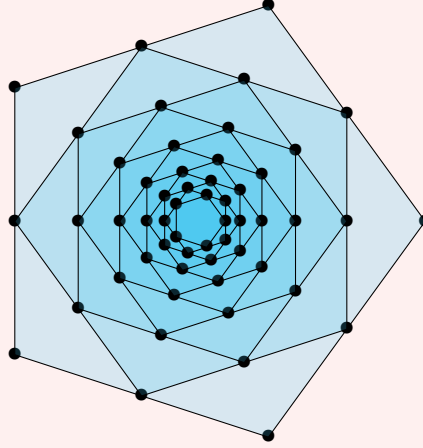
et le déterminant  $\det(\Omega)$  est non nul (en tant que déterminant de Vandermonde à paramètres deux-à-deux distincts). D'où :

$$\det(A) = P(1)P(\omega) \dots P(\omega^{n-1})$$

□

[I-P]  
p. 389

**Théorème 2** (Suite de polygones). Soit  $P_0$  un polygone dont les sommets sont  $\{z_{0,1}, \dots, z_{0,n}\}$ . On définit la suite de polygones  $(P_k)$  par récurrence en disant que, pour tout  $k \in \mathbb{N}^*$ , les sommets de  $P_{k+1}$  sont les milieux des arêtes de  $P_k$ .



Alors la suite  $(P_k)$  converge vers l'isobarycentre de  $P_0$ .

*Démonstration.* On identifie  $P_k$  au vecteur colonne  $Z_k = \begin{pmatrix} z_{k,1} \\ \vdots \\ z_{k,n} \end{pmatrix} \in \mathbb{C}^n$ . Il s'agit de montrer que la

suite  $(Z_k)$  converge vers  $\begin{pmatrix} g \\ \vdots \\ g \end{pmatrix}$  où  $g$  désigne l'isobarycentre de  $P_0$ .

En utilisant la notation matricielle, la relation de récurrence s'écrit

$$\forall k \in \mathbb{N}, Z_{k+1} = \begin{pmatrix} \frac{z_{k,1} + z_{k,2}}{2} \\ \vdots \\ \frac{z_{k,n} + z_{k,1}}{2} \end{pmatrix} = AZ_k \text{ où } A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & \dots & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \dots & 0 & \frac{1}{2} \end{pmatrix}$$

Par une récurrence immédiate (c'est une suite géométrique), on a donc  $\forall k \in \mathbb{N}, Z_k = A^k Z_0$ . Il suffit donc de montrer que  $(A^k)$  converge dans  $\mathcal{M}_n(\mathbb{C})$  (muni d'une norme quelconque par équivalence des normes en dimension finie).

Pour cela, étudions les valeurs propres de  $A$  :

$$\chi_A = \det(A - XI_n) = \begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{vmatrix}$$

avec  $a_0 = \frac{1}{2} - X$ ,  $a_1 = \frac{1}{2}$  et  $\forall i > 2, a_i = 0$ . On reconnaît le déterminant circulant du Théorème 1 et

en posant  $P(Y) = \sum_{k=0}^{n-1} a_k Y^k$  et  $\omega = e^{\frac{2i\pi}{n}}$ , la formule du déterminant circulant nous donne :

$$\chi_A = \prod_{j=1}^n P(\omega^j) = \prod_{j=1}^n \left( \sum_{k=0}^{n-1} a_k \omega^{kj} \right) = \prod_{j=1}^n \left( \frac{1}{2} - X + \frac{1}{2} \omega^j \right) = \prod_{j=1}^n (\lambda_j - X)$$

où  $\lambda_j = \frac{1+\omega^j}{2}$ . Et comme  $\lambda_i = \lambda_j \iff i = j$ , le polynôme  $\chi_A$  est scindé à racines simples. Donc  $\exists Q \in \text{GL}_n(\mathbb{C})$  telle que  $A = QDQ^{-1}$  et  $D = \text{Diag}(\lambda_1, \dots, \lambda_n)$ . Or pour  $j \neq n$ ,

$$|\lambda_j| = \left| \frac{1+\omega^j}{2} \right| = \left| e^{\frac{ij\pi}{n}} \frac{e^{\frac{ij\pi}{n}} + e^{-\frac{ij\pi}{n}}}{2} \right| = \left| \cos\left(\frac{\pi j}{n}\right) \right| < 1$$

Ainsi,  $\lambda_j^k \longrightarrow 0$  si  $j < n$ , donc la suite  $(A^k)$  converge dans  $\mathcal{M}_n(\mathbb{C})$  vers la matrice  $B = Q \text{Diag}(0, \dots, 0, 1) Q^{-1}$  par continuité de l'application  $M \mapsto QMQ^{-1}$ .

On pose donc  $X = BZ_0$ , de sorte que la suite  $(Z_k)$  converge vers  $X$ . Par continuité de  $M \mapsto AM$ , la limite  $X$  vérifie forcément  $X = AX$  ie.  $X$  est vecteur propre de  $A$  associé à la valeur propre 1. Or

l'espace propre de  $A$  associé à la valeur propre 1 contient le vecteur  $\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$  et est de dimension 1

(car  $\chi_A$  possède  $n$  racines distinctes), donc il est engendré par ce vecteur. Ainsi, il existe  $a \in \mathbb{C}$  tel

que  $X = \begin{pmatrix} a \\ \vdots \\ a \end{pmatrix}$  ie.  $(Z_k)$  converge vers le point d'affixe  $a$ .

Enfin, on remarque que si  $g$  est l'isobarycentre de  $P_0$ , il est aussi égal à celui de  $P_k$  pour tout  $k$  (que l'on note  $g_k$ ) car pour tout  $k \geq 1$  :

$$g_k = \frac{1}{n} \sum_{i=1}^n z_{k,i} = \frac{1}{n} \sum_{i=1}^n \frac{z_{k-1,i} + z_{k-1,i+1}}{2} = \frac{1}{n} \sum_{i=1}^n z_{k-1,i} = g_{k-1}$$

(en considérant les indices  $i$  modulo  $n$ ). Or, la suite  $(Z_k)$  converge vers  $\begin{pmatrix} a \\ \vdots \\ a \end{pmatrix}$ , et la fonction  $\varphi$  qui

à  $n$  points du plan associe son isobarycentre est continue. Donc,

$$g_k = \varphi(Z_k) \longrightarrow \varphi(a, \dots, a) = a$$

et comme pour tout  $k$ ,  $g_k = g$ , on a bien  $g = a$ . □

## 24 $\exp : \mathcal{M}_n(\mathbb{R}) \rightarrow \mathrm{GL}_n(\mathbb{R})$ est surjective

Dans ce développement, on démontre que l'exponentielle de matrices est surjective en utilisant des théorèmes d'analyse.

**Lemme 1.** Soit  $M \in \mathrm{GL}_n(\mathbb{C})$ . Alors  $M^{-1} \in \mathbb{C}[X]$  (ie.  $M^{-1}$  est un polynôme en  $M$ ).

[I-P]  
p. 396

*Démonstration.* D'après le théorème de Cayley-Hamilton,  $\chi_M(M) = 0$ . Or, en notant  $\chi_M = \sum_{k=0}^n a_k X^k$ , on a  $a_0 = (-1)^n \det(M)$ , d'où

$$0 = M^n + \cdots + a_1 M + (-1)^n \det(M) I_n$$

En notant  $Q = X^{n-1} + a_{n-1} X^{n-2} + \cdots + a_2 X + a_1$ , on en déduit que  $(-1)^{n+1} \det(M) I_n = Q(M)M$ . D'où

$$M^{-1} = \frac{(-1)^{n+1}}{\det(M)} Q(M) \in \mathbb{C}[M]$$

ce qu'il fallait démontrer. □

**Lemme 2.** Soit  $M \in \mathcal{M}_n(\mathbb{C})$ . Alors,  $\exp(M) \in \mathrm{GL}_n(\mathbb{C})$ .

*Démonstration.*  $M$  et  $-M$  commutent, donc

$$\exp(M) \exp(-M) = \exp(M - M) = I_n = \exp(-M) \exp(M)$$

Ainsi  $\exp(M)$  est inversible, d'inverse  $\exp(-M)$ . □

**Notation 3.** Soit  $C \in \mathcal{M}_n(\mathbb{C})$ . On note  $\mathbb{C}[C]^* = \mathbb{C}[C] \cap \mathrm{GL}_n(\mathbb{C})$ .

**Lemme 4.** Soit  $C \in \mathcal{M}_n(\mathbb{C})$ .  $\mathbb{C}[C]^*$  est un sous-groupe de  $\mathrm{GL}_n(\mathbb{C})$ .

*Démonstration.* —  $I_n \in \mathbb{C}[C]$  et  $I_n \in \mathrm{GL}_n(\mathbb{C})$ , donc  $I_n \in \mathbb{C}[C]^*$ .

— Soit  $M \in \mathbb{C}[C]^*$ . Comme  $M \in \mathrm{GL}_n(\mathbb{C})$ ,  $M^{-1}$  existe, est inversible, et, par le Théorème 1,  $M^{-1} \in \mathbb{C}[C]$ .

— Enfin,  $\mathbb{C}[C]^*$  est clairement stable par multiplication. □

**Lemme 5.**  $\exp$  est différentiable en 0 et,

$$d\exp_0 = I_n$$

*Démonstration.* Soit  $H \in \mathcal{M}_n(\mathbb{C})$ .

$$\begin{aligned} \exp(0 + H) - \exp(H) &= \sum_{k=0}^{+\infty} \frac{H^k}{k!} \\ &= I_n + H + \sum_{k=2}^{+\infty} \frac{H^k}{k!} \end{aligned}$$

Soit  $\|\cdot\|$  une norme d'algèbre sur  $\mathcal{M}_n(\mathbb{C})$ . On a :

$$\begin{aligned} \left\| \sum_{k=2}^{+\infty} \frac{H^k}{k!} \right\| &\leq \sum_{k=2}^{+\infty} \left\| \frac{H^k}{k!} \right\| \\ &\leq \sum_{k=2}^{+\infty} \frac{\|H\|^k}{k!} \\ &= e^{\|H\|} - \|H\| - 1 \end{aligned}$$

En effectuant un développement limité de l'exponentielle réelle à l'origine, on obtient bien  $\left\| \sum_{k=2}^{+\infty} \frac{H^k}{k!} \right\| = o(\|H\|)$ .  $\square$

**Théorème 6.**  $\exp : \mathcal{M}_n(\mathbb{C}) \rightarrow \mathrm{GL}_n(\mathbb{C})$  est surjective.

*Démonstration.* Fixons  $C \in \mathcal{M}_n(\mathbb{C})$  pour le reste de la démonstration. Comme  $\mathbb{C}[C]$  est un sous-espace vectoriel de l'espace  $\mathcal{M}_n(\mathbb{C})$ , il est de dimension finie et est donc fermé. En particulier,  $\exp(C) \in \mathbb{C}[C]$ . Le Théorème 2 combiné au Théorème 4, nous dit que  $\exp : \mathbb{C}[C] \rightarrow \mathbb{C}[C]^*$  est bien définie. Il s'agit de plus d'un morphisme de groupes. En effet,  $\forall A, B \in \mathbb{C}[C]$ , on a  $AB = BA$ , d'où  $\exp(A)\exp(B) = \exp(A+B) = \exp(B)\exp(A)$ .

Montrons que  $\mathbb{C}[C]^*$  est un ouvert connexe de  $\mathbb{C}[C]$ . Notons qu'il s'agit bien d'un ouvert de  $\mathbb{C}[C]$ , car c'est l'intersection de  $\mathbb{C}[C]$  avec  $\mathrm{GL}_n(\mathbb{C})$  qui est ouvert dans  $\mathcal{M}_n(\mathbb{C})$ . Ensuite, soient  $A, B \in \mathbb{C}[C]^*$ . On pose

$$P = \det((1 - X)A + XB)$$

$P$  ne s'annule ni en 0, ni en 1 par inversibilité de  $A$  et  $B$ .  $P$  a un nombre fini de racines car n'est pas nul : on peut trouver une fonction continue  $\gamma : [0, 1] \rightarrow \mathbb{C}$  qui évite ces racines. Ainsi,

$$\forall t \in [0, 1], (1 - \gamma(t))A + \gamma(t)B \in \mathbb{C}[C]^*$$

donc  $\mathbb{C}[C]^*$  est connexe par arcs, donc est en particulier connexe.

Il s'agit maintenant de montrer que  $\exp(\mathbb{C}[C])$  est un ouvert-fermé de  $\mathbb{C}[C]^*$ . Commençons par montrer qu'il est ouvert en montrant qu'il contient un voisinage de chacun de ses points. Par le théorème d'inversion locale appliqué à  $\exp : \mathbb{C}[C] \rightarrow \mathbb{C}[C]$  (qui est bien  $\mathcal{C}^1$  sur l'espace de Banach  $\mathbb{C}[C]$  et, par le Théorème 5,  $\det(d\exp_0) \neq 0$ ) : il existe  $U$  un voisinage de 0 dans  $\mathbb{C}(C)$  et un ouvert  $V$  de  $\mathbb{C}(C)$  contenant  $\exp(0) = I_n$  tels que  $\exp : U \rightarrow V$  soit un difféomorphisme de classe  $\mathcal{C}^1$ . Soit

$A \in \mathbb{C}[C]$ . Posons

$$f_A : \begin{array}{ccc} \mathbb{C}[C] & \rightarrow & \mathbb{C}[C] \\ M & \mapsto & \exp(A)^{-1}M \end{array}$$

et montrons que  $\exp(A)V = f^{-1}(V)$ . Pour tout  $B \in V$ ,  $f_A(\exp(A)B) = \exp(A)^{-1}(\exp(A)B) = B \in V$ , donc  $\exp(A)V \subseteq f^{-1}(V)$ .

Soit  $B \in f^{-1}(V)$ , alors  $f_A(B) \in V$ . Or,  $f_A(B) = \exp(A)^{-1}B$ , donc  $B = \exp(A)f_A(B) \in \exp(A)V$ . On en déduit que  $\exp(A)V = f^{-1}(V)$  et que  $\exp(A)V$  est un ouvert par continuité de  $f$ .

Comme  $V$  contient  $I_n$ ,  $\exp(A)V$  est un voisinage de  $\exp(A)$ . Or,  $\exp(A)V$  est inclus dans  $\mathbb{C}[C]$  car pour tout  $B \in V$ , il existe  $M \in \mathbb{C}[C]$  tel que  $\exp(M) = B$ . Ainsi,

$$\exp(A)V = \exp(A)\exp(M) = \exp(A + M) \in \exp(\mathbb{C}[C])$$

On en déduit que  $\exp(\mathbb{C}[C])$  est un ouvert.

Posons maintenant  $O = \mathbb{C}[C]^* \setminus \exp(\mathbb{C}[C])$  et montrons que

$$O = \bigcup_{A \in O} A \exp(\mathbb{C}[C]) \quad (*)$$

Soient  $A \in O$  et  $B \in \exp(\mathbb{C}[C])$ . Alors  $AB \in \mathbb{C}[C]^*$ . Supposons par l'absurde que  $AB \in \exp(\mathbb{C}[C])$ . Il existe donc  $M \in \exp(\mathbb{C}[C])$  tel que  $AB = M$  et  $A = MB^{-1}$ . Comme  $\exp(\mathbb{C}[C])$  est un groupe multiplicatif, alors  $A \in \exp(\mathbb{C}[C])$  : absurde. On conclut que

$$\bigcup_{A \in O} A \exp(\mathbb{C}[C]) \subseteq O$$

Réciproquement, supposons que  $M \in O$ . Comme  $I_n \in \exp(\mathbb{C}[C])$ , alors  $M \in M \exp(\mathbb{C}[C])$ . On en déduit (\*), ainsi que la fermeture de  $\exp(\mathbb{C}[M])$  par passage au complémentaire.

$\exp(\mathbb{C}[M])$  est un ouvert fermé non vide (car contient  $I_n$ ) de  $\mathbb{C}[M]^*$ , alors  $\exp(\mathbb{C}[M]) = \mathbb{C}[M]^*$ . Pour conclure, si  $M \in \mathrm{GL}_n(\mathbb{C})$ , alors  $M \in \mathbb{C}[M]$  et donc  $M \in \mathbb{C}[M]^*$ . Ainsi,  $M \in \exp(\mathbb{C}[M])$ , et  $\exp$  est bien surjective.  $\square$

**Application 7.**  $\exp(\mathcal{M}_n(\mathbb{R})) = \mathrm{GL}_n(\mathbb{R})^2$ , où  $\mathrm{GL}_n(\mathbb{R})^2$  désigne les carrés de  $\mathrm{GL}_n(\mathbb{R})$ .

*Démonstration.* Soit  $M \in \mathcal{M}_n(\mathbb{R})$ . Alors,

$$\exp(M) = \exp\left(\frac{M}{2}\right)^2$$

d'où  $\exp(\mathcal{M}_n(\mathbb{R})) \subseteq \mathrm{GL}_n(\mathbb{R})^2$ . Réciproquement, soit  $A \in \mathrm{GL}_n(\mathbb{R})^2$ . Posons  $B = A^2$ . D'après le Théorème 6,

$$\exists P \in \mathbb{C}[X] \text{ telle que } A = \exp(P(A))$$

Comme  $A$  est une matrice réelle, alors en passant au conjugué, on obtient  $A = \exp(\overline{P}(A))$ . Ainsi,

$$B = A^2 = \exp((P + \overline{P})(A)) \in \exp(\mathcal{M}_n(\mathbb{R}))$$

d'où  $\mathrm{GL}_n(\mathbb{R})^2 \subseteq \exp(\mathcal{M}_n(\mathbb{R}))$ .  $\square$



## 25 Théorème central limite

En établissant d'abord le théorème de Lévy, on démontre le théorème central limite, qui dit que si  $(X_n)$  est une suite de variables aléatoires identiquement distribuées admettant un moment d'ordre 2, alors  $\frac{X_1 + \dots + X_n - n\mathbb{E}(X_1)}{\sqrt{n}}$  converge en loi vers  $\mathcal{N}(0, \text{Var}(X_1))$ .

**Notation 1.** Si  $X$  est une variable aléatoire réelle, on note  $\phi_X$  sa fonction caractéristique.

**Théorème 2 (Lévy).** Soient  $(X_n)$  une suite de variables aléatoires réelles définies sur un espace probabilité  $(\Omega, \mathcal{A}, \mathbb{P})$  et  $X$  une variable aléatoire réelle définie sur le même espace. Alors :

$$X_n \xrightarrow{(d)} X \iff \phi_{X_n} \text{ converge simplement vers } \phi_X$$

[Z-Q]  
p. 544

*Démonstration.* Sens direct : On suppose que  $(X_n)$  converge en loi vers  $X$ . Pour tout  $t \in \mathbb{R}$ , la fonction  $g_t : x \mapsto e^{itx}$  est continue et bornée sur  $\mathbb{R}$ . Donc par définition de la convergence en loi :

$$\lim_{n \rightarrow +\infty} \mathbb{E}(g_t(X_n)) = \mathbb{E}(g_t(X))$$

ce que l'on voulait.

Réciproque : Soit  $\varphi \in L_1(\mathbb{R})$ . On suppose que sa transformée de Fourier,  $f = \hat{\varphi}$  appartient également à  $L_1(\mathbb{R})$ . Alors

$$\mathbb{E}(f(X_n)) = \mathbb{E}\left(\int_{\mathbb{R}} e^{itX_n} \varphi(t) dt\right)$$

Comme la fonction  $(\omega, t) \mapsto e^{itX_n(\omega)} \varphi(t)$  est intégrable pour la mesure  $\mathbb{P} \otimes \lambda$ , on peut appliquer le théorème de Fubini-Lebesgue pour intervertir espérance et intégrale :

$$\mathbb{E}(f(X_n)) = \int_{\mathbb{R}} \mathbb{E}(e^{itX_n}) \varphi(t) dt$$

On définit maintenant la suite de fonction  $g_n : t \mapsto \mathbb{E}(e^{itX_n}) \varphi(t)$ . Alors :

- $\forall n \in \mathbb{N}$ ,  $g_n$  est mesurable.
- La suite de fonction  $(g_n)$  converge presque partout vers  $g : t \mapsto \mathbb{E}(e^{itX}) \varphi(t)$  par hypothèse.
- $\forall n \in \mathbb{N}$  et pp. en  $t \in \mathbb{R}$ ,  $|g_n(t)| \leq \mathbb{E}(|e^{itX_n}|) |\varphi(t)| \leq \mathbb{P}(\Omega) |\varphi(t)| = |\varphi(t)|$  avec  $|\varphi| \in L_1(\mathbb{R})$ .

