Développements pour l'agrégation externe de mathématiques

Arnaud Girand

Dernière modification : 15 octobre 2013.

Mode d'emploi

Avertissement sans frais : ce document contient très certainement un nombre proprement colossal de coquilles, fautes de frappe et autres erreurs éhontées. Je ne saurais en aucun cas être tenu responsable des dégâts occasionnés à votre scolarité et/ou à votre santé mentale par les coquilles suscitées. Vous faites usage de ce document à vos risques et périls.

Ce document présente une série d'idées [1] de développements pour les épreuves orales de l'agrégation externe de mathématiques. Il est organisé en trois grandes parties :

- mes couplages leçons/développements pour l'année 2012 ; je tiens à préciser que si ces derniers m'ont effectivement permis d'obtenir l'agrégation, seuls deux d'entre eux (à savoir 109 et 239, avec développements 1.6 et 2.6) ont été testé devant un véritable jury d'agrégation [2] et qu'il est probable que certains (tous ?) contiennent de véritables morceaux de mauvaise foi ;
- ma liste définitive de développements, classés non pas selon leur thèmes généraux [3] mais selon les leçons où je les utilisait ;
- une lise de développements "coupés au montage", i.e que j'ai préparé sans en avoir finalement l'utilité mais que j'ai inclus dans le présent document car je déteste le gaspillage.

Chaque développement est quant à lui fourni avec les informations suivantes :

- une (des) référence(s) : il s'agit du (des) ouvrage(s) dont je me suis servi [4] lors de l'élaboration du développement concerné ;
- une liste des prérequis notables ; comprendre par là que je n'ai précisé que ce qui me semblait ne pas relever de la mémoire génétique de l'espèce humaine ;
- le corps du développement lui–même ;
- quelques détails supplémentaires si nécessaire.

Le lecteur pointilleux trouvera également un index des notations et une bibliographie à la fin de ce document, qui au passage est à peu près intégralement hyper–lié pour votre confort (numérique) de lecture.

Note bibliographique : Il va sans dire que [QZ95] $\subset$ [QZ07]. J'ai choisi de conserver les deux éditions dans le présent document afin que les numéros de page annoncés restent exacts. Vous êtes en droit de maudire ma paresse [5].

1. Non nécessairement bonnes.
2. Appellation d'origine contrôlée.
3. Je n'aurais pas la prétention de pouvoir effectuer un classement aussi arbitraire.
4. D'aucun diraient "que j'ai honteusement pompé".
5. Même si cela n'aura pas grand effet concernant la résolution de l'anomalie bibliographique précité.

Table des matières

Couplages

Algèbre :

101 Groupe opérant sur un ensemble. Exemples et applications.

- ▷ 1.1 Action de $PSL_2(\mathbb{R})$ sur le demi–plan de Poincaré.
- ▷ 1.21 Théorème de Wedderburn.

103 Exemples et applications des notions de sous-groupe distingué et de groupe quotient.

- ▷ 1.5 Groupes d'ordre pq.
- ▷ 1.13 Simplicité du groupe alterné.

104 Groupes finis. Exemples et applications.

- ▷ 1.5 Groupes d'ordre pq.
- ▷ 1.16 Théorème de Burnside.

105 Groupe des permutations d'un ensemble fini. Applications.

- ▷ 1.13 Simplicité du groupe alterné.
- ▷ 1.15 Table de caractères de $\mathfrak{S}_4$.

106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.

- ▷ 1.16 Théorème de Burnside.
- ▷ 3.8 Sous–groupes compacts de $GL_n(\mathbb{R})$.

107 Représentations et caractères d'un groupe fini sur un $\mathbb{C}$–espace vectoriel.

- ▷ 1.14 Table de caractères du groupe diédral.
- ▷ 1.15 Table de caractères de $\mathfrak{S}_4$.

108 Exemples de parties génératrices d'un groupe. Applications.

- ▷ 1.13 Simplicité du groupe alterné.
- ▷ 1.14 Table de caractères du groupe diédral.

109 Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

- ▷ 1.5 Groupes d'ordre pq.
- ▷ 1.6 Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$.

110 Nombres premiers. Applications.

- ▷ 1.6 Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$.
- ▷ 1.19 Théorème des deux carrés.

111 Anneaux principaux. Applications.

- ▷ 1.2 Algorithme des facteurs invariants.
- ▷ 1.19 Théorème des deux carrés.

112 Corps finis. Applications.

- ▷ 1.11 Polynômes irréductibles sur $\mathbb{F}_q$.
- ▷ 1.18 Théorème de Chevalley–Warning.

113 Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

- ▷ 1.6 Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$.

Analyse

Chapitre 1

Développements d'algèbre

1.1 Action de $PSL_2(\mathbb{R})$ sur le demi–plan de Poincaré

Référence :
- [Mé06], p. 568–570

Prérequis :
- espace $\mathbb{P}^1(\mathbb{C})$;
- homographies, birapport.

On considère le demi–plan de Poincaré, défini par $\mathcal{H} := \{z \in \mathbb{C} \,|\, \Im(z) > 0\} \cup \{\infty\} \subset \mathbb{P}^1(\mathbb{C})$. On appelle droite hyperbolique de $\mathcal{H}$ les demi–cercles (épointés) de $\mathcal{H}$ dont le centre est réel, ainsi que les demi–droites (toujours épointées) verticales (i.e parallèles à $i\mathbb{R}_+^*$) et on note D_h l'ensemble des telles droites.

Lemme 1.1
Soient z, w deux points distincts de $\mathcal{H}$.
Alors il existe une unique droite hyperbolique passant par z et w.

Démonstration :
- *Existence.* Soit $\mathcal{C}$ le cercle ou droite de $\mathbb{P}^1(\mathbb{C})$ passant par w, z et $\bar{z}$. On remarque alors que $\overline{[z, w, \bar{z}, \bar{w}]} = [z, w, \bar{z}, \bar{w}]$ donc $[z, w, \bar{z}, \bar{w}] \in \mathbb{R}$. De fait, les points $z, w, \bar{z}$ et $\bar{w}$ sont cocycliques ou alignés (nécessairement verticalement,h vu la présence des conjugués), i.e $\bar{w} \in \mathcal{C}$. De fait, comme le conjugué $\bar{\mathcal{C}}$ de $\mathcal{C}$ contient les quatre points $z, w, \bar{z}, \bar{w} \in \mathcal{C}$ on a $\mathcal{C} = \bar{\mathcal{C}}$.
  De fait, $\mathcal{C}$ est une droite verticale ou un cercle de centre réelle, ce qui signifie que $\mathcal{C} \cap \mathcal{H} \in D_h$, d'où l'existence d'une droite hyperbolique passant par z et w.
- *Unicité.* C'est immédiat : soit z et w sont alignés verticalement, auquel cas on a unicité de la droite verticale passant par ces deux points et absence de demi–cercle de centre réel faisant de même, soit ils ne le sont pas et auquel cas il existe un unique demi cercle de centre réel passant par z et w (car ce cercle doit nécessairement passer par —par exemple— $\overline{z}$).

Proposition 1.1
On a les deux propriétés suivantes :
(i) $PSL_2(\mathbb{R})$ agit transitivement sur $\mathcal{H}$;
(ii) $PSL_2(\mathbb{R})$ agit transitivement sur D_h.

Démonstration : Remarquons que deux matrices M et N donnent la même homographie si et seulement si il existe $\lambda \in \mathbb{R}$ tel que $M = \lambda N$; ainsi $PSL_2(\mathbb{R}) = \{h \in PGL_2(\mathbb{R}) \,|\, \det(h) > 0\}$: seul le signe du déterminant d'une homographie est bien défini.

(i) Soit $z \in \mathcal{H}$ et $h : z \mapsto \frac{az+b}{cz+d} \in PSL_2(\mathbb{R})$. Alors, si on pose $z = x + iy$ on a :

$$\begin{aligned} h(z) &= \frac{ax + b + iay}{cx + d + icy} \\ &= \frac{(ax + b + iay)(cx + d - icy)}{(cx + d)^2 + (cy)^2} \\ &= \frac{acx^2 + ad - iacyx + bcx + bd - ibcy + iacyx + iady + 1acy^2}{(cx + d)^2 + (cy)^2} \end{aligned}$$

De fait, $\Im(h(z))$ est du signe de $-bcy + ady = (ad - bc)\Im(y) > 0$ car $ad - bc > 0$. Ainsi, par stabilité, $PSL_2(\mathbb{R})$ agit sur $\mathcal{H}$. Enfin, $PSL_2(\mathbb{R})$ contient les translations et homothéties de rapport positif, d'où la transitivité (faire un dessin, sans oublier que l'on ne part jamais vraiment de l'axe réel donc que les homothéties positives font remonter "en diagonale").

(ii) Comme les homographies conservent les cercles ou droites, $PGL_2(\mathbb{R})$ agit naturellement sur l'ensemble des cercles ou droites de $\mathbb{P}^1(\mathbb{C})$. De plus, les homographies positives conservent $\mathcal{H}$ (cf. supra), donc on a bien une action de $PSL_2(\mathbb{R})$ sur D_h. Soit $z \in \mathcal{H}$ et soit $D \in D_h$ passant par z. D'après le point (i), il existe $g \in PSL_2(\mathbb{R})$ tel que $g(z) = i$: $g(D)$ est alors une droite hyperbolique passant par i.

Soit D_i une droite hyperbolique passant par i telle que $D_i \neq i\mathbb{R}_+^*$: c'est alors un demi–cercle coupant l'axe réel en deux points ; considérons l'un de ces points, soit t. Il existe alors un unique réel $\theta \in (-\pi, \pi)$ tel que $\tan(\theta) = t$. On note alors $h_\theta \in PSL_2(\mathbb{R})$ l'homographie associée à la rotation $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \in SL_2(\mathbb{R})$ et on remarque que :

$$\begin{aligned} h_\theta(i) &= \frac{i\cos(\theta) - \sin(\theta)}{i\sin(\theta) + \cos(\theta)} \\ &= e^{-i\theta}(i\cos(\theta) - \sin(\theta)) \\ &= e^{-i\theta} i(\cos(\theta) + \sin(\theta)) \\ &= i \end{aligned}$$

Ainsi $h_\theta \in \mathrm{Stab}_{PSL_2(\mathbb{R})}(i)$. De plus :

$$\begin{aligned} h_\theta(t) &= \frac{t\cos(\theta) - \sin(\theta)}{t\sin(\theta) + \cos(\theta)} \\ &= \frac{\tan(\theta)\cos(\theta) - \sin(\theta)}{t\sin(\theta) + \cos(\theta)} \\ &= 0 \end{aligned}$$

In fine, si on note D'_i le cercle ou droite correspondant à D_i dans $\mathbb{P}^1(\mathbb{C})$, $h_\theta(D'_i)$ passe par i et 0. Comme $h_\theta(D_i)$ est une droite hyperbolique, on a nécessairement $h_\theta(D'_i) = i\mathbb{R}$ et donc $h_\theta(D_i) = i\mathbb{R}_+^*$.

Ainsi, quitte à remplacer g par une composée de la forme $h_\theta \circ g$, avec θ bien choisi, on a $g(D) = i\mathbb{R}_+^*$: l'action considérée est bien transitive.

Détails supplémentaires :

- Soient quatre points $a, b, c, d \in \mathbb{P}^1(\mathbb{C})$; on suppose $[a, b, c, d] \in \mathbb{R}$. Notons h l'homographie définissant ce birapport, i.e telle que $h(a) = 0, h(b) = 1, h(c) = \infty$. Alors $h(a), h(b), h(c)$ et $h(d) = [a, b, c, d]$ sont alignés et comme l'homographie h^{-1} conserve les cercles ou droites on a bien que a, b, c et d sont alignés ou cocycliques.

1.2 Algorithme des facteurs invariants

Référence :

- [BMP05], p. 285–288

On se propose de démontrer de façon algorithmique l'existence[1] de la décomposition suivante :

Proposition 1.2
Soit $(\mathbb{A}, \delta)$ *un anneau euclidien.*
Soit $U \in \mathcal{M}_{m,n}(\mathbb{A})$.

1. Le lecteur averti aura remarqué qu'on peut également énoncer un résultat d'unicité de cette dernière. On peut d'ailleurs en trouver une démonstration dans [BMP05], p. 289.

Alors il existe $d_1, \ldots, d_s \in \mathbb{A}^*$ *tels que* $\forall i \in [s-1]$, $d_i | d_{i+1}$ *et* $(P, Q) \in GL_m(\mathbb{A}) \times GL_n(\mathbb{A})$ *tels que :*

$$U = PDQ, \text{ où } D := \begin{pmatrix} d_1 & & & (0) \\ & \ddots & & \\ & & d_s & \\ & & & (0) \\ (0) & & & \end{pmatrix}$$

On considère donc l'algorithme [2] suivant :

Algorithme 1.1 (Facteurs invariants)
`Entrée` *:* $U \in \mathcal{M}_{m,n}(\mathbb{A})$
`Sortie` *:* $D \in \mathcal{M}_{m,n}(\mathbb{A})$ *correspondant à la réduction de* U *donnée dans la proposition 1.2.*
On suit alors les étapes suivantes :

1. `Si` $U = 0$, *renvoyer* U. `Sinon`, *passer à l'étape* 2.
2. Choix d'un pivot. *Sélectionner* $(i_0, j_0) \in [m] \times [n]$ *tel que* $\delta(u_{i_0,j_0}) = inf\{\delta(u_{i,j}) \mid u_{i,j} \neq 0\}$. *Effectuer ensuite les opérations élémentaires suivantes :*

$$C_1 \leftrightarrow C_{j_0} \tag{1.2.1}$$
$$L_1 \leftrightarrow L_{i_0} \tag{1.2.2}$$

3. Traitement de la première colonne. *Initialiser un compteur* $i \leftarrow 2$.
   (a) *Par division euclidienne, on peut écrire (dans* $\mathbb{A}$*) :*

   $$u_{i,1} = u_{1,1}q + r_i, \text{ avec } r_i = 0 \text{ ou } \delta(r_i) < \delta(u_{1,1})$$

   Effectuer alors l'opération suivante :

   $$L_i \leftarrow L_i - qL_1 \tag{1.2.3}$$

   On a ainsi remplacé $u_{i,1}$ *par* r_i.

   (b) `Si` $r_i \neq 0$, *effectuer l'opération suivante :*

   $$L_i \leftrightarrow L_1 \tag{1.2.4}$$

   Retourner ensuite en 3.(a).

   (c) `Si` $r_i = 0$ *et* $i < m$, *incrémenter* i *(*$i \leftarrow i+1$*) et retourner en* 3.(a).

   (d) `Sinon` *passer à l'étape* 4. *On a désormais :*

   $$C_1 = \begin{pmatrix} u_{1,1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

4. Traitement de la première ligne. *Initialiser un compteur* $j \leftarrow 2$.
   (a) *Par division euclidienne on a :*

   $$u_{1,j} = u_{1,1}q + s_j, \text{ avec } s_j = 0 \text{ ou } \delta(s_j) < \delta(u_{1,1})$$

   Effectuer ensuite l'opération suivante :

   $$C_j \leftarrow C_j - qC_1 \tag{1.2.5}$$

   On a ainsi remplacé $u_{1,j}$ *par* s_j.

   (b) `Si` $s_j \neq 0$, *effectuer l'opération suivante :*

   $$C_j \leftrightarrow C_1 \tag{1.2.6}$$

   Retourner ensuite en 4.(a).

2. On ne se privera donc pas de faire usage des conventions d'écriture propres à l'algorithmique, par exemple en continuant de noter U notre matrice quelques soient les sévices que nous lui ferons subir.

(c) `Si` *$s_j = 0$ et $j < n$, incrémenter j et retourner en $4.(a)$.*

(d) `Sinon` *passer à l'étape 5. On a désormais :*

$$U = \begin{pmatrix} u_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ \vdots & & (*) & \\ 0 & & & \end{pmatrix}$$

5. Vérification de la divisibilité.

(a) `Si` *il existe $i_1, j_1 \geq 2$ tels que $u_{1,1} \nmid u_{i_1,j_1}$, effectuer l'opération suivante :*

$$C_1 \leftarrow C_1 + C_{j_1} \tag{1.2.7}$$

Retourner ensuite en 3.

(b) `Sinon` *retourner en 1 avec $U \leftarrow (u_{i,j})_{2 \leq i \leq m, 2 \leq j \leq n}$ (i.e on finit le traitement de façon récursive).*

TERMINAISON : L'idée est ici de montrer que chaque retour en arrière fait strictement décroître l'entier $\delta(u_{1,1})$. On conclura alors qu'il n'est possible d'effectuer qu'un nombre fini d'étapes et donc que l'algorithme termine.

Les étapes 1 et 2 ne posent pas de problèmes[3]. Lors de l'étape 3, on ne rebrousse chemin que si $r_i \neq 0$ (étape $3.(b)$) et alors on remplace $u_{1,1}$ par r_i ce que implique une décroissance stricte de $\delta(u_{1,1})$. Ceci ne pouvant de facto arriver qu'un nombre fini de fois, on passera[4] nécessairement à l'étape 4.

Durant l'étape 4, on ne retournera en arrière qu'à l'expresse condition que $s_j \neq 0$ $(4.(b))$. Comme précédemment, on en déduit qu'on passera nécessairement à l'étape 5.

Passer de l'étape 5 à une étape antérieure (en l'occurence 3) requière qu'il $i_1, j_1 \geq 2$ tels que $u_{1,1} \nmid u_{i_1,j_1}$. On remplace alors C_1 par $C_1 + C_{j_1}$ ce qui, au vu de l'état de notre matrice U, laisse $u_{1,1}$ inchangé et remplace $u_{i_1,1}$ par u_{i_1,j_1} et donc $r_{i_1} \neq 0$. Ainsi ce passage par l'étape 3 verra strictement décroître $\delta(u_{1,1})$; on ne pourra donc se permettre qu'un nombre fini de telles excentricités, entraînant que l'algorithme termine.

CORRECTION : Au bout d'une itération de l'algorithme (i.e avant de poursuivre récursivement) on obtient une matrice U' de la forme suivante[5] :

$$U' = \begin{pmatrix} u'_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ \vdots & & U_1 & \\ 0 & & & \end{pmatrix}$$

L'étape 5 nous assure par ailleurs que $u'_{1,1}$ divise tous les coefficients de U_1. Chaque étape de notre algorithme n'étant au final, une fois les tests conditionnels et autres fioritures éliminées, qu'une succession d'opérations élémentaires sur les lignes et colonnes, il existe $(P, Q) \in GL_m(\mathbb{A}) \times GL_n(\mathbb{A})$ telles que $U = PU'Q$.

De même, il va exister $(P_1, Q_1) \in GL_{m-1}(\mathbb{A}) \times GL_{n-1}(\mathbb{A})$ telles que $U_1 = P_1 U'_1 Q_1$, où :

$$U'_1 = \begin{pmatrix} u''_{2,2} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ \vdots & & U_2 & \\ 0 & & & \end{pmatrix}$$

3. Ou alors c'est que vous vous y prenez *très* mal ...
4. Un jour ...
5. Ce paragraphe contenant un raisonnement mathématique, il n'est plus réellement tolérable de continuer à la noter U. Ceci étant, chacun reste libre d'en faire à sa guise.

Ainsi, si on pose :

$$P_1' = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & P_1 & \\ 0 & & & \end{pmatrix} \quad \text{et} \quad Q_1' = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & Q_1 & \\ 0 & & & \end{pmatrix}$$

On a :

$$U = PP_1' \begin{pmatrix} u'_{1,1} & 0 & \dots & 0 \\ 0 & u''_{2,2} & & \\ \vdots & & & \\ \vdots & & U_2 & \\ 0 & & & \end{pmatrix} Q_1'Q$$

Comme nous n'avons effectué que des opérations élémentaires que que $u_{1,1}$ divisait tous les coefficients de U_1 il divise tous ceux de U_2 ainsi que $u''_{2,2}$. De plus l'étape 5 (itération 2) nous assure que $u''_{2,2}$ divise tous les coefficients de U_2. Par récurrence (utiliser l'invariant de boucle que l'on vient d'énoncer concernant la divisibilité), l'algorithme est correct.