On peut donc appliquer le théorème de convergence dominée pour obtenir

$$\mathbb{E}(f(X_n)) \longrightarrow \int_{\mathbb{R}} \mathbb{E}(e^{itX}) \varphi(t) dt = \mathbb{E}(f(X))$$

Ainsi, le résultat est vrai pour toute fonction  $L_1(\mathbb{R})$  dans l'image de  $L_1(\mathbb{R})$  par la transformée de Fourier. En particulier, il est vrai pour tout  $f \in \mathcal{S}(\mathbb{R})$ , dense dans  $(\mathcal{C}(\mathbb{R}), \|\cdot\|_{\infty})$ . Soient maintenant

$f \in \mathcal{C}(\mathbb{R})$  et  $(f_k)$  une suite de fonctions de  $\mathcal{S}(\mathbb{R})$  qui converge uniformément vers  $f$ . Alors,

$$\begin{aligned} |\mathbb{E}(f(X_n)) - \mathbb{E}(f(X))| &= |\mathbb{E}(f(X_n)) - \mathbb{E}(f_k(X_n)) + \mathbb{E}(f_k(X_n)) \\ &\quad - \mathbb{E}(f_k(X)) + \mathbb{E}(f_k(X)) - \mathbb{E}(f(X))| \\ &\leq 2\|f - f_k\|_\infty + |\mathbb{E}(f_k(X_n)) - \mathbb{E}(f_k(X))| \\ &\longrightarrow 0 \end{aligned}$$

□

**Lemme 3.** Soient  $u, v \in \mathbb{C}$  de module inférieur ou égal à 1 et  $n \in \mathbb{N}^*$ . Alors

$$|z^n - u^n| \leq n|z - u|$$

[G-K]  
p. 307

*Démonstration.*  $|z^n - u^n| = |(z - u) \sum_{k=0}^{n-1} z^k u^{n-1-k}| \leq n|z - u|$ .

□

**Théorème 4** (Central limite). Soit  $(X_n)$  une suite de variables aléatoires réelles indépendantes de même loi admettant un moment d'ordre 2. On note  $m$  l'espérance et  $\sigma^2$  la variance commune à ces variables. On pose  $S_n = X_1 + \dots + X_n - nm$ . Alors,

$$\left( \frac{S_n}{\sqrt{n}} \right) \xrightarrow{(d)} \mathcal{N}(0, \sigma^2)$$

*Démonstration.* On a  $S_n = \sum_{k=1}^n (X_k - m)$ . Notons  $\phi$  la fonction caractéristique de  $X_1 - m$ . Comme les variables aléatoires  $X_1 - m, \dots, X_n - m$  sont indépendantes de même loi, la fonction caractéristique de  $\frac{S_n}{\sqrt{n}}$  vaut  $\forall t \in \mathbb{R}$ ,

$$\begin{aligned} \phi_{\frac{S_n}{\sqrt{n}}}(t) &= \mathbb{E} \left( e^{iS_n \left( \frac{t}{\sqrt{n}} \right)} \right) \\ &= \mathbb{E} \left( \prod_{k=1}^n e^{i(X_k - m) \left( \frac{t}{\sqrt{n}} \right)} \right) \\ &= \prod_{k=1}^n \phi_{X_k - m} \left( \frac{t}{\sqrt{n}} \right) \\ &= \phi \left( \frac{t}{\sqrt{n}} \right)^n \end{aligned}$$

D'après le Théorème 2, pour montrer que  $\frac{S_n}{\sqrt{n}}$  converge en loi vers  $\mathcal{N}(0, \sigma^2)$ , il suffit de montrer que

$$\forall t \in \mathbb{R}, \lim_{n \rightarrow +\infty} \phi \left( \frac{t}{\sqrt{n}} \right)^n = e^{-\frac{\sigma^2}{2} t^2}$$

car  $t \mapsto e^{-\frac{\sigma^2}{2} t^2}$  est la fonction caractéristique de la loi  $\mathcal{N}(0, \sigma^2)$ .

Comme  $X_1$  admet un moment d'ordre 2,  $\phi$  est de classe  $\mathcal{C}^2$  et

- $\phi(0) = 1$ .
- $\phi'(0) = i^1 \mathbb{E}(X_1^1) = 0$ .
- $\phi''(0) = i^2 \mathbb{E}(X_1^2) = -E(X^2) = -\sigma^2$  (car  $m = 0$ ).

Ce qui donne le développement limité en 0 de  $\phi$  à l'ordre 2 (par la formule de Taylor-Young) :

$$\phi(t) = \phi(0) + \frac{\phi'(0)}{1!}(t-0) + \frac{\phi''(0)}{2!}(t-0)^2 + o(t^2) = 1 - \frac{\sigma^2 t^2}{2} + o(t^2) \quad (*)$$

Et, en appliquant le Théorème 3 :

$$\begin{aligned} \left| \phi\left(\frac{t}{\sqrt{n}}\right)^n - e^{-\frac{\sigma^2}{2}t^2} \right| &= \left| \phi\left(\frac{t}{\sqrt{n}}\right)^n - \left(e^{-\frac{\sigma^2}{2n}t^2}\right)^n \right| \\ &\leq n \left| \phi\left(\frac{t}{\sqrt{n}}\right) - e^{-\frac{\sigma^2}{2n}t^2} \right| \end{aligned}$$

On a d'une part, par développement limité :

$$e^{-\frac{\sigma^2}{2n}t^2} = 1 - \frac{\sigma^2}{2n}t^2 + o\left(\frac{1}{n}\right)$$

Et d'autre part, par (\*) :

$$\phi\left(\frac{t}{\sqrt{n}}\right) = 1 - \frac{\sigma^2}{2n}t^2 + o\left(\frac{1}{n}\right)$$

On obtient ainsi le résultat cherché, à savoir :

$$n \left| \phi\left(\frac{t}{\sqrt{n}}\right) - e^{-\frac{\sigma^2}{2n}t^2} \right| = o(1)$$

□

## 26 Théorème chinois

On montre le théorème chinois et on propose une application à la résolution d'un système de congruences.

Soit  $A$  un anneau principal. Soient  $r \geq 2$  un entier et  $a_1, \dots, a_r \in A$  des éléments premiers entre eux deux à deux.

[ROM21]  
p. 250

**Notation 1.** Pour tout  $i \in \llbracket 1, r \rrbracket$ , on note

$$\pi_i = \pi_{(a_i)} : A \rightarrow A/(a_i)$$

la surjection canonique de  $A$  sur  $A/(a_i)$ . On note également  $\pi = \pi_{(a_1 \dots a_r)} : A \rightarrow A/(a_1 \dots a_r)$ .

**Théorème 2 (Chinois).** Alors :

(i) L'application :

$$\begin{aligned} \varphi : A &\rightarrow A/(a_1) \times \dots \times A/(a_r) \\ x &\mapsto (\pi_1(x), \dots, \pi_r(x)) \end{aligned}$$

est un morphisme d'anneaux de noyau  $\text{Ker}(\varphi) = (a_1 \dots a_r)$ .

(ii) Il existe  $u_1, \dots, u_r \in A$  tels que

$$\sum_{i=1}^r u_i b_i = 1$$

où  $\forall i \in \llbracket 1, r \rrbracket$ ,  $b_i = \frac{a}{a_i}$  et  $a = a_1 \dots a_r$ .

(iii)  $\varphi$  est surjectif et induit un isomorphisme  $\overline{\varphi} : A/(a_1 \dots a_r) \rightarrow A/(a_1) \times \dots \times A/(a_r)$ . On a,

$$\begin{aligned} \overline{\varphi}^{-1} : A/(a_1) \times \dots \times A/(a_r) &\rightarrow A/(a_1 \dots a_r) \\ (\pi_1(x_1), \dots, \pi_r(x_r)) &\mapsto \pi\left(\sum_{i=1}^r x_i u_i b_i\right) \end{aligned}$$

où  $\pi$  est la surjection canonique de  $A$  sur le quotient  $A/(a_1 \dots a_r)$ .

*Démonstration.* (i) On vérifie sans difficulté que  $\varphi$  est un morphisme d'anneaux (du fait que les projections canoniques sur les quotients en sont). De là,

$$\begin{aligned} \text{Ker}(\varphi) &= \{x \in A \mid \forall i \in \llbracket 1, r \rrbracket, \pi_i(x) = 0\} \\ &= \{x \in A \mid \forall i \in \llbracket 1, r \rrbracket, a_i \mid x\} \\ &= \{x \in A \mid \text{ppcm}(a_1, \dots, a_r) \mid x\} \end{aligned}$$

Mais,  $a_1, \dots, a_r$  sont premiers entre eux deux à deux. Donc,

$$\text{ppcm}(a_1, \dots, a_r) = a_1 \dots a_r$$

et on conclut que  $\text{Ker}(\varphi) = (a_1 \dots a_r)$ .

(ii) Supposons par l'absurde que  $b_1, \dots, b_r$  ne sont pas premiers entre eux dans leur ensemble.

Comme  $A$  est principal, donc factoriel, il existe un premier  $p \in A$  tel que

$$\forall i \in \llbracket 1, r \rrbracket, p \mid b_i$$

Comme  $p$  divise  $b_1 = a_2 \dots a_r$ , il existe  $i \in \llbracket 2, r \rrbracket$  tel que  $p \mid a_i$ . Mais, divisant  $b_i$ , il divise  $a_j$  où  $j \in \llbracket 1, r \rrbracket \setminus \{i\}$ . Contradiction car  $a_1$  et  $a_j$  sont premiers entre eux. La fin du raisonnement est une conséquence directe du théorème de Bézout valable dans les anneaux principaux.

(iii) Pour  $i, j \in \llbracket 1, r \rrbracket$  tels que  $i \neq j$ , on a

$$\pi_j(b_i) = \pi_j(0)$$

puisque  $b_i$  est multiple de  $a_j$ . Ceci permet d'écrire

$$\pi_j(1) = \pi_j\left(\sum_{i=1}^r u_i b_i\right) = \pi_j(u_j) \pi_j(b_j)$$

Donc,  $\pi_j(b_j)$  est inversible dans  $A/(a_j)$ , d'inverse  $\pi_j(u_j)$ . Ainsi, soient  $\pi_1(x_1), \dots, \pi_r(x_r) \in A/(a_1) \times \dots \times A/(a_r)$ . En posant

$$x = \sum_{i=1}^r x_i u_i b_i$$

on a

$$\pi_j(x) = \pi_j(x_j) \pi_j(u_j) \pi_j(b_j) = \pi_j(x_j)$$

donc  $\varphi(x) = (\pi_1(x_1), \dots, \pi_r(x_r))$ . Le morphisme  $\varphi$  est surjectif. Par le théorème de factorisation des morphismes, il induit un isomorphisme

$$\begin{array}{ccc} \overline{\varphi}: A/(a_1 \dots a_r) & \rightarrow & A/(a_1) \times \dots \times A/(a_r) \\ \pi(x) & \mapsto & (\pi_1(x), \dots, \pi_r(x)) \end{array}$$

et on a même prouvé que l'inverse  $\overline{\varphi}^{-1}$  est défini par

$$\overline{\varphi}^{-1}: \begin{array}{ccc} A/(a_1) \times \dots \times A/(a_r) & \rightarrow & A/(a_1 \dots a_r) \\ (\pi_1(x_1), \dots, \pi_r(x_r)) & \mapsto & \pi\left(\sum_{i=1}^r x_i u_i b_i\right) \end{array}$$

□

**Exemple 3.** Le système

$$\begin{cases} u \equiv 1 \pmod{3} \\ u \equiv 3 \pmod{5} \\ u \equiv 0 \pmod{7} \end{cases}$$

admet une unique solution dans  $\mathbb{Z}/105\mathbb{Z} : \overline{28}$ . Les solutions dans  $\mathbb{Z}$  sont donc de la forme  $28 + 105k$  avec  $k \in \mathbb{Z}$ .

[ULM18]  
p. 58

*Démonstration.* On se place dans l'anneau principal  $A = \mathbb{Z}$ . Les entiers 3, 5 et 7 sont premiers entre eux : le triplet  $(1 + (3), 3 + (5), 0 + (7)) = (x_1 + (3), x_2 + (5), x_3 + (3))$  admet un unique antécédent

par  $\overline{\varphi}^{-1}$  du Théorème 2. On a ainsi existence et unicité d'une solution modulo  $3 \times 5 \times 7 = 105$ . On explicite une relation de Bézout pour 15, 21, 35 :

$$\underbrace{-1}_{=u_1} \times \underbrace{35}_{=b_1} + \underbrace{6}_{=u_2} \times \underbrace{21}_{=b_2} + \underbrace{(-6)}_{=u_3} \times \underbrace{15}_{=b_3} = 1$$

Reste à calculer

$$\begin{aligned} \overline{\varphi}^{-1}(1 + (3), 3 + (5), 0 + (7)) &= \sum_{i=1}^3 x_i u_i b_i + (105) \\ &= 1 \times (-1) \times 35 + 3 \times 6 \times 21 + 0 \times (-6) \times 15 + (105) \\ &= 343 + (105) \\ &= 28 + (105) \end{aligned}$$

Les solutions sont bien de la forme escomptée. □

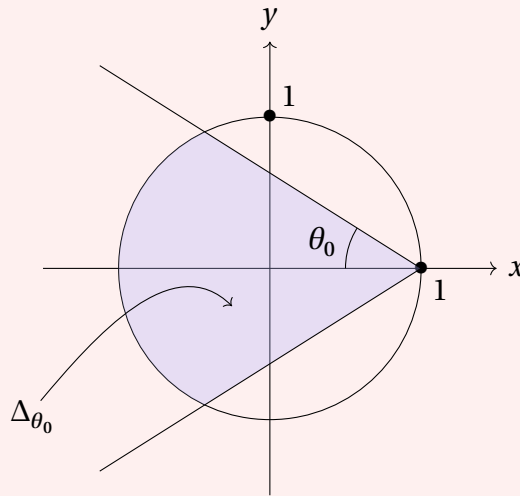
**[ULM18]** utilise un autre algorithme pour trouver la solution. Le fait de chercher un antécédent permet de faire un lien “direct” avec le Théorème 2. Attention, il faut réussir à trouver les coefficients de Bézout...

## 27 Théorème d'Abel angulaire

On montre le théorème d'Abel "angulaire", qui permet d'intervertir certaines sommes et limites, et on l'applique justement au calcul de deux sommes.

**Théorème 1** (Abel angulaire). Soit  $\sum a_n z^n$  une série entière de rayon de convergence supérieur ou égal à 1 telle que  $\sum a_n$  converge. On note  $f$  la somme de cette série sur le disque unité  $D$  de  $\mathbb{C}$ . On fixe  $\theta_0 \in [0, \frac{\pi}{2}[$  et on pose  $\Delta_{\theta_0} = \{z \in D \mid \exists \rho > 0 \text{ et } \exists \theta \in [-\theta_0, \theta_0] \text{ tels que } z = 1 - \rho e^{i\theta}\}$ .

[GOU20]  
p. 263



Alors  $\lim_{\substack{z \rightarrow 1 \\ z \in \Delta_{\theta_0}}} f(z) = \sum_{n=0}^{+\infty} a_n$ .

*Démonstration.* On note  $\forall n \in \mathbb{N}, S = \sum_{n=0}^{+\infty} a_n, S_n = \sum_{k=0}^n a_k$  et  $R_n = S - S_n$ . On cherche à majorer  $|f(z) - S|$ ; on va effectuer une transformation d'Abel en écrivant  $\forall n \geq 1, a_n = R_{n-1} - R_n$ . Soit  $z \in D \setminus \{0\}$ .  $\forall N \in \mathbb{N}^*$ , on a

$$\begin{aligned}
 \sum_{n=0}^N a_n z^n - S_N &= \sum_{n=0}^N a_n (z^n - 1) \\
 &= \sum_{n=1}^N (R_{n-1} - R_n)(z^n - 1) \\
 &= \sum_{n=0}^{N-1} R_n (z^{n+1} - 1) - \sum_{n=1}^N R_n (z^n - 1) \\
 &= \sum_{n=0}^{N-1} R_n (z^{n+1} - z^n) - R_N (z^N - 1) \\
 &= (z - 1) \sum_{n=0}^{N-1} R_n z^n - R_N (z^N - 1)
 \end{aligned}$$

Donc en faisant  $N \rightarrow +\infty$  :

$$f(z) - S = (z - 1) \sum_{n=0}^{+\infty} R_n z^n \quad (*)$$

Soit  $\epsilon > 0$ .  $\exists N \in \mathbb{N}$  tel que  $\forall n \geq N$ ,  $|R_n| < \epsilon$ . D'après (\*),  $\forall z \in D$ ,

$$\begin{aligned} |f(z) - S| &\leq |z - 1| \left| \sum_{n=0}^N R_n z^n \right| + \epsilon |z - 1| \left( \sum_{n=N+1}^{+\infty} |z|^n \right) \\ &\leq |z - 1| \left( \sum_{n=0}^N |R_n| \right) + \epsilon \frac{|z - 1|}{1 - |z|} \end{aligned} \quad (**)$$

Soit  $z \in \Delta_{\theta_0}$  de sorte que  $z = 1 - \rho e^{i\theta}$  avec  $\rho > 0$  et  $|\theta| \leq \theta_0$ . Notons avant toute chose que  $|z - 1| = \rho$ . Cherchons maintenant des conditions sur  $z$  pour majorer les deux termes :

— On a :

$$\begin{aligned} |z|^2 &= (1 - \rho \cos(\theta))^2 + (\rho \sin(\theta))^2 \\ &= 1 - 2\rho \cos(\theta) + \rho^2 (\cos(\theta)^2 + \sin(\theta)^2) \\ &= 1 - 2\rho \cos(\theta) + \rho^2 \end{aligned}$$

En supposant  $\rho \leq \cos(\theta_0)$ , cela permet de majorer le deuxième terme de (\*\*):

$$\begin{aligned} \frac{|z - 1|}{1 - |z|} &= \frac{|z - 1|}{1 - |z|^2} (1 + |z|) \\ &= \frac{\rho}{2\rho \cos(\theta) - \rho^2} (1 + |z|) \\ &\leq \frac{2}{2 \cos(\theta) - \rho} \\ &\leq \frac{2}{2 \cos(\theta_0) - \cos(\theta_0)} \\ &= \frac{2}{\cos(\theta_0)} \end{aligned}$$

— Soit  $\alpha > 0$  suffisamment petit pour que  $\alpha \sum_{n=0}^N |R_n| < \epsilon$ . Si  $z \in \Delta_{\theta_0}$  tel que  $|z - 1| \leq \alpha$ , alors on peut majorer le premier terme de (\*\*):

$$|z - 1| \left( \sum_{n=0}^N |R_n| \right) \leq \alpha \left( \sum_{n=0}^N |R_n| \right) < \epsilon$$

Donc, en faisant  $z \rightarrow 1$  tel que  $z \in \Delta_{\theta_0}$  (on aura bien  $\rho = |z - 1| \leq \inf\{\alpha, \cos(\theta_0)\}$ ), et en injectant les deux majorations trouvées dans (\*\*):

$$|f(z) - S| \leq \epsilon + \epsilon \frac{2}{\cos(\theta_0)} = \epsilon \left( 1 + \frac{2}{\cos(\theta_0)} \right)$$

d'où le résultat. □

### Application 2.

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} = \frac{\pi}{4}$$



*Démonstration.* En appliquant le Théorème 1 :

$$\begin{aligned}
 \sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} &= \lim_{\substack{x \rightarrow 1 \\ x < 1}} \sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} x^n \\
 &\stackrel{x \geq 0}{=} \lim_{\substack{x \rightarrow 1 \\ x < 1}} \frac{1}{\sqrt{x}} \sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)} \sqrt{x}^{2n+1} \\
 &= \lim_{\substack{x \rightarrow 1 \\ x < 1}} \frac{1}{\sqrt{x}} \arctan(\sqrt{x}) \\
 &= \arctan(1) \\
 &= \frac{\pi}{4}
 \end{aligned}$$

□

La preuve de l'application précédente écrite dans [GOU20] est un peu lacunaire. Merci aux personnes qui l'ont signalée et corrigée.