1.3 Décomposition de Dunford

Références :
- [FGN09a] p.134–135 et [BMP05] p. 210–211 et 215–216.

Proposition 1.3 (Dunford)
Soit $\mathbb{K}$ un corps.
Soit E un $\mathbb{K}$–e.v de dimension finie.
Soit $f \in \mathcal{L}(E)$.
On suppose que χ_f est scindé sur $\mathbb{K}$.
Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que :

(i) *d soit diagonalisable ;*
(ii) *n soit nilpotent ;*
(iii) *$f = d + n$;*
(iv) *$n \circ d = d \circ n$.*

De plus, d et n sont alors des polynômes en f.

Démonstration :
- *Existence.* Comme χ_f est scindé on peut l'écrire sous la forme :

$$\chi_f = (-1)^n \prod_{i=1}^{s} (X - \lambda_i)_i^\alpha$$

Si on pose pour $i \in [s]$ $N_i := \ker(f - \lambda_i \mathrm{id}_E)^{\alpha_i}$ on a alors par lemme des noyaux appliqué à χ_f :

$$E = \ker(\chi_f(f)) = \bigoplus_{i=1}^{s} N_i$$

On définit alors d et n de la façon suivante :

$$\forall i \in [s],\ \forall x \in N_i,\ \begin{cases} d(x) := \lambda_i x \\ n(x) := f(x) - \lambda_i x \end{cases}$$

Il est alors clair que $d + n = f$, que d est diagonalisable (prendre une base adaptée à la décomposition $E = \oplus_{i=1}^{s} N_i$) et que :

$$\forall i \in [s],\ \forall x \in N_i,\ n^{\alpha_i}(x) = (f - \lambda_i \mathrm{id}_E)_i^\alpha(x) = 0$$

Ainsi, si on pose $\alpha := \max_i(\alpha_i)$ et si on décompose $x \in E$ en $x = x_1 + \ldots + x_s$, avec $\forall i \in [s]$, $x_i \in N_i$ alors :

$$\begin{aligned} n^\alpha(x) &= n^\alpha\left(\sum_{i=1}^{s} x_i\right) \\ &= \sum_{i=1}^{s} n^\alpha(x_i) \text{ par linéarité} \\ &= 0 \text{ car } n^\alpha = 0 \text{ sur chaque } N_i \end{aligned}$$

Donc n est bien nilpotent.
Si on note, pour $i \in [s]$, p_i le projecteur sur N_i parallèlement à $\oplus_{j\neq i} N_j$ on a de plus :

$$\begin{aligned} \forall x = x_1 + \ldots + x_s \in E, \text{ les } x_i \in N_i, \ \sum_{i=1}^{s} \lambda_i \underbrace{p_i(x)}_{=x_i} &= \sum_{i=1}^{s} \lambda_i x_i \\ &= \sum_{i=1}^{s} d(x_i) \\ &= d(x) \end{aligned}$$

I.e :

$$d := \sum_{i=1}^{s} \lambda_i p_i \tag{1.3.1}$$

Démontrons à présent que les p_i sont des polynômes en f. Les polynômes $(X - \lambda_i)^{\alpha_i}$ étant premiers entre eux, le théorème chinois nous affirme l'existence de $P \in \mathbb{K}[X]$ tel que :

$$\forall i \in [s], \qquad P \equiv \lambda_i[(X - \lambda_i)^{\alpha_i}]$$

Formulé autrement, ceci signifie que pour tout $i \in [s]$ il existe $R_i \in \mathbb{K}[X]$ tel que :

$$P = \lambda_i + R_i(X - \lambda_i)^{\alpha_i}$$

Or, par décomposition en sous–espaces caractéristiques (cf. supra), tout élément $x \in E$ admet une unique écriture sous la forme $x = x_1 + \ldots + x_s$ avec pour tout $i \in [s]$ $x_i \in N_i$. De plus :

$$\forall i \in [s], \qquad P(f)(x_i) = \lambda_i x_i + R_i(f) \circ (f - \lambda_i \mathrm{id}_E)^{\alpha_i}(x_i) = \lambda_i x_i$$

Ainsi :

$$\forall x \in E, \qquad P(f)(x) = d(x)$$

Et donc $d = P(f)$ est bien un polynôme en f, donc $n = u - d$ également. Ceci implique naturellement que d et n commutent.

– *Unicité.* Soient d' et n' vérifiant (i), (ii), (iii) et (iv). Comme d' (resp. n') commute avec n' (resp. d') (par hypothèse (iv)) et avec lui–même, il commute avec $f = d' + n'$ (hypothèse (iii)) donc avec les polynômes en f. En particulier d commute avec d' et n avec n'. Le premier résultat implique que d et d' sont co–diagonalisables et donc que $d - d'$ est diagonalisable, le second que $n' - n$ est nilpotente. De fait l'endomorphisme $d - d' = n' - n$ est diagonalisable et nilpotent, donc nul, d'où le résultat.

Corollaire 1.3.1
Soit $f \in \mathcal{L}(\mathbb{C}^d)$.
Alors :

$$\exp(f) \textit{ est diagonalisable } \Leftrightarrow f \textit{ est diagonalisable}$$

Démonstration :

$(\Leftarrow)$ Immédiat.

($\Rightarrow$) Notons $f = d + n$ la décomposition de Dunford de f (avec notations évidentes). D'après la proposition 1.4, il existe un endomorphisme nilpotent n' tel que $\exp(n) = n' + \mathrm{id}_{\mathbb{C}^d}$ et donc, comme n et d commutent, on a :

$$\exp(f) = \exp(d) + \exp(d)n' \tag{1.3.2}$$

Or, toujours comme d et n commutent, e^d et e^n commutent et donc e^d et $n' = e^n - \mathrm{id}_{\mathbb{C}^d}$ également. De fait e^d et $e^d n'$ commutent. Or e^d est diagonalisable et $e^d n'$ nilpotent donc par unicité la décomposition de Dunford de e^f est donnée la relation (1.3.2) et donc nécessairement, comme e^f est diagonalisable on a $e^d n' = 0$. Comme $e^d \in GL(\mathbb{C}^d)$, on a $n' = 0$ d'où $e^n = \mathrm{id}_{\mathbb{C}^d}$ ce qui implique (toujours par la proposition 1.4) que $n = 0$. D'où le résultat.

Détails supplémentaires :

– *$n' - n$ est nilpotente.* Supposons que $n^p = 0$ et $n'^q = 0$. Alors :

$$(n' - n)^{p+q} = \sum_{i=1}^{p+q} C_{p+q}^i {n'}^i (-1)^{p+q-i} n^{p+q-i} \text{ car } n \text{ et } n' \text{ commutent}$$

Or si $i < q$, $p + q - i > p$ et donc $n^{p+q-i} = 0$; et si $i \geq q$ alors ${n'}^i = 0$. In fine $(n' - n)^{p+q} = 0$ d'où le résultat (cf. [Gou94], p. 191).

– *Une autre démonstration du fait que d et n sont des polynômes en u peut être trouvée dans [Gou94], p. 192.* Pour $i \in [s]$ on définit le polynôme suivant :

$$Q_i := \prod_{j \neq i} (X - \lambda_j)^{\alpha_j}$$

Les Q_i sont premiers entre eux et donc par identité de Bézout il existe $U_1, \ldots, U_s \in \mathbb{K}[X]$ tels que :

$$\sum_{i=1}^{s} U_i Q_i = 1 \tag{1.3.3}$$

Posons $\forall i \in [s]$, $f_i := U_i Q_i(f) = U_i(f) \circ Q_i(f)$ et montrons que $f_i = p_i$ ce qui donnera le résultat voulu. Fixons $i \in [s]$.

* Pour tous $i \neq j$, $\chi_f | Q_i Q_j$ donc :

$$\forall i \neq j \; f_i \circ f_j = U_i Q_i(f) \circ U_j Q_j(f) = U_i U_j(f) \circ Q_i Q_j(f) = 0 \tag{1.3.4}$$

Or d'après (1.3.3) :

$$f_i = \mathrm{id}_E \circ f_i = \left(\sum_{j=1}^{s} U_j Q_j(f) \right) \circ f_i = \sum_{j=1}^{s} f_j \circ f_i = f_i^2$$

Donc les f_i sont bien des projecteurs.

* Montrons que $(Im)(f_i) = N_i$.

Soit $y = f_i(x) \in (Im)(f_i)$. Alors :

$$\begin{aligned}(f - \lambda_i \mathrm{id}_E)^{\alpha_i}(y) &= (X - \lambda_i)^{\alpha_i}(f) \circ U_i Q_i(f) \\ &= U_i(f) \circ (X - \lambda_i)^{\alpha_i} Q_i(f) \\ &= U_i(f) \circ \chi_f(f) \\ &= 0\end{aligned}$$

Donc $y \in N_i$.

Réciproquement, si $x \in N_i$ alors par (1.3.3) on a $x = \sum_j f_j(x)$. Or, si $j \neq i$ $f_j(x) = U_j(f) \circ Q_j(f) = 0$ car $(X - \lambda_i)^{\alpha_i} | Q_j$. In fine $x = f_i(x) \in \mathrm{Im}(f_i)$.

* Montrons que $\ker(f_i) = \oplus_{j \neq i} N_j$.

Si $j \neq i$ et $x \in N_j$ alors $f_i(x) = U_i(f) \circ Q_i(f) = 0$ car $(X - \lambda_j)^{\alpha_j} | Q_i$. La somme directe étant le sous espace vectoriel engendré par la réunion on a alors $\oplus_{j \neq i} N_j \subset \ker(f_i)$.

Réciproquement, si $x \in E$ vérifie $f_i(x) = 0$ alors par (1.3.3) $x = \sum_{j \neq i} f_j(x)$. Or $\forall j \in s$, on a montré que $f_j(x) \in N_j$, d'où l'inclusion réciproque et le résultat.

– On admet le résultat suivant (cf. [MT97]) :

Proposition 1.4
On note $\mathcal{N}$ (resp. $\mathcal{U}$) l'ensemble des endomorphisme nilpotents (resp. unipotents) de $\mathbb{C}^d$. Alors les applications suivantes sont des homéomorphismes :

$$\begin{aligned} \mathcal{N} &\to \mathcal{U} \\ n &\mapsto \exp(n) \end{aligned}$$

Et :

$$\begin{aligned} \mathcal{U} &\to \mathcal{N} \\ u &\mapsto u - \mathrm{id}_{\mathbb{C}^d} \end{aligned}$$

1.4 Dual de $\mathcal{M}_n(\mathbb{K})$

Référence :
– [FGN07], p. 329–331

Proposition 1.5
Soit $\mathbb{K}$ un corps.
Pour $A \in \mathcal{M}_n(\mathbb{K})$ on définit l'application suivante :

$$\begin{aligned} f_A : \mathcal{M}_n(\mathbb{K}) &\to \mathbb{K} \\ X &\mapsto \mathrm{Tr}(AX) \end{aligned}$$

Alors l'application suivante est un isomorphisme :

$$\begin{aligned} f : \mathcal{M}_n(\mathbb{K}) &\to \mathcal{M}_n(\mathbb{K})^* \\ A &\mapsto f_A \end{aligned}$$

Démonstration : Il est clair que f est linéaire et il ne nous reste qu'à (par un argument de dimension) montrer que f est injective ; soit donc $A \in \ker(f)$. Alors, si on note $(E_{i,j})_{i,j}$ la base canonique de $\mathcal{M}_n(\mathbb{K})$ on a, pour tous $i_0, j_0 \in [n]$:

$$\begin{aligned} 0 &= \mathrm{Tr}(AE_{i_0,j_0} \\ &= \mathrm{Tr}\left(\left(\sum_{i=1}^n \sum_{j=1}^n a_{i,j}E_{i,j}\right) E_{i_0,j_0}\right) \\ &= \sum_{i=1}^n a_{i,i_0}\mathrm{Tr}\left(E_{i,j_0}\right) \text{ car } E_{i,j}E_{k,\ell} = \delta_{j,k}E_{i,\ell} \\ &= a_{j_0,i_0} \end{aligned}$$

Et donc $A = 0$, d'où le résultat.

Corollaire 1.5.1
Soit $\mathbb{K}$ un corps.
Soit $\phi \in \mathcal{M}_n(\mathbb{K})^*$ telle que :

$$\forall X, Y \in \mathcal{M}_n(\mathbb{K}), \quad \phi(XY) = \phi(YX)$$

Alors :

$$\exists \lambda \in \mathbb{K}, \, \phi = \lambda \mathrm{Tr}$$

Démonstration : Soit A tel que $\phi = f_A$. Alors l'hypothèse se réécrit :

$$\forall X, Y \in \mathcal{M}_n(\mathbb{K}), \quad \mathrm{Tr}(AXY) = \mathrm{Tr}(AYX)$$

Or, si $X, Y \in \mathcal{M}_n(\mathbb{K})$ $\mathrm{Tr}(AYX) = \mathrm{Tr}(XAY)$ et donc on a :

$$\forall X, Y \in \mathcal{M}_n(\mathbb{K}), \quad \mathrm{Tr}((AX - XA)Y) = 0$$

Et donc, par injectivité de f on a :

$$\forall X \in \mathcal{M}_n(\mathbb{K}), \quad AX = XA$$

Ce qui signifie que pour tous $i, j \in [n]$ on a $AE_{i,j} = E_{i,j}A$ soit :

$$\sum_{k=1}^{n} a_{k,i} E_{k,j} = \sum_{k=1}^{n} a_{j,k} E_{i,k}$$

Et donc pour tous $i, j \in [n]$ $a_{i,i} = a_{j,j}$ et tous les autres coefficients de A sont nuls. De fait, il existe $\lambda \in \mathbb{K}$ tel que $A = \lambda I_n$, d'où le résultat.

Corollaire 1.5.2
Soit $\mathbb{K}$ un corps.
Alors tout hyperplan de $\mathcal{M}_n(\mathbb{K})$ coupe $GL_n(\mathbb{K})$.

DÉMONSTRATION : Soit $\mathcal{H}$ un tel hyperplan ; alors il existe une forme linéaire non nulle ϕ telle que $\mathcal{H} = \ker(\phi)$. Soit alors $A \in \mathcal{M}_n(\mathbb{K})$ tel que $\phi = f_A$ et posons $r := \mathrm{rg}(A)$. On sait qu'alors il existe $P, Q \in GL_n(\mathbb{K})$ telles que $A = PJ_rQ$, où J_r est la matrice par blocs $\begin{pmatrix} I_r & (0) \\ (0) & (0) \end{pmatrix}$.

De fait, si $X \in \mathcal{M}_n(\mathbb{K})$, on a :

$$\begin{aligned} \phi(X) &= \mathrm{Tr}(AX) \\ &= \mathrm{Tr}(PJ_rQX) \\ &= \mathrm{Tr}(J_rQXP) \end{aligned}$$

Pour peu que l'on puisse trouver une matrice $Y \in \mathcal{M}_n(\mathbb{K})$ telle que $\mathrm{Tr}(J_rY) = 0$, on aura le résultat en posant $X = Q^{-1}YP^{-1}$. Or la matrice suivante convient :

$$Y := \begin{pmatrix} 0 & \dots & \dots & 0 & 1 \\ 1 & & & \vdots & 0 \\ 0 & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

1.5 Groupes d'ordre pq

Référence :
- [Per96], p. 27–28

Prérequis :
- théorème de Sylow.

Proposition 1.6
Soient p, q deux nombres premiers tels que $p < q$.
Alors :

(i) si $p \nmid q - 1$ tout groupe d'ordre pq est cyclique ;

(ii) si $p \mid q - 1$ il existe exactement (à isomorphisme près) deux groupes d'ordre pq : le groupe cyclique et un produit semi–direct non abélien.

DÉMONSTRATION : Soit G un groupe d'ordre pq. Si on note c_q le nombre de q–Sylow de G, le théorème du éponyme nous affirme que $c_q | p$ et $c_q \equiv 1[q]$. De fait $c_q = 1$ et donc l'unique q–Sylow $S_q \cong \mathbb{Z}/q\mathbb{Z}$ de G vérifie $S_q \lhd G$. De fait, si on se donne un p–Sylow $S_p \cong \mathbb{Z}/p\mathbb{Z}$ de G on a, comme $|G| = |S_p||S_q|$ et $S_p \cap S_q = \{e\}$ que $G \cong S_q \rtimes_\varphi S_p \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ avec φ un morphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

Soit donc φ un morphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Alors si $a \in \mathbb{Z}/p\mathbb{Z}$ on a $\mathrm{id} = \varphi(pa) = \varphi(a)^p$ et donc l'ordre $\omega(a)$ de $\varphi(a)$ divise p donc $\omega(a) \in \{1, p\}$. De plus, par théorème de Lagrange, $\omega(a) \mid q - 1$.

- *Cas 1 :* $p \nmid q-1$. Alors $\omega(a) = 1$ et donc φ est le morphisme trivial, ce qui implique que notre produit semi–direct est en fait direct et donc $G \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.
- *Cas 2 :* $p \mid q-1$. Alors $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ possède un unique sous–groupe d'ordre p, soit H. Comme de plus $|\mathrm{Im}(\varphi)| \leq p$ et$p \nmid |\mathrm{Im}(\varphi)|$ (car comme φ est non trivial son image possède un élément d'ordre p), on a soit $|\mathrm{Im}(\varphi)| = 1$, auquel cas on retombe sur le produit direct, soit $|\mathrm{Im}(\varphi)| = p$ auquel cas $\mathrm{Im}(\varphi) = H$.
  Dans ce second cas, si on se donne ψ un morphisme *non trivial* de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ alors $\mathrm{Im}(\psi) = H$. Alors φ (resp. ψ) induit un morphisme surjectif $\hat{\varphi}$ (resp. $\hat{\psi}$) de $\mathbb{Z}/p\mathbb{Z}$ sur H. Par un argument de cardinaux, on a que $\hat{\varphi}$ et $\hat{\psi}$ sont des isomorphismes et donc $\alpha := \hat{\psi}^{-1} \circ \hat{\varphi}$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. On peut alors définir l'application suivante :
  $$\begin{aligned} A : \mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/q\mathbb{Z} \rtimes_{\psi} \mathbb{Z}/p\mathbb{Z} \\ (k,l) &\mapsto (k, \alpha(l)) \end{aligned}$$
  A définit clairement un morphisme de groupes injectif donc bijectif (cardinaux) et donc on a bien $\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/p\mathbb{Z} \cong ZZ/q\mathbb{Z} \rtimes_{\psi} \mathbb{Z}/p\mathbb{Z}$ d'où le résultat.

Détails supplémentaires :

- Cas $p = 2$. Le produit semi–direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est alors le groupe diédral D_q. En effet si on pose $s := (0,1)$ et $r := (1,0)$ alors $\{r,s\}$ engendre le produit semi–direct et comme le seul morphisme non trivial de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est $x \mapsto (-1)^x\mathrm{id}$ (i.e $(i,j)*(k,\ell) = (i+(-1)^j k, j\ell)$ on a :
  $$\begin{aligned} s^2 &= (0,1)*(0,1) = (0,1+1) = (0,0) \\ r^q &= (1,0)^{*q} = (q,0) = (0,0) \end{aligned}$$
  $$s*r*s = (0,1)*(1,0)*(0,1) = (0,1)*(1+(-1)^0*0,1) = (0-1,0) = (-1,0) = (q-1,0) = r^{-1}$$
  D'où le résultat.

1.6 Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$

Référence :

- [Gou94], p. 92 – 94

Soit $n \geq 1$. Dans toute la suite on notera ϕ_n le n–ième polynôme cyclotomique sur $\mathbb{C}$. On rappelle que :
$$X^n - 1 = \prod_{d|n} \phi_d$$

Proposition 1.7
ϕ_n est irréductible sur $\mathbb{Q}$.

Démonstration : Comme $\mathbb{Q}[X]$ est factoriel (car $\mathbb{Q}$ l'est [6]), il existe un (unique) r–uplet $(G_1, \ldots, G_r) \in \mathbb{Q}[X]^n$ tel que :
$$\phi_n = \prod_{i=1}^{r} G_i$$
De plus, à $i \in [r]$ fixé, il existe $\alpha_i \in \mathbb{N}^*$ tel que $\alpha_i G_i \in \mathbb{Z}[X]$ (prendre le ppcm des dénominateurs des coefficients de G_i, par exemple). De fait :
$$\left(\prod_{i=1}^{r} \alpha_i\right) \phi_n = \prod_{i=1}^{r} \alpha_i G_i$$
D'après le lemme de Gauss (lemme 1.3), on a alors (la première égalité découlant du fait que ϕ_n est unitaire) :
$$\prod_{i=1}^{r} \alpha_i = c\left(\left(\prod_{i=1}^{r} \alpha_i\right) \phi_n\right) = \prod_{i=1}^{r} c(\alpha_i G_i)$$

6. C'est un corps !

Posons pour $i \in [r]$ $F_i := \dfrac{\alpha_i G_i}{c(\alpha_i G_i)}$. Alors :

$$\forall i \in [r],\ F_i \in \mathbb{Z}[X] \text{ est unitaire et irréductible sur } \mathbb{Q} \text{ et } \phi_n = \prod_{i=1}^{r} F_i$$

On se maintenant propose de démontrer par récurrence sur $s \geq 1$ la propriété suivante : *pour tout entier $s \geq 1$, pour tout entier k premier avec n de décomposition en produit de facteurs premiers*[7] *$k = p_1 \dots p_s$ et pour toute racine ξ de F_1, on a $F_1(\xi^k) = 0$.*

- $s = 1$. Soit ξ une racine de F_1 et soit p un nombre premier tel que $p \nmid n$. On se propose de montrer que $F_1(\xi^p) = 0$. Pour commencer, remarquons que ξ est une racine de ϕ_n donc une racine primitive n–ième de l'unité. Comme $p \wedge n = 1$, ξ^p est également un racine primitive n–ième de l'unité donc une racine de ϕ_n, ergo il existe $i \in [r]$ tel que $F_i(\xi^p) = 0$
  Supposons à présent que $F_1(X)$ et $F_i(X^p)$ soient premiers entre eux dans $\mathbb{Q}[X]$. Alors (lemme de Bézout) :
  $$\exists U, V \in \mathbb{Q}[X], \quad U(X)F_1(X) + V(X)F_i(X^p) = 1$$
  En évaluant cette égalité en "$X = \xi$", on obtient la contradiction[8] $1 = 0$. Or F_1 est irréductible sur $\mathbb{Q}$ donc on a nécessairement $F_1(X)|F_i(X^p)$ dans $\mathbb{Q}[X]$. Comme le coefficient dominant de F_1 est inversible dans $\mathbb{Z}$ on a de plus que $F_1(X)|F_i(X^p)$ dans $\mathbb{Z}[X]$ (même raisonnement que dans l'hérédité du lemme 1.2). Si on note, pour $P \in \mathbb{Z}[X]$, $\overline{P} \in \mathbb{F}_p[X]$ la classe de P modulo p, on a alors $\overline{F_1}(X)|\overline{F_i}(X^p) = \overline{F_i}(X)^p$ dans $\mathbb{F}_p[X]$.
  Soit à présent $\overline{P} \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{F_1}$ sur $\mathbb{F}_p$. Alors $\overline{P} \mid \overline{F_i}^p$ donc par irréductibilité de $\overline{P}$ $\overline{P}|\overline{F_i}$ et donc si $i \neq 1$ $\overline{P}^2 \mid \overline{\phi_n}$. Posons :
  $$R := \prod_{d|n,\, d \neq n} \phi_d$$
  Alors $X^n - 1 = \phi_n R$ et donc $X^n - \overline{1} = \overline{P}^2 \overline{S}$, où $S \in \mathbb{Z}[X]$. En dérivant (formellement) cette égalité on obtient que $\overline{n}X^{n-1} = 2\overline{PP'S} + \overline{P}^2\overline{S'}$, ergo $\overline{P}|\overline{n}X^{n-1}$ dans $\mathbb{F}_p[X]$. Or $\overline{P}|X^n - \overline{1}|\overline{n}X^n - \overline{n}$ ainsi par différence $\overline{P}|\overline{n} \neq 0$ donc $\overline{P}$ est constant ce qui est absurde.
  In fine $F_1(\xi^p) = 0$.
- Supposons la propriété vérifiée au rang $s \geq 1$. Soit ξ une racine de F_1 et $k = p_1 \dots p_{s+1}$ un entier premier avec n. Alors l'entier $p_1 \dots p_s$ l'est également et donc par hypothèse de récurrence $F_1(\xi^{p_1 \cdots p_s}) = 0$. De plus $p_{s+1} \wedge n = 1$ (car $p_{s+1} \nmid n$) donc comme la propriété est vraie au rang 1 et que $\xi^{p_1 \cdots p_s}$ est une racine de F_1 on a $F(\xi^{(p_1 \cdots p_s) p_{s+1}}) = 0$, d'où le résultat.

Pour conclure, fixons une racine ξ de F_1. Alors ξ est une racine de ϕ_n et donc $\mu_n^*(\mathbb{C}) = \{\xi^k \mid k \wedge n = 1\}$. De fait, les racines de ϕ_n sont comprises dans celles de F_1 donc $\phi_n | F_1$. Or $F_1 | \phi_n$ et ces deux polynômes sont unitaires ergo $F_1 = \phi_n$, d'où le résultat.

Détails supplémentaires :

- Présentons d'abord un lemme sans lequel notre développement n'a pas grand sens :

  Lemme 1.2
  $\phi_n \in \mathbb{Z}[X]$.
  DÉMONSTRATION : On le démontre par récurrence sur $n \geq 1$.
  - $n = 1$. $\phi_1 = (X - 1) \in \mathbb{Z}[X]$.
  - Supposons la propriété validée pour tous $k \leq n$, avec $n \geq 1$. Alors, par hypothèse de récurrence :
    $$P := \prod_{d|n+1,\, d<n+1} \phi_d \in \mathbb{Z}[X]$$
    De plus, $X^{n+1} - 1 = P\phi_{n+1}$. P est de coefficient dominant inversible dans $\mathbb{Z}$ donc il existe $Q, R \in \mathbb{Z}[X]$ tels que $X^{n+1} - 1 = PQ + R$, avec $\deg(R) < \deg(P)$. Par division euclidienne,

7. Notons qu'alors aucun des p_i ne peut diviser n.
8. Car $\mathbb{Q}$ est un corps donc distinct de l'anneau trivial.

de tels Q, R sont uniques dans $\mathbb{C}[X]$ donc dans $\mathbb{Z}[X]$ et donc $R = 0$ et $Q = \phi_{n+1}$, d'où le résultat.
- On trouve le résultat suivant dans [Gou94], p.58 :

Lemme 1.3 (Gauss)
Soient $P, Q \in \mathbb{Z}[X]$.
Alors $c(PQ) = c(P)c(Q)$.
Démonstration : Posons $P_1 := \dfrac{1}{c(P)}P$ et $Q_1 := \dfrac{1}{c(Q)}Q$. Alors $P_1, Q_1 \in \mathbb{Z}[X]$ et $c(P_1) = c(Q_1) = 1$.
Supposons $c(P_1Q_1) > 1$. Alors il existe un nombre premier p divisant $c(P_1Q_1)$, donc divisant tous les coefficients de P. De fait on a, dans $\mathbb{F}_p[X]$:

$$\overline{P_1Q_1} = \overline{P_1}\,\overline{Q_1} = \overline{0}$$

Comme $\mathbb{F}_[X]$ est intègre, on a donc que p divise tous les coefficients de P_1 ou tous les coefficients de Q_1, ce qui est impossible. Ainsi $c(P_1Q_1) = 1$. In fine :

$$c(PQ) = c(P)c(Q)c(P_1Q_1) = c(P)c(Q)$$

- Soit $\mathbb{K}$ un corps et soit $\xi \in \mu_n^*(\mathbb{K})$. Alors par définition $\{\xi^k \mid k \in \mathbb{N}\} = \mu_n(\mathbb{K})$. De plus, si on se donne k premier avec n et que l'on suppose qu'il existe $j < n$ tel que $(\xi^k)^j = 1$ alors par théorème de Lagrange appliqué à ξ dans le groupe $\mu_n(\mathbb{K})$, $n|kj$ et donc comme $k \wedge n = 1$ par lemme de Gauss on a que $n|j$, ce qui est impossible. Donc $\{\xi^k \mid k \wedge n = 1\} \subset \mu_n^*(\mathbb{K})$. Réciproquement si k et n ont un diviseur commun non trivial u, avec $n = un_1$ et $k = uk_1$, alors $(\xi^k)^n_1 = \xi^{uk_1n_1} = \xi^{nk_1} = 1$, avec $n_1 < n$ ergo $\xi^k \notin \mu_n^*(\mathbb{K})$. In fine :

$$\{\xi^k \mid k \wedge n = 1\} = \mu_n^*(\mathbb{K})$$

- Soit $P \in \mathbb{Z}[X]$. Alors on a, dans $\mathbb{F}_p[X]$, $\overline{P}(X^p) = \overline{P}(X)^p$. Démontrons le par récurrence (forte) sur $m = \deg(P)$.
  - $m = -\infty$. Chut.
  - $m = 0$. Trivial
  - Supposons la propriété vraie au rang $m \geq 1$. Alors $P = G + aX^{m-1}$, avec $\deg(P) \leq m$. Le résultat découle alors de l'identité de Frobenius : *si $\mathbb{A}$ est un anneau commutatif de caractéristique p alors $x \mapsto x^p$ est un endomorphisme d'anneau.* Ce dernier résultat suinte à son tour de la tristement célèbre formule du binôme de Newton et du fait que si $1 \leq k \leq p-1$ alors comme $p|k!(p-k)!C_p^k = p!$ et que $p \wedge k!(p-k)! = 1$ le lemme de Gauss nous affirme[9] que $p|C_p^k$ et donc que $C_p^k \equiv 0[p]$.

1.7 Isométries du cube

Référence :
- [Ale99], p. 64–66

On considère le cube C_6 centré en l'origine O canonique de l'espace $\mathbb{R}^3$ (cf. figure 1.7). On note G le sous–groupe des isométries affines de l'espace conservant C_6 et G^+ le sous–groupe de G formé des transformations de déterminant positif.

Notons $\mathcal{D} := \{D_1, \ldots, D_4$ l'ensemble des grandes diagonales (i.e passant par O) de C_6 (en orange sur la figure 1.7). Alors, comme G conserve les distances, que la longueur commune à chaque élément de $\mathcal{D}$ est la plus grande distance possible entre deux points du cube et que cette propriété caractérise $\mathcal{D}$, G agit sur $\mathcal{D}$. Ceci nous livre un morphisme de groupes :

$$\rho : G \to \mathfrak{S}(\mathcal{D}) \cong \mathfrak{S}_4$$

Une symétrie axiale (ou rotation d'angle π) par rapport à un axe reliant les milieux de deux côtés et passant par 0 réalise (au sens de ρ) une transposition ; par exemple, la symétrie par rapport à (MN) échange $[AG]$ et $[CE]$. Ainsi, comme on peut réaliser toutes les transpositions de $\mathcal{S}_4$, ρ est surjectif.

9. À raison.

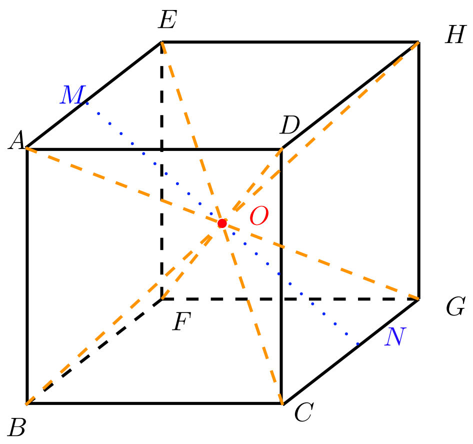


FIGURE 1.1 – Le cube C_6

Soit à présent $f \in \ker(\rho)$, que l'on suppose différente de l'identité. En pratique, cela signifie que $\forall i \in [4]$, $f(D_i) = D_i$ mais qu'il existe un indice i_0 tel que f échange les sommets de D_{i_0}. On peut, sans perdre de généralité [10] supposer que $f(A) = G$. Alors $f(B) \in \{B, H\}$ et $d(f(A), f(B)) = d(A, B)$ donc on a nécessairement $f(B) = H$. En itérant ce procédé, on trouve que f échange les sommets de toutes les grandes diagonales de C_6, ergo f est la symétrie s_O par rapport à l'origine (car elle lui est égale sur les sommets donc sur tout le cube qui est l'enveloppe convexe de ces derniers). On en déduit donc que :

$$\ker(\rho) = \{\mathrm{id}_{\mathbb{R}^3}, s_O\}$$

De fait on obtient un isomorphisme :

$$G/\{\mathrm{id}_{\mathbb{R}^3}, s_O\} \cong \mathfrak{S}_4$$

Les classe modulo $\ker(\rho)$ sont de la forme $\{f, s_0 \circ f\}$. Or $\det(s_0 \circ f) = \det(s_O)\det(f) = -\det(f)$. De fait, chaque classe d'équivalence contient exactement un déplacement (et un antidéplacement), ce qui signifie que :

$$G/\{\mathrm{id}_{\mathbb{R}^3}, s_O\} \cong G^+$$

On en déduit alors par composition que :

$$G^+ \cong \mathfrak{S}_4 \tag{1.7.1}$$

On remarque à présent que, si on pose $\mathbf{C} := \langle s_O \rangle = \{\mathrm{id}_{\mathbb{R}^3}, s_O\} \cong \mathbb{Z}/2\mathbb{Z}$, on a :

- $|G| = |G^+||\mathbf{C}|$, égalité obtenue car $\mathbf{C} = \ker(\rho)$ et que $G/\ker(\rho) \cong \mathfrak{S}_4 \cong G^+$ d'après ce qui précède ;
- $G^+ \cap \mathbf{C} = \{\mathrm{id}_{\mathbb{R}^3}\}$ car $\det(s_O) = -1$;
- $G^+ \lhd G$ car $(G : G^+) = 2$;

De fait on a :

$$G \cong G^+ \rtimes \mathbf{C}$$

De plus, $\mathbf{C} \lhd G$ car $\mathbf{C} = \ker(\rho)$. En particulier, si $a \in G$, $as_O = as_O a^{-1} a \in \{a, s_O a\}$ et comme s_O est inversible on a nécessairement $as_O = s_O a$. La conjugaison par $\mathbf{C}$ étant triviale, le produit semi–direct interne ci–dessus est direct.

In fine, on a l'isomorphisme suivant :

$$G \cong G^+ \times \mathbf{C} \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z} \tag{1.7.2}$$

Détails supplémentaires :

- On peut donner un "dictionnaire" de l'isomorphisme $G^+ \cong \mathfrak{S}_4$.
  * L'identité . . . Ahem.

10. Car après tout, qu'est-ce qu'un nom ?

* Les transpositions sont réalisées comme on l'a vu par les retournements d'axes joignant les milieux de deux côtés en passant par O.
* Les 3–cycles sont réalisés par les rotations d'angle (géométrique) $\frac{2\pi}{3}$ autour de l'une des diagonales. Par exemple, le 3–cycle (1 2 3) (où l'on identifie *naturellement*[11] $\mathfrak{S}(\mathcal{D})$ à $\mathfrak{S}_4$ via $D_i \mapsto i$) a pour axe D_4.
* Les 4–cycles correspondent quant à eux aux rotations d'angle $\frac{\pi}{2}$ autour d'un axe orthogonal à 2 faces du cube.
* Les doubles–transpositions sont réalisés par le carré de l'une des rotations d'angle $\frac{\pi}{2}$ ci–dessus.

Au final on a :

▷ 6 axes d'ordre 2 (pour 6 transpositions) ;

▷ 4 axes d'ordre 3 (pour 8 3–cycles : une rotation d'angle $\frac{2\pi}{3}$ et une d'angle $-\frac{2\pi}{3}$) ;

▷ 3 axes d'ordre 4 (pour 6 4–cycles).

1.8 Partitions d'un entier en parts fixées

Référence :

– [FGN09b], p. 194–196

Proposition 1.8
Soient $a_1, \ldots, a_k \in \mathbb{N}^*$ premiers entre eux dans leur ensemble.
Pour $n \geq 1$ on pose (avec la convention $u_0 = 0$) :

$$u_n := \operatorname{card}\left(\left\{(x_1, \ldots, x_k) \in \mathbb{N}^k \;\middle|\; \sum_{i=1}^{k} a_i x_i = n\right\}\right)$$

Alors on a l'équivalent suivant :

$$u_n \sim_{n\to\infty} \frac{1}{a_1 \ldots a_k} \frac{n^{k-1}}{(k-1)!}$$

Démonstration : Pour tout $i \in [k]$, la série entière $\sum_{(x)} z^{x a_i}$ a pour rayon de convergence 1 (le lecteur avisé vérifiera aisément que $|z^{a_i}| < 1 \Leftrightarrow |z| < 1$ et pour tout $n \geq 0$ le coefficient en z^n dans le produit de Cauchy de ces dernières séries est :

$$\sum_{\underline{x} \in \mathbb{N}^k,\, \sum a_i x_i = n} 1 = u_n$$

De fait, si $|z| < 1$ on peut définir :

$$f(z) := \sum_{n=0}^{\infty} u_n z^n = \prod_{i=1}^{k} \left(\sum_{x=0}^{\infty} z^{x a_i}\right) = \prod_{i=1}^{k} \frac{1}{1 - z^{a_i}}$$

f est alors une fraction rationnelle[12] donc les pôles sont les racines $a_1, \ldots, a_{k-1}$ et a_k–ièmes de l'unité. 1 est un pôle de multiplicité k et tous les autres sont de multiplicité au plus $k-1$; en effet si $\omega \in \mathbb{C}$ vérifie que $\forall i \in [k]$, $\omega^{a_i} = 1$ alors, comme les a_i sont premiers entre eux, le théorème de Bézout nous affirme l'existence de $\underline{u} \in \mathbb{N}^k$ tel que $\sum_i u_i a_i = 1$ et donc :

$$\omega = \omega^{\sum_i u_i a_i} = \prod_{i=1}^{k} (\omega^{a_i})^{u_i} = 1$$

Notons $P := \{\omega_1, \ldots, \omega_p\}$ l'ensemble des pôles de f, avec $\omega_1 = 1$. Alors, par décomposition en éléments simples, il existe une famille de nombres complexes $(c_{i,j})_{1 \leq i \leq p,\, 1 \leq j \leq k-1}$ et $\alpha \in \mathbb{C}$ tels que si $|z| < 1$ on ait :

$$f(z) = \frac{\alpha}{(1-z)^k} + \sum_{i=1}^{p} \sum_{j=1}^{k-1} \frac{c_{i,j}}{(\omega_i - z)^j}$$

11. Ne soyons pas tordus ...
12. Ainsi que la série génératrice de $(u_n)_n$.

Si $\omega \in P$ et $j \in \mathbb{N}$ alors la fonction $z \mapsto \dfrac{1}{(\omega - z)^j}$ est développable en série entière avec un rayon de convergence 1 et on peut obtenir les coefficients dudit développement en dérivant terme à terme le développement en série entière de $z \mapsto \dfrac{1}{\omega - z}$; or si $|z| < 1$:

$$\frac{1}{\omega - z} = \frac{1}{\omega}\frac{1}{1 - \frac{z}{\omega}}$$

Et donc, pour $j \leq k - 1$:

$$\frac{(j-1)!}{(\omega - z)^j} = \sum_{n=j-1}^{\infty} \frac{n!}{(n-j+1)!}\frac{z^{n-j+1}}{\omega^{n+1}}$$

Ainsi :

$$\frac{1}{(\omega - z)^j} = \sum_{n=0}^{\infty} C_{n+j}^{n}\frac{z^n}{\omega^{n+j}}$$

On en déduit que :

$$\forall n \geq 1,\, u_n = f(0) = \alpha \underbrace{C_{n+k-1}^{n}}_{\sim \frac{n^{k-1}}{(k-1)!}} + \sum_{i=1}^{p}\sum_{j=1}^{k-1} c_{i,j} \underbrace{C_{n+j}^{n}\frac{1}{\omega^{n+j}}}_{=o(n^{k-1})}$$

Ainsi :

$$u_n \sim_{n\to\infty} \alpha\frac{n^{k-1}}{(k-1)!}$$

Il ne nous reste alors plus qu'à calculer la constante α. On utilise la méthode usuelle de calcul de la décomposition en éléments simples, i.e on écrit d'abord :

$$(1-z)^k f(z) = \prod_{i=1}^{k}\frac{1-z}{1-z^{a_i}} = \prod_{i=1}^{k}\frac{1}{1+z+\ldots+z^{a_i-1}}$$

Ensuite on fait "$z = 1$" et on trouve :

$$\alpha = \frac{1}{a_1 \ldots a_k}$$

Et voila !