### Application 3.

$$\sum_{n=0}^{+\infty} \frac{(-1)^{n-1}}{n} = \ln(2)$$

*Démonstration.* Toujours en appliquant le Théorème 1 :

$$\begin{aligned}
 \sum_{n=0}^{+\infty} \frac{(-1)^{n-1}}{n} &= \lim_{\substack{x \rightarrow 1 \\ x < 1}} \sum_{n=0}^{+\infty} \frac{(-1)^{n-1}}{n} x^n \\
 &= \lim_{\substack{x \rightarrow 1 \\ x < 1}} \ln(1+x) \\
 &= \ln(2)
 \end{aligned}$$

□

## 28 Théorème de Cauchy-Lipschitz linéaire

*En construisant un raisonnement autour du théorème du point fixe de Banach, on montre le théorème de Cauchy-Lipschitz, qui garantit l'existence d'une solution répondant à une condition initiale et l'unicité d'une solution maximale.*

Soit  $\mathbb{K} = \mathbb{R}$  ou  $\mathbb{C}$ .

**Lemme 1.** Soit  $I$  un intervalle compact. L'espace  $(\mathcal{C}(I, \mathbb{K}^d), \|\cdot\|_\infty)$  est complet.

*Démonstration.* Soit  $(f_n)$  une suite de Cauchy de  $(\mathcal{C}(I, \mathbb{K}^d), \|\cdot\|_\infty)$ . Soit  $x \in I$ , on a

$$\forall p, q \in \mathbb{N}, |f_p(x) - f_q(x)| \leq \|f_p - f_q\|_\infty$$

donc  $(f_n(x))$  est de Cauchy dans  $\mathbb{K}$ . Comme  $\mathbb{K}$  est complet, la suite  $(f_n(x))$  converge vers une limite notée  $f(x)$ . Ainsi, la suite de fonctions  $(f_n)$  converge simplement vers la fonction  $f : I \rightarrow \mathbb{K}$  nouvellement définie. Il reste à montrer que la fonction  $f$  est continue.

Notons déjà que  $(f_n)$  est de Cauchy, et est en particulier bornée :

$$\exists M \geq 0 \text{ tel que } \|f_n\|_\infty \leq M$$

donc en particulier, si  $x \in I$ ,  $|f_n(x)| \leq M$ . Par passage à la limite, on obtient  $|f(x)| \leq M$ . Donc  $f$  est bornée et écrire  $\|f\|_\infty$  a bien du sens.

Soit  $\epsilon > 0$ . Par définition,

$$\exists N \in \mathbb{N} \text{ tel que } \forall p, q \geq N, \|f_p - f_q\|_\infty < \epsilon$$

Donc,

$$\forall x \in I, \forall p, q \geq N, |f_p(x) - f_q(x)| \leq \|f_p - f_q\|_\infty < \epsilon$$

En faisant tendre  $p$  vers l'infini, on obtient :

$$\forall x \in I, \forall q \geq N, |f(x) - f_q(x)| < \epsilon$$

Nous venons d'écrire exactement la définition de la convergence uniforme ! Ainsi,  $(f_n)$  est une suite de fonctions continues qui converge uniformément vers  $f$ , donc  $f$  est continue.  $\square$

**Théorème 2** (Cauchy-Lipschitz linéaire). Soient  $A : I \rightarrow \mathcal{M}_d(\mathbb{K})$  et  $B : I \rightarrow \mathbb{K}^d$  deux fonctions continues. Alors  $\forall t_0 \in I$ , le problème de Cauchy

$$\begin{cases} Y' = A(t)Y + B(t) \\ Y(t_0) = y_0 \end{cases} \quad (C)$$

admet une unique solution définie sur  $I$  tout entier.

*Démonstration.* Commençons par supposer l'intervalle  $I$  compact. On va montrer l'existence d'une solution globale. On écrit l'équation sous forme intégrale :

$$Y \in \mathcal{C}^1 \text{ vérifie (C)} \iff Y(t) = y_0 + \int_{t_0}^t A(u)Y(u) + B(u) du \quad (*)$$

et on introduit la suite de fonctions  $(Y_n)$  définie par récurrence sur  $I$  par  $Y_0 = y_0$  et :

$$\forall n \in \mathbb{N}^*, Y_{n+1}(t) = y_0 + \int_{t_0}^t A(u)Y_n(u) + B(u) du \quad (**)$$

Notons  $\alpha = \sup_{t \in I} \|A(t)\|$  et  $\beta = \sup_{t \in I} \|B(t)\|$ . Montrons par récurrence que pour tout  $n \geq 1$  et tout  $t \in I$  :

$$\|Y_n(t) - Y_{n-1}(t)\| \leq (\alpha \|y_0\| + \beta) \frac{\alpha^{n-1} |t - t_0|^n}{n!}$$

Le résultat est clairement vrai pour  $n = 1$ , supposons donc le vrai à rang  $n \geq 1$ . Pour  $t \geq t_0$  :

$$\begin{aligned} \|Y_{n+1}(t) - Y_n(t)\| &= \left\| \int_{t_0}^t A(u) \times (Y_n(u) - Y_{n-1}(u)) du \right\| \\ &\leq \alpha \int_{t_0}^t (\alpha \|y_0\| + \beta) \frac{\alpha^{n-1} |u - t_0|^n}{n!} du \\ &\leq (\alpha \|y_0\| + \beta) \frac{\alpha^n |t - t_0|^{n+1}}{(n+1)!} \end{aligned}$$

et on procède de même pour  $t \leq t_0$ , ce qui achève la récurrence.

Soit  $L$  la longueur de  $I$ . On obtient donc :

$$\forall n \in \mathbb{N}^*, \|Y_n - Y_{n-1}\|_\infty \leq (\alpha \|y_0\| + \beta) \frac{\alpha^{n-1}}{n!} L^n$$

Il en résulte que la série de fonction  $\sum (Y_n - Y_{n-1})$  est normalement convergente. Comme  $(\mathcal{C}(I, \mathbb{K}^d), \|\cdot\|_\infty)$  est complet, la série est uniformément convergente. On a donc l'existence d'une fonction  $Y \in \mathcal{C}(I, \mathbb{K}^d)$  telle que

$$\left\| \sum_{n=1}^N (Y_n - Y_{n-1}) - Y \right\|_\infty = \|Y_N - (Y + Y_0)\|_\infty \longrightarrow 0$$

ie.  $(Y_n)$  converge vers  $Y + Y_0 = Y + y_0 = Z$ . Par convergence uniforme sur un intervalle compact, il est possible de passer à la limite dans  $(**)$ . D'où :

$$\forall t \in I, Z(t) = y_0 + \int_{t_0}^t A(u)Z(u) + B(u) du$$

et comme  $Z$  est continue, elle est  $\mathcal{C}^1$  et vérifie donc bien  $(*)$ .

On peut maintenant montrer l'unicité. Soient  $Y$  et  $Z$  deux solutions de  $(C)$  sur  $I$ . Par récurrence sur l'entier  $n$ , on montre comme ci-dessus que pour tout  $t \in I$  :

$$\|Y(t) - Z(t)\| \leq \frac{\alpha^n |t - t_0|^n}{n!} \|Y - Z\|_\infty \longrightarrow 0$$

donc  $Y$  et  $Z$  coïncident bien sur  $I$ .

Supposons maintenant  $I$  quelconque. Il existe donc  $(K_n)$  une suite croissante d'intervalles compacts telle que  $I = \bigcup_{n=0}^{+\infty} K_n$ . En particulier, on définit bien l'application

$$\theta: \begin{array}{lcl} I & \rightarrow & \mathbb{K}^d \\ t & \mapsto & Y_n(t) \end{array}$$

(où  $Y_n$  est la solution de (C) sur  $K_n \ni t$ ). En particulier,  $\theta$  est dérivable sur  $I$  tout entier, vérifie (C), et prolonge toute solution.  $\square$

La preuve, telle qu'elle est écrite ici, est en grande partie issue d'un livre d'Alain Pommellet. Elle est également disponible (sous une forme un peu différente) comme l'indique la référence, dans [DAN]. Selon la leçon, on pourra préférer le théorème suivant (dont la démonstration utilise des arguments semblables).

**Théorème 3** (Cauchy-Lipschitz local). Soient  $I$  un intervalle de  $\mathbb{R}$  et  $\Omega$  un ouvert de  $E$ . Soit  $F : I \times \Omega \rightarrow E$  une fonction continue et localement lipschitzienne en la seconde variable. Alors, pour tout  $(t_0, y_0) \in I \times \Omega$ , le problème de Cauchy

$$\begin{cases} y' = F(t, y) \\ y(t_0) = y_0 \end{cases} \quad (C)$$

admet une unique solution maximale.

[GOU20]  
p. 374

*Démonstration.* Nous commençons par montrer l'existence en 4 étapes.

- Localisation : Fixons un réel  $r > 0$  tel que le produit  $P = [t_0 - r, t_0 + r] \times \overline{B}(y_0, r)$  soit contenu dans  $I \times \Omega$ .  $F$  est continue sur  $P$  qui est compact, donc est bornée par  $M$  sur  $P$ .
- Mise sous forme intégrale : Comme une solution de  $y' = F(t, y)$  est de ce fait  $\mathcal{C}^1$ , on a

$$y \in \mathcal{C}^1 \text{ vérifie (C)} \iff y(t) = y_0 + \int_{t_0}^t F(u, y(u)) du \quad (*)$$

- Choix d'un domaine stable : Soit  $\alpha \in ]0, r[$ . Introduisons l'intervalle  $I_\alpha = [t_0 - \alpha, t_0 + \alpha]$ , l'espace  $A_\alpha = \mathcal{C}(I_\alpha, \overline{B}(y_0, r))$ , puis l'application

$$\Psi: \begin{array}{lcl} A_\alpha & \rightarrow & \mathcal{C}(I_\alpha, E) \\ \varphi & \mapsto & \left( t \mapsto y_0 + \int_{t_0}^t F(u, \varphi(u)) du \right) \end{array}$$

Le problème est ici de rendre  $A_\alpha$  stable par  $\Psi$ . Pour tout  $t \in I_\alpha$ ,

$$\begin{aligned} \|F(t, \varphi(t))\| &\leq M \\ \implies \|\Psi(\varphi)(t) - y_0\| &\leq M|t - t_0| \leq \alpha M \end{aligned}$$

Par suite, en choisissant  $\alpha M < r$ , le domaine  $A_\alpha$  est stable par  $\Psi$ .

- Détermination d'un domaine de contraction : Ici,  $A_\alpha$  est normé par la norme  $\|\cdot\|_\infty$ , et on veut faire de  $\Psi$  une contraction stricte. Soient  $\varphi, \phi \in A_\alpha$ , par définition, pour tout  $t \in I_\alpha$ ,

$$\begin{aligned} \|(\Psi(\varphi) - \Psi(\phi))(t)\| &= \left\| \int_{t_0}^t (F(u, \varphi(u)) - F(u, \phi(u))) \, du \right\| \\ &\leq k|t - t_0| \|\varphi - \phi\|_\infty \\ &\leq k\alpha \|\varphi - \phi\|_\infty \end{aligned}$$

où  $k$  désigne le rapport de lipschitzianité de  $F$ . On choisit désormais  $\alpha$  tel que  $k\alpha < 1$  et  $\alpha M < r$ .

- Conclusion : L'application  $\Psi$  est, par choix de  $\alpha$ , une contraction stricte de  $(A_\alpha, \|\cdot\|_\infty)$  dans lui-même. Le fermé  $\overline{B}(y_0, r)$  de l'espace de Banach de  $E$  est complet, par suite  $(A_\alpha, \|\cdot\|_\infty)$  l'est aussi.

Par le théorème du point fixe de Banach,  $\Psi$  possède donc un point fixe  $\varphi$  dans  $A_\alpha$ .  $\varphi$  est alors de classe  $\mathcal{C}^1$  et vérifie (C) par (\*).

Il reste maintenant à montrer l'unicité. On note  $\mathcal{S}$  l'ensemble des solutions de (C).  $\mathcal{S} \neq \emptyset$ , donc peut définir  $J$  comme la réunion des intervalles de définition des solutions de (C).

Soient  $\varphi, \phi \in \mathcal{S}$  (on note  $K$  et  $L$  leur intervalle de définition). Une récurrence sur  $n$  donne

$$\begin{aligned} \forall t \in K \cap L, \forall n \in \mathbb{N}, \|\varphi(t) - \phi(t)\| &\leq \left| \int_{t_0}^t \|F(u, \varphi(u)) - F(u, \phi(u))\| \, du \right| \\ &\leq \frac{|t - t_0|^n}{n!} k^n \sup_{t \in K \cap L} |\varphi(t) - \phi(t)| \\ &\longrightarrow 0 \end{aligned}$$

Donc  $\varphi$  et  $\phi$  coïncident sur  $K \cap L$ .

Ainsi, on définit correctement l'application

$$\theta: \begin{array}{lcl} J & \rightarrow & E \\ t & \mapsto & \phi(t) \end{array}$$

(où  $\phi \in \mathcal{S}$  tel que  $t$  est dans son intervalle de définition). Si  $t \in J$ , il existe  $\phi \in \mathcal{S}$  tel que  $t$  soit dans son intervalle de définition  $K$ . Comme  $\phi$  et  $\theta$  coïncident sur  $K$ ,  $\theta$  est dérivable sur  $K$  et

$$\forall t \in K, \theta'(t) = \phi'(t) = F(t, \phi(t)) = F(t, \theta(t))$$

Et comme  $\theta(t_0) = y_0$ ,  $\theta \in \mathcal{S}$  et prolonge toute solution. Donc  $\theta$  est maximale et est bien unique.  $\square$

## 29 Théorème de Dirichlet faible

En raisonnant par l'absurde et en utilisant certaines propriétés des polynômes cyclotomiques, on démontre que l'ensemble des premiers congrus à 1 modulo un certain entier  $n$  est infini.

**Lemme 1.** Soient  $a \in \mathbb{N}$  et  $p$  premier tels que  $p \mid \Phi_n(a)$  mais  $p \nmid \Phi_d(a)$  pour tout diviseur strict  $d$  de  $n$ . Alors  $p \equiv 1 \pmod n$  ou  $p \mid n$ .

[GOU21]  
p. 99

*Démonstration.* On a,

$$X^n - 1 = \prod_{d \mid n} \Phi_d = \Phi_n \underbrace{\prod_{d \mid n} \Phi_d}_{=F}$$

Comme  $F \in \mathbb{Z}[X]$ , en évaluant en  $a$  :

$$a^n - 1 = \Phi_n(a)F(a) \implies p \mid a^n - 1 \text{ car } F(a) \in \mathbb{Z}$$

Autrement dit,  $a^n \equiv 1 \pmod p$ . En notant  $m$  l'ordre de  $\bar{a}$  dans  $(\mathbb{Z}/p\mathbb{Z})^*$ , on a  $a^m \equiv 1 \pmod p$ . D'où  $m \mid n$ . Ainsi :

- Si  $m = n$ , alors  $\bar{a}$  est d'ordre  $n$ . Donc par le théorème de Lagrange,  $n \mid |(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$  ie.  $p \equiv 1 \pmod n$ .
- Sinon,  $m < n$ . Comme  $m \mid n$ ,

$$X^n - 1 = \prod_{d \mid n} \Phi_d = \Phi_n \left( \prod_{d \mid m} \Phi_d \right) \left( \prod_{\substack{d \mid n \\ d \nmid m}} \Phi_d \right) = \Phi_n(X^m - 1) \left( \prod_{\substack{d \mid n \\ d \nmid m}} \Phi_d \right)$$

Mais,  $\bar{a}$  est racine de  $\overline{\Phi_n}$  et  $X^m - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$ . En particulier,  $\bar{a}$  est (au moins) racine double de  $X^n - 1$ . On peut donc écrire,

$$X^n - 1 \equiv (X - a)^2 G(X) \pmod p$$

Avec  $X = Y + a$ , cela donne :

$$(Y + a)^n - 1 \equiv Y^2 G(Y + a) \pmod p$$

Le polynôme de droite est de degré  $\geq 2$ , donc  $p$  divise les coefficients des termes de degré 0 et 1 de  $(Y + a)^n - 1$ , ie.

$$p \mid a^n - 1 \text{ et } p \mid \binom{n}{1} a^{n-1} = n a^{n-1}$$

De la première égalité, on en tire  $p \nmid a$ . Ainsi,  $a$  est premier avec  $p$  (c'est donc également vrai pour  $a^{n-1}$ ). Finalement, on tire de la deuxième égalité que  $p \mid n$ .

□

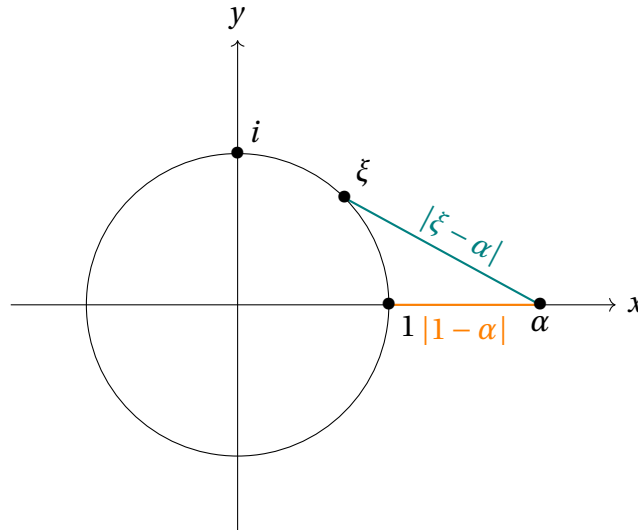
**Théorème 2** (Dirichlet faible). Pour tout entier  $n$ , il existe une infinité de nombres premiers congrus à 1 modulo  $n$ .

*Démonstration.* On suppose par l'absurde qu'il n'existe qu'un nombre fini de premiers de la forme  $1 + kn$ , que l'on note  $p_1, \dots, p_m$ . On considère  $N = \Phi_n(\alpha)$  où  $\alpha = np_1 \dots p_m$ . On remarque en particulier que  $N \equiv a_0 \pmod{\alpha}$ , où  $a_0$  est le coefficient constant de  $\Phi_n$  (cela se voit en écrivant  $\Phi_n = \sum_{k=0}^{\varphi(n)} a_k X^k$ , ce qui donne  $N = a_0 + \alpha \sum_{k=1}^{\varphi(n)} a_k \alpha^{k-1}$  une fois évalué en  $\alpha$ ).

Or,  $X^n - 1 = \prod_{d|n} \Phi_d$ . En évaluant en 0, on en tire :

$$-1 = \prod_{d|n} \Phi_d(0) \implies \pm 1 = a_0, \text{ car } \forall d | n, \Phi_d \in \mathbb{Z}[X]$$

Ainsi,  $N \equiv \pm 1 \pmod{\alpha}$ . Or  $|N| = |\Phi_n(\alpha)| = \prod_{\xi \in \pi_n^*} |\alpha - \xi| > 1$ . On peut en effet interpréter  $|\alpha - \xi|$  comme la distance du complexe  $\alpha$  au complexe  $\xi$  ; le premier est sur l'axe réel et est supérieur ou égal à 2, le second est sur le cercle unité :



En particulier, il existe  $p$  premier tel que  $p \mid N$ . Par le Théorème 1 :

- Ou bien  $p \mid n$ , dans ce cas  $p \mid \alpha = np_1 \dots p_m$ .
- Ou bien  $p \equiv 1 \pmod{n}$ , dans ce cas  $p = p_k$  pour un certain  $k \in \llbracket 1, m \rrbracket$ . Et on a encore  $p \mid \alpha$ .

Pour conclure, on écrit  $N = \alpha q \pm 1$  (par division euclidienne), et on a  $p \mid N - \alpha q = \pm 1$  : absurde.  $\square$

Si vous choisissez de présenter ce développement, il faut au moins connaître l'énoncé de la version forte du théorème.

**Théorème 3** (Progression arithmétique de Dirichlet). Pour tout entier  $n$  et pour tout  $m$  premier avec  $n$ , il existe une infinité de nombres premiers congrus à  $m$  modulo  $n$ .

## 30 Théorème de Fejér

Dans ce développement, on montre le théorème de Fejér, qui assure la convergence de la série de Fourier d'une fonction au sens de Cesàro.

**Lemme 1.** Soit  $f : \mathbb{R} \rightarrow \mathbb{C}$  une fonction continue et  $T$ -périodique. Alors  $f$  est uniformément continue sur  $\mathbb{R}$ .

*Démonstration.* Le théorème de Heine implique la continuité uniforme de  $f$  sur  $[-T, 2T]$ , ce qui s'écrit :

$$\forall \epsilon > 0, \exists \eta > 0 \text{ tel que } \forall x, y \in [-T, 2T], |x - y| < \eta \implies |f(x) - f(y)| < \epsilon \quad (*)$$

Soit  $\epsilon > 0$  et soit le  $\eta > 0$  correspondant donné par  $(*)$ , que l'on peut supposer strictement inférieur à  $T$ . Soient  $x, y \in \mathbb{R}$  tels que  $|x - y| < \eta$ . Il existe  $k \in \mathbb{Z}$  tel que  $x' = x + kT \in [0, T]$ . Alors,

$$y' = y + kT \in [x' - \eta, x' + \eta] \subseteq [-T, 2T]$$

Comme  $|x' - y'| < \eta$ , on en déduit

$$|f(x) - f(y)| = |f(x') - f(y')| < \epsilon$$

ce qu'il fallait démontrer. □

**Notation 2.** On note  $\forall n \in \mathbb{Z}$ ,  $e_n : x \mapsto e^{inx}$  et, pour toute fonction  $f$  continue et  $2\pi$ -périodique,  $c_n(f)$  son  $n$ -ième coefficient de Fourier.

[GOU21]  
p. 306

**Théorème 3 (Fejér).** Soit  $f : \mathbb{R} \rightarrow \mathbb{C}$  une fonction continue et  $2\pi$ -périodique. On note pour tout  $n \in \mathbb{N}$ ,  $S_n$  le  $n$ -ième terme de sa série de Fourier et

$$C_n = \frac{1}{n+1} \sum_{k=0}^n S_k$$

la suite des moyennes de Cesàro correspondante. Alors  $(C_n)$  converge uniformément vers  $f$  sur  $\mathbb{R}$ .

*Démonstration.* On commence par noter, pour tout  $n \in \mathbb{N}$ ,  $D_n = \sum_{k=-n}^n e_k$  et  $F_n = \frac{1}{n+1} \sum_{k=0}^n D_k$  les noyaux de Dirichlet et de Fejér. Comme, pour tout  $k \in \mathbb{Z}^*$ ,  $\int_{-\pi}^{\pi} e_n(t) dt = 0$ , on a pour tout  $n \in \mathbb{N}$ ,

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} D_n(t) dt = \frac{1}{2\pi} \int_{-\pi}^{\pi} e_0(t) dt = 1$$

et donc,

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} F_n(t) dt = \frac{1}{n+1} \left( \sum_{k=0}^n \frac{1}{2\pi} \int_{-\pi}^{\pi} D_k(t) dt \right) = 1 \quad (*)$$



Calculons le noyau de Dirichlet. Soit  $x \in \mathbb{R} \setminus 2\pi\mathbb{Z}$ . On a pour tout  $N \in \mathbb{N}$ ,

$$\begin{aligned}
 D_N(x) &= e^{-iNx} \sum_{n=0}^{2N} e^{inx} \\
 &= e^{-iNx} \frac{e^{(2N+1)ix} - 1}{e^{ix} - 1} \\
 &= e^{-iNx} \frac{e^{(2N+1)i\frac{x}{2}} \left( e^{(2N+1)i\frac{x}{2}} - e^{-(2N+1)i\frac{x}{2}} \right)}{e^{i\frac{x}{2}} \left( e^{i\frac{x}{2}} - e^{-i\frac{x}{2}} \right)} \\
 &= \frac{2i \sin\left((N + \frac{1}{2})x\right)}{2i \sin\left(\frac{x}{2}\right)} \\
 &= \frac{\sin\left((N + \frac{1}{2})x\right)}{\sin\left(\frac{x}{2}\right)}
 \end{aligned}$$

D'où, pour tout  $N \in \mathbb{N}^*$  :

$$\begin{aligned}
 NF_{N-1} &= \sum_{n=0}^{N-1} D_n \\
 &= \sum_{n=0}^{N-1} \frac{\sin\left((n + \frac{1}{2})x\right)}{\sin\left(\frac{x}{2}\right)} \\
 &= \frac{1}{\sin\left(\frac{x}{2}\right)} \operatorname{Im} \left( \sum_{n=0}^{N-1} e^{i(n+\frac{1}{2})x} \right) \\
 &= \frac{1}{\sin\left(\frac{x}{2}\right)} \operatorname{Im} \left( e^{\frac{ix}{2}} \frac{e^{iNx} - 1}{e^{ix} - 1} \right) \\
 &= \frac{1}{\sin\left(\frac{x}{2}\right)} \operatorname{Im} \left( e^{\frac{ix}{2}} \frac{e^{\frac{iNx}{2}} 2i \sin\left(\frac{Nx}{2}\right)}{e^{\frac{ix}{2}} 2i \sin\left(\frac{x}{2}\right)} \right) \\
 &= \frac{\sin\left(\frac{Nx}{2}\right)}{\sin\left(\frac{x}{2}\right)^2} \operatorname{Im} \left( e^{\frac{iNx}{2}} \right) \\
 &= \frac{\sin\left(\frac{Nx}{2}\right)^2}{\sin\left(\frac{x}{2}\right)^2} \quad (**)
 \end{aligned}$$

Maintenant, on remarque que pour tout  $n \in \mathbb{N}$  et pour tout  $x \in \mathbb{R}$ ,

$$S_n(x) = \frac{1}{2\pi} \sum_{k=0}^n \left( \int_{-\pi}^{\pi} f(t) e^{-ikt} dt \right) e^{ikx} = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(t) D_n(x-t) dt = f * D_n$$

donc  $C_n = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(t) F_n(x-t) dt = f * F_n = F_n * f$  par commutativité du produit de convolution. Soit  $\epsilon > 0$ . Le Théorème 1 assure l'existence de  $\eta \in ]0, \pi[$  tel que

$$\forall x, y \in \mathbb{R}, |x - y| < \eta \implies |f(x) - f(y)| < \epsilon$$

De plus,  $|f|$  est continue sur tous les compacts de la forme  $[2k\pi, 2(k+1)\pi]$ , on peut donc la

majorer par un réel  $M > 0$ . Alors, pour tout  $x \in \mathbb{R}$ ,

$$\begin{aligned}
 |f(x) - C_n(x)| &= \left| \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x-t) F_n(t) dt - f(x) \times \underbrace{\frac{1}{2\pi} \int_{-\pi}^{\pi} F_n(t) dt}_{=1 \text{ par } (*)} \right| \\
 &= \left| \frac{1}{2\pi} \int_{-\pi}^{\pi} (f(x-t) - f(x)) F_n(t) dt \right| \\
 &\leq \frac{1}{2\pi} \int_{\eta \leq |t| \leq \pi} 2M F_n(t) dt + \frac{1}{2\pi} \int_{-\eta}^{\eta} \epsilon F_n(t) dt \\
 &\leq \frac{2M}{2\pi} \int_{\eta \leq |t| \leq \pi} F_n(t) dt + \epsilon
 \end{aligned}$$

Or,  $(**)$  montre que

$$\forall n \in \mathbb{N}, \forall x \in [-\pi, \pi] \text{ tel que } |x| > \eta, \text{ on a } |F_n(x)| \leq \frac{1}{(n+1) \sin\left(\frac{\eta}{2}\right)^2}$$

donc  $(F_n)$  converge uniformément vers 0 sur  $[-\pi, \pi] \setminus [-\eta, \eta]$ . Il existe ainsi  $N \in \mathbb{N}$  tel que

$$\forall n \geq N, \int_{\eta \leq |t| \leq \pi} F_n(t) dt < \epsilon$$

de sorte que

$$\forall n \geq N, \forall x \in \mathbb{R}, |f(x) - C_n(x)| \leq \left( \frac{M}{\pi} + 1 \right) \epsilon$$

D'où le résultat. □

Je préfère la preuve de **[GOU21]**, qui est plus “clés en main”. Il est possible de passer les calculs des noyaux de Dirichlet et de Fejér dans un premier temps, puis de les montrer à la fin selon le temps restant.

## 31 Théorème de Frobenius-Zolotarev

Nous démontrons le théorème de Frobenius-Zolotarev qui permet de calculer la signature d'un endomorphisme d'un espace vectoriel sur un corps fini possédant au moins 3 éléments.

Soient  $p \geq 3$  un nombre premier et  $V$  un espace vectoriel sur  $\mathbb{F}_p$  de dimension finie.

**Définition 1.** Soit  $H$  un hyperplan de  $V$  et soit  $G$  une droite supplémentaire de  $H$  dans  $V$ . La dilatation  $u$  de base  $H$ , de direction  $G$ , et de rapport  $\lambda \in \mathbb{K}^*$  est l'unique endomorphisme de  $V$  défini par

$$\forall g \in G, \forall h \in H, u(g + h) = h + \lambda g$$

[I-P]  
p. 203

*Remarque 2.* On suppose connu le fait que les transvections et les dilatations engendrent  $GL(V)$ .

[PER]  
p. 99

**Lemme 3.** Soient  $u \in GL(V)$  et  $H$  un hyperplan de  $V$  tel que  $u|_H = \text{id}_H$ . Si  $\det(u) \neq 1$ , alors  $u$  est une dilatation.

p. 96

*Démonstration.* On note  $n = \dim(V)$ . Comme  $u|_H = \text{id}_H$  et  $\dim(H) = n - 1$ , on en déduit que 1 est valeur propre de multiplicité  $n - 1$  de  $u$  et que  $H$  est le sous-espace propre associé :

$$H = E_1(u) = \text{Ker}(u - \text{id}_V)$$

On pose  $\lambda = \det(u) \notin \{0, 1\}$ .  $\lambda$  est valeur propre de  $u$  (on peut le voir par exemple en calculant le polynôme caractéristique de  $u$ ) de multiplicité 1. Donc  $u$  est diagonalisable, et dans une base  $\mathcal{B}$  adaptée à la diagonalisation, on a :

$$\text{Mat}(u, \mathcal{B}) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & \lambda \end{pmatrix}$$

d'où le résultat. □

**Lemme 4.** Les dilatations engendrent  $GL(V)$ .

[I-P]  
p. 203

*Démonstration.* Pour obtenir le résultat, il suffit de montrer que toute transvection est la composée de deux dilatations (cf. Théorème 2). Soit  $u$  une transvection d'hyperplan  $H$ . Comme  $\mathbb{F}_p$  contient au moins 3 éléments, il existe alors  $v$  une dilatation d'hyperplan  $H$  et de rapport  $\lambda \neq 1$ .

Ainsi, l'application  $w = u \circ v$  est dans  $GL(V)$  et fixe  $H$ . Comme  $\det(w) = \det(v) = \lambda \neq 1$ , le Théorème 3 permet de conclure que  $w$  est une dilatation. Ainsi,  $u = w \circ v^{-1}$  est le produit de deux dilatations  $v^{-1}$  est une dilatation (toujours d'après le Théorème 3). □

**Notation 5.** Soit  $a \in \mathbb{F}_p$ . On note  $\left(\frac{a}{p}\right)$  le symbole de Legendre de  $a$  modulo  $p$ .

**Théorème 6** (Frobenius-Zolotarev).

$$\forall u \in \text{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où  $u$  est vu comme une permutation des éléments de  $V$ .

*Démonstration.* Le groupe multiplicatif d'un corps fini est cyclique, donc il existe  $a \in \mathbb{F}_p^*$  tel que

$$\mathbb{F}_p^* = \langle a \rangle$$

En conséquence, si  $u$  est la dilatation de  $V$  de base  $H$ , de direction  $G$ , et de rapport  $\lambda \in \mathbb{F}_p^*$ , alors il existe  $k \in \mathbb{N}^*$  tel que  $\lambda = a^k$ . On en déduit que si  $v$  est la dilatation de  $V$  de base  $H$ , de direction  $G$ , et de rapport  $a$ , alors  $\forall x \in V$  écrit  $x = g + h$  avec  $g \in G$  et  $h \in H$  :

$$v^k(x) = v^k(g + h) = h + a^k g = h + \lambda g = u(g + h) = u(x)$$

d'où  $v^k = u$ . Ainsi, toute dilatation est une puissance d'une dilatation de rapport  $a$ .

Comme  $\det$ ,  $\left(\frac{\cdot}{p}\right)$  et  $\epsilon$  sont tous trois des morphismes de groupes, et comme les dilatations engendrent  $\text{GL}(V)$  (cf. Théorème 4), il suffit de montrer le résultat pour les dilatations de rapport  $a$ .

Soit  $u$  une dilatation de base  $H$ , de direction  $G$ , et de rapport  $a$ . Supposons par l'absurde que  $\left(\frac{\det(u)}{p}\right) = 1$ . Comme  $\det(u) = a$ , on a  $\left(\frac{a}{p}\right) = 1$ . Mais,  $\mathbb{F}_p^* = \langle a \rangle$ , donc  $\forall x \in \mathbb{F}_p^*$ ,  $\left(\frac{x}{p}\right) = 1$  ie. tout élément de  $\mathbb{F}_p^*$  est un carré. Or, il y a  $\frac{p-1}{2}$  carrés dans  $\mathbb{F}_p^*$  (et  $|\mathbb{F}_p^*| = p-1$ , bien-sûr) : contradiction.

Il ne reste qu'à montrer que  $\epsilon(u) = -1$ . Pour cela, on va étudier les orbites des éléments  $V$  sous l'action de  $u$ .

Soit  $h \in H$ . On a  $u(h) = h$ , donc son orbite est réduite à  $\{h\}$  qui est de cardinal 1. Elle compte donc comme un  $+$  dans le signe de  $\epsilon(u)$ .

Soit maintenant  $x \in V$  écrit  $x = g + h$  avec  $g \in G \setminus \{0\}$  et  $h \in H$  de sorte que  $u^k(x) = h + a^k g$  pour tout  $k \in \mathbb{N}$ .

- $\mathbb{F}_p^*$  est cyclique d'ordre  $p-1$ , donc  $a^{p-1} = 1$ . Ainsi,  $u^{p-1}(x) = x$ .
- Supposons par l'absurde que  $\exists 1 \leq i < j \leq p-1$  tel que  $u^i(x) = u^j(x)$ . On a,

$$\begin{aligned} h + a^j g = h + a^i g &\iff a^{j-i}(a^i - 1) \underset{\neq 0}{g} = 0 \\ &\implies a^{j-i} = 0 \text{ ou } a^i = 1 \end{aligned}$$

ce qui est absurde dans les deux cas.

L'orbite de  $x$  sous l'action de  $u$  est donc  $\{x, \dots, u^{p-2}(x)\}$  qui est de cardinal  $p-1$  (pair) et compte donc comme un  $-$  dans le signe de  $\epsilon(u)$ .

Il ne reste qu'à compter le nombre d'orbites de cardinal  $p - 1$ . Les éléments contenus dans ces orbites forment exactement l'ensemble

$$\bigcup_{h \in H} \{g + h \mid g \in G, g \neq 0\}$$

et il y en a donc

$$|H| \times (|G| - 1) = p^{n-1}(p - 1)$$

(car  $H$  est un hyperplan et  $G$  est une droite). Comme ces orbites sont de cardinal  $p - 1$ , il y a donc exactement  $p^{n-1}$  orbites. Or,  $p^{n-1}$  est impair, donc  $\epsilon(u)$  est de signe négatif. Ainsi,  $\epsilon(u) = -1$ .  $\square$

## 32 Théorème de Kronecker

En utilisant les polynômes symétriques, nous montrons ici que toutes les racines d'un polynôme unitaire à coefficients entiers dont les racines sont dans  $D(0, 1) \setminus \{0\}$ , sont en fait des racines de l'unité.

**Lemme 1** (Relations de Viète). Soient  $A$  un anneau commutatif unitaire intègre et  $P = \sum_{i=1}^n a_i X^i \in A[X]$  que l'on suppose scindé dans  $A[X]$  et tel que  $a_n \in A^*$ . Si on note  $\Sigma_k(X_1, \dots, X_n)$  le  $k$ -ième polynôme symétrique élémentaire en  $n$  variables et  $\alpha_1, \dots, \alpha_n$  les racines de  $P$  (comptées avec multiplicité), alors  $\Sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k a_{n-k} a_n^{-1}$ .

*Démonstration.* On a  $P = a_n \prod_{i=1}^n (X - \alpha_i)$ . En développant partiellement  $P$ , on a de même :

$$P = a_n X^n - a_n(\alpha_1 + \dots + \alpha_n) X^{n-1} + \dots + (-1)^n a_n \alpha_1 \dots \alpha_n$$

Par identification avec la forme développée, les coefficients de  $X^{n-1}$  doivent être égaux. En particulier :

$$a_{n-1} = -a_n(\alpha_1 + \dots + \alpha_n) \iff \underbrace{\alpha_1 + \dots + \alpha_n}_{=\Sigma_1(\alpha_1, \dots, \alpha_n)} = -a_{n-1} a_n^{-1}$$

Et on procède de même pour trouver les autres coefficients. Par exemple,  $a_0 = (-1)^n a_n \alpha_1 \dots \alpha_n \iff \Sigma_n(\alpha_1, \dots, \alpha_n) = (-1)^n a_0 a_n^{-1}$ .  $\square$

*Remarque 2.* Tout au long de ce développement, nous utiliserons implicitement le fait que tout polynôme à coefficients dans  $\mathbb{C}$  (donc à fortiori aussi dans  $\mathbb{Z}$ ) admet  $n$  racines complexes comptées avec multiplicité. Il s'agit du théorème de d'Alembert-Gauss.

**Théorème 3** (Kronecker). Soit  $P \in \mathbb{Z}[X]$  unitaire tel que toutes ses racines complexes appartiennent au disque unité épointé en l'origine (que l'on note  $D$ ). Alors toutes ses racines sont des racines de l'unité.

[I-P]  
p. 279

*Démonstration.* Notons par  $\Omega_n$  l'ensemble des polynômes unitaires à coefficients dans  $\mathbb{Z}$  tels que toutes leurs racines complexes appartiennent à  $D$ . Soit  $P \in \Omega_n$  dont on note  $a_0, \dots, a_n$  les coefficients et  $z_1, \dots, z_n$  les racines complexes. On note  $\forall k \in \llbracket 0, n \rrbracket$ ,  $\sigma_k = \Sigma_k(z_1, \dots, z_n)$ . D'après le Théorème 1, on a :

$$\forall k \in \llbracket 0, n \rrbracket, \sigma_k = (-1)^k a_{n-k} \quad (*)$$

D'où  $\forall k \in \llbracket 0, n \rrbracket$  :

$$\begin{aligned} |\sigma_k| &= \left| \sum_{I \in \mathcal{P}_k(\llbracket 1, n \rrbracket)} \prod_{i \in I} z_i \right| \\ &\leq \sum_{I \in \mathcal{P}_k(\llbracket 1, n \rrbracket)} \prod_{i \in I} |z_i| \\ &\leq |\mathcal{P}_k(\llbracket 1, n \rrbracket)| \times 1 \\ &= \binom{n}{k} \end{aligned}$$

Et par (\*),

$$\forall k \in \llbracket 0, n \rrbracket, |a_k| \leq \binom{n}{n-k} = \binom{n}{k}$$

$\Omega_n$  est donc un ensemble fini (car on n'a qu'un nombre limité de choix possibles pour les coefficients  $a_k$ ).