1.9 Points extrémaux de la boule unité de $\mathcal{L}(E)$

Référence :
- [FGN10], p. 130–131

Proposition 1.9
Soit E un espace euclidien de dimension $n \geq 0$.
On munit $\mathcal{L}(E)$ de la norme subordonnée à la norme euclidienne sur E et on note $\mathcal{B}$ la boule unité fermée de $\mathcal{L}(E)$.
Alors l'ensemble des points extrémaux de $\mathcal{B}$ est le groupe orthogonal $\mathcal{O}(E)$.

DÉMONSTRATION : Soit $u \in \mathcal{O}(E)$; alors $\|u\| = 1$ donc $u \in \mathcal{B}$. Supposons qu'il existe $v, w \in \mathcal{B}$ tels que $u = \frac{1}{2}(v + w)$ et donnons nous $x \in E$ unitaire. Alors :

$$\begin{aligned} 1 = \|x\| &= \|u(x)\| \\ &= \frac{1}{2}\|v(x) + w(x)\| \\ &\leq \frac{1}{2}(\|v(x)\| + \|w(x)\|) \\ &\leq \frac{1}{2}(\|v\| + \|w\|) \\ &\leq 1 \end{aligned}$$

De fait toutes ces inégalités sont des égalités et donc $\|v(x)+w(x)\| = \|v(x)\|+\|w(x)\|$ et donc il existe $\lambda \geq 0$ tel que $v(x) = \lambda w(x)$. De plus, comme $\frac{1}{2}(\|v(x)\|+\|w(x)\|) = 1$ et que $\|v(x)\|, \|w(x)\| \leq 1$ alors $\|v(x)\| = \|w(x)\| = 1$ d'où $\lambda = 1$ soit $v(x) = w(x)$. Par linéarité on a alors $v = w$ et donc u est extrémal dans $\mathcal{B}$.

Réciproquement, soit $u \in \mathcal{B}\backslash\mathcal{O}(E)$. Fixons B une b.o.n de E et posons $A := \mathrm{mat}_B(u)$. Alors par décomposition polaire "généralisée" (cf. [FGN10], p. 128–129) il existe $O \in O_n(\mathbb{R})$ et $S \in S_n^+(\mathbb{R})$ telles que $A = OS$. De plus, il existe $D := \mathrm{diag}(d_1, \ldots, d_n)$, avec $0 \leq d_1 \leq \ldots \leq d_n$, et $P \in O_n(\mathbb{R})$ tel que $S = {}^tPDP$. Par orthogonalité de O on a finalement $\|u\| = \|A\| = \|S\| = \|D\|$.

Comme $\|u\| \leq 1$, les d_k sont nécessairement dans $[0, 1]$ et comme $A \notin O(E)$ on a $d_1 < 1$. De fait d_1 n'est pas un point extrémal de $[-1, 1]$ et donc il existe $-1 \leq \alpha < \beta \leq 1$ tels que $d_1 = \frac{1}{2}(\alpha + \beta)$. On pose alors $D_1 := \mathrm{diag}(\alpha, d_2, \ldots, d_n)$ et $D_2 := \mathrm{diag}(\beta, d_2, \ldots, d_n)$ et on a $D_1 \neq D_2$ et $D = \frac{1}{2}(D_1 + D_2)$, ergo :

$$A = \frac{1}{2}(O^tPD_1P + O^tPD_2P) \text{ avec } O^tPD_1P \neq O^tPD_2P$$

De plus, si $X \in \mathbb{R}^n$ et $i \in \{1, 2\}$ on a :

$$\begin{aligned} \|O^tPD_iPX\| &= {}^tX^tPD_iP^tOO^tPD_iPX \\ &= {}^t(PX)D_i(PX) \\ &\leq \|PX\| \text{ car } \|D_i\| \leq \|D\| \leq 1 \\ &\leq \|X\| \text{ car } P \text{ est orthogonale} \end{aligned}$$

De fait $\|O^tPD_iP\| \leq 1$ et donc u peut bien s'écrire comme milieu de deux points distincts de $\mathcal{B}$, ergo n'est pas extrémal.

Détails supplémentaires :

- On rappelle qu'un point A d'un convexe C est dit *extrémal* si $C \setminus \{A\}$ est convexe, ce qui est équivalent à dire que A n'est pas milieux de deux points (distincts !) de C.
- Si on admet le théorème de Krein–Milman suivant on peut déduire de notre résultat que l'enveloppe convexe de $\mathcal{O}(E)$ est $\mathcal{B}(E)$:

  Théorème 1.10 (Krein–Milman)
  Tout convexe compact d'un espace vectoriel de dimension finie est enveloppe convexe de l'ensemble de ses points extrémaux.

1.10 Polygones réguliers constructibles

Référence :
- [Car89], p. 48–52 et 214–219

Prérequis :
- théorème de Wantzel.

Lemme 1.4
Soit m et n deux entiers premiers entre eux.
Alors :

$$\text{l'angle } \widehat{\frac{2\pi}{mn}} \text{ est constructible} \Leftrightarrow \text{ les angles } \widehat{\frac{2\pi}{m}} \text{ et } \widehat{\frac{2\pi}{n}} \text{ sont constructibles}$$

DÉMONSTRATION :

(⇒) Immédiat car ces angles sont des multiples de $\widehat{\frac{2\pi}{mn}}$; il suffit alors de reporter avec un compas le bon nombre de fois la corde formée par ce dernier angle sur le cercle unité.

(⇐) Par théorème de Bézout, il existe $a, b \in \mathbb{N}$ tels que $an + bm = 1$; de fait :

$$\widehat{\frac{2\pi}{mn}} = a\widehat{\frac{2\pi}{m}} + b\widehat{\frac{2\pi}{n}}$$

$\widehat{\frac{2\pi}{mn}}$ est alors une combinaison entière d'angles constructibles, donc l'est.

Lemme 1.5
Soit $n \geq 3$ de décomposition en produit de facteurs premiers :

$$n =: \prod_{i=1}^{k} p_i^{\alpha_i}$$

Alors :

$$\textit{le polygone régulier à } n \textit{ côtés est constructible} \Leftrightarrow \textit{les angles } \widehat{\frac{2\pi}{p_i^{\alpha_i}}} \textit{ le sont}$$

DÉMONSTRATION : Découle par récurrence du lemme 1.4.

Proposition 1.11 (Gauss–Wantzel)
Soit $\alpha \in \mathbb{N}^*$.
Alors :

(i) les angles $\widehat{\frac{2\pi}{2^\alpha}}$ sont constructibles ;

(ii) soit p un nombre premier impair ; alors :

$$\textit{l'angle } \widehat{\frac{2\pi}{p^\alpha}} \textit{ est constructible } \Leftrightarrow \alpha = 1 \textit{ et } p = 1 + 2^{2^\beta} \textit{ avec } \beta \in \mathbb{N}$$

Ainsi on obtient (en combinant ce résultat avec le lemme 1.5) que :

le polygone régulier à n côtés est constructible
$\Leftrightarrow$
n est le produit d'une puissance de 2 (éventuellement égale à 1) et d'un nombre fini (éventuellement nul) de nombres de Fermat premiers distincts

DÉMONSTRATION :

(i) On se ramène à la construction de bissectrices via une récurrence sur α.

(ii) $(\Rightarrow)$ Si on suppose $\widehat{\frac{2\pi}{p^\alpha}}$ constructible alors $\cos\left(\frac{2\pi}{p^\alpha}\right)$ l'est également et donc par théorème de Wantzel :

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right) : \mathbb{Q}\right] = 2^m \text{ avec } m \in \mathbb{N} \tag{1.10.1}$$

Posons $q := p^\alpha$ et $\omega := e^{2i\pi/q}$. Alors ω est algébrique sur $\mathbb{Q}$ et son polynôme minimal est le polynôme cyclotomique ϕ_q (il est annulateur irréductible unitaire), qui est de degré $\phi(q) = p^{\alpha-1}(p-1)$, donc :

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = p^{\alpha-1}(p-1) \tag{1.10.2}$$

Comme $\omega + \omega^{-1} = 2\cos\left(\frac{2\pi}{p^\alpha}\right)$ on a $\cos\left(\frac{2\pi}{p^\alpha}\right) \in \mathbb{Q}(\omega)$ et $\omega^2 - 2\omega\cos\left(\frac{2\pi}{p^\alpha}\right) + 1 = 0$ ergo :

$$\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right)\right] = 2 \tag{1.10.3}$$

Or :

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right)\right]\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p^\alpha}\right)\right) : \mathbb{Q}\right]$$

Et donc par (1.10.2) , (1.10.3) et (1.10.1) on a :

$$p^{\alpha-1}(p-1) = 2^{m+1}$$

Donc, comme p est un nombre premier impair on a nécessairement $\alpha = 1$ et $p = 2^{m+1}+1$. Par décomposition en produits de facteurs premiers, $m+1 = \lambda 2^\beta$, avec $\beta \in \mathbb{N}$ et $\lambda \in \mathbb{N}^*$ impair. De fait $p = 1 + (2^{2^\beta})^\lambda$.
Comme λ est impair, $1 + X | 1 + X^\lambda$ et donc $1 + 2^{2^\beta} | p$ donc, par primalité, $p = 1 + 2^{2^\beta}$ est un nombre de Fermat.

($\Leftarrow$) Posons $n = 2^\beta$, de telle sorte que $p = 1 + 2^n$, et $\omega := e^{2i\pi/p}$. De fait on a, comme le polynôme minimal de ω est ϕ_p, que :

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$$

Soit $g \in G := \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)$; alors comme $g(\mathbb{Q}) = \mathbb{Q}$ g est entièrement déterminé par $g(\omega)$. De plus on a :

$$0 = g(0) = g(\phi_p(\omega)) = \phi_p(g(\omega)) = \sum_{i=0}^{p-1} g(\omega)^i$$

Ainsi $g(\omega) \in \mathrm{Rac}_{\mathbb{C}}(\phi_p) = \{\omega, \omega^2, \ldots, \omega^{p-1}\}$ et donc on a :

$$G = \{g_k : \omega \mapsto \omega^k \mid k \in [p-1]\}$$

En particulier, $|G| = p-1$ et donc l'application surjective suivante est un isomorphisme :

$$\begin{aligned} \psi : G &\to (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \\ g_k &\mapsto \bar{k} \end{aligned}$$

Ainsi G contient un élément g_0 d'ordre $p - 1 = 2^n$ et donc si pose, pour $0 \leq i \leq n$ $\mathbb{K}_i := \{z \in \mathbb{Q}(\omega) \mid g_0^{2^i}(z) = z\}$. Il est clair que les $\mathbb{K}_i$ sont des sous–corps de $\mathbb{Q}(\omega)$ ($\mathbb{K}_i = \ker(g^{2^i} - \mathrm{id})$). De plus, $\mathbb{Q} \subset \mathbb{K}_0$ et si $z \in \mathbb{K}_0$ alors comme $(g_0(\omega)^i)_{0 \leq i \leq p-2}$ forme une base de $\mathbb{Q}(\omega)/\mathbb{Q}$ (image d'une base par un isomorphisme) on a l'existence de $\lambda_0, \ldots, \lambda_{p-2} \in \mathbb{Q}$ tels que $z = \lambda_0\omega + \ldots + \lambda_{p-2}g_0^{p-2}(\omega)$ et donc :

$$\sum_{i=0}^{p-2} \lambda_i g_0^i(\omega) = z = g_0(z) = \sum_{i=0}^{p-2} \lambda_i g_0^{i+1}(\omega)$$

Par identification tous les λ_i sont égaux et donc $z = \lambda_0 g_0(\omega + \ldots + \omega^{p-1}) = -\lambda_0 \in \mathbb{Q}$. On a donc une tour d'extensions :

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \ldots \subset \mathbb{K}_n = \mathbb{Q}(\omega) \tag{1.10.4}$$

Les inclusions sont de plus strictes car pour tout i, l'élément suivant appartient à $\mathbb{K}_{i+1} \setminus \mathbb{K}_i$:

$$\sum_{k=0}^{2^{n-i-1}-1} g_0^{2^{i+1}k}(\omega)$$

Posons $f := g_0^{2^{n-1}}$ et $\omega^\lambda := f(\omega)$. $f^2 = \mathrm{id}$ donc :

$$\omega = f^2(\omega) = \omega^{\lambda^2}$$

De fait $\omega^{\lambda^2 - 1} = 1$ et donc $p|\lambda^2 - 1$, i.e $\overline{\lambda^2 - 1} = \bar{0}$ dans $\mathbb{F}_p$ et donc $\overline{\lambda} = \pm\bar{1}$. Comme $f \neq \mathrm{id}$ on a alors nécessairement $\overline{\lambda} = -\bar{1}$, i.e $f(\omega) = \omega^{-1}$.

Remarquons ensuite que $f\left(\cos\left(\dfrac{2\pi}{p}\right)\right) = \dfrac{1}{2}(f(\omega) + f(\omega^1)) = \cos\left(\dfrac{2\pi}{p}\right)$ et donc $\cos\left(\dfrac{2\pi}{p}\right) \in \mathbb{K}_{n-1}$. On a donc :

$$\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subset \mathbb{K}_{n-1} \subsetneq \mathbb{K}_n = \mathbb{Q}(\omega)$$

D'où :

$$1 < [\mathbb{Q}(\omega) : \mathbb{K}_{n-1}] \leq \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] \tag{1.10.5}$$

De plus, on montre de la même façon qu'en (i) (en substituant p à q) que :

$$\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] = 2 \tag{1.10.6}$$

Et donc au final :

$$[\mathbb{Q}(\omega):\mathbb{K}_{n-1}]=2 \text{ ergo } \mathbb{K}_{n-1}=\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$$

À présent, si on passe au degré dans la tour (1.10.4) on trouve :

$$2^n=p-1=[\mathbb{Q}(\omega):\mathbb{Q}]=\underbrace{[\mathbb{Q}(\omega):\mathbb{K}_{n-1}]\times\ldots\times[\mathbb{K}_1:\mathbb{Q}]}_{n \text{ facteurs}}$$

On a donc nécessairement tous les $[\mathbb{K}_{i+1}:\mathbb{K}_i]$ égaux à 2. En particulier :

$$[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right):\mathbb{Q}]=2^{n-1}$$

D'où la constructibilité voulue (par la caractérisation usuelle, que l'on peut par exemple trouver dans [Car89] p. 25).

1.11 Polynômes irréductibles sur $\mathbb{F}_q$

Référence :
- [FG97], p. 189–191

Prérequis :
- formule d'inversion de Möbius.

Soit p un nombre premier et soit $r\in\mathbb{N}^*$. On pose $q:=p^r$ et on s'intéresse, pour $n\geq 1$, à l'ensemble $A(n,q)$ des polynômes de degré n irréductibles sur $\mathbb{F}_q$. On pose également $I(n,q):=\text{card}(A(n,q))$.

Proposition 1.12
Soit $n\geq 1$. Alors :

(i) *on a la factorisation suivante :*

$$X^{q^n}-X=\prod_{d|n}\prod_{P\in A(d,q)}P$$

(ii) *si on note μ la fonction de Möbius on a :*

$$I(n,q)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$$

(iii) *on a l'équivalent $I(n,q)\sim_{n\to\infty}\frac{q^n}{n}$.*

Démonstration :

(i) – Soit $d|n$ et soit $P\in A(d,q)$, dont on fixe une racine x dans une clôture algébrique de $\mathbb{F}_q$. $\mathbb{K}:=\mathbb{F}_q(x)$ est alors un corps de rupture de P et $[K:\mathbb{F}_q]=\deg(P)=d$ donc $\mathbb{K}\cong\mathbb{F}_{q^d}$ (par "unicité" des corps finis). Or tout élément de $\mathbb{F}_{q^d}$ est racine du polynôme $X^{q^d}-X$, donc $x^{q^d}=x$ et alors :

$$x^{q^n}=\left(\left(\ldots\left(x^{q^d}\right)^{q^d}\ldots\right)^{q^d}\right)^{q^d}=x$$

De fait x est racine de $X^{q^n}-X$ donc P divise ce dernier polynôme. Par irréductibilité on a alors $\prod_{d|n}\prod_{P\in A(d,q)}P|X^{q^n}-X$.

– Soit P un facteur irréductible de $X^{q^n}-X$, de degré $d\geq 1$ et soit $x\in\mathbb{F}_{q^n}$ une racine de ce polynôme[13]. Si on pose à nouveau $\mathbb{K}:=\mathbb{F}_q(x)$ on a $[\mathbb{F}_{q^n}:\mathbb{K}][\mathbb{K}:\mathbb{F}_q]=[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$. De fait $d=[\mathbb{K}:\mathbb{F}_q]$ divise n.
De plus, les racines de $X^{q^n}-X$ dans $\mathbb{F}_{q^n}$ sont toutes simples, de fait ce polynôme est sans facteur carrés. On a donc bien et donc $X^{q^n}-X\mid\prod_{d|n}\prod_{P\in A(d,q)}P$.

13. Qui est scindé sur ce dernier corps

– Les deux polynômes considérés étant unitaires, on a bien l'égalité voulue.

(*ii*) Passons au degré dans le résultat du (*i*) :

$$q^n = \sum_{d|n} dI(d,q)$$

En appliquant la formule d'inversion de Möbius à $g : n \mapsto q^n$ et $f : n \mapsto nI(n,q)$ on obtient alors :

$$I(n,q) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

(*iii*) Posons :

$$r_n := \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) q^d$$

Alors :

$$\begin{aligned} |r_n| &\leq \sum_{d=1}^{\lfloor n/2 \rfloor} q^d \\ &= q\frac{q^{\lfloor n/2 \rfloor} - 1}{q-1} \\ &= \frac{q^{\lfloor n/2 \rfloor + 1}}{q-1} \end{aligned}$$

Ainsi :

$$I(n,q) = \frac{q^n + r_n}{n} \sim_{n\to\infty} \frac{q^n}{n}$$

Détails supplémentaires :

– Rappelons que la fonction de Möbius est définie comme suit :

$$\begin{aligned} \mu : \mathbb{N} \to\ & \{-1,0,1\} \\ n \mapsto & \begin{cases} 0 & \text{si } n \text{ a un facteur carré} \\ (-1)^k & \text{sinon, où } k \text{ est le nombre de facteurs premiers distincts de } n \end{cases} \end{aligned}$$

On a alors le résultat suivant :

Proposition 1.13 (Formule d'inversion de Möbius)
Soient $f, g : \mathbb{N} \to \mathbb{C}$ telles que :

$$\forall n \geq 1, \qquad g(n) = \sum_{d|n} f(d)$$

Alors :

$$\forall n \geq 1, \qquad f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

1.12 Réduction des endomorphismes auto–adjoints

Référence :

– [Gou94], p. 240–241

Tout ce qui suit est valable dans un espace hermitien, au prix de quelques substitutions dont nous laissons l'entreprise au lecteur.

Proposition 1.14
Soit E un espace euclidien.
Soit $f \in \mathcal{S}(E)$.
Alors :

(i) $\mathrm{Sp}(f) \subset \mathbb{R}$;

(ii) E admet une base orthonormée formée de vecteurs propres de E.