On pose maintenant

$$\forall k \in \mathbb{N}, P_k = \prod_{j=0}^n (X - z_j^k)$$

qui sont des polynômes unitaires de degré  $n$  dont les racines  $z_1^k, \dots, z_n^k$  appartiennent toutes à  $D$ . Soient  $k \in \mathbb{N}$  et  $r \in \llbracket 0, n \rrbracket$ . D'après le Théorème 1, le coefficient de  $X^{n-r}$  de  $P_k$  est  $(-1)^r \Sigma_r(z_1^k, \dots, z_n^k)$ . Mais,  $\Sigma_r(X_1^k, \dots, X_n^k) \in \mathbb{Z}[X]$ , donc on peut y appliquer le théorème fondamental des polynômes symétriques :

$$\exists Q_{r,k} \in \mathbb{Z}[X] \text{ tel que } \Sigma_r(X_1^k, \dots, X_n^k) = Q_{r,k}(\Sigma_1(X_1, \dots, X_n), \dots, \Sigma_n(X_1, \dots, X_n))$$

Or, comme  $P \in \mathbb{Z}[X]$ , on a  $\forall j \in \llbracket 0, n \rrbracket, \Sigma_j(z_1, \dots, z_n) \in \mathbb{Z}$  d'après le Théorème 1. En particulier, on a  $\Sigma_r(X_1^k, \dots, X_n^k) \in \mathbb{Z}[X]$  car  $Q_{r,k} \in \mathbb{Z}[X]$ . On en déduit que  $\forall k \in \mathbb{N}, P_k \in \Omega_n$ .

Comme  $\Omega_n$  est fini, l'ensemble des racines de tous les  $P_k$  ; qui est  $\{z \in \mathbb{C} \mid \exists k \in \mathbb{N}, P_k(z) = 0\}$  est fini. Soit  $j \in \llbracket 1, n \rrbracket$ . L'ensemble  $\{z_j^k \mid k \in \mathbb{N}\}$  est inclus dans l'ensemble de ces racines, qui est fini ; il est donc lui-même fini :

$$\exists k \neq k' \text{ tel que } z_j^k = z_j^{k'}$$

Quitte à échanger les deux, on peut supposer  $k \geq k'$ . Comme  $z_j \neq 0$ , on a  $z_j^{k-k'} = 1$ . Donc  $z_j$  est une racine de l'unité ; ce que l'on voulait.  $\square$

**Corollaire 4.** Soit  $P \in \mathbb{Z}[X]$  unitaire et irréductible sur  $\mathbb{Q}$  tel que toutes ses racines complexes soient de module inférieur ou égal à 1. Alors  $P = X$  ou  $P$  est un polynôme cyclotomique.

*Démonstration.* Si 0 est racine de  $P$ , alors  $X \mid P$ , donc  $P = X$  par irréductibilité et unitarité. Sinon, 0 n'est pas racine de  $P$ . On peut donc appliquer le Théorème 3 à  $P$  ; et donc les racines de  $P$  sont des racines de l'unité. Ainsi, en notant  $N$  le maximum des ordres des racines de  $P$ , on a :

$$P \mid (X^N - 1)^n \text{ où } n = \deg(P)$$

Or, la décomposition en irréductibles de  $X^N - 1$  est

$$X^N - 1 = \prod_{d|N} \Phi_d$$

Puisque  $\mathbb{Q}[X]$  est un anneau factoriel,  $P$  est premier. Donc d'après le lemme de Gauss, comme  $P \mid X^N - 1$  :

$$\exists d \mid N \text{ tel que } P = \Phi_d$$

□



### 33 Premier théorème de Sylow

En procédant par récurrence sur le cardinal du groupe, on montre l'existence d'un sous-groupe de Sylow.

**Théorème 1** (Cauchy “faible”). Soit  $G$  un groupe abélien fini et soit  $p$  un diviseur premier de l'ordre de  $G$ . Alors, il existe un sous-groupe de  $G$  d'ordre  $p$ .

[GOU21]  
p. 44

*Démonstration.*  $G$  est fini, on peut donc l'écrire

$$G = \langle x_1, \dots, x_n \rangle$$

où  $(x_1, \dots, x_n)$  est un système de générateurs de  $G$ . On définit

$$\varphi : \begin{array}{ccc} \langle x_1 \rangle \times \dots \times \langle x_n \rangle & \rightarrow & G \\ (y_1, \dots, y_n) & \mapsto & y_1 \dots y_n \end{array}$$

Comme  $G$  est abélien,  $\varphi$  est clairement un morphisme de groupes. Et comme  $(x_1, \dots, x_n)$  est un système de générateurs de  $G$ ,  $\varphi$  est surjectif. On peut appliquer le premier théorème d'isomorphisme pour obtenir

$$G \cong (\langle x_1 \rangle \times \dots \times \langle x_n \rangle) / \text{Ker}(\varphi)$$

En particulier,  $|G| \times |\text{Ker}(\varphi)| = |\langle x_1 \rangle| \times \dots \times |\langle x_n \rangle|$ . On note, pour tout  $i \in \llbracket 1, n \rrbracket$ ,  $r_i = |\langle x_i \rangle|$ . On a ainsi,

$$G \mid r_1 \dots r_n \implies p \mid r_1 \dots r_n$$

par transitivité de  $\mid$ . Par le lemme d'Euclide, il existe  $i \in \llbracket 1, n \rrbracket$  tel que  $p \mid r_i$ . On écrit  $r_i = pq$  avec  $q \in \mathbb{N}^*$ , et on pose  $x = x_i^q$ . Alors,  $x$  est d'ordre  $p$  et  $H = \langle x \rangle$  est un sous-groupe de  $G$  d'ordre  $p$ .  $\square$

**Théorème 2** (Premier théorème de Sylow). Soit  $G$  un groupe fini d'ordre  $np^\alpha$  avec  $n, \alpha \in \mathbb{N}$  et  $p$  premier tel que  $p \nmid n$ . Alors, il existe un sous-groupe de  $G$  d'ordre  $p^\alpha$ .

*Démonstration.* Posons  $h = |G|$ . On va procéder par récurrence forte sur  $h$ .

- Si  $h = 1$  : Alors,  $n = 1$  et  $\alpha = 0$ . La propriété est donc triviale.
- On suppose la propriété vraie pour les groupes d'ordre strictement inférieur à  $h$ . Si  $\alpha = 0$ , c'est encore une fois trivial, pour les mêmes raisons qu'à l'initialisation de la propriété. Supposons donc  $\alpha \geq 1$ . On fait agir  $G$  sur lui-même par conjugaison, via l'action :

$$(g, h) \mapsto ghg^{-1}$$

Soit  $\Omega$  un système de représentants associé à la relation “être dans la même orbite”. La formule des classes donne

$$|G| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \text{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\text{Stab}_G(\omega)|} \quad (*)$$

Mais,

$$\text{Stab}_G(\omega) = G \iff \forall g \in G, g\omega g^{-1} = \omega \iff \omega \in Z(G)$$

donc, en regroupant, on peut réécrire (\*) :

$$\begin{aligned} |G| &= \sum_{\omega \in \Omega} \frac{|G|}{|\text{Stab}_G(\omega)|} \\ &= \sum_{\omega \in Z(G)} \frac{|G|}{|\text{Stab}_G(\omega)|} + \sum_{\omega \notin Z(G)} \frac{|G|}{|\text{Stab}_G(\omega)|} \\ &= |Z(G)| + \sum_{\omega \notin Z(G)} \frac{|G|}{|\text{Stab}_G(\omega)|} \end{aligned} \quad (**)$$

On a maintenant deux cas :

- Il existe  $\omega$  tel que  $p^\alpha \mid |\text{Stab}_G(\omega)|$  : Alors, comme  $\text{Stab}_G(\omega)$  est un sous-groupe de  $G$  d'ordre divisant strictement celui de  $G$ , on peut y appliquer l'hypothèse de récurrence pour obtenir un sous-groupe d'ordre  $p^\alpha$ . Ce sous-groupe est donc également un sous-groupe de  $G$ .
- Pour tout  $\omega$ ,  $p^\alpha \nmid |\text{Stab}_G(\omega)|$  : Alors, en factorisant par  $p$  dans les termes de la somme de (\*\*), on constate que  $p \mid \frac{|G|}{|\text{Stab}_G(\omega)|}$  pour tout  $\omega \notin Z(G)$ . Comme  $p \mid h$ , toujours d'après (\*\*), on a

$$p \mid |Z(G)|$$

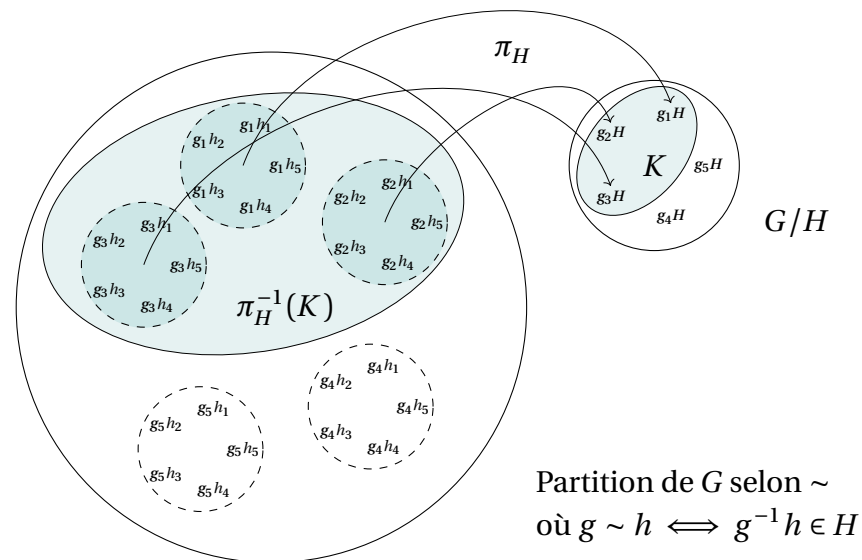
$Z(G)$  étant commutatif, on peut appliquer le Théorème 1. On obtient l'existence d'un sous-groupe  $H$  de  $Z(G)$  d'ordre  $p$ , qui est de plus distingué dans  $G$  car inclus dans  $Z(G)$ . Alors,

$$|G/H| = \frac{|G|}{|H|} = np^{\alpha-1}$$

Il suffit maintenant d'appliquer l'hypothèse de récurrence à  $G/H$ , qui donne l'existence d'un sous-groupe  $K$  de  $G/H$  d'ordre  $p^{\alpha-1}$ . On considère la surjection canonique

$$\pi_H : G \rightarrow G/H$$

Alors,  $\pi_H^{-1}(K) = \{g \in G \mid gH \in K\}$  est un sous-groupe de  $G$  d'ordre  $|K| \times |H| = p^\alpha$  :



ce qu'on voulait.

□

## 34 Théorème de Wantzel

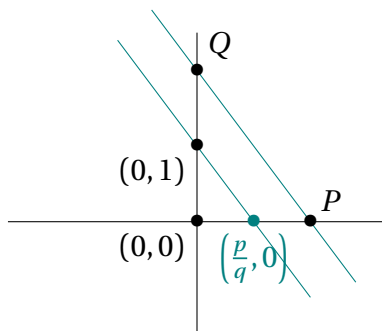
*Une application sympathique de la théorie des corps en géométrie. Les arguments sont assez simples et donnent lieu à de jolies applications.*

**Notation 1.** On note  $\mathbb{E}$  l'ensemble des nombres constructibles. Tout au long du développement, on se permettra de confondre points et coordonnées.

**Lemme 2.**  $\mathbb{E}$  contient le corps  $\mathbb{Q}$ .

[GOZ]  
p. 49

*Démonstration.* Tout élément  $z \in \mathbb{Z}$  est constructible. Soit  $(p, q) \in \mathbb{Z}^* \times \mathbb{N}^*$ . Les points  $P = (p, 0)$  et  $Q = (0, q)$  sont constructibles. On considère la droite  $(d)$ , parallèle à  $(PQ)$  passant par  $(0, 1)$ . Cette droite est constructible, et son point d'intersection avec la droite passant par les points  $(0, 0)$  et  $(1, 0)$  est  $(\frac{p}{q}, 0)$  par le théorème de Thalès.

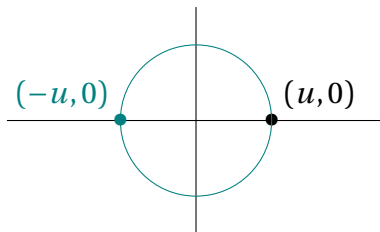


Donc  $\frac{p}{q} \in \mathbb{E}$ . Comme  $0 \in \mathbb{E}$ , on a bien  $\mathbb{Q} \subseteq \mathbb{E}$ . □

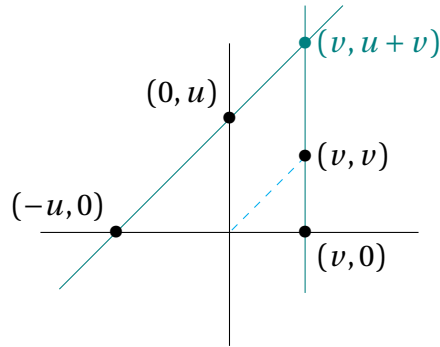
**Lemme 3.**  $\mathbb{E}$  est un sous-corps de  $\mathbb{R}$  stable par racine carrée.

*Démonstration.* Soient  $u, v \in \mathbb{E}$ . Commençons par montrer que  $\mathbb{E}$  est un sous-corps de  $\mathbb{R}$ .

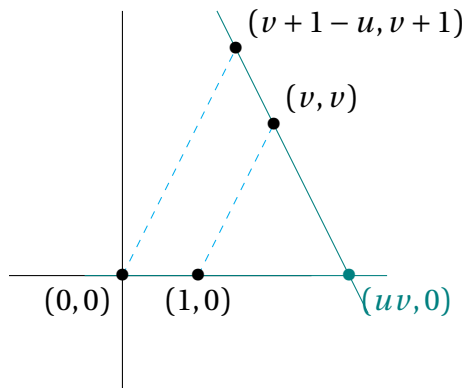
— Le point  $(u, 0)$  est constructible donc son symétrique  $(-u, 0)$  l'est aussi. Donc  $-u \in \mathbb{E}$ .



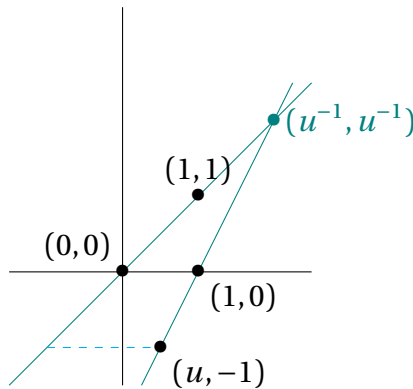
— La droite passant par les points  $(0, u)$  et  $(-u, 0)$  et la droite passant par les points  $(v, 0)$  et  $(v, v)$  ont pour point d'intersection  $(v, u + v)$  (par le théorème de Thalès). Donc  $u + v \in \mathbb{E}$ .



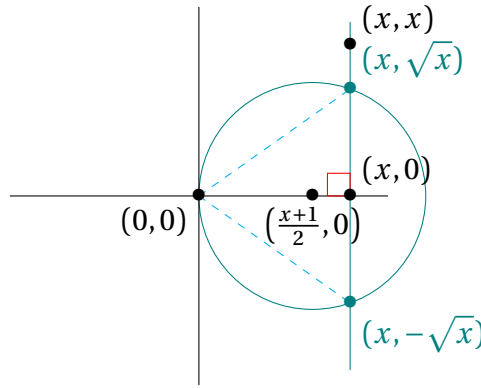
- D'après ce qui précède,  $v+1$  et  $v+1-u$  appartiennent à  $\mathbb{E}$ . La droite passant par les points  $(v+1-u, v+1)$  et  $(u, v)$  et la droite passant par les points  $(0,0)$  et  $(1,0)$  ont pour point d'intersection  $(uv, 0)$  (par le théorème de Thalès). Donc  $uv \in \mathbb{E}$ .



- On suppose  $u \neq 0$ . La droite passant par les points  $(1,0)$  et  $(u, -1)$  et la droite passant par les points  $(0,0)$  et  $(1,1)$  ont pour point d'intersection  $(u^{-1}, u^{-1})$  (par le théorème de Thalès). Donc  $u^{-1} \in \mathbb{E}$ .



Ainsi,  $\mathbb{E}$  est un sous-corps de  $\mathbb{R}$ , qui contient  $\mathbb{Q}$  par le Théorème 2. Maintenant, soit  $x \in \mathbb{E}$  avec  $x > 0$ . Comme  $\mathbb{E}$  est un sous-corps de  $\mathbb{R}$ , on a  $\frac{x+1}{2} \in \mathbb{E}$ . Le cercle de centre  $(\frac{x+1}{2}, 0)$  passant par  $(0,0)$  et la droite passant par les points  $(x, 0)$  et  $(x, x)$  ont pour point d'intersection  $(x, \sqrt{x})$  et  $(x, -\sqrt{x})$  par le théorème de Pythagore. Donc  $\sqrt{x} \in \mathbb{E}$ .



□

**Théorème 4** (Wantzel). Soit  $\alpha \in \mathbb{R}$ . Alors,  $\alpha \in \mathbb{E}$  si et seulement s'il existe une suite finie  $(L_0, \dots, L_p)$  de sous-corps de  $\mathbb{R}$  vérifiant :

- (i)  $L_0 = \mathbb{Q}$ .
- (ii)  $\forall i \in \llbracket 0, p-1 \rrbracket$ ,  $L_{i+1}$  est une extension quadratique (de degré 2) de  $L_i$ .
- (iii)  $\alpha \in L_p$ .

*Démonstration.* On suppose  $\alpha$  constructible. Alors, il existe un point  $M$  tel que  $\alpha$  est l'abscisse de  $M$ .  $M$  s'obtient à l'aide d'un nombre fini de constructions de points  $M_1, \dots, M_m$ . Pour tout  $i \in \llbracket 1, m \rrbracket$ , on note  $(x_i, y_i)$  les coordonnées de  $M_i$ . De ce fait, on a une tour d'extension

[ULM18]  
p. 103

$$\underbrace{K_0}_{=\mathbb{Q}} \subseteq K_1 \subseteq \dots \subseteq K_m$$

avec  $\alpha \in K_m$  et pour tout  $0 \in \llbracket 1, m-1 \rrbracket$ ,  $K_{i+1} = K_i(x_i, y_i)$ . Soit  $i \in \llbracket 1, m-1 \rrbracket$ . Montrons que  $[K_{i+1} : K_i] \leq 2$ . On a différents cas possibles :

- $M_i$  est l'intersection de deux droites passant par des nombres constructibles de  $K_i$ . Alors, les coordonnées  $(x_i, y_i)$  de  $M_i$  sont solution d'un système d'équations de la forme

$$\begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases}$$

avec  $a, b, c, a', b', c' \in K_i$  par construction. Donc,  $x_i, y_i \in K_i$  et ainsi,  $[K_{i+1} : K_i] = 1$ .

- $M_i$  est l'intersection d'une droite et d'un cercle passant par des points dont les coordonnées sont des nombres constructibles de  $K_i$  et de rayon un nombre constructible de  $K_i$ . Alors, les coordonnées  $(x_i, y_i)$  de  $M_i$  sont solution d'un système d'équations de la forme

$$\begin{cases} ax + by = c \\ (x - a')^2 + (y - b')^2 = c' \end{cases}$$

avec  $a, b, c, a', b', c' \in K_i$  par construction. Raisonnons selon la nullité de  $a$ .

— Si  $a \neq 0$ , la première équation donne

$$x = -\frac{by + c}{a}$$

et en réinjectant dans la deuxième équation, on obtient que  $y_i$  est racine d'un polynôme de degré 2. Ainsi,  $[K_i(y_i) : K_i] \leq 2$ . Puisque  $x_i = -\frac{by_i + c}{a} \in K_i(y_i)$ , on a bien  $[K_{i+1} : K_i] \leq 2$ .

— Si  $a = 0$ , alors  $y_i = \frac{c}{b} \in K_i$  (on ne peut pas avoir  $b = 0$  dans ce cas). Or, cette fois-ci c'est  $x_i$  qui est racine d'un polynôme de degré 2. On peut conclure de la même manière que ci-dessus.

—  $M_i$  est l'intersection de deux cercles passant par des points dont les coordonnées sont des nombres constructibles de  $K_i$  et de rayon un nombre constructible de  $K_i$ . Alors, les coordonnées  $(x_i, y_i)$  de  $M_i$  sont solution d'un système d'équations de la forme

$$\begin{cases} (x - a)^2 + (y - b)^2 = c \\ (x - a')^2 + (y - b')^2 = c' \end{cases}$$

avec  $a, b, c, a', b', c' \in K_i$  par construction. On soustrait la deuxième équation à la première, pour obtenir le système équivalent :

$$\begin{cases} -2(a - a')x - 2(b - b')y = c - c' - (a^2 - a'^2) - (b^2 - b'^2) \\ (x - a')^2 + (y - b')^2 = c' \end{cases}$$

ce qui nous ramène au cas précédent.