Démonstration : On procède[14] par récurrence sur la dimension de E. Plus précisément on souhaite montrer pour tout $n \geq 0$ la propositions suivante :

$\mathcal{P}(n)$ pour tout espace euclidien E de dimension n et tout $f \in \mathcal{S}(E)$ on a (i) et (ii)

- *n=0.* Trivial : une b.o.n de $\{0\}$ est () qui est formée de vecteurs propres de l'endomorphisme nul zéro–dimensionnel.
- Supposons $\mathcal{P}(n)$ pour $n \geq 0$. Soit E un espace euclidien de dimension $n+1$ et $f \in \mathcal{S}(E)$. On peut alors définir une forme bilinéaire symétrique comme suit :

$$\begin{aligned} \varphi : E \times E &\to \mathbb{R} \\ (x,y) &\mapsto \langle x, f(y) \rangle \end{aligned}$$

Notons ϕ la forme quadratique associée à φ. Alors par compacité de la sphère $\mathbb{S}$ de centre 0 et de rayon 1 de E et continuité (par dimension finie) de ϕ, il existe $x_0 \in \mathbb{S}$ tel que $\phi(x_0) = \lambda := \sup_{\mathbb{S}} \phi$.

Posons $g := \lambda \mathrm{id}_E - f$ et $\varphi_1(x,y) \mapsto \langle x, g(y) \rangle$. Alors φ_1 définit une forme bilinéaires symétrique positive (par définition de λ) et $\varphi_1(x_0, x_0) = 0$. Comme $x_0 \neq 0$, φ_1 n'est pas définie donc possède un noyau[15], i.e il existe $x \neq 0$ tel que pour tout $y \in E$ $\varphi_1(x,y) = 0$, ce qui est équivalente à $(x \neq 0) \wedge (x \in \mathrm{Im}(g)^{\perp})$.

De fait, $\mathrm{Im}(g) \neq E$, i.e g n'est pas surjectif. Par dimension finie, il n'est pas non plus injectif et donc il existe un vecteur unitaire e_1 tel que $g(e_1) = 0$ i.e $f(e_1) = \lambda e_1$. De fait $\lambda \in \mathrm{Sp}(f)$ et comme ϕ est une forme quadratique $\lambda \in \mathbb{R}$.

Posons à présent $H := \langle e_1 \rangle^{\perp}$. Alors comme $\langle e_1 \rangle$ est stable par f, H est stable par $f^* = f$ et donc f induit sur H un endomorphisme $f_H \in \mathcal{L}(H)$. Par hypothèse de récurrence, comme $\dim(H) \leq n$ et que f_H est symétrique, il existe une b.o.n $(e_2, \ldots, e_n)$ de H formée de vecteurs propres de f_H, donc de f, et $\mathrm{Sp}(f_H) \subset \mathbb{R}$. De fait $\mathrm{Sp}(f) = \{\lambda\} \cup \mathrm{Sp}(f_H) \subset \mathbb{R}$ et $(e_1, \ldots, e_n)$ est une b.o.n de E constituée de vecteurs propres de f, d'où le résultat.

Les deux corollaires qui suivent ne sont que reformulations du résultat.

Corollaire 1.14.1 (Version matricielle)
Soit $M \in S_n(\mathbb{R})$.
Alors il existe $P \in O_n(\mathbb{R})$ et $D \in \mathcal{M}_n(\mathbb{R})$ diagonale tel que $M = {}^tPDP$.

Corollaire 1.14.2
Soit E un espace euclidien.
Soit ϕ, ψ deux formes quadratiques sur E telles que ψ soit définie positive.
Alors il existe une base de E ψ–orthonormée dans laquelle la matrice de ϕ est diagonale.

Corollaire 1.14.3 (Pseudo-réduction simultanée)
Soient $M, N \in S_n(\mathbb{R})$ telles que M soit définie positive.
Alors il existe $C \in GL_n(\mathbb{R})$ telle que ${}^tCNC$ soit diagonale et que ${}^tCMC = I_n$.

Démonstration : On applique le corollaire 1.14.2 à $E := \mathbb{R}^n$, $\phi : (X,Y) \mapsto {}^tXNY$ et $\psi : (X,Y) \mapsto {}^tXMY$ puis on traduit matriciellement.

On peut aussi citer le corollaire suivant :

Corollaire 1.14.4 (Racine carrée d'un endomorphisme auto–adjoint positif, [FGN10] p. 107)
Soit E un espace euclidien.
Soit $u \in \mathcal{S}^+(E)$.
Alors il existe un unique $h \in \mathcal{S}^+(E)$ tel que $u = h^2$. De plus, h est un polynôme en u.

Démonstration :

14. Hélas.
15. On dit aussi "est dégénérée", mais vous et moi sommes au dessus de ce genre d'attaques *ad hominem*, n'est-ce pas ?

- *Existence.* Soit $(e_i)_{i\in[n]}$ une base de diagonalisation de u, chaque e_i étant associé à une valeur propre λ_i de u. Les λ_i étant réels positifs, on peut définir $h : e_i \mapsto \sqrt{\lambda_i} e_i$, qui convient.
- *Unicité.* Soit $k \in \mathcal{S}^+(E)$ tel que $k^2 = u$ et soit λ une valeur propre de u, de sous–espace propre associé E_λ. Alors k commute avec u donc induit un endomorphisme $\bar{k} \in \mathcal{S}^+(E_\lambda)$ tel que $\bar{k}^2 = \lambda \mathrm{id}_{E_\lambda}$. On a alors que $\bar{k}$ est diagonalisable de spectre réduit à $\{\sqrt{\lambda}\}$ (car ses valeurs propres doivent être positives) donc $\bar{k} = \sqrt{\lambda}\mathrm{id}_{E_\lambda}$. Ainsi, si $(e_i)_{i\in[n]}$ est une base de diagonalisation de u, on a nécessairement $k(e_i) = \sqrt{\lambda_i} e_i = h(e_i)$ pour tout $i \in [n]$. Ainsi, $k = h$.
- Pour voir que h est un polynôme en u, il suffit de remarquer que par interpolation (de Lagrange par exemple) il existe un polynôme $P \in \mathbb{R}[X]$ tel que pour tout $\lambda \in \mathrm{Sp}(u)$, $P(\lambda) = \sqrt{\lambda}$. $P(u)$ coïncide alors avec h sur $(e_i)_{i\in[n]}$ donc sur E tout entier.

1.13 Simplicité du groupe alterné

Référence :
- [Per96], p. 28–29

Prérequis :
- théorèmes de Sylow.

Proposition 1.15
Le groupe $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Démonstration : Traitons premièrement le cas $n = 5$, en commençant par passer en revue les éléments de $\mathfrak{A}_5$. Ce groupe, de cardinal 60, contient :
- un élément d'ordre 1. Vous l'aurez deviné, il s'agit du neutre () ...
- des produits de deux transpositions à supports disjoints, qui sont d'ordre 2. On dispose de $C_5^2 = 10$ possibilités pour la première et de $C_3^2 = 3$ possibilités pour sa collègue, pour un total de 30 choix possible, en tenant compte de l'ordre dans lequel on compose. Nos permutations étant à support disjoints, elles commutent donc il n'en reste que 15 qui soient distinctes.
- des 3–cycles (rappelons qu'un cycle d'ordre k est de signature $(-1)^k$). Le choix de 3 éléments distincts i, j, k de [5] nous livre deux 3–cycles distincts $(i \quad j \quad k)$ et $(i \quad k \quad j)$, ergo $\mathfrak{A}_5$ accueille $2 \times C_5^3 = 20$ 3–cycles en son sein.
- des 5–cycles. Notons que si on se donne $i, j, k, l, m \in [5]$ deux à deux distincts alors les cycles suivants sont égaux : $(i \quad j \quad k \quad l \quad m)$, $(m \quad i \quad j \quad k \quad l)$, $(l \quad m \quad i \quad j \quad k)$, $(k \quad l \quad m \quad i \quad j)$ et $(j \quad k \quad l \quad m \quad i)$, ainsi $\mathfrak{A}_5$ contient $\frac{5!}{5} = 24$ 5–cycles distincts.

Comme $60 = 1 + 15 + 20 + 24$, on a bien décrit le groupe $\mathfrak{A}_5$.

Soit $H \lhd \mathfrak{A}_5$ non trivial. Remarquons que comme les 3–cycles (resp. les produits de deux transpositions à supports disjoints) sont tous conjugués dans $\mathfrak{A}_5$, si H contient un élément d'ordre 3 (resp. 2), il les contient tous. De plus, si H contient un 5–cycle σ, il contient $\langle\sigma\rangle$, qui est un 5–Sylow de $\mathfrak{A}_5$. Ces derniers étant tous conjugués[16], H contient alors tous les éléments d'ordre 5 de $\mathfrak{A}_5$. Cependant, aucun des entiers $15 + 1$, $20 + 1$ et $24 + 1$ ne divise 60 donc H doit être dans au moins deux des cas précédents et donc $|H| \geq 15 + 20 + 1 = 36|$, ce qui implique –toujours car $|H||60$ – que $|H| = 60$ et donc $H = \mathfrak{A}_5$. On a bien démontré la simplicité de $\mathfrak{A}_5$.

Supposons à présent $n > 5$ et donnons nous $H \lhd \mathfrak{A}_n$ non trivial et $\sigma \in H \setminus \{()\}$. Il existe alors $a \in [n]$ tel que $b := \sigma(a) \neq a$. Donnons nous également $c \notin \{a, b, \sigma(b)\}$ et posons $\tau := (a \quad c \quad b)$ et $\rho := [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1}$. On a alors[17] :

$$\rho = (a \quad c \quad \underbrace{b}_{=\sigma(a)})(\sigma(a) \quad \sigma(b) \quad \sigma(c))$$

ρ agit donc sur au plus 5 éléments, ceux de l'ensemble $E := \{a, b, c, \sigma(b), \sigma(c)\}$, i.e on a $\rho(E) = E$ et $\rho_{|[n]\setminus E} = \mathrm{id}_{[n]\setminus E}$. Quitte à rajouter des éléments inutiles, on peut supposer que $|E| = 5$ et comme $\rho(b) = \tau\sigma(b) \neq b$ (car $\tau^{-1}(b) = c \neq \sigma(b)$, $\rho_{|E} \neq \mathrm{id_E}$.

16. Attention cependant, tous les éléments d'ordre 5 de $\mathfrak{A}_5$ ne sont pas conjugués, car sinon l'orbite d'un 5–cycle pour l'action de $\mathfrak{A}_5$ sur lui–même par conjugaison serait d'ordre $24 \nmid 60$.

17. Pour les calculs explicites, remarquer que $\rho = \tau\nu$ où ν est le conjugué de τ par σ.

L'ensemble $\mathfrak{A}$ des permutations paires de E est alors isomorphe à $\mathfrak{A}_5$ et on dispose de l'injection suivante :

$$\begin{aligned} \mathfrak{A} &\hookrightarrow \mathfrak{A}_n \\ u &\mapsto \overline{u} : x \mapsto \begin{cases} u(x) & \text{si } \; x \in E \\ x & \text{sinon} \end{cases} \end{aligned}$$

Posons alors (quitte à identifier) :

$$H_0 := \{u \in \mathfrak{A} \,|\, \overline{u} \in H\} = \text{"} H \cap \mathfrak{A} \text{"}$$

Remarquons alors que $H_0 \lhd \mathfrak{A} \cong \mathfrak{A}_5$ et que $\rho_{|E}$ est un élément non trivial de H_0. Ergo, par simplicité de $\mathfrak{A}_5$, $H_0 = \mathfrak{A}$.

Soit $u \in \mathfrak{A}$ un 3–cycle. Alors $\overline{u}$ est un 3–cycle de $\mathfrak{A}_n$ (l'injection $\mathfrak{A} \hookrightarrow \mathfrak{A}_n$ conservant le cardinal du support). Comme tous les 3–cycles sont conjugués dans $\mathfrak{A}_n$, H contient tous les 3–cycles. On conclut que $H = \mathfrak{A}_n$ en remarquant que le groupe alterné est engendré par les 3–cycles.

Détails supplémentaires :

- *$\mathfrak{A}_n$ est engendré par les 3–cycles.* Comme $\mathfrak{S}_n$ est engendré par les transpositions, $\mathfrak{A}_n$ est engendré par les produits de deux transpositions. On a de plus les relations suivantes :

  $$(a \quad b)(b \quad c) = (a \quad b \quad c) \text{ et } (a \quad b)(a \quad c) = (a \quad c \quad b)$$

  In fine :

  $$(a \quad b)(c \quad d) = (a \quad c \quad b)(a \quad c \quad d)$$

  D'où le résultat ([Per96], p.11).
- *Les 3–cycles sont conjugués dans $\mathfrak{A}_n$ ($n \geq 5$).* Ceci découle du résultat suivant ([Per96], p.16) :

  Lemme 1.6
  Soit $n \geq 3$.
  Soient $a_1, \ldots, a_n \in [n]$ deux à deux distincts.
  Soient $b_1, \ldots, b_n \in [n]$ deux à deux distincts.
  Alors il existe $\sigma \in \mathfrak{A}_n$ telle que $\forall i \in [n-2]$, $\sigma(a_i) = b_i$.
  Démonstration : On sait qu'il existe une telle permutation σ dans $\mathfrak{S}_n$. Si $\varepsilon(\sigma) = 1$, c'est terminé, sinon on compose par $(a_{n-1} \quad a_n)$ et on obtient une permutation paire adéquate.

  Ainsi, si $\rho = (a_1 \quad a_2 \quad a_3)$ et $\tau = (b_1 \quad b_2 \quad b_3)$ sont dans $\mathfrak{A}_n$, comme $n - 2 \geq 3$ il existe une permutation $\sigma \in \mathfrak{A}_n$ telle que $\forall i \in [3]$, $\sigma(a_i) = b_i$ et donc $\tau = \sigma\rho\sigma^{-1}$.
- *Les produits de deux permutations de supports disjoints sont conjugués dans $\mathfrak{A}_n$ ($n \geq 5$).* Si $n > 5$ cela découle immédiatement du lemme 1.6. Si $n = 5$, soient $\rho := (a \quad b)(c \quad d)(e)$ et $\tau := (a' \quad b')(c' \quad d')(e')$. D'après le lemme 1.6, il existe $\sigma \in \mathfrak{A}_5$ telle que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$. On a alors $\tau = \sigma\rho\sigma^{-1}$.
- *Simplicité pour $n \geq 4$.* $\mathfrak{A}_2 = \{()\}$ et $\mathfrak{A}_3 = \{(), (1 \quad 2 \quad 3), (1 \quad 3 \quad 2)$ sont simples. $\mathfrak{A}_4$ n'est pas simple car il admet le sous–groupe distingué suivant :

  $$H := \{(), (1 \quad 2)(3 \quad 4), (1 \quad 3)(2 \quad 4), (1 \quad 4)(2 \quad 3)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

1.14 Table de caractères du groupe diédral

Référence :
- [Ser98], p. 27–28

Soit $n \geq 3$. On cherche ici à déterminer la table de caractères du groupe diédral $D_n := \langle r, s \,|\, s^2 = r^n = \mathrm{id}, srs = r^{-1} \rangle$.

***Représentations de degré* 1.** Soit ψ une représentation de degré 1 de D_n. Alors $\psi(r)^n = \psi(r^n) = 1$.
De fait $\psi(r) \in \mu_n(\mathbb{C})$. De même $\psi(s) \in \{-1, 1\}$ et $\psi(srs) = \psi(s)^2\psi(r) = \psi(r)$ donc $\psi(r) = \psi(r)^{-1}$) ergo $\psi(r)^2 = 1$ donc $\psi(r) \in \{-1, 1\}$. On a donc 4 caractères de degré 1 :

	s	r
χ_1	1	1
χ_2	1	-1
χ_3	-1	1
χ_4	-1	-1

Ou, de façons plus exhaustive :

	r^k	sr^k
χ_1	1	1
χ_2	1	-1
χ_3	$(-1)^k$	$(-1)^k$
χ_4	$(-1)^k$	$(-1)^{k+1}$

Représentations de degré **2.** Soient $\omega := e^{2i\pi/n}$ et $h \in \mathbb{Z}$. On peut alors définir une représentation de degré 2 ρ^h (dont nous noterons le caractère χ^h) de D_n comme suit :

$$\rho^h(r^k) := \begin{pmatrix} \omega^{hk} & 0 \\ 0 & \omega^{-hk} \end{pmatrix} \text{ and } \rho^h(sr^k) := \begin{pmatrix} 0 & \omega^{-hk} \\ \omega^{hk} & 0 \end{pmatrix}$$

De façon équivalente, ρ^h est l'unique morphisme de groupes $D_n \to GL_2(\mathbb{C})$ tel que :

$$\rho^h(r) := \begin{pmatrix} \omega^{h} & 0 \\ 0 & \omega^{-h} \end{pmatrix} \text{ and } \rho^h(s) := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Il est immédiat que ρ^h ne dépend que de la classe de h modulo n ; de plus, les représentations ρ^h et ρ^{n-h} sont isomorphes. En effet, si on pose $T := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ on a $T\rho^h(r) = \rho^{-h}(r)T = \rho^{n-h}(r)T$ et $T\rho^h(s) = \rho^{-h}(s)T = \rho^{n-h}(s)T$. On peut donc se réduire au cas $0 \leq h \leq \dfrac{n}{2}$.

- $h = 0$. On vérifie aisément que $\chi^0 = \chi_1 + \chi_2$. De fait, ρ^0 est isomorphe à la somme directe des représentations associées à χ_1 et χ_2 donc est réductible.
- $h = \dfrac{n}{2}$. Comme $\omega^{n/2} = e^{i\pi} = -1$ on a $\chi^{n/2} = \chi_3 + \chi_4$ et donc $\rho^{n/2}$ est réductible.
- $0 < h < \dfrac{n}{2}$. Notons que dans ce cas, $\omega^h \neq \omega^{-h}$, et donc les seules droites de $\mathbb{C}^2$ $\rho^h(r)$–stables sont les axes de coordonnées $\langle(1,0)\rangle$ et $\langle(0,1)\rangle$. Mais ces sous–espaces ne sont pas $\rho^h(s)$–stables ergo ρ^h n'admet aucune sous–représentation non triviale i.e est irréductible. On peut donc ajouter la ligne suivante à notre table :

	r^k	sr^k
χ^h	$2\cos\left(\dfrac{2hk\pi}{n}\right)$	0

Supposons à présent qu'il existe $T \in GL_2(\mathbb{C})$ et $h \neq h'$ ($0 < h, h' < \dfrac{n}{2}$) tels que $T\rho^h = \rho^{h'}T$. Alors $T\rho^h(r)T^{-1} = \rho^{h'}(r)$ ce qui implique que $\rho^h(r)$ et $\rho^{h'}(r)$ ont le même spectre, i.e $\omega^h = \omega^{\pm h'}$, ce qui est absurde. De fait, les représentations ρ^k pour $0 < k < \dfrac{n}{2}$ sont deux à deux non isomorphes.

Comme $|D_n| = 2n = 4 \times 1 + \left(\dfrac{n}{2} - 1\right) \times 2^2$, nous avons trouvé toutes les classes de caractères irréductibles de D_n et sommes donc en mesure de dresser sa table de caractères :

	r^k	sr^k
χ_1	1	1
χ_2	1	-1
χ_3	$(-1)^k$	$(-1)^k$
χ_4	$(-1)^k$	$(-1)^{k+1}$
χ^h $0 < h < n/2$	$2\cos\left(\dfrac{2hk\pi}{n}\right)$	0

Si n est impaire, nous avons seulement deux représentations de degré 1 possibles :

	s	r
χ_1	1	1
χ_2	1	-1

On conclut alors comme précédemment que les représentations ρ^h pour $0 < h \leq \dfrac{n-1}{2}$ sont irréductibles et deux à deux non isomorphes. Comme $2n = 2 \times 1 + \dfrac{n-1}{2} \times 2^2$ on a alors bien la table de caractères suivante :

	s	r
χ_1	1	1
χ_2	1	-1
χ^h $0 < h \leq (n-1)/2$	$2\cos\left(\dfrac{2hk\pi}{n}\right)$	0

Détails supplémentaires :
- La présentation proposée ici de la table de caractères est "non standard" au sens ou ses colonnes ne sont pas agencées selon les classes de conjugaisons. En fait, les classes de conjugaison de D_n sont les suivantes :
  * *si n est pair* : $\{\text{id}\}$, $\{r^{n/2}\}$, $\{s, r^2s, r^4s, \ldots, r^{2n-2}s\}$, $\{rs, r^3s, r^5s, \ldots, r^{2n-1}s\}$ et les $\{r^h, r^{-h}\}$ pour $0 < h < \dfrac{n}{2}$;
  * *si n est impair* : $\{\text{id}\}$, $\{s, rs, \ldots, r^{n-1}s\}$ et les $\{r^h, r^{-h}\}$ pour $0 < h \leq \dfrac{n-1}{2}$.

1.15 Table de caractères de $\mathfrak{S}_4$

Référence :
- [Pey04], p. 228–230

Commençons par dénombrer les classes de conjugaisons de $\mathfrak{S}_4$ qui, comme chacun sait, son caractérisées par le profil :
- l'identité ( ) est seule dans sa classe ;
- les permutations, telle (1 2), forment une classe de cardinal 6 ;
- il y a 8 3–cycles, dont l'un est (1 2 3) ;
- les 4–cycles constituent une classe de 6 éléments comprenant (1 2 3 4) ;
- les doubles permutations [18], telle (1 2)(3 4), sont 3.

Attaquons nous à présent aux caractères.
- On connaît deux représentations de degré 1 de $\mathfrak{S}_4$: la représentation triviale, de caractère χ_1, et la signature, de caractère χ_ε :

	( )	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1

- Considérons la représentation par permutation de $\mathfrak{S}_4$, définie par :

$$\begin{aligned} \rho_p : \mathfrak{S}_4 &\to GL_4(\mathbb{C}) \\ \sigma &\mapsto (\delta_{i,\sigma(j)})_{1\leq i,j\leq n} \end{aligned}$$

  Cette représentation (de degré 4) n'est pas irréductible ; en effet, la droite $\mathcal{D} := \langle(1,1,1,1)\rangle$ y est $\mathfrak{S}_4$–stable et admet pour supplémentaire stable l'hyperplan $\mathcal{H} := \{\underline{x} \in \mathbb{C}^4 \,|\, x_1+x_2+x_3+x_4 = 0\}$. ρ_p induit sur $\mathcal{D}_h$ la représentation triviale et sur $\mathcal{H}$ une certaine représentation, que nous noterons ρ_s. On a alors, avec notations évidentes, $\chi_p = \chi_1 + \chi_s$ et comme pour tout $\sigma \in \mathfrak{S}_4$ $\chi_p(\sigma)$ est égal aux nombres de points fixes de σ on a :

$$\begin{aligned} |\mathfrak{S}_4|\langle\chi_s, \chi_s\rangle &= \chi_s(()\,)^2 + 6\chi_s((1\,2))^2 + 8\chi_s((1\,2\,3))^2 + 6\chi_s((1\,2\,3\,4))^2 + 3\chi_s((1\,2)(3\,4))^2 \\ &= 3^2 + 6 \times 1^2 + 8 \times 0^2 + 6 \times (-1)^2 + 3 \times (-1)^2 \\ &= 24 \end{aligned}$$

  Donc $\langle\chi_s, \chi_s\rangle = 1$: χ_s est irréductible, ce qui nous permet d'ajouter la ligne suivante à notre table :

18. À supports disjoints !

	( )	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_s	3	1	0	-1	-1

- On sait qu'il existe autant de classes de représentations irréductibles de $\mathfrak{S}_4$ que de classes de conjugaison dans ce dernier, donc il nous reste deux représentations à trouver, de dimensions n_4, n_5. De plus on sait que l'on doit avoir $n_4^2 + n_5^2 = 24 - (1^2 + 1^2 + 3^2) = 13$ d'où $n_4 = 2$ et $n_5 = 3$.
- Avec notations évidentes, posons $W := \mathcal{L}(V_s, V_\varepsilon)$. Cette représentation est de dimension $3 \times 1 = 3$ et son caractère est $\chi_W = \chi_s \overline{\chi_\varepsilon}$. Un calcul rapide montre alors que $\langle \chi_W, \chi_W \rangle = 1$ et donc χ_W est irréductible ; on peut donc ajouter à notre table :

	( )	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_W	3	-1	0	1	-1

- Le dernier caractère peut être déduit de la relation d'orthogonalité des colonne :

	( )	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
$\chi_{W'}$	2	0	-1	0	2

Au final on a la table de caractères suivante :

	( )	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
$\chi_{W'}$	2	0	-1	0	2
χ_s	3	1	0	-1	-1
χ_W	3	-1	0	1	-1

Détails supplémentaires :

- *Orthogonalité des colonnes.* Si $((\chi_i, n_i))_{i \in [p]}$ sont des couples (caractère, dimension) décrivant exactement l'ensemble des classes de représentations irréductibles d'un groupe G on :

$$\forall s \in G \setminus \{e_G\}, \qquad \sum_{i=1}^{p} n_i \chi_i(s) = 0$$

- Alternativement (c'est d'ailleurs plutôt conseillé), on peut construire χ_W à l'aide du "dictionnaire" $\mathfrak{S}_4 \cong \mathrm{Isom}^+(C_6)$. Pour trouver les entrées de la table de caractères il suffit alors de prendre les traces des rotations correspondantes.

1.16 Théorème de Burnside

Référence :
- [FGN09a], p. 185–186

Lemme 1.7 ([FGN09a], p. 111)
Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$.
Soit $A \in \mathcal{M}_n(\mathbb{K})$ telle que :

$$\forall k \geq 1, \quad \mathrm{Tr}(A^k) = 0$$

Alors A est nilpotente.

Démonstration : Supposons A non nilpotente : on peut alors noter $\lambda_1, \ldots, \lambda_r$ ($r \geq 1$) ses valeurs propres (sur $\mathbb{C}$) non nulles et $n_1, \ldots, n_r$ leurs multiplicités respectives. Alors il existe $P \in GL_n(\mathbb{C})$ telle que $A = P^{-1}TP$ où T est triangulaire de diagonale $(\underbrace{\lambda_1 \ \ldots \ \lambda_1}_{n_1} \ldots \underbrace{\lambda_r \ \ldots \ \lambda_r}_{n_r}, 0 \ldots 0)$. De plus, comme pour $k \geq 1$ on a $A^k = P^{-1}T^kP$ alors :

$$\forall k \geq 1, \quad 0 = \mathrm{Tr}(A^k) = \sum_{i=1}^{r} n_i \lambda_i^k$$

De fait, le vecteur $\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix}$ est solution du système suivant :

$$\begin{pmatrix} \lambda_1 & \dots & \dots & \lambda_r \\ \lambda_1^2 & & & \lambda_r^2 \\ \vdots & & & \vdots \\ \lambda_1^r & \dots & \dots & \lambda_r^r \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_r \end{pmatrix} = 0 \tag{1.16.1}$$

Le déterminant de ce système est alors, par déterminant de Vandermonde (cf infra) :

$$\left(\prod_{i=1}^{r} \lambda_i\right) \prod_{1\leq i<j\leq r} (\lambda_j - \lambda_i) \neq 0$$

Donc les n_i sont tous nuls, ce qui est absurde.

Proposition 1.16 (Burnside)
Soit $G \leq GL_n(\mathbb{C})$.
Alors G est fini si et seulement G est d'exposant fini[19].

Démonstration : Le sens direct est immédiat par théorème de Lagrange. Pour le sens indirect, commençons par fixer une base $(M_i)_{1\leq i\leq m} \in G^m$ du s-e.v $\langle G\rangle_{\mathbb{C}}$ engendré par G dans $\mathcal{M}_n(\mathbb{C})$ et considérons l'application suivante :

$$\begin{aligned} f : G &\to \mathbb{C}^m \\ A &\mapsto (\mathrm{Tr}(AM_i))_{1\leq i\leq m} \end{aligned}$$

Supposons que l'on ait A et B dans G telles que $f(A) = f(B)$. Alors, par linéarité de la trace on a :

$$\forall M \in \langle G\rangle_{\mathbb{C}}, \quad \mathrm{Tr}(AM) = \mathrm{Tr}(BM)$$

En particulier si on pose $D := AB^{-1} \in G$ et si $k \geq 1$ on a :

$$\begin{aligned} \mathrm{Tr}(D^k) &= \mathrm{Tr}(A\underbrace{B^{-1}D^{k-1}}_{\in G\subset\langle G\rangle_{\mathbb{C}}}) \\ &= \mathrm{Tr}(BB^{-1}D^{k-1} \\ &= \mathrm{Tr}(D^{k-1} \\ &\vdots \\ &= \mathrm{Tr}(I_n) \\ &= n \end{aligned}$$

Ainsi :

$$\begin{aligned} \mathrm{Tr}((D-I_n)^k) &= \mathrm{Tr}\left(\sum_{j=0}^{k} C_k^j (-1)^j D^{k-j}\right) \\ &= \sum_{j=0}^{k} C_k^j (-1)^j \mathrm{Tr}(D^{k-j}) \\ &= n(1-1)^k \\ &= 0 \end{aligned}$$

De fait $D - I_n$ est nilpotente (lemme 1.7).

Comme G est d'exposant fini $N \geq 1$, toutes ses matrices sont diagonalisables (car racines du polynôme scindé simple $X^N - 1$). Donc D est diagonalisable ce qui implique que $D - I_n$ l'est également (car $\forall P \in GL_n(\mathbb{C})$, $P^{-1}(D - I_n)P = P^{-1}DP - I_n$). Donc, par nilpotence, $D = I_n$ et donc f est injective.

Remarquons ensuite que $f(G) \subset X^m$ où $X := \{\mathrm{Tr}(A) \,|\, A \in G\}$ est fini car les valeurs propres d'éléments de G sont des racines N–ièmes de l'unité. De fait, par injectivité de f, G est fini.

19. I.e $\exists N \in \mathbb{N}^*$, $\forall g \in G$, $g^N = I_n$.

Détails supplémentaires :

- *Déterminant de Vandermonde.* On désire calculer le déterminant suivant ([FGN09a], p. 17), les $x_i \in \mathbb{C}$:

$$V(x_1, \dots, x_n) = \begin{vmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \dots & x_n^{n-1} \end{vmatrix}$$

Il est clair que si deux des x_i sont égaux ce déterminant est nul. Dans le cas contraire on pose :

$$P := V(x_1, \dots, x_{n-1}, X) \in \mathbb{C}_{n-1}[X]$$

En développant selon la première colonne on trouve que le coefficient de degré $n-1$ de P est $V(x_1, \dots, x_{n-1}$; il est également clair d'après la remarque précédente que si $i \in [n-1]$, $P(x_i) = 0$. De fait, le polynôme unitaire de degré $n-1$ $\prod_{i\in[n-1]}(X - x_i)$ divise P et donc :

$$P = V(x_1, \dots, x_{n-1} \prod_{i=1}^{n-1} (X - x_i)$$

Ergo :

$$V(x_1, \dots, x_n) = P(x_n) = V(x_1, \dots, x_{n-1} \prod_{i=1}^{n-1} (x_n - x_i)$$

Et donc par récurrence :

$$V(x_1, \dots, x_n) = \prod_{1\le i<j\le n} (x_j - x_i)$$

1.17 Théorème de Caratheodory

Référence :

- [FGN10], p. 316 – 317

Proposition 1.17 (Caratheodory)
Soit $X \subset \mathbb{R}^n$ un ensemble non vide.
On note $\mathcal{C}(X)$ l'enveloppe convexe de X.
Alors tout point de $\mathcal{C}(X)$ est barycentre à coefficients positifs d'une famille de $n+1$ points de X.

Démonstration : Soit $x \in \mathcal{C}(X)$. Par définition de l'enveloppe convexe, x est barycentre à coefficients positifs de points de x, i.e

$$\exists p > 0,\ \exists \lambda_1, \dots, \lambda_p \ge 0,\ \exists x_1, \dots, x_p \in X,\ \text{tels que } \sum_{k=1}^{p} \lambda_k = 1 \text{ et } \sum_{k=1}^{p} \lambda_k x_k = x$$

Supposons $p > n+1$. Alors $p - 1 > n = \dim(\mathbb{R}^n)$ donc la famille $(x_i - x_1)_{2\le i\le p}$ est liée dans $\mathbb{R}^n$, i.e il existe $\alpha_1, \dots, \alpha_p \in \mathbb{R}$ non tous nuls tels que ;

$$\sum_{i=2}^{p} \alpha_i (x_i - x_1) = 0 \tag{1.17.1}$$

Posons également :

$$\alpha_1 := -\sum_{i=2}^{p} \alpha_i$$

Alors :

$$\begin{aligned}\sum_{i=1}^{p}\alpha_i x_i &= \sum_{i=2}^{p}\alpha_i x_i + \alpha_1 x_1\\ &= \sum_{i=2}^{p}\alpha_i x_1 + \alpha_1 x_1 \text{ par (1.17.1)}\\ &= \sum_{i=2}^{p}\alpha_i x_1 - \left(\sum_{i=2}^{p}\alpha_i\right) x_1\\ &= 0\end{aligned}$$

Ergo :

$$\forall t\in\mathbb{R},\ x = \sum_{i=1}^{p}\lambda_i x_i + t\sum_{i=1}^{p}\alpha_i x_i = \sum_{i=1}^{p}(\lambda_i + t\alpha_i)x_i$$

Les α_i sont non tous nuls de somme nul donc il existe un indice i tel que $\alpha_i < 0$. De fait, on peut poser :

$$\tau := \min\left\{ -\frac{\lambda_i}{\alpha_i} \,\middle|\, \alpha_i < 0\right\}$$

On pose ensuite pour tout $i\in[p]$ $\mu_i := \lambda_i + \tau\alpha_i$. Alors :

- les μ_i sont positifs ou nuls par construction de τ ;
- on a :

$$\sum_{i=1}^{p}\mu_i = \sum_{i=1}^{p}\lambda_i + \tau\sum_{i=1}^{p}\alpha_i = \sum_{i=1}^{p}\lambda_i = 1$$

- l'un des μ_i au moins est nul (prendre l'indice j pour lequel le minimum τ est atteint).

In fine :

$$\sum_{i\neq j}\mu_i x_i = \sum_{i=1}^{p}\mu_i x_i = \sum_{i=1}^{p}(\lambda_i + \tau\alpha_i)x_i = x$$

On a donc écrit x comme barycentre à coefficients positifs de $p-1$ points de X. On obtient alors le résultat en itérant ce procédé.

Corollaire 1.17.1

Soit $X\subset\mathbb{R}^n$ un compact *non vide.*
Alors $\mathcal{C}(X)$ est compacte.

DÉMONSTRATION : On considère le simplexe Λ de $\mathbb{R}^{n+1}$:

$$\Lambda := \left\{\lambda\in\mathbb{R}_+^{n+1} \,\middle|\, \sum_{k=1}^{n+1}\lambda_k = 1\right\}$$

Définissons également l'application suivante :

$$\begin{aligned} f : \Lambda\times X^{n+1} &\to \mathbb{R}^n\\ (\lambda, x) &\mapsto \sum_{k=1}^{n+1}\lambda_k x_k\end{aligned}$$

Alors f est continue (car — entre autres — bilinéaire en dimension finie) et par théorème de Caratheodory, $\mathcal{C}(X) = f(\Lambda\times X^{n+1})$. De fait, par compacité de $\Lambda\times X^{n+1}$, $\mathcal{C}(X)$ est bien compacte.

Détails supplémentaires :

- *Compacité du simplexe.* Le simplexe Λ est clairement borné (par exemple par 1 en norme $\|.\|_\infty$. De plus, si $(\lambda^p)_p\in\Lambda^{\mathbb{N}}$ converge vers $\lambda\in\mathbb{R}^{n+1}$ (par exemple pour $\|.\|_\infty$) alors par convergence coordonnée par coordonnée :

$$1 = \sum_{k=1}^{n+1}\lambda_k^p \xrightarrow[p\to\infty]{} \sum_{k=1}^{n+1}\lambda_k$$

Donc $\lambda\in\Lambda$ et donc le simplexe est fermé, d'où le résultat par dimension finie.

1.18 Théorème de Chevalley–Warning

Référence :
- [Ser95], p. 12–13

Soit p un nombre premier et $r \geq 1$; on pose $q := p^r$.

Lemme 1.8
Soit $u \in \mathbb{N}$.
On pose :

$$S(X^u) := \sum_{x \in \mathbb{F}_q} x^u$$

Alors :

$$S(X^u) = \begin{cases} -1 & \text{si } u \geq 1 \text{ et } q-1|u \\ 0 & \text{sinon} \end{cases}$$

Démonstration :
- Si $u = 0$, on a $S(X^u) = q \times 1 = 0$, d'où le résultat.
- Si $u \geq 1$ et $q-1|u$, i.e $\exists k \in \mathbb{N}$, $u = (q-1)k$, alors $0^u = 0$ et, par théorème de Lagrange, $\forall x \in \mathbb{F}_q^*$, $x^u = (x^{q-1})^k = 1^k = 1$. De fait, $S(X^u) = q - 1 = 1$.
- Si $u \geq 1$ et $q-1 \nmid u$, alors comme $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$ il existe $y \in \mathbb{F}_q^*$ tel que $y^u \neq 1$ (cf. infra). De fait :

$$\begin{aligned} S(X^u) &= \sum_{x \in \mathbb{F}_q} x^u \\ &= \sum_{x \in \mathbb{F}_q^*} x^u \\ &= \sum_{x \in \mathbb{F}_q^*} (xy)^u \\ &= y^u S(X^u) \end{aligned}$$

  De fait $(1 - y^u)S(X^u) = 0$ donc (comme $y^u \neq 1$) $S(X^u) = 0$.

Proposition 1.18 (Chevalley–Warning)
Soit A un ensemble fini.
Soit $(f_\alpha)_{\alpha \in A} \in \mathbb{F}_q[X_1, \ldots, X_n]^A$ telle que :

$$\sum_{\alpha \in A} \deg(f_\alpha) < n$$

On considère la courbe algébrique $V := \{\underline{x} \in \mathbb{F}_q^n \,|\, \forall \alpha \in A,\ f_\alpha(\underline{x}) = 0\}$ définie par les f_α.
Alors :

$$\mathrm{card}(V) \equiv 0[p]$$

Démonstration : Commençons par fixer $\underline{x} \in \mathbb{F}_q^n$ et posons :

$$P := \prod_{\alpha \in A} (1 - f_\alpha^{q-1})$$

- Si $\underline{x} \in V$, alors il est clair que $P(\underline{x}) = 1$.
- Dans le cas contraire, il existe $\alpha_0 \in A$ tel que $f_{\alpha_0}(\underline{x}) \neq 0$ et donc $f_{\alpha_0}^{q-1}(\underline{x}) = 1$, d'où $P(\underline{x}) = 0$.

De fait P est la fonction caractéristique χ_V de V.

Soit $f \in \mathbb{F}_q[X_1, \ldots, X_n]$; on pose :

$$S(f) := \sum_{\underline{x} \in \mathbb{F}_q^n} f(\underline{x})$$

Comme $P = \chi_V$ on a nécessairement $\mathrm{card}(V) \equiv S(P)[p]$. Il nous reste donc à montrer que $S(P) = 0$ dans $\mathbb{F}_q$.

Comme $\sum \deg(f_\alpha) < n$ on a $\deg(P) < n(q-1)$ donc P est combinaison linéaire de monômes $\underline{X}^{\underline{u}} := \prod_{i=1}^n X_i^{u_i}$, avec $|\underline{u}| < n(q-1)$. Or :

$$\begin{aligned}
S(\underline{X}^{\underline{u}}) &= \sum_{\underline{x}\in\mathbb{F}_q^n} \prod_{i=1}^n x_i^{u_i} \\
&= \prod_{i=1}^n \sum_{x\in\mathbb{F}_q} x^{u_i} \\
&= \prod_{i=1}^n S(X^{u_i}) \\
&= 0 \text{ car au moins l'un des } u_i \text{ vérifie } u_i < q-1 \text{ donc } q-1 \nmid u_i \text{ (lemme 1.8)}
\end{aligned}$$

Détails supplémentaires :

– *Il existe $y \in \mathbb{F}_q^*$ tel que $y^u \neq 1$ $(u \geq 1$ et $q-1 \nmid u)$* . Dans le cas contraire on aurait, si y_0 engendre $\mathbb{F}_q^*$, $y_0^u = 1$ et alors par division euclidienne $u = a(q-1) + r$, avec $0 < r < q-1$. Or ceci impliquerait $y_0^r = 1$ ce qui est absurde car y_0 est d'ordre $q-1$.