Il suffit alors d'extraire de la suite  $(K_0, \dots, K_m)$  une sous-suite  $(L_0, \dots, L_p)$  strictement croissante (au sens de l'inclusion) en ne conservant dans la suite initiale que les corps extension quadratique du précédent (avec  $L_0 = K_0$  et  $L_p = K_n$ ). On obtient une suite de sous-corps de  $\mathbb{R}$  (par le Théorème 3) qui remplit les trois conditions annoncées.

Réciproquement, supposons l'existence d'une suite  $(L_0, \dots, L_p)$  de sous-corps de  $\mathbb{R}$  répondant aux trois conditions de l'énoncé. Montrons par récurrence que

$$\forall j \in \llbracket 0, p \rrbracket, L_j \subseteq \mathbb{E}$$

— Initialisation :  $L_0 = \mathbb{Q}$  : cela résulte du Théorème 2.

— Hérédité : Supposons  $L_j \subseteq \mathbb{E}$  pour  $j \in \llbracket 0, p-1 \rrbracket$ . Soit  $x \in L_{j+1}$ . Comme, par hypothèse,

$$[L_{j+1} : L_j] = 2$$

la famille  $(1, x, x^2)$  est  $L_j$ -liée :

$$\exists a, b, c \in L_j \text{ non tous nuls tels que } ax^2 + bx + c = 0$$

— Si  $a = 0$ , alors,  $x = -\frac{c}{b} \in L_j$ . Donc  $x \in \mathbb{E}$ .

— Si  $a \neq 0$ , alors,  $x = \frac{1}{2a}(-b \pm \sqrt{b^2 - 4ac})$ . Donc, comme  $\mathbb{E}$  est un sous-corps de  $\mathbb{R}$  stable par racine carrée (cf. Théorème 3),  $x \in \mathbb{E}$ .

Ainsi,  $L_{j+1} \subseteq \mathbb{E}$ . En conclusion,  $L_p \subseteq \mathbb{E}$ , donc  $\alpha$  est constructible. □

La réciproque et la conclusion du sens direct du théorème sont mieux rédigées dans [GOZ], à mon avis.

**Corollaire 5.** Si  $\alpha \in \mathbb{R}$  est constructible, il existe  $e \in \mathbb{N}$  tel  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^e$ .

[GOZ]  
p. 52

*Démonstration.* Soit  $\alpha \in \mathbb{E}$ . D'après le théorème précédent, il existe une suite finie  $(L_0, \dots, L_p)$  de sous-corps de  $\mathbb{R}$  vérifiant :

- (i)  $L_0 = \mathbb{Q}$ .
- (ii)  $\forall i \in \llbracket 0, p-1 \rrbracket$ ,  $L_{i+1}$  est une extension quadratique (de degré 2) de  $L_i$ .
- (iii)  $\alpha \in L_p$ .

Par le théorème de la base télescopique,

$$[L_p : \mathbb{Q}] = 2^p$$

et par ce même théorème,

$$[L_p : \mathbb{Q}] = [L_p : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

et en particulier,  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  est un diviseur de  $2^p$  : ce qu'on voulait. □

**Application 6** (Duplication du cube). Soit un cube de volume  $\mathcal{V}$  dont on suppose son arête  $a$  constructible. Il est impossible de dessiner, à la règle et au compas, l'arête d'un cube de volume  $2\mathcal{V}$ .

*Démonstration.* On a  $\mathcal{V} = a^3$  et donc  $2\mathcal{V} = 2a^3$ . L'arête d'un cube est la racine cubique de son volume. Il faut donc construire le nombre

$$\sqrt[3]{2a^3} = a\sqrt[3]{2}$$

Comme  $a$  est constructible, ceci revient à construire le nombre

$$\alpha = \sqrt[3]{2}$$

Le polynôme  $P = X^3 - 2$  est irréductible sur  $\mathbb{Q}$  (par le critère d'Eisenstein) et annule  $\alpha$  : c'est son polynôme minimal sur  $\mathbb{Q}$ . On a ainsi

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

donc  $\alpha$  n'est pas constructible par le Théorème 5. □



## 35 Théorème de Wedderburn

En utilisant les polynômes cyclotomiques, nous montrons que tout corps fini est commutatif.

**Lemme 1.** Soient  $\mathbb{K}$  et  $\mathbb{L}$  deux corps finis tels que  $\mathbb{K}$  est commutatif et  $\mathbb{K} \subseteq \mathbb{L}$ . Alors  $\exists d \in \mathbb{N}^*$  tel que  $|\mathbb{L}| = |\mathbb{K}|^d$ .

[GOU21]  
p. 100

*Démonstration.*  $\mathbb{L}$  est un espace vectoriel sur  $\mathbb{K}$  de dimension finie  $d$  (car  $\mathbb{L}$  est fini). Donc  $\mathbb{L}$  est isomorphe en tant que  $\mathbb{K}$ -espace vectoriel à  $\mathbb{K}^d$ . En particulier,  $|\mathbb{L}| = |\mathbb{K}|^d$ .  $\square$

**Théorème 2 (Wedderburn).** Tout corps fini est commutatif.

*Démonstration.* Soit  $\mathbb{K}$  un corps. L'idée va être de procéder par récurrence sur le cardinal du corps.

- Si  $|\mathbb{K}| = 2$  : alors  $\mathbb{K} = \{0, 1\}$  est commutatif.
- On suppose le résultat vrai pour tout corps fini de cardinal strictement inférieur à  $|\mathbb{K}|$ . On veut montrer que  $\mathbb{K}$  est commutatif. Supposons par l'absurde que  $\mathbb{K}$  ne l'est pas. On pose

$$Z = Z(\mathbb{K}) = \{x \in \mathbb{K} \mid \forall y \in \mathbb{K}, xy = yx\}$$

le centre de  $\mathbb{K}$  dont on note  $q$  le cardinal. C'est un sous-corps de  $\mathbb{K}$  qui est (par hypothèse) inclus strictement dans  $\mathbb{K}$ . Donc  $Z$  est commutatif, et par le Théorème 1, on peut écrire  $|\mathbb{K}| = q^n$  où  $n \in \mathbb{N}^*$ . Si  $x \in \mathbb{K}$ , on pose

$$\mathbb{K}_x = Z_{\mathbb{K}}(\{x\}) = \{y \in \mathbb{K} \mid xy = yx\}$$

Montrons que

$$\exists d \mid n \text{ tel que } |\mathbb{K}_x| = q^d \quad (*)$$

Notons déjà encore une fois que  $\mathbb{K}_x$  est un sous-corps de  $\mathbb{K}$ .

- Si  $\mathbb{K}_x = \mathbb{K}$ , on a  $|\mathbb{K}_x| = |\mathbb{K}| = q^n$ . Il suffit donc de prendre  $d = n$ .
- Sinon,  $\mathbb{K}_x \subsetneq \mathbb{K}$ , donc  $\mathbb{K}_x$  est commutatif par hypothèse. Par le Théorème 1, il existe  $k \in \mathbb{N}^*$  tel que  $|\mathbb{K}| = |\mathbb{K}_x|^k$ .

Mais,  $Z$  est un sous-corps (commutatif) de  $\mathbb{K}_x$ , donc d'après le Théorème 1, il existe  $d \in \mathbb{N}^*$  tel que  $|\mathbb{K}_x| = |Z|^d$ . Donc on a

$$q^n = |\mathbb{K}| = |\mathbb{K}_x|^k = (q^d)^k = q^{dk}$$

d'où  $d \mid n$ .

On considère l'action par conjugaison de  $\mathbb{K}^*$  sur lui-même  $(x, y) \mapsto xyx^{-1}$ . Si  $y \in \mathbb{K}^*$ , alors

$$\text{Stab}_{\mathbb{K}^*}(y) = \{x \in \mathbb{K}^* \mid x.y = y\} = \mathbb{K}_y^*$$

Soit  $\Omega$  un système de représentants associé à la relation d'équivalence "être dans la même orbite". L'équation aux classes donne alors

$$|\mathbb{K}^*| = \sum_{\omega \in \Omega} \frac{|\mathbb{K}^*|}{|\text{Stab}_{\mathbb{K}^*}(\omega)|}$$

Or,

$$\text{Stab}_{\mathbb{K}^*}(\omega) = \mathbb{K}^* \iff \forall x \in \mathbb{K}^*, \omega x = x\omega \iff \omega \in Z^*$$

donc en notant  $\Omega' = \Omega \setminus Z^*$ , on a :

$$|\mathbb{K}^*| = \sum_{\omega \in Z^*} \frac{|\mathbb{K}^*|}{|\text{Stab}_{\mathbb{K}^*}(\omega)|} + \sum_{\omega \in \Omega'} \frac{|\mathbb{K}^*|}{|\text{Stab}_{\mathbb{K}^*}(\omega)|} = |Z^*| + \sum_{\omega \in \Omega'} \frac{|\mathbb{K}^*|}{|\mathbb{K}_{\omega}^*|} \quad (**)$$

Soit  $\omega \in \Omega'$ . Par (\*),

$$\exists d \mid n \text{ tel que } |\text{Stab}_{\mathbb{K}^*}(\omega)| = |\mathbb{K}_{\omega}^*| = q^d - 1$$

De plus,  $d \neq n$  (car  $\omega \notin Z^*$ ). Si maintenant on pose

$$\forall d \mid n, \lambda_d = |\{\omega \in \Omega' \mid |\text{Stab}_{\mathbb{K}^*}(\omega)| = q^d - 1\}|$$

on peut alors écrire en remplaçant dans (\*\*):

$$q^n - 1 = |\mathbb{K}^*| = (q - 1) + \sum_{d \mid n} \lambda_d \left( \frac{q^n - 1}{q^d - 1} \right) \quad (***)$$

Si  $d \parallel n$ , on a

$$X^n - 1 = \prod_{k \mid n} \Phi_k = \Phi_n \left( \prod_{k \mid d} \Phi_k \right) \left( \prod_{\substack{k \mid n \\ k \nmid d}} \Phi_k \right) = \Phi_n (X^d - 1) \left( \prod_{\substack{k \mid n \\ k \nmid d}} \Phi_k \right)$$

Donc,  $\Phi_n \mid \frac{X^n - 1}{X^d - 1}$  dans  $\mathbb{Z}[X]$ . Ceci étant vrai quelque soit  $d$  divisant strictement  $n$ , on en déduit

$$\Phi_n \mid \sum_{d \parallel n} \lambda_d \frac{X^n - 1}{X^d - 1} \text{ dans } \mathbb{Z}[X]$$

Comme de plus,  $\Phi_n \mid X^n - 1$  dans  $\mathbb{Z}[X]$ , on conclut que

$$\Phi_n \mid X^n - 1 - \sum_{d \parallel n} \lambda_d \frac{X^n - 1}{X^d - 1} \text{ dans } \mathbb{Z}[X]$$

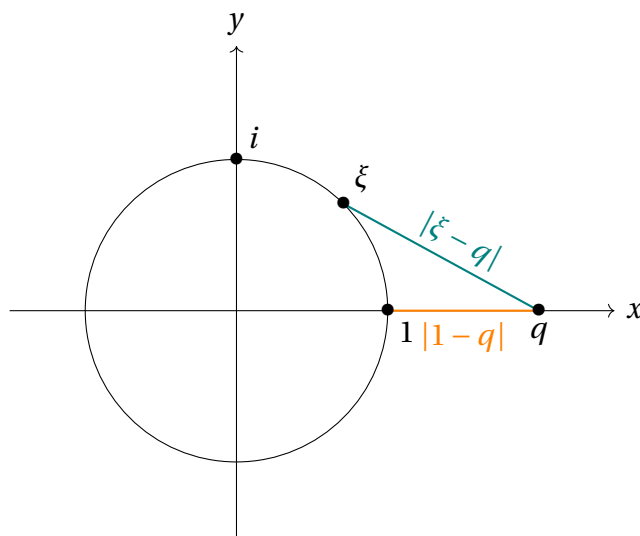
ce qui donne, une fois évalué en  $q$  :

$$\Phi_n(q) \mid q^n - 1 - \sum_{d \parallel n} \lambda_d \frac{q^n - 1}{q^d - 1} \stackrel{(***)}{=} q - 1 \implies |\Phi_n(q)| \leq q - 1$$

Mais  $n \geq 2$ , donc

$$\begin{aligned} |\Phi_n(q)| &= \prod_{\xi \in \mu_n^*} |q - \xi| \\ &> \prod_{i=1}^{\varphi(n)} |q - 1| \\ &\geq |q - 1| \end{aligned}$$

On peut en effet interpréter  $|q - \xi|$  comme la distance du complexe  $q$  au complexe  $\xi$  ; le premier est sur l'axe réel et est supérieur ou égal à 2, le second est sur le cercle unité mais n'est pas sur l'axe réel :



cela nous permet de justifier l'inégalité stricte. On a donc une contradiction.

□

## 36 Théorème de Weierstrass (par la convolution)

On montre le théorème de Weierstrass par la convolution (sans forcément développer toute la théorie derrière, ce qui peut être utile dans certaines leçons).

**Notation 1.**  $\forall n \in \mathbb{N}$ , on note :

$$a_n = \int_{-1}^1 (1-t^2)^n dt \text{ et } p_n : t \mapsto \frac{(1-t^2)^n}{a_n} \mathbb{1}_{[-1,1]}(t)$$

[GOU20]  
p. 304

**Lemme 2.** La suite  $(p_n)$  vérifie :

- (i)  $\forall n \in \mathbb{N}, p_n \geq 0$ .
- (ii)  $\forall n \in \mathbb{N}, \int_{\mathbb{R}} p_n(t) dt = 1$ .
- (iii)  $\forall \alpha > 0, \lim_{n \rightarrow +\infty} \int_{|t| > \alpha} p_n(t) dt = 0$ .

Autrement dit,  $(p_n)$  est une **approximation positive de l'identité**.

*Démonstration.* Notons tout d'abord que

$$\forall n \in \mathbb{N}^*, a_n = 2 \int_0^1 (1-t^2)^n dt \geq 2 \int_0^1 t(1-t^2)^n dt = \left[ -\frac{(1-t^2)^{n+1}}{n+1} \right]_0^1 = \frac{1}{n+1}$$

- (i)  $\forall n \in \mathbb{N}, p_n \geq 0$  car  $a_n \geq 0$  et  $(1-t^2)^n \geq 0$  pour tout  $t \in [-1, 1]$ .
- (ii)  $\forall n \in \mathbb{N}, \int_{\mathbb{R}} p_n(t) dt = \frac{1}{a_n} \int_{-1}^1 (1-t^2)^n dt = 1$ .
- (iii) Soit  $\alpha > 0$ .

— Si  $\alpha < 1$  :  $\forall n \in \mathbb{N}^*$ ,

$$\int_{|t| \geq \alpha} p_n(t) dt = \frac{2}{a_n} \int_{\alpha}^1 (1-t^2)^n dt \leq \frac{2}{a_n} (1-\alpha^2)^n \leq 2(n+1)(1-\alpha^2)^n$$

et comme  $|1-\alpha^2| < 1$ , on a  $\int_{|t| \geq \alpha} p_n(t) dt \rightarrow 0$ .

— Si  $\alpha \geq 1$  :

$$\int_{|t| \geq \alpha} p_n(t) dt = 0$$

□

**Théorème 3 (Weierstrass).** Toute fonction continue  $f : [a, b] \rightarrow \mathbb{R}$  (avec  $a, b \in \mathbb{R}$  tels que  $a \leq b$ ) est limite uniforme de fonctions polynômiales sur  $[a, b]$ .

*Démonstration.* Soit  $f \in \mathcal{C}_c(\mathbb{R})$  continue. Montrons que  $(f * p_n)$  converge uniformément vers  $f$ . Soit  $\epsilon > 0$ . Par le théorème de Heine  $f$  est uniformément continue sur son support, donc l'est aussi sur  $\mathbb{R}$  entier :

$$\exists \eta > 0 \text{ tel que } \forall x, y \in \mathbb{R}, |x - y| < \eta \implies |f(x) - f(y)| < \epsilon$$

De plus,  $f$  est bornée et atteint ses bornes (donc écrire  $\|f\|_\infty$  a du sens). On peut appliquer le Théorème 2 Point (iii) :

$$\exists N \in \mathbb{N} \text{ tel que } \forall n \geq N, \int_{|t| \geq \eta} p_n(t) dt < \epsilon$$

Donc, toujours avec le Théorème 2, pour tout  $n \geq N$  et pour tout  $x \in \mathbb{R}$ ,

$$\begin{aligned} |f * p_n(x) - f(x)| &\stackrel{(ii)}{=} \left| \int_{\mathbb{R}} f(x-t) p_n(t) dt - f(x) \int_{\mathbb{R}} p_n(t) dt \right| \\ &= \left| \int_{\mathbb{R}} (f(x-t) - f(x)) p_n(t) dt \right| \\ &\leq \int_{\mathbb{R}} |f(x-t) - f(x)| p_n(t) dt \\ &\stackrel{(i)}{=} \int_{\mathbb{R}} |f(x-t) - f(x)| p_n(t) dt \\ &= \int_{|t| \geq \eta} |f(x-t) - f(x)| p_n(t) dt + \int_{-\eta}^{\eta} |f(x-t) - f(x)| p_n(t) dt \\ &= 2\|f\|_\infty \epsilon + \epsilon \int_{-\eta}^{\eta} p_n(t) dt \\ &\stackrel{(i)}{\leq} 2\|f\|_\infty \epsilon + \epsilon \int_{\mathbb{R}} p_n(t) dt \\ &= (2\|f\|_\infty + 1)\epsilon \end{aligned}$$

d'où la convergence uniforme. Soit maintenant  $n \in \mathbb{N}$ . Supposons que  $f$  est à support dans  $I = [-\frac{1}{2}, \frac{1}{2}]$  et montrons que pour tout  $f * p_n$  est une fonction polynômiale.

$$\forall x \in I, (f * p_n)(x) = (p_n * f)(x) = \int_{-\frac{1}{2}}^{\frac{1}{2}} p_n(x-t) f(t) dt \quad (*)$$

Notons que  $\forall x, t \in I, |x-t| \leq 1$ , donc

$$p_n(x-t) = \frac{(1-(x-t)^2)^n}{a_n} \stackrel{\text{développement}}{=} \sum_{k=0}^{2n} q_k(t) x^k$$

où  $\forall k \in [0, 2n]$ ,  $q_k$  est une fonction polynômiale. En remplaçant dans (\*), on obtient :

$$\forall x \in I, (f * p_n)(x) = \sum_{k=0}^{2n} \left( \int_{-\frac{1}{2}}^{\frac{1}{2}} q_k(t) f(t) dt \right) x^k$$

qui est bien une fonction polynômiale sur  $I$ .

Soient maintenant  $[a, b]$  un intervalle fermé de  $\mathbb{R}$  et  $f : [a, b] \rightarrow \mathbb{R}$ . On considère  $[c, d]$  un intervalle plus grand avec  $c < a$  et  $b < d$  et on prolonge  $f$  par :

- Une fonction affine sur  $[c, a]$  qui vaut 0 en  $c$  et  $f(a)$  en  $a$ .
- Une fonction affine sur  $[b, d]$  qui vaut 0 en  $d$  et  $f(b)$  en  $b$ .

Et on peut encore prolonger cette fonction sur  $\mathbb{R}$  tout entier en une fonction  $\tilde{f}$  telle que  $\tilde{f} = 0$  pour tout  $x \notin [c, d]$ . On a donc  $\tilde{f} \in \mathcal{C}_c(\mathbb{R})$ . Nous allons maintenant avoir besoin du changement de

variable suivant :

$$\varphi : \begin{array}{ll} I & \rightarrow [c, d] \\ x & \mapsto (d-c)x + \frac{c+d}{2} \end{array}$$

Comme  $\tilde{f} \circ \varphi$  est continue, à support dans  $I$ , on peut maintenant affirmer que  $\tilde{f} \circ \varphi$  est limite uniforme d'une suite de polynômes  $(\rho_n)$ . Donc  $\tilde{f}$  est limite uniforme de la suite  $(\rho_n \circ \varphi^{-1})$  où  $\forall n \in \mathbb{N}$ ,  $\rho_n \circ \varphi^{-1}$  est bien une fonction polynômiale car  $\varphi$  (donc  $\varphi^{-1}$  aussi) est affine. A fortiori,  $f = \tilde{f}|_{[a,b]}$  est aussi limite de fonctions polynômiales sur  $[a, b]$ .  $\square$

La fin de la preuve me semble mieux écrite dans **[I-P]**.