1.19 Théorème des deux carrés

Référence :

– [Per96], p. 56–58

Prérequis :

– structure de $\mathbb{Z}[i]$.

On considère dans toute la suite l'ensemble suivant : $\Sigma := \{a^2+b^2 \mid a, b \in \mathbb{N}\}$. Il s'agit d'un monoïde commutatif (lemme 1.10).

Lemme 1.9 (Théorème des deux carrés, version faible)
Soit p un nombre premier.
Alors

$$p \in \Sigma \quad \Leftrightarrow \quad p = 2 \text{ ou } p \equiv 1[4]$$

Démonstration :

Remarquons que (cf. infra) $p \in \Sigma \Leftrightarrow p$ est réductible dans $\mathbb{Z}[i]$. $\mathbb{Z}[i]$ étant euclidien, il est factoriel et donc :

$$\begin{aligned}
p \text{ est réductible } &\Leftrightarrow (p) \text{ n'est pas premier} \\
&\Leftrightarrow \mathbb{Z}[i]/(p) \text{ n'est pas intègre}
\end{aligned}$$

Or $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$ ergo :

$$\begin{aligned}
\mathbb{Z}[i]/(p) &\cong (\mathbb{Z}[X]/(X^2+1))/(p) \\
&\cong \mathbb{F}_p[X]/(X^2+1)
\end{aligned}$$

De fait :

$$\begin{aligned}
(p) \text{ n'est pas premier } &\Leftrightarrow X^2+1 \text{ est réductible sur} \mathbb{F}_p \\
&\Leftrightarrow X^2+1 \text{ admet une racine sur } \mathbb{F}_p \\
&\Leftrightarrow -1 \in (\mathbb{F}_p^*)^2 \\
&\Leftrightarrow p = 2 \text{ ou } p \cong 1[4]
\end{aligned}$$

La dernière équivalence provient du fait que $x \in (\mathbb{F}_p^*)^2 \Leftrightarrow x^{(p-1)/2} = 1$. On raisonne [20] ensuite sur l'ensemble $X := \{x \in \mathbb{F}_p \mid x^{(p-1)/2} = 1$ qui est de cardinal inférieur ou égal à $\frac{q-1}{2}$ et contient $(\mathbb{F}_p^*)^2$ donc y est égal par égalité de leurs [21] cardinaux respectifs. D'où le résultat.

20. Raisonnement valable sur tout corps fini.
21. Le lecteur pointilleux pourra me reprocher le pluriel ici. Tant pis.

Proposition 1.19 (Théorème des deux carrés) *Soit $n \geq 2$ un entier dont la décomposition en produit de facteurs premiers est donnée par :*

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

Alors :

$$n \in \Sigma \quad \Leftrightarrow \quad \forall p \in \mathcal{P} \text{ tel que } p \equiv 3[4],\ v_p(n) \equiv 0[2]$$

DÉMONSTRATION :

($\Leftarrow$) Clair en combinant les lemmes 1.10 et 1.9.

($\Rightarrow$) Soit $p \in \mathcal{P}$ congru à 3 modulo 4. Démontrons le résultat par récurrence[22] "sur $v_p(n)$" i.e montrons que si pour tout $k \geq 0$ et tout $n \in \Sigma$ tel que $v_p(n) \leq k$ alors $v_p(n)$ est pair.
- $k = 0$. 0 est pair.
- Supposons la propriété vrai pour $v_p(n) \leq k$, avec $k \geq 0$ et supposons $v_p(n) \leq k+1$. Alors $p | n = a^2 + b^2 = (a+ib)(a-ib)$ dans $\mathbb{Z}[i]$, avec $a, b \in \mathbb{N}$. De fait, p divise (par exemple) $a + ib$. Comme p est entier, on a de fait $p|a$ et $p|b$ ergo $p^2|n$.
  En posant $a = pa'$ et $b = pb'$ on remarque que $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$. Or $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 \leq k$ donc par hypothèse de récurrence (comme $\frac{n}{p^2} \in \Sigma$) $v_p(n) - 2$ est pair donc $v_p(n)$ l'est. D'où le résultat.

Détails supplémentaires :
- On fait usage du lemme suivant ([Per96], p. 56) :

  Lemme 1.10
  $(\Sigma, \times)$ est un sous-monoïde de $\mathbb{N}$.
  DÉMONSTRATION : Commençons par remarquer que, si note N le stathme usuel sur $\mathbb{Z}[i]$:

  $$n \in \Sigma \quad \Leftrightarrow \quad \exists z \in \mathbb{Z}[i],\ n = N(z)$$

  Il est clair que Σ est non vide ($0 \in \Sigma$). De plus, si $z, z' \in \mathbb{Z}[i]$, on a $N(z)N(z') = N(zz')$ et donc Σ est stable par multiplication. On retrouve au passage l'identité dite de Lagrange :

  $$\forall a, b, c, d \in \mathbb{N}, \quad (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{1.19.1}$$

- *Pour un nombre premier p, $p \in \Sigma \Leftrightarrow p$ est réductible dans $\mathbb{Z}[i]$.*
  - Pour le sens direct, on suppose $p = a^2 + b^2$. Alors a et b sont non nuls et donc $p = (a+ib)(a-ib)$ est réductible.
  - Réciproquement, si $p = zz'$ avec z, z' n.n.n.i. Alors $N(p) = N(z)N(z') = p^2$. Comme $N(z), N(z') \neq 1$ ils sont égaux à p et donc (par exemple) $p = N(z) \in \Sigma$.

1.20 Théorème de Kronecker

Référence :
- [Szp09], p. 573

Proposition 1.20
Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $n \geq 1$:

$$P =: X^n + \sum_{i=1}^{n} a_i X^{n-i}$$

On fait les hypothèse suivantes :
- *les racines de P sur $\mathbb{C}$ sont de module inférieur ou égal à 1 ;*
- *$a_n \neq 0$ (i.e $X \nmid P$).*

Alors les racines de P sont des racines de l'unité.

DÉMONSTRATION : Dans toute la suite, on dira qu'un polynôme $R \in \mathbb{Z}[X]$ vérifie la propriété (K_n) si :

22. Comme pour le grand théorème de Fermat.

- R est unitaire de degré n ;
- les racines de R sur $\mathbb{C}$ sont de module inférieur ou égal à 1 ;
- X ne divise pas R.

Il va sans dire que P vérifie (K_n). Notons $\alpha_1, \ldots, \alpha_n$ les racines de P comptées avec multiplicité ; on a alors, par relations coefficients–racines :

$$\begin{aligned}\forall k \in [n], \quad |a_k| &= \left| \sum_{1 \leq i_1 < \ldots < i_k \leq n} \prod_{j=1}^{k} \alpha_{i_j} \right| \\ &\leq C_n^k \text{ car } \forall \ell \in [n],\ |\alpha_\ell| \leq 1\end{aligned}$$

Soit $R := X^n + \sum_{i=1}^{n} b_i X^{n-i} \in \mathbb{Z}[X]$ un polynôme vérifiant la propriété (K_n) ; alors on a de même que pour tout $k \in [n]$, $|b_k| \leq C_n^k$ et donc b_k appartient à l'ensemble $\{-C_n^k, \ldots, C_n^k\}$, qui est de cardinal $2C_n^k + 1$. De fait le nombre de polynômes de $\mathbb{Z}[X]$ vérifiant (K_n) est majoré par $\prod_{k=1}^{n}(1 + 2C_n^k)$ donc est fini.

Pour $k \in \mathbb{N}^*$ on pose à présent :

$$P_k := \prod_{i=1}^{n}(X - \alpha_i^k) \text{ et } Q_k := X^k - Y \in \mathbb{Z}[X, Y]$$

On pose ensuite, toujours pour $k \geq 1$: $R_k := \mathrm{Res}_X(P, Q_k)$, i.e :

$$R_k = \begin{vmatrix} 1 & & & 1 & & \\ a_1 & \ddots & & & \ddots & \\ \vdots & \ddots & 1 & & & 1 \\ a_n & & a_1 & -Y & & \\ & \ddots & \vdots & & \ddots & \\ & & a_n & & & -Y \end{vmatrix}$$

Il est alors clair que $R_k \in \mathbb{Z}[Y]$ et que son coefficient dominant est $(-1)^n Y^n$. De plus on a :

$$R_k(Y) = \prod_{i=1}^{n} Q_k(\alpha_i) = (-1)^n P_k(Y)$$

Il est de fait immédiat que $P_1 = P$ et que les P_k vérifient (K_n).

Comme les P_k vérifient (K_n), il existe $k > 1$ tel que $P_k = P_1 = P$ et donc P et P_k ont les mêmes racines avec les mêmes multiplicité. De fait, si α est une racine de P, α^k est une racine de P_k donc de P. Mais alors, $(\alpha^k)^k = \alpha^{k^2}$ est une racine de P_k donc de P, ... In fine, tous les éléments de la suite $(\alpha^{k^p})_{p \in \mathbb{N}^*}$ sont des racines de P. P ayant un nombre fini de racines on a alors l'existence de $p, q \geq 1$ avec $p < q$ tels que $\alpha^{k^p} = \alpha^{k^q}$ et donc $\alpha^{k^p - k^q} = 1$: α est bien une racine de l'unité.

1.21 Théorème de Wedderburn

Référence :
- [Per96], p. 82

Proposition 1.21 (Wedderburn)
Tout anneau à division fini est un corps.

Démonstration : Soit $\mathbb{K}$ un anneau à division fini. Considérons son centre $Z := \{a \in \mathbb{K} \mid \forall x \in \mathbb{K},\ ax = xa\}$. Alors Z est un corps contenu dans $\mathbb{K}$, de cardinal $q \geq 2$ (car $0, 1 \in Z$). De fait, on peut munir $\mathbb{K}$ d'une structure de Z–espace vectoriel de dimension finie $n \geq 1$, qui nous donne l'égalité $|\mathbb{K}| = q^n$.

Supposons à présent $\mathbb{K}$ non commutatif, i.e $n > 1$. Remarquons que le groupe $\mathbb{K}^*$ agit sur lui–même par conjugaison. Si $x \in \mathbb{K}^*$, on note $\omega(x)$ son orbite sous cette action, $\mathbb{K}_x := \{y \in \mathbb{K} \mid yx = xy\}$ et $\mathbb{K}_x^* := \{y \in \mathbb{K}^* \mid yx = xy\}$ son stabilisateur. $\mathbb{K}_x$ est un sous–anneau de $\mathbb{K}$ contenant Z et peut donc être vu comme un Z–espace vectoriel de dimension finie $d \geq 1$ avec de facto l'égalité $|\mathbb{K}_x| = q^d$.

Comme $\mathbb{K}_x^*$ est un sous–groupe de $\mathbb{K}^*$, alors par théorème de Lagrange $q^d - 1 | q^n - 1$ et donc comme $q \geq 2$, $d|n$. Ainsi, pour $x \in \mathbb{K}^* x$, on a :

$$|\omega(x)| = \frac{|\mathbb{K}^*|}{|\mathbb{K}_x^*|} = \frac{q^n - 1}{q^d - 1} = \frac{\prod_{m|n} \phi_m(q)}{\prod_{m|d} \phi_m(q)} = \prod_{m|n,\, m\nmid d} \phi_m(q)$$

Où ϕ_m dénote le m–ième polynôme cyclotomique sur $\mathbb{C}$. Alors, dans le cas où $d \neq n$ (possible car $n > 1$), on a :

$$\phi_n(q) \,|\, \frac{q^n - 1}{q^d - 1} \tag{1.21.1}$$

La formule des classes s'écrit alors :

$$|\mathbb{K}^*| = |Z^*| + \sum |\omega(x)| \tag{1.21.2}$$

Où la somme compte chaque orbite une fois. On a donc :

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}$$

Où la somme décrit un sous ensemble des diviseurs stricts de n associé aux orbites par le procédé précédent. Comme $\phi_n(q)$ divise $q^n - 1$ et par la relation (1.21.1), on a :

$$\phi_n(q) \,|\, q - 1$$

De fait, $|\phi_n(q)| \leq q - 1$. Mais si on note $\xi_1, \ldots, \xi_\ell$ les racines primitives n–ièmes de l'unité sur $\mathbb{C}$ (les $\xi_i \neq 1$ car $n \neq 1$) alors :

$$\phi_n(q) = \prod_{i=1}^{\ell} (q - \xi_i)$$

De plus $\forall i \in [\ell]$, $|q - \xi_i| > 1$ (car les ξ_i sont sur le cercle unité et différentes de 1 : faire un dessin), d'où :

$$|\phi_n(q)| > (q - 1)^\ell \geq q - 1$$

Ce qui apporte la contradiction désirée.

Détails supplémentaires :

– Il est bon de savoir démontrer le lemme suivant :

  Lemme 1.11
  Soit $q \in \mathbb{N}$, $q \geq 2$.
  Soient $n, d \in \mathbb{N}$ tels que $q^d - 1 \,|\, q^n - 1$.
  Alors $d|n$.
  Démonstration : Par division euclidienne, il existe un unique couple (a, b) d'entiers naturels tels que $n = ad + b$ et $0 \leq b < d$. En remarquant que $q^d \equiv 1[q^d - 1]$, on a :

  $$q^n \equiv (q^d)^a q^b \equiv q^b [q^d - 1]$$

  Or $q^n \equiv 1[q^d - 1]$ par hypothèse d'où $q^d - 1 \,|\, q^b - 1$. Cependant, $b < d$ et $q \geq 2$ donc $q^b - 1 < q^d - 1$ donc nécessairement $b = 0$.

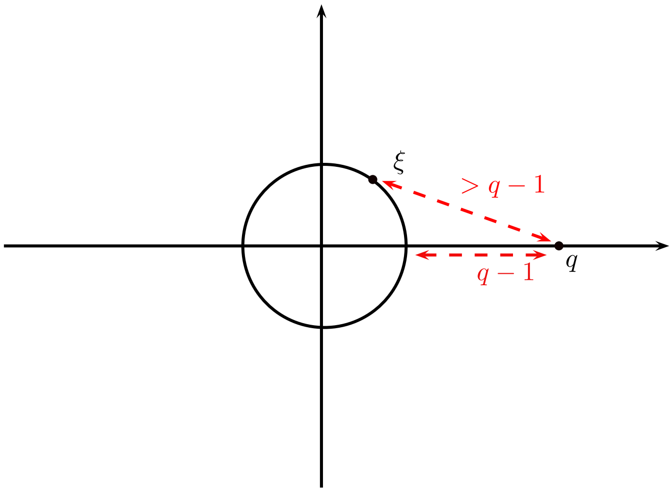
– On trouve l'écriture suivante de la formule (1.21.2) dans [Per96] :

  $$|\mathbb{K}^*| = |Z^*| + \sum_{x \notin Z} |\omega(x)|$$

  Cependant on "compte" alors chaque orbite plusieurs fois, d'où la nécessité de restreindre la somme à un représentant par orbite (on peut aussi sommer sur l'espace quotient $\mathbb{K}^*/\sim$, où $x \sim y \Leftrightarrow \exists g \in \mathbb{K}^*,\, gxg^{-1} = y$). On pourra se référer à [Art91], p. 198.

– Si ξ est une racine primitive n–ième de l'unité alors les autres sont les ξ^m, avec $m \wedge n = 1$. Ainsi dans la démonstration, $\ell = \varphi(n)$ (cf. [Per96], p.80).

– En bonus, un dessin pour mieux comprendre la fin de la démonstration :



Chapitre 2

Développements d'analyse

2.1 Critère de Weyl

Référence :
- [FGN09b], p. 47–49

Proposition 2.1 (Weyl)
Soit $u \in [0,1]^{\mathbb{N}}$.
Pour $0 \leq a \leq b \leq 1$ *et* $n \in \mathbb{N}^*$ *on pose :*

$$X_n(a,b) := \operatorname{card}\{k \in [n] \mid u_k \in [a,b]\}$$

On a alors équivalence entre les trois propriétés suivantes :

(i) Pour tous $0 \leq a \leq b \leq 1$ *on a :*

$$\frac{X_n(a,b)}{n} \xrightarrow[n\to\infty]{} b-a$$

(ii) pour toute fonction $f \in \mathcal{C}^0([0,1],\mathbb{R})$ *on a :*

$$\frac{1}{n}\sum_{k=1}^{n} f(u_k) \xrightarrow[n\to\infty]{} \int_0^1 f(t)dt$$

(iii) pour tout $p \in \mathbb{N}^*$ *on a :*

$$\frac{1}{n}\sum_{k=1}^{n} e^{2i\pi p u_k} \xrightarrow[n\to\infty]{} 0$$

Démonstration :

$(i) \Rightarrow (ii)$ On se donne $\leq a \leq b \leq 1$. Commençons par remarquer que :

$$\forall n \geq 1, \quad \frac{X_n(a,b)}{n} = \frac{1}{n}\sum_{k=1}^{n} 1_{[a,b]}(u_k) \text{ et } \int_0^1 1_{[a,b]}(t)dt = b-a$$

De fait, la conditions (ii) est vérifiée par les fonctions indicatrices de segments inclus dans $[0,1]$ et donc, par linéarité, aux fonctions en escalier sur $[0,1]$.
Soient à présent $f \in \mathcal{C}^0([0,1],\mathbb{R})$ et $\varepsilon > 0$: on sait qu'on dispose alors par densité d'une application g en escalier sur $[0,1]$ telle que $\|f-g\|_\infty \leq \varepsilon$. Or :

$$\left|\frac{1}{n}\sum_{k=1}^{n} f(u_k) - \int_0^1 f(t)dt\right| \leq \left|\frac{1}{n}\sum_{k=1}^{n} f(u_k) - g(u_k)\right| \tag{2.1.1}$$

$$+\left|\frac{1}{n}\sum_{k=1}^{n} g(u_k) - \int_0^1 g(t)dt\right| \tag{2.1.2}$$

$$+\left|\int_0^1 g(t)dt - \int_0^1 f(t)dt\right| \tag{2.1.3}$$

Le terme(2.1.1) est aisément majoré par $\frac{1}{n}\sum_{k=0}^{n}\|f-g\|_\infty = \|f-g\|_\infty \le \varepsilon$, de même que (2.1.3) l'est par $\int_0^1 \|f-g\|_\infty dt = \|f-g\|_\infty \le \varepsilon$. De plus, g est une fonction en escalier donc il existe[1] $N \in \mathbb{N}^*$ tel que :

$$\forall n \ge N, \quad \left| \frac{1}{n}\sum_{k=1}^{n} g(u_k) - \int_0^1 g(t)dt \right| \le \varepsilon$$

D'où une majoration de (2.1.2) par ε pour n assez grand et donc la propriété (ii).

$(ii) \Rightarrow (i)$ Soient $0 < \alpha < \beta < 1$. Pour $k \ge 1$ on définit deux fonctions ψ_k et ϕ_k continues sur $[0,1]$ comme suit : ψ_k (resp. ϕ_k) est nulle sur $[0,\alpha] \cup [\beta,1]$ (resp. sur $\left[0,\alpha-\frac{1}{k}\right] \cup \left[\beta+\frac{1}{k},1\right]$), constante égale à 1 sur $\left[\alpha+\frac{1}{k},\beta-\frac{1}{k}\right]$ (resp. sur $[\alpha,\beta]$) et affine partout ailleurs.