## 37 Théorème de Weierstrass (par les probabilités)

On montre le théorème de Weierstrass en faisant un raisonnement sur des variables aléatoires suivant une loi de Bernoulli.

**Théorème 1 (Bernstein).** Soit  $f : [0, 1] \rightarrow \mathbb{R}$  continue. On note

$$\forall n \in \mathbb{N}^*, B_n(f) : x \mapsto \sum_{k=0}^n \binom{n}{k} f\left(\frac{k}{n}\right) x^k (1-x)^{n-k}$$

le  $n$ -ième polynôme de Bernstein associé à  $f$ . Alors la suite de fonctions  $(B_n(f))$  converge uniformément vers  $f$ .

[G-K]  
p. 195

*Démonstration.* Soit  $x \in ]0, 1[$ . On se place sur un espace probabilité  $(\Omega, \mathcal{A}, \mathbb{P})$  et considère  $(X_k)$  une suite de variables aléatoires indépendantes de même loi  $\mathcal{B}(x)$ . On note  $\forall n \in \mathbb{N}^*, S_n = \sum_{k=1}^n X_k$ . Ainsi,  $S_n \sim \mathcal{B}(n, x)$  et donc par la formule de transfert,

$$\mathbb{E}\left(f\left(\frac{S_n}{n}\right)\right) = \sum_{k=0}^n \binom{n}{k} f\left(\frac{k}{n}\right) x^k (1-x)^{n-k} = B_n(f)(x)$$

La fonction  $f$  est continue sur  $[0, 1]$  qui est un compact de  $\mathbb{R}$ , donc par le théorème de Heine; elle y est uniformément continue. Soit donc  $\epsilon > 0$ ,

$$\exists \eta > 0 \text{ tel que } \forall x, y \in [0, 1], |x - y| < \eta \implies |f(x) - f(y)| < \epsilon$$

On a,

$$\begin{aligned} |B_n(f)(x) - f(x)| &= \left| \mathbb{E}\left(f\left(\frac{S_n}{n}\right)\right) - f(x) \right| \\ &= \left| \mathbb{E}\left(f\left(\frac{S_n}{n}\right) - f(x)\right) \right| \\ &\leq \mathbb{E}\left|f\left(\frac{S_n}{n}\right) - f(x)\right| \\ &\leq \mathbb{E}\left(\mathbb{1}_{\left\{\left|\frac{S_n}{n} - x\right| < \eta\right\}} \left|f\left(\frac{S_n}{n}\right) - f(x)\right|\right) + \mathbb{E}\left(\mathbb{1}_{\left\{\left|\frac{S_n}{n} - x\right| \geq \eta\right\}} \left|f\left(\frac{S_n}{n}\right) - f(x)\right|\right) \\ &\leq \mathbb{E}(\epsilon) + 2\|f\|_\infty \mathbb{E}\left(\mathbb{1}_{\left\{\left|\frac{S_n}{n} - x\right| \geq \eta\right\}}\right) \\ &= \epsilon + 2\|f\|_\infty \mathbb{P}\left(\left|\frac{S_n}{n} - x\right| \geq \eta\right) \end{aligned} \quad (*)$$

Comme  $\mathbb{E}\left(\frac{S_n}{n}\right) = x$ , on peut appliquer l'inégalité de Bienaymé-Tchebychev :

$$\mathbb{P}\left(\left|\frac{S_n}{n} - x\right| \geq \eta\right) = \mathbb{P}\left(\left|\frac{S_n}{n} - \mathbb{E}\left(\frac{S_n}{n}\right)\right| \geq \eta\right) \leq \frac{1}{\eta^2} \text{Var}\left(\frac{S_n}{n}\right)$$

Comme les  $X_k$  sont indépendantes et de même loi :

$$\text{Var}\left(\frac{S_n}{n}\right) = \frac{1}{n^2} \text{Var}(S_n) = \frac{1}{n} \text{Var}(X_1) = \frac{x(1-x)}{n} \leq \frac{1}{n}$$

En réinjectant cela dans (\*), cela donne

$$|B_n(f)(x) - f(x)| \leq \epsilon + \frac{2\|f\|_\infty}{n\eta^2}$$

qui est une majoration indépendante de  $x$ . Comme la fonction  $B_n(f) - f$  est continue sur  $[0, 1]$ , on peut passer à la borne supérieure :

$$\|B_n(f) - f\|_\infty = \sup_{x \in [0,1]} |B_n(f)(x) - f(x)| \leq \epsilon + \frac{2\|f\|_\infty}{n\eta^2}$$

ce qui donne après un passage à la limite supérieure :

$$\begin{aligned} \limsup_{n \rightarrow +\infty} \|B_n(f) - f\|_\infty &\leq \epsilon \\ \stackrel{\epsilon \rightarrow 0}{\Rightarrow} \limsup_{n \rightarrow +\infty} \|B_n(f) - f\|_\infty &= 0 \\ \Rightarrow \lim_{n \rightarrow +\infty} \|B_n(f) - f\|_\infty &= 0 \end{aligned}$$

□

**Théorème 2 (Weierstrass).** Toute fonction continue  $f : [a, b] \rightarrow \mathbb{R}$  (avec  $a, b \in \mathbb{R}$  tels que  $a \leq b$ ) est limite uniforme de fonctions polynômiales sur  $[a, b]$ .

*Démonstration.* On va avoir besoin du changement de variable suivant :

$$\begin{aligned} \varphi : [0, 1] &\rightarrow [a, b] \\ x &\mapsto a + (b - a)x \end{aligned}$$

Par le Théorème 1, la fonction  $f \circ \varphi^{-1}$  est limite uniforme d'une suite de fonctions polynômiales  $(p_n)$ . Donc  $f$  est limite uniforme de la suite  $(p_n \circ \varphi)$  où  $\forall n \in \mathbb{N}$ ,  $p_n \circ \varphi$  est bien une fonction polynômiale car  $\varphi$  est affine. □



## 38 Théorème des deux carrés de Fermat

Nous démontrons le théorème des deux carrés de Fermat (qui donne des conditions sur la décomposition en facteurs premiers d'un entier pour que celui-ci soit somme de deux carrés) à l'aide de l'anneau des entiers de Gauss  $\mathbb{Z}[i]$ .

**Lemme 1.** Soit  $p \geq 3$  un nombre premier. Alors  $x \in \mathbb{F}_p^*$  est un carré si et seulement si  $x^{\frac{p-1}{2}} = 1$ .

[I-P]  
p. 137

*Démonstration.* On pose  $X = \{x \in \mathbb{F}_p \mid x^{\frac{p-1}{2}} = 1\}$ , et on note  $S$  l'ensemble des carrés de  $\mathbb{F}_p^*$ . Comme un polynôme de degré  $d$  sur  $\mathbb{F}_p$  possède au plus  $d$  racines, on a  $|X| \leq \deg(X^{\frac{p-1}{2}} - 1) = \frac{p-1}{2}$ .

D'autre part, si  $x \in S$ , on peut écrire  $x = y^2$  et on a donc  $x^{\frac{p-1}{2}} = y^{p-1} = 1$  car  $|\mathbb{F}_p^*| = p-1$ . Donc,  $S \subseteq X$ .

Pour conclure, calculons le cardinal de  $S$ . Pour cela, considérons le morphisme

$$\begin{array}{ccc} \mathbb{F}_p^* & \rightarrow & S \\ x & \mapsto & x^2 \end{array}$$

dont le noyau est  $\{x \in \mathbb{F}_p^* \mid x^2 = 1\} = \{\pm 1\}$  qui est de cardinal 2. En appliquant le premier théorème d'isomorphisme, et en considérant les cardinaux; on obtient  $|S| = \frac{p-1}{2}$ . Donc  $S = X$ .  $\square$

Introduisons maintenant des notations qui seront utiles pour la suite.

**Notation 2.** On note

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \rightarrow & \mathbb{N} \\ a + ib & \mapsto & a^2 + b^2 \end{array}$$

et  $\Sigma$  l'ensemble des entiers qui sont somme de deux carrés.

*Remarque 3.*  $n \in \Sigma \iff \exists z \in \mathbb{Z}[i] \text{ tel que } N(z) = n$ .

**Lemme 4.** Voici quelques propriétés sur  $N$  et  $\mathbb{Z}[i]$  dont nous aurons besoin :

- (i)  $N$  est multiplicative.
- (ii)  $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\} = \{\pm 1, \pm i\}$ .
- (iii)  $\mathbb{Z}[i]$  est euclidien de stathme  $N$ .

*Démonstration.* (i) On a  $\forall z, z' \in \mathbb{C}, |zz'||^2 = |z|^2 |z'|^2$  (par multiplicativité de  $(.)^2$  et de  $|\cdot|$ ). Et  $N$  n'est que la restriction de  $|\cdot|^2$  à  $\mathbb{Z}[i]$ . Il est également tout-à-fait possible de montrer cette propriété par un calcul direct.

- (ii) Soit  $z \in \mathbb{Z}[i]^*$ . On a  $N(z)N(z^{-1}) = N(zz^{-1}) = N(1) = 1$ . Comme  $N$  est à valeurs dans  $\mathbb{N}$ , on a  $N(z) = N(z^{-1}) = 1$ . En écrivant  $z = a + ib$ , on a  $N(z) = a^2 + b^2 = 1$ , d'où  $a = \pm 1$  ou  $b = \pm 1$ . Réciproquement,  $\pm 1$  et  $\pm i$  sont bien inversibles dans  $\mathbb{Z}[i]$  et de module 1.

(iii) Soient  $z, t \in \mathbb{Z}[i]$ . On pose  $\frac{z}{t} = x + iy \in \mathbb{C}$  avec  $x, y \in \mathbb{R}$ . Soient  $a, b \in \mathbb{Z}$  tels que :

- $|x - a| \leq \frac{1}{2}$ .
- $|y - b| \leq \frac{1}{2}$ .

(Ces nombres existent bien, ne pas hésiter à faire un dessin pour s'en convaincre.) On pose  $q = a + ib \in \mathbb{Z}[i]$ , et on a

$$\left| \frac{z}{t} - q \right|^2 = (x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} < 1$$

On pose alors  $r = z - qt$ , et on a bien

$$z = tq + r \text{ et } N(r) = r^2 = |t|^2 \left| \frac{z}{t} - q \right|^2 < |t|^2 = N(t)$$

□

**Lemme 5.** Soit  $p$  un nombre premier. Si  $p$  n'est pas irréductible dans  $\mathbb{Z}[i]$ , alors  $p \in \Sigma$ .

*Démonstration.* On suppose que  $p$  n'est pas irréductible dans  $\mathbb{Z}[i]$ . On peut donc écrire  $p = uv$  avec  $u, v \in \mathbb{Z}[i]$  non inversibles. Ainsi,

$$p^2 = N(p) = N(uv) = \underbrace{N(u)}_{\neq 1} \underbrace{N(v)}_{\neq 1} \stackrel{p \text{ premier}}{\implies} N(u) = N(v) = p$$

Par la Théorème 3,  $p \in \Sigma$ .

□

**Théorème 6** (Deux carrés de Fermat). Soit  $n \in \mathbb{N}^*$ . Alors  $n \in \Sigma$  si et seulement si  $\nu_p(n)$  est pair pour tout  $p$  premier tel que  $p \equiv 3 \pmod{4}$  (où  $\nu_p(n)$  désigne la valuation  $p$ -adique de  $n$ ).

*Démonstration.* Sens direct : On écrit  $n = a^2 + b^2$  avec  $a, b \in \mathbb{Z}$ . Soit  $p \mid n$  tel que  $p \equiv 3 \pmod{4}$ . Montrons que  $p \in \Sigma$ . On suppose par l'absurde que l'on peut écrire  $p = c^2 + d^2$  avec  $c, d \in \mathbb{Z}$ . On va discerner les cas :

- Si  $c \equiv \pm 1 \pmod{4}$ , alors  $c^2 \equiv 1 \pmod{4}$  (et de même pour  $d^2$ ).
- Si  $c \equiv \pm 2 \pmod{4}$ , alors  $c^2 \equiv 0 \pmod{4}$  (et de même pour  $d^2$ ).

Donc  $p = c^2 + d^2 \equiv 0, 1$  ou  $2 \pmod{4}$  : absurde. En particulier, par le Théorème 5 (en prenant la contraposée),  $p$  est irréductible dans  $\mathbb{Z}[i]$ . Comme  $\mathbb{Z}[i]$  est euclidien (cf. Théorème 4),  $p$  est un élément premier de  $\mathbb{Z}[i]$ . Mais,  $p \mid n = (a + ib)(a - ib)$ . Donc  $p \mid a + ib$  ou  $p \mid a - ib$ . Dans les deux cas, on a  $p \mid a$  et  $p \mid b$ . Ainsi,

$$\left( \frac{a}{p} \right)^2 + \left( \frac{b}{p} \right)^2 = \frac{n}{p^2}$$

donc de deux choses l'une; on a :

$$p^2 \mid n \text{ et } \frac{n}{p^2} \in \Sigma$$

Il suffit alors d'itérer le processus (en remplaçant  $n$  par  $\frac{n}{p^2}$ )  $k$  fois jusqu'à ce que  $p$  ne divise plus  $\frac{n}{p^{2k}}$ . On a alors  $n = p^{2k}u$  avec  $p \nmid u$ . D'où  $v_p(n) = 2k$ .

Réciproque : Soit  $p$  premier diviseur de  $n$  tel que  $p \equiv 3 \pmod{4}$ . Alors  $p^{v_p(n)} = \left(p^{\frac{v_p(n)}{2}}\right)^2$  est un carré, donc  $p^{v_p(n)} \in \Sigma$ .

Soit maintenant  $p$  premier tel que  $p = 2$  ou  $p \equiv 1 \pmod{4}$ . Alors en conséquence du Théorème 1 (le cas  $p = 2$  étant trivial),  $-1$  est un carré de  $\mathbb{F}_p$  ie.  $\exists a \in \mathbb{Z}$  tel que  $-1 \equiv a^2 \pmod{p}$ . Donc  $p \mid a^2 + 1 = (a - i)(a + i)$ . Oui mais,  $p$  ne divise ni  $a - i$ , ni  $a + i$ . Donc  $p$  n'est pas un élément premier de  $\mathbb{Z}[i]$  et n'est donc pas irréductible dans  $\mathbb{Z}[i]$  (toujours parce que  $\mathbb{Z}[i]$  est euclidien, cf. Théorème 4). En vertu du Théorème 5,  $p \in \Sigma$ .

Comme  $N$  est multiplicative, par la Théorème 3, on en déduit que  $\Sigma$  est stable par multiplication. Donc  $n \in \Sigma$  (en décomposant  $n$  en produit de facteurs premiers).  $\square$

*Remarque 7.* Le fait qu'un élément irréductible d'un anneau euclidien est premier est une conséquence directe du lemme d'Euclide, vrai dans les anneaux factoriels (donc à fortiori aussi dans les anneaux euclidiens).

[PER]  
p. 48

## 39 Théorème des événements rares de Poisson

On établit la convergence en loi vers une loi de Poisson d'une suite de variables aléatoires.

**Lemme 1.** Soient  $z_1, \dots, z_n, u_1, \dots, u_n \in \mathbb{C}$  de module inférieur ou égal à 1. Alors

$$|z_1 \dots z_n - u_1 \dots u_n| \leq |z_1 - u_1| + \dots + |z_n - u_n|$$

[G-K]  
p. 372

*Démonstration.*  $|z_1 z_2 - u_1 u_2| = |z_1(z_2 - u_2) + u_2(z_1 - u_1)| \leq |z_1 - u_1| + |z_2 - u_2|$ . On procède ensuite par récurrence pour montrer le résultat.  $\square$

**Théorème 2** (des événements rares de Poisson). Soit  $(N_n)_{n \geq 1}$  une suite d'entiers tendant vers l'infini. On suppose que pour tout  $n$ ,  $A_{n,N_1}, \dots, A_{n,N_n}$  sont des événements indépendants avec  $\mathbb{P}(A_{n,N_k}) = p_{n,k}$ . On suppose également que :

- (i)  $\lim_{n \rightarrow +\infty} s_n = \lambda > 0$  où  $\forall n \in \mathbb{N}, s_n = \sum_{k=1}^{N_n} p_{n,k}$ .
- (ii)  $\lim_{n \rightarrow +\infty} \sup_{k \in \llbracket 1, N_n \rrbracket} p_{n,k} = 0$ .

Alors, la suite de variables aléatoires  $(S_n)$  définie par

$$\forall n \in \mathbb{N}^*, S_n = \sum_{k=1}^{N_n} \mathbb{1}_{A_{n,k}}$$

converge en loi vers la loi de Poisson de paramètre  $\lambda$ .

p. 390

*Démonstration.* Pour la suite, on note  $\forall n \in \mathbb{N}, m_n = \max_{k \in \llbracket 1, N_n \rrbracket} p_{n,k}$ . On calcule

$$\begin{aligned} \phi_{S_n}(t) &= \mathbb{E}(e^{itS_n}) \\ &= \mathbb{E}\left(e^{it \sum_{k=1}^{N_n} \mathbb{1}_{A_{n,k}}}\right) \\ &= \mathbb{E}\left(\prod_{k=1}^{N_n} e^{it \mathbb{1}_{A_{n,k}}}\right) \\ &= \prod_{k=1}^{N_n} \mathbb{E}(e^{it \mathbb{1}_{A_{n,k}}}) \text{ par indépendance} \\ &= \prod_{k=1}^{N_n} ((1 - p_{n,k}) + e^{it} p_{n,k}) \\ &= \prod_{k=1}^{N_n} (p_{n,k}(e^{it} - 1) + 1) \end{aligned}$$

l'avant-dernière égalité étant justifiée par le fait que

$$\mathbb{P}(e^{it \mathbb{1}_{A_{n,k}}} = e^{it}) = \mathbb{P}(A_{n,k} = 1) = p_{n,k} \text{ et } \mathbb{P}(e^{it \mathbb{1}_{A_{n,k}}} = 1) = \mathbb{P}(A_{n,k} = 0) = 1 - p_{n,k}$$

Soient  $P_{n,k}$  des variables aléatoires indépendantes suivant les lois de Poisson de paramètres

respectifs  $p_{n,k}$ . On pose

$$S'_n = \sum_{k=1}^{N_n} P_{n,k}$$

et on calcule la fonction caractéristique de cette nouvelle variable aléatoire :

$$\begin{aligned}\phi_{S'_n}(t) &= \prod_{k=1}^{N_n} \phi_{P_{n,k}}(t) \text{ par indépendance} \\ &= \prod_{k=1}^{N_n} \exp(p_{n,k}(e^{it} - 1)) \\ &= \exp(s_n(e^{it} - 1))\end{aligned}$$

Par différence, on obtient

$$|\phi_{S_n}(t) - \phi_{S'_n}(t)| = \left| \prod_{k=1}^{N_n} (p_{n,k}(e^{it} - 1) + 1) - \prod_{k=1}^{N_n} \exp(p_{n,k}(e^{it} - 1)) \right|$$

ce qui, après application du Théorème 1, donne l'inégalité

$$|\phi_{S_n}(t) - \phi_{S'_n}(t)| \leq \sum_{k=1}^{N_n} g(p_{n,k}(e^{it} - 1))$$

avec  $g : z \mapsto |e^z - 1 - z|$ . Mais, par développement en série entière :

$$\begin{aligned}g(z) &= \left| \sum_{k=2}^{+\infty} \frac{z^k}{k!} \right| \\ &= \left| \sum_{k=0}^{+\infty} \frac{z^{k+2}}{(k+2)!} \right| \\ &= \left| z^2 \sum_{k=0}^{+\infty} \frac{z^k}{k!} \frac{1}{(k+1)(k+2)} \right| \\ &\leq |z|^2 \sum_{k=0}^{+\infty} \frac{|z|^k}{k!} \left| \frac{1}{(k+1)(k+2)} \right| \\ &\leq |z|^2 \frac{e^{|z|}}{2}\end{aligned}$$

Mais, comme  $|p_{n,k}(e^{it} - 1)| \leq 2p_{n,k} \leq 2$ , on a :

$$\begin{aligned}|\phi_{S_n}(t) - \phi_{S'_n}(t)| &\leq \sum_{k=1}^{N_n} (2p_{n,k})^2 \frac{e^2}{2} \\ &= 2e^2 \sum_{k=1}^{N_n} 2p_{n,k}^2 \\ &\leq 2e^2 \underbrace{s_n}_{\xrightarrow{\lambda}} \underbrace{m_n}_{\xrightarrow{0}} \\ &\longrightarrow 0\end{aligned}$$

Enfin,

$$\begin{aligned}
 |\phi_{S_n}(t) - \exp(\lambda(e^{it} - 1))| &\leq |\phi_{S_n}(t) - \phi_{S'_n}(t)| + |\phi_{S'_n}(t) - \exp(\lambda(e^{it} - 1))| \\
 &\leq \underbrace{|\phi_{S_n}(t) - \phi_{S'_n}(t)|}_{\rightarrow 0} + \underbrace{|\exp(s_n(e^{it} - 1)) - \exp(\lambda(e^{it} - 1))|}_{\rightarrow 0 \text{ car } s_n \rightarrow \lambda} \longrightarrow 0
 \end{aligned}$$

et le théorème de Lévy permet de conclure. □

## 40 Transformée de Fourier d'une gaussienne

On calcule la transformée de Fourier d'une fonction de type gaussienne  $x \mapsto e^{-ax^2}$  à l'aide du théorème intégral de Cauchy.