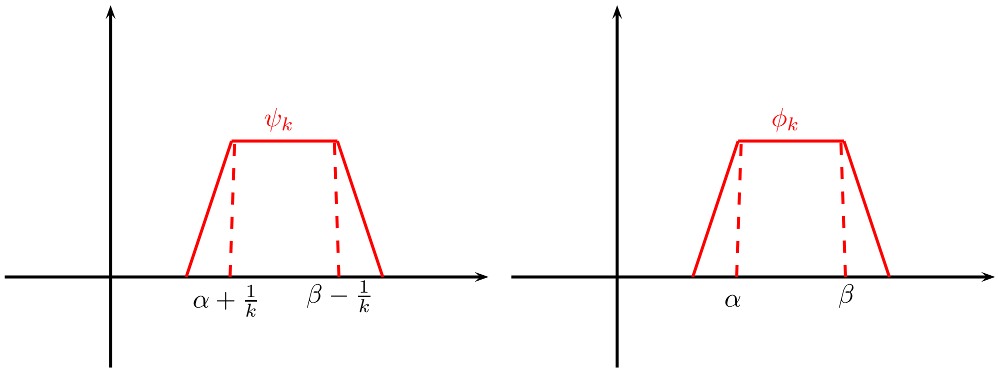


FIGURE 2.1 – Allure des fonctions ψ_k et ϕ_k.

Il est alors clair que pour tout $p \in \mathbb{N}^*$, $\psi_p \le 1_{[\alpha,\beta]} \le \phi_p$ et donc, comme $\frac{X_n(\alpha,\beta)}{n} = \frac{1}{n}\sum_{k=1}^{n} 1_{[\alpha,\beta]}(u_k)$:

$$\forall n \ge 1, \quad \frac{1}{n}\sum_{k=1}^{n}\psi_p(u_k) \le \frac{X_n(\alpha,\beta)}{n} \le \frac{1}{n}\sum_{k=1}^{n}\phi_p(u_k) \tag{2.1.4}$$

Or, par (ii), $\frac{1}{n}\sum_{k=1}^{n}\psi_p(u_k) \xrightarrow[n\to\infty]{} \int_0^1 \psi_p(t)dt = \beta-\alpha-\frac{1}{p}$ et $\frac{1}{n}\sum_{k=1}^{n}\phi_p(u_k) \xrightarrow[n\to\infty]{} \int_0^1 \phi_p(t)dt = \beta-\alpha+\frac{1}{p}$ donc si on fixe $\varepsilon > 0$ et p tel que $\frac{1}{p} < \varepsilon$ on a par (2.1.4) :

$$\exists N \ge 0,\ \forall n \ge N, \quad \left|\frac{1}{n}\sum_{k=1}^{n}\psi_p(u_k) - \beta + \alpha\right| \le \varepsilon \text{ et } \left|\frac{1}{n}\sum_{k=1}^{n}\phi_p(u_k) - \beta + \alpha\right| \le \varepsilon$$

D'où :

$$\forall n \ge N, \quad \left|\frac{X_n(\alpha,\beta)}{n} - \beta + \alpha\right| \le 2\varepsilon$$

D'où le résultat (sauf au bord). On adapte ensuite ψ_k et ϕ_k aux cas où $\alpha = 0$ et/ou $\beta = 1$ et on obtient le dernier "morceau" du résultat en suivant exactement le même raisonnement.

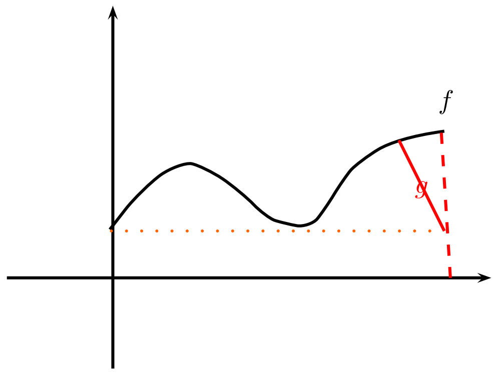
$(ii) \Rightarrow (iii)$ Immédiat en remarquant que $e^{2i\pi p u_k} = \cos(2i\pi p u_k) + i\sin(2i\pi p u_k)$.

$(iii) \Rightarrow (ii)$ Par linéarité, on déduit de (iii) que (ii) est vérifiée par les polynômes trigonométriques. Or, d'après le théorème de Weierstrass (version trigonométrique), si on se donne $f \in \mathcal{C}^0([0,1])$ telle que $f(0) = f(1)$ il existe une suite de polynôme trigonométrique convergeant uniformément vers f. On conclut alors exactement comme en $(i) \Rightarrow (ii)$. Si $f(0) \ne f(1)$ alors pour tout $\varepsilon > 0$ on peut trouver une fonction continue g telle que $g(0) = g(1)$ et $\int_0^1 |f(t)-g(t)|dt \le \varepsilon$ ce qui permet à nouveau de conclure comme en $(i) \Rightarrow (ii)$.

Détails supplémentaires :

- Un dessin pour se convaincre du tout dernier résultat de densité énoncé. Il s'agit juste de contrôler l'aire entre les deux courbes, ce qui reste raisonnable.
- On peut faire un lien entre ce critère et la méthode de Monte–Carlo (point (ii)) pour le calcul approché d'intégrales.

1. Prendre $\frac{1}{N}$ suffisamment proche du pas d'une subdivision de $[0,1]$ adaptée à g.



2.2 Équation de Schrödinger

Référence :
- [Zui02], p. 152–154

Prérequis :
- espaces $\mathcal{C}^\infty(\mathbb{R}, \mathcal{S}'(\mathbb{R}^n))$.

Commençons par conventionner [2] ; pour $v \in \mathcal{S}(\mathbb{R}^n)$ on pose :

$$\overline{\mathcal{F}}v : x \mapsto \frac{1}{(2\pi)^n} \int_{\mathbb{R}^n} e^{i\langle x,\xi\rangle} v(\xi) d\xi \text{ et } \widehat{v} := \mathcal{F}v : x \mapsto \int_{\mathbb{R}^n} e^{-i\langle x,\xi\rangle} v(\xi)$$

On a alors $\mathcal{F}\overline{\mathcal{F}} = \overline{\mathcal{F}}\mathcal{F} = \mathrm{id}_{\mathcal{S}(\mathbb{R}^n)}$. On étend ces deux opérateurs à $\mathcal{S}'(\mathbb{R}^n)$ par le procédé standard $\langle Tg, \varphi\rangle := \langle g, T\varphi\rangle$.

Proposition 2.2
Soit $g \in \mathcal{S}'(\mathbb{R}^n)$.
Alors il existe une unique solution $u = (u_t)_{t\in\mathbb{R}} \in \mathcal{C}^\infty(\mathbb{R}, \mathcal{S}'(\mathbb{R}^n))$ au problème suivant :

$$\left\{ \begin{array}{l} \partial_t u - i\Delta u = 0 \textit{ dans } \mathcal{D}'(\mathbb{R} \times \mathbb{R}^n) \\ u_0 = g \end{array} \right. \tag{2.2.1}$$

DÉMONSTRATION :
- *Existence.* Pour $t \in \mathbb{R}$, posons $u_t := \overline{\mathcal{F}}(e^{-it\|\cdot\|^2}\widehat{g})$. Cette expression a un sens car $\widehat{g} \in \mathcal{S}'(\mathbb{R}^n)$ et on a même $u_t \in \mathcal{S}'(\mathbb{R}^n)$. De plus $u_0 = g$ et et on a bien $u \in \mathcal{C}^\infty(\mathbb{R}, \mathcal{S}'(\mathbb{R}^n))$.
  De plus on a :

$$\begin{aligned}
\forall \psi \in \mathcal{S}(\mathbb{R} \times \mathbb{R}^n),\ \langle \partial_t u - i\Delta u, \psi\rangle &= -\langle u, \partial_t\psi - i\Delta\psi\rangle \\
&= -\int_{\mathbb{R}} \langle u_t, \partial_t\psi(t,.) + i\Delta\psi(t,.)\rangle dt \\
&= -\int_{\mathbb{R}} \langle \overline{\mathcal{F}}(e^{-it\|\cdot\|^2}\widehat{g}), \partial_t\psi(t,.) + i\Delta\psi(t,.)\rangle dt \\
&= -\int_{\mathbb{R}} \langle e^{-it\|\cdot\|^2}\widehat{g}, \overline{\mathcal{F}}(\partial_t\psi(t,.) + i\Delta\psi(t,.))\rangle dt \\
&= -\int_{\mathbb{R}} \langle e^{-it\|\cdot\|^2}\widehat{g}, (\partial_t - i\|.\|^2)(\overline{\mathcal{F}}(\psi(t,.))\rangle dt \\
&= -\int_{\mathbb{R}} \langle \widehat{g}, e^{-it\|\cdot\|^2}(\partial_t - i\|.\|^2)(\overline{\mathcal{F}}(\psi(t,.))\rangle dt
\end{aligned}$$

  Remarquons à présent que, pour tous $t \in \mathbb{R}$ et $\xi \in \mathbb{R}^n$:

$$\partial_t(e^{-it\|\xi\|^2}\overline{\mathcal{F}}(\psi(t,.))(\xi)) = e^{-it\|\xi\|^2}((\partial_t - i\|\xi\|^2)\overline{\mathcal{F}}(\psi(t,.))(\xi))$$

2. Vous avez ma promesse qu'il n'y aura aucun dépassement d'honoraires.

D'où :

$$\begin{aligned}\forall\psi\in\mathcal{S}(\mathbb{R}\times\mathbb{R}^n),\ \langle\partial_t u-i\Delta u,\psi\rangle &= -\int_{\mathbb{R}}\langle\widehat{g},\partial_t(e^{-it\|\cdot\|^2}\overline{\mathcal{F}}(\psi(t,.)))\rangle dt\\ &= -\int_{\mathbb{R}}\partial_t\langle\widehat{g},e^{-it\|\cdot\|^2}\overline{\mathcal{F}}(\psi(t,.))\rangle dt \text{ par dérivation sous le signe intégral}\\ &= -\lim_{N\to\infty}[\langle\widehat{g},e^{-it\|\cdot\|^2}\overline{\mathcal{F}}(\psi(t,.))\rangle]_{t=-N}^{t=N}\end{aligned}$$

Or, par passage à la limite sous le signe intégral on a :

$$\forall\xi\in\mathbb{R},\quad \overline{\mathcal{F}}(\psi(t,.))(\xi)\xrightarrow[t\to\infty]{}0$$

Et donc un nouveau passage à la limite sous le signe intégral nous donne :

$$\forall\psi\in\mathcal{S}(\mathbb{R}\times\mathbb{R}^n),\ \langle\partial_t u-i\Delta u,\psi\rangle=\lim_{N\to\infty}[\langle\widehat{g},e^{-it\|\cdot\|^2}\overline{\mathcal{F}}(\psi(t,.))\rangle]_{t=-N}^{t=N}=0$$

Ainsi, u est bien une solution du problème (2.2.1).

– *Unicité.* Commençons par remarquer que la différence de deux solutions de (2.2.1) est une solution $u\in\mathcal{C}^\infty(\mathbb{R},\mathcal{S}'(\mathbb{R}^n))$ du problème suivant :

$$\begin{cases}\partial_t u-i\Delta u=0 \text{ dans } \mathcal{D}'(\mathbb{R}\times\mathbb{R}^n)\\ u_0=0\end{cases}\tag{2.2.2}$$

Montrer l'unicité de la solution au problème (2.2.1) revient donc à montrer que 0 est l'unique solution du problème (2.2.2). Soit donc u une solution de (2.2.2) ; on a alors :

$$\begin{aligned}\forall\psi\in\mathcal{S}(\mathbb{R}\times\mathbb{R}^n),\ 0&=\langle\partial_t u-i\Delta u,\psi\rangle\\ &=-\langle u,(\partial_t+\Delta)\psi\rangle\\ &=-\int_{\mathbb{R}}\langle u_t,(\partial_t+\Delta)\psi(t,.)\rangle dt\\ &=-\int_{\mathbb{R}}\langle u_t,\partial_t\psi(t,.)\rangle dt-\int_{\mathbb{R}}\langle u_t,\Delta\psi(t,.)\rangle dt\end{aligned}$$

Or (par la relation (2.2.6), cf. infra) :

$$\partial_t\langle u_t,\psi(t,.)\rangle=\langle u_t^{(1)},\psi(t,.)\rangle+\langle u_t,\partial_t\psi(t,.)\rangle$$

Ergo :

$$0=\int_{\mathbb{R}}\partial_t\langle u_t,\psi(t,.)\rangle dt+\int_{\mathbb{R}}\langle u_t^{(1)},\psi(t,.)\rangle-i\langle u_t,\Delta\psi(t,.)\rangle dt$$

De la même façon que précédemment on montre que, comme $\psi(t,\xi)\xrightarrow[t\to\infty]{}0$:

$$\int_{\mathbb{R}}\partial_t\langle u_t,\psi(t,.)\rangle dt=0$$

Et donc on a :

$$\int_{\mathbb{R}}\langle u_t^{(1)},\psi(t,.)\rangle-i\langle u_t,\Delta\psi(t,.)\rangle dt=0\tag{2.2.3}$$

De plus, on vérifie que $\mathcal{F}(u_t^{(1)})=\mathcal{F}(u_t)^{(1)}$:

$$\begin{aligned}\forall\varphi\in\mathcal{S}(\mathbb{R}^n),\ \forall t\in\mathbb{R},\ \langle\mathcal{F}(u_t^{(1)}),\varphi\rangle&=\langle u_t^{(1)},\widehat{\varphi}\rangle\\ &=dr_t\langle u_t,\widehat{\varphi}\rangle+\langle u_t,\underbrace{\partial_t\widehat{\varphi}}_{=0\text{ (indépendance en }t)}\rangle\\ &=\partial_t\langle\widehat{u}_t,\varphi\rangle\\ &=\langle\widehat{u}_t^{(1)},\varphi\rangle+0\text{ par (2.2.6)}\end{aligned}$$

Ainsi, d'après (2.2.3) on a (en utilisant l'identité $\langle T,\varphi\rangle = \langle \mathcal{F}T, \overline{\mathcal{F}}\varphi\rangle$) :

$$\int_{\mathbb{R}} \langle \widehat{u_t}^{(1)}, \overline{\mathcal{F}}\psi(t,.)\rangle + i\langle \widehat{u_t}, \|.\|^2\overline{\mathcal{F}}\psi(t,.)\rangle dt = 0 \tag{2.2.4}$$

Soient $\varphi \in \mathcal{S}(\mathbb{R}^n)$ et $\chi \in \mathcal{S}(\mathbb{R})$; la relation (2.2.4) s'applique alors à $\psi \in \mathcal{S}(\mathbb{R}\times\mathbb{R}^n)$ telle que $\overline{\mathcal{F}}\psi(t,\xi) = e^{it\|\xi\|^2}\varphi(\xi)\chi(t)$, ce qui nous donne :

$$\forall \varphi \in \mathcal{S}(\mathbb{R}^n),\ \forall \chi \in \mathcal{S}(\mathbb{R}), \quad \int_{\mathbb{R}} \langle (\widehat{u_t}^{(1)}, e^{it\|\cdot\|^2}\varphi\rangle + i\langle \widehat{u_t}, \|.\|^2 e^{it\|\cdot\|^2}\varphi\rangle)\chi(t)dt = 0 \tag{2.2.5}$$

Or :

$$\partial_t\langle \widehat{u_t}, e^{it\|\cdot\|^2}\varphi\rangle = \widehat{u_t}^{(1)}, e^{it\|\cdot\|^2}\varphi\rangle + i\langle \widehat{u_t}, \|.\|^2 e^{it\|\cdot\|^2}\varphi\rangle$$

Ainsi la distribution $t \mapsto \partial_t\langle \widehat{u_t}, e^{it\|\cdot\|^2}\varphi\rangle$ est nulle dans $\mathcal{S}'(\mathbb{R})$ donc $t \mapsto \partial_t\langle \widehat{u_t}, e^{it\|\cdot\|^2}\varphi\rangle$ est nulle presque partout sur $\mathbb{R}$ (et donc nulle partout car de classe $\mathcal{C}^\infty$). Ainsi on a :

$$\forall t \in \mathbb{R}, \quad \langle \widehat{u_t}, e^{it\|\cdot\|^2}\varphi\rangle = \langle \widehat{u_0}, \varphi\rangle = 0$$

Pour finir, fixons $t_0 \in \mathbb{R}$ et $\theta \in \mathcal{S}(\mathbb{R}^n)$, avant de poser $\varphi : \xi \mapsto e^{-it_0\|\xi\|^2}\theta(\xi) \in \mathcal{S}(\mathbb{R}^n)$. On a alors $\langle \widehat{u_{t_0}}, e^{it_0\|\cdot\|^2}\varphi\rangle = 0$ i.e $\langle \widehat{u_{t_0}}, \theta\rangle = 0$ donc $\widehat{u_{t_0}} = 0$ donc $u_{t_0} = 0$. In fine on a bien $u = 0$.

Détails supplémentaires :

- L'espace $\mathcal{C}^\infty(\mathbb{R}, \mathcal{S}'(\mathbb{R}^n))$ s'injecte dans $\mathcal{S}'(\mathbb{R}\times\mathbb{R}^n)$ via la formule :

$$\langle u,\psi\rangle := \int_{\mathbb{R}} \langle u_t, \psi(t,.)\rangle dt$$

- *Transformée de Fourier de l'opérateur* $\partial_t + i\Delta$. Un théorème de dérivation sous le signe intégral nous montre que ∂_t et $\overline{\mathcal{F}}$ commutent. En ce qui concerne le laplacien, le résultat découle du fait que $\overline{\mathcal{F}}(\partial_{x_i}\psi) = -i\xi_i\overline{\mathcal{F}}\psi$.
- On trouve le lemme suivant dans [Zui02], p.61 :

Lemme 2.1
Soit $T \in \mathcal{C}^\infty(\mathbb{R}, \mathcal{S}'(\mathbb{R}^n))$.
Alors pour tout $t \in \mathbb{R}$ *il existe* $T^{(1)} \in \mathcal{C}^\infty(\mathbb{R}, \mathcal{S}'(\mathbb{R}^n))$ *tel que :*

$$\forall \varphi \in \mathcal{S}(\mathbb{R}^n),\ \forall t_0 \in \mathbb{R}, \quad \partial_t(\langle T_t, , \varphi\rangle)(t_0) = \langle T^{(1)}_{t_0}, \varphi\rangle$$

Si de plus $\psi \in \mathcal{S}(\mathbb{R}\times\mathbb{R}^n)$ *on a la relation suivante :*

$$\partial_t\langle T_t, \psi(t,.)\rangle = \langle T^{(1)}_t, \psi(t,.)\rangle + \langle T_t, \partial_t\psi(t,.)\rangle \tag{2.2.6}$$

2.3 Espace de Sobolev $H^1(I)$

Référence :

- [Bre05], p. 121–123 et 129

Prérequis :

- théorème d'Ascoli.

Soit $I = (a,b)$ un intervalle ouvert borné de $\mathbb{R}$.
On considère l'espace de Sobolev $H^1(I)$ défini comme suit :

$$H^1(I) := \left\{ u \in L^2(I) \,\middle|\, \exists g \in L^2(I),\ \forall \varphi \in \mathcal{C}_c^\infty(I), \quad \int_I u\varphi' = -\int_I g\varphi \right\}$$

La fonction $g \in L^2(I)$ est alors unique : on la note u'. On munit $H^1(I)$ de la topologie associée au produit scalaire suivant :

$$\begin{aligned} \langle .,.\rangle : H^1(I) \times H^1(I) &\to \mathbb{R} \\ (u,v) &\mapsto \int_I uv + \int_I u'v' \end{aligned}$$

La norme induite par $\langle .,.\rangle$ est notée $\|.\|_{H^1}$ et vérifie :

$$\forall u \in H^1(I), \qquad \|u\|^2_{H^1} = \|u\|^2_{L^2} + \|u'\|^2_{L^2}$$

Proposition 2.3
On a les résultats suivants :
(i) $H^1(I)$ *est un espace de Hilbert ;*
(ii) $H^1(I)$ *s'injecte de façon compacte dans* $\mathcal{C}^0(\overline{I})$.
(iii) $H^1(I)$ *s'injecte de façon continue dans* $L^2(I)$ *;*

DÉMONSTRATION :

(i) Il est clair que $(H^1(I), \langle.,.\rangle$ est préhilbertien. Soit $(u_n)_n$ une suite de Cauchy dans $H^1(I)$. Alors, si on fixe $\varepsilon > 0$ il existe $N \geq