**Proposition 1.** On définit  $\forall a \in \mathbb{R}_*^+$ ,

$$\gamma_a : \begin{array}{ccc} \mathbb{R} & \rightarrow & \mathbb{R} \\ x & \mapsto & e^{-ax^2} \end{array}$$

Alors,

$$\forall \xi \in \mathbb{R}, \widehat{\gamma_a}(\xi) = \sqrt{\frac{\pi}{a}} e^{-\frac{\xi^2}{4a}}$$

[AMR08]  
p. 156

*Démonstration.* Soit  $a \in \mathbb{R}_*^+$ . On a

$$\forall \xi \in \mathbb{R}, \widehat{\gamma_a}(\xi) = \int_{-\infty}^{+\infty} e^{-ax^2} e^{-ix\xi} dx$$

et en écrivant

$$ax^2 + ix\xi = a \left( x^2 + i \frac{x\xi}{a} \right) = a \left( \left( x + i \frac{\xi}{2a} \right)^2 + \frac{\xi^2}{4a^2} \right)$$

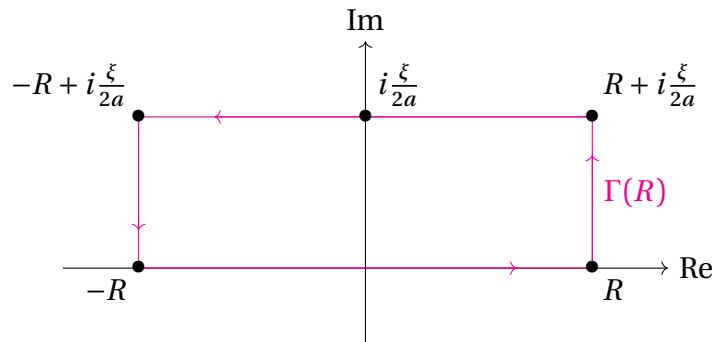
on en déduit que

$$\forall \xi \in \mathbb{R}, \widehat{\gamma_a}(\xi) = e^{-\frac{\xi^2}{4a}} \int_{-\infty}^{+\infty} e^{-a \left( x + i \frac{\xi}{2a} \right)^2} dx \quad (*)$$

On va considérer la fonction

$$\begin{array}{ccc} \mathbb{C} & \rightarrow & \mathbb{C} \\ z & \mapsto & e^{-az^2} \end{array}$$

Pour  $R > 0$  et  $\xi \in \mathbb{R}$ , on note  $\Gamma(R)$  le rectangle de sommets  $-R, R, R + i \frac{\xi}{2a}, -R + i \frac{\xi}{2a}$  parcouru dans le sens direct :



On a,

$$\underbrace{\int_{\Gamma(R)} e^{-az^2} dz}_{=I(R)} = \underbrace{\int_{-R}^R e^{-az^2} dz}_{=I_1(R)} + \underbrace{\int_R^{R+i\frac{\xi}{2a}} e^{-az^2} dz}_{=I_2(R)} + \underbrace{\int_{R+i\frac{\xi}{2a}}^{-R+i\frac{\xi}{2a}} e^{-az^2} dz}_{=I_3(R)} + \underbrace{\int_{-R+i\frac{\xi}{2a}}^{-R} e^{-az^2} dz}_{=I_4(R)}$$

Nous allons traiter les intégrales séparément.

- Pour  $I_1(R)$  : On a affaire à une intégrale sur l'axe réel. Or, on connaît la valeur de l'intégrale de Gauss :

$$\int_{-\infty}^{+\infty} e^{-y^2} dy = \sqrt{\pi}$$

Donc en faisant le changement de variable  $y = \sqrt{ax}$ , on obtient :

$$\sqrt{a} \int_{-\infty}^{+\infty} e^{-ax^2} dx = \sqrt{\pi} \iff \int_{-\infty}^{+\infty} e^{-ax^2} dx = \sqrt{\frac{\pi}{a}}$$

D'où :

$$I_1(R) \longrightarrow \sqrt{\frac{\pi}{a}}$$

quand  $R \longrightarrow +\infty$ .

- Pour  $I_2(R)$  : On a :

$$\begin{aligned} \forall z \in \left[ R, R + i \frac{\xi}{2a} \right], z = R + it \text{ avec } t \in \left[ 0, \frac{\xi}{2a} \right] \\ \implies dz = i dt \end{aligned}$$

D'où :

$$I_2(R) = i \int_0^{\frac{\xi}{2a}} e^{-a(R+it)^2} dt$$

On en déduit,

$$\begin{aligned} |I_2(R)| &\leq \int_0^{\frac{\xi}{2a}} \left| e^{-a(R+it)^2} \right| dt \\ &= \int_0^{\frac{\xi}{2a}} \left| e^{-a(R^2-t^2)} \right| \underbrace{|e^{i2aRt}|}_{=1} dt \\ &= \int_0^{\frac{\xi}{2a}} e^{-a(R^2-t^2)} dt \\ &= e^{-aR^2} \int_0^{\frac{\xi}{2a}} e^{at^2} dt \\ &\longrightarrow 0 \end{aligned}$$

quand  $R \longrightarrow +\infty$ .

- Pour  $I_3(R)$  : On a :

$$\begin{aligned} \forall z \in \left[ R + i \frac{\xi}{2a}, -R + i \frac{\xi}{2a} \right], z = t + i \frac{\xi}{2a} \text{ avec } t \in [R, -R] \\ \implies dz = dt \end{aligned}$$

D'où :

$$I_3(R) = \int_R^{-R} e^{-a\left(t+i\frac{\xi}{2a}\right)^2} dt = - \int_{-R}^R e^{-a\left(t+i\frac{\xi}{2a}\right)^2} dt = -e^{\frac{\xi^2}{4a}} \int_{-R}^R e^{-a\left(t+i\frac{\xi}{2a}\right)^2} dt$$



qui est une intégrale généralisée absolument convergente. Ainsi par (\*),

$$I_3(R) \longrightarrow -e^{\frac{\xi^2}{4a}} \widehat{\gamma}_a(\xi)$$

quand  $R \longrightarrow +\infty$ .

— Pour  $I_4(R)$  : Ce cas-ci se traite exactement comme  $I_2(R)$ . On a :

$$\begin{aligned} \forall z \in \left[ -R + i\frac{\xi}{2a}, -R \right], z = -R + it \text{ avec } t \in \left[ \frac{\xi}{2a}, 0 \right] \\ \implies dz = i dt \end{aligned}$$

D'où :

$$I_4(R) = i \int_{\frac{\xi}{2a}}^0 e^{-a(-R+it)^2} dt = -i \int_0^{\frac{\xi}{2a}} e^{-a(-R+it)^2} dt$$

On en déduit,

$$|I_4(R)| \leq \int_0^{\frac{\xi}{2a}} \left| e^{-a(-R+it)^2} \right| dt = e^{-aR^2} \int_0^{\frac{\xi}{2a}} e^{at^2} dt \longrightarrow 0$$

quand  $R \longrightarrow +\infty$ .

— Pour  $I(R)$  : La fonction  $z \mapsto e^{-az^2}$  est holomorphe et le contour  $\Gamma(R)$  est fermé. Donc  $I(R) = 0$  en vertu du théorème intégral de Cauchy.

En passant à la limite, on obtient ainsi :

$$0 = \sqrt{\frac{\pi}{a}} + 0 - e^{\frac{\xi^2}{4a}} \widehat{\gamma}_a(\xi) + 0 \iff \widehat{\gamma}_a(\xi) = \sqrt{\frac{\pi}{a}} e^{-\frac{\xi^2}{4a}}$$

□

## 41 Trigonalisation simultanée

Nous montrons le théorème de trigonalisation simultanée grâce à l'utilisation des applications transposées (et donc, de la dualité).

Soit  $E$  un espace vectoriel de dimension  $n$  sur un corps  $\mathbb{K}$ .

[GOU21]  
p. 176

**Lemme 1.** Soit  $g \in \mathcal{L}(E)$  un endomorphisme. Soit  $F$  un sous-espace vectoriel de  $E$  stable par  $g$ . Alors,

$$\chi_{g|_F} \mid \chi_g$$

*Démonstration.* On note  $m$  la dimension de  $F$ . Considérons  $G$ , un supplémentaire de  $F$  dans  $E$ . Soient  $\mathcal{B}_F$  et  $\mathcal{B}_G$  des bases respectives de  $F$  et de  $G$ . Alors, la matrice de  $g$  dans la base de  $E$  constituée de l'union disjointe de  $\mathcal{B}_F$  et  $\mathcal{B}_G$  est de la forme

$$M = \begin{pmatrix} A & * \\ 0 & * \end{pmatrix}$$

avec  $A \in \mathcal{M}_m(\mathbb{K})$ , qui est la matrice de l'endomorphisme induit  $g|_F$ . On constate clairement que  $\chi_{g|_F} = \chi_A \mid \chi_M = \chi_g$ .  $\square$

**Lemme 2.** Soit  $g \in \mathcal{L}(E)$  un endomorphisme trigonalisable. Soit  $F$  un sous-espace vectoriel de  $E$  stable par  $g$ . Alors,  $g|_F$  est trigonalisable.

*Démonstration.*  $g$  est trigonalisable si et seulement si son polynôme caractéristique est scindé sur  $\mathbb{K}$ . Dans ce cas, le polynôme caractéristique de sa restriction à  $F$  l'est aussi au vu du Théorème 1.  $\square$

**Lemme 3.** Soient  $f, g \in \mathcal{L}(E)$ . On suppose que  $f$  et  $g$  sont trigonalisables et commutent. Alors,  $f$  et  $g$  ont un vecteur propre commun.

*Démonstration.*  $f$  est trigonalisable, donc  $f$  admet une valeur propre  $\lambda \in \mathbb{K}$  (cf. première colonne de la matrice de  $f$  dans une base de trigonalisation). Le sous-espace propre  $E_\lambda = \text{Ker}(f - \lambda \text{id}_E)$  est alors stable par  $g$  :

$$\forall x \in E_\lambda, (f - \lambda \text{id}_E)(g(x)) = g((f - \lambda \text{id}_E)(x))$$

car  $f$ ,  $g$  et  $\lambda \text{id}_E$  commutent. Ainsi,

$$\forall x \in E_\lambda, (f - \lambda \text{id}_E)(g(x)) = 0$$

Par le Théorème 2, la restriction de  $g$  à  $E_\lambda$  est trigonalisable. Donc,  $g|_{E_\lambda}$  admet un vecteur propre  $x \in E_\lambda$  qui est, par construction, un vecteur propre commun à  $f$  et  $g$ .  $\square$

**Théorème 4** (Trigonalisation simultanée). Soient  $f, g \in \mathcal{L}(E)$ . On suppose que  $f$  et  $g$  sont trigonalisables et commutent. Alors, il existe une base de trigonalisation commune de  $f$  et  $g$ .

*Démonstration.* On va procéder par récurrence sur  $n$ .

- Si  $n = 1$  : c'est évident.
- Supposons le résultat vrai au rang  $n - 1$ . Pour tout  $\varphi \in E^*$ ,

$$\begin{aligned} ({}^t f \circ {}^t g)(\varphi) &= {}^t f(\varphi \circ g) \\ &= \varphi \circ g \circ f \\ &= \varphi \circ f \circ g \\ &= ({}^t g \circ {}^t f)(\varphi) \end{aligned}$$

ie.  ${}^t f {}^t g = {}^t g {}^t f$ . De plus,  ${}^t f$  et  ${}^t g$  sont trigonalisables (car possèdent les mêmes polynômes caractéristiques que  $f$  et  $g$ ). Par le Théorème 3 appliqué à  ${}^t f$  et  ${}^t g$ , il existe un vecteur propre  $\psi \in E^*$  commun à ces deux endomorphismes. Le sous-espace vectoriel  $\text{Vect}(\psi)$  est ainsi stable par  ${}^t f$  et  ${}^t g$ . Notons

$$H = \text{Vect}(\psi)^\circ = \{x \in E \mid \psi(x) = 0\} = \text{Ker}(\psi)$$

c'est un hyperplan de  $E$  (donc de dimension  $n - 1$ ), qui est de plus stable par  $f$  et  $g$ . En effet, en notant  $\lambda \in \mathbb{K}$  la valeur propre de  $f$  associée à  $\psi$ , on a :

$$\forall x \in H, \psi(f(x)) = {}^t f(\psi)(x) = \lambda \psi(x) = 0$$

et un même calcul montre la stabilité par  $g$ . D'après l'hypothèse de récurrence appliquée aux endomorphismes induits  $f|_H$  et  $g|_H$ , on obtient une base  $\mathcal{B}_H$  de  $H$  de cotrigonalisation pour  $f|_H$  et  $g|_H$ . On la complète en une base quelconque  $\mathcal{B}$  de  $E$ , dans laquelle on obtient

$$\text{Mat}(f, \mathcal{B}) = \begin{pmatrix} \text{Mat}(f|_H, \mathcal{B}_H) & \begin{smallmatrix} * \\ \vdots \\ * \end{smallmatrix} \\ 0 & \dots & 0 & * \end{pmatrix} \text{ et } \text{Mat}(g, \mathcal{B}) = \begin{pmatrix} \text{Mat}(g|_H, \mathcal{B}_H) & \begin{smallmatrix} * \\ \vdots \\ * \end{smallmatrix} \\ 0 & \dots & 0 & * \end{pmatrix}$$

où  $\text{Mat}(f|_H, \mathcal{B}_H)$  et  $\text{Mat}(g|_H, \mathcal{B}_H)$  sont triangulaires supérieures d'ordre  $n - 1$ .

□

# Bibliographie

## **Analyse de Fourier dans les espaces fonctionnels**

[AMR08]

Mohammed EL-AMRANI. *Analyse de Fourier dans les espaces fonctionnels. Niveau M1*. Ellipses, 28 août 2008.

<https://www.editions-ellipses.fr/accueil/3908-14232-analyse-de-fourier-dans-les-espaces-fonctionnels-niveau-m1-9782729839031.html>.

## **Objectif agrégation**

[BMP]

Vincent BECK, Jérôme MALICK et Gabriel PEYRÉ. *Objectif agrégation*. 2<sup>e</sup> éd. H&K, 22 août 2005.

<https://objectifagregation.github.io>.

## **Nouvelles histoires hédonistes de groupes et de géométries**

[C-G]

Philippe CALDERO et Jérôme GERMONI. *Nouvelles histoires hédonistes de groupes et de géométries. Tome 1*. Calvage & Mounet, 13 mai 2017.

<http://www.calvage-et-mounet.fr/2022/05/09/nouvelles-histoires-hedoniste-de-groupes-et-de-geometrie/>.

## **Mathématiques pour l'agrégation**

[DAN]

Jean-François DANTZER. *Mathématiques pour l'agrégation. Analyse et probabilités*. De Boeck Supérieur, 20 avr. 2021.

<https://www.deboecksuperieur.com/ouvrage/9782807332904-mathematiques-pour-l-agregation-analyse-et-probabilites>.

## **Analyse numérique et équations différentielles**

[DEM]

Jean-Pierre DEMAILLY. *Analyse numérique et équations différentielles*. 4<sup>e</sup> éd. EDP Sciences, 11 mai 2016.

<https://www.uga-editions.com/menu-principal/collections-et-revues/collections/grenoble-sciences/analyse-numerique-et-equations-differentielles-239866.kjsp>.

## **Oraux X-ENS Mathématiques**

[FGN2]

Serge FRANCINO, Hervé GIANELLA et Serge NICOLAS. *Oraux X-ENS Mathématiques. Volume 2*. 2<sup>e</sup> éd. Cassini, 16 mars 2021.

<https://store.cassini.fr/fr/enseignement-des-mathematiques/111-oraux-x-ens-mathematiques-nouvelle-serie-vol-2.html>.

## **De l'intégration aux probabilités**

[G-K]

Olivier GARET et Aline KURTZMANN. *De l'intégration aux probabilités*. 2<sup>e</sup> éd. Ellipses, 28 mai 2019.

<https://www.editions-ellipses.fr/accueil/4593-14919-de-l-integration-aux-probabilites-2e-edition-augmentee-9782340030206.html>.

---

**Les maths en tête****[GOU20]**

Xavier GOURDON. *Les maths en tête. Analyse*. 3<sup>e</sup> éd. Ellipses, 21 avr. 2020.

<https://www.editions-ellipses.fr/accueil/10446-les-maths-en-tete-analyse-3e-edition-9782340038561.html>.

---

**Les maths en tête****[GOU21]**

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3<sup>e</sup> éd. Ellipses, 13 juill. 2021.

<https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html>.

---

**Théorie de Galois****[GOZ]**

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1*. 2<sup>e</sup> éd. Ellipses, 1<sup>er</sup> avr. 2009.

<https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html>.

---

**L'oral à l'agrégation de mathématiques****[I-P]**

Lucas ISENMANN et Timothée PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2<sup>e</sup> éd. Ellipses, 26 mars 2024.

<https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html>.

---

**Cours d'analyse fonctionnelle****[LI]**

Daniel LI. *Cours d'analyse fonctionnelle. avec 200 exercices corrigés*. Ellipses, 3 déc. 2013.

<https://www.editions-ellipses.fr/accueil/6558-cours-danalyse-fonctionnelle-avec-200-exercices-corriges-9782729883058.html>.

---

**Cours d'algèbre****[PER]**

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.

<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.

---

**Éléments d'analyse réelle****[ROM19-1]**

Jean-Étienne ROMBALDI. *Éléments d'analyse réelle*. 2<sup>e</sup> éd. EDP Sciences, 6 juin 2019.

<https://laboutique.edpsciences.fr/produit/1082/9782759823789/elements-d-analyse-reelle>.

---

**Mathématiques pour l'agrégation****[ROM21]**

Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2<sup>e</sup> éd. De Boeck Supérieur, 20 avr. 2021.

<https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie>.

## **Petit guide de calcul différentiel**

**[ROU]**

François ROUVIÈRE. *Petit guide de calcul différentiel. à l'usage de la licence et de l'agrégation.* 4<sup>e</sup> éd. Cassini, 27 fév. 2015.

<https://store.cassini.fr/fr/enseignement-des-mathematiques/94-petit-guide-de-calcul-differentiel-4e-ed.html>.

## **Anneaux, corps, résultants**

**[ULM18]**

Felix ULMER. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation.* Ellipses, 28 août 2018.

<https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-13-m1-agregation-9782340025752.html>.

## **Analyse pour l'agrégation**

**[Z-Q]**

Claude ZUILY et Hervé QUEFFÉLEC. *Analyse pour l'agrégation. Agrégation/Master Mathématiques.* 5<sup>e</sup> éd. Dunod, 26 août 2020.

<https://www.dunod.com/prepas-concours/analyse-pour-agregation-agregationmaster-mathematiques>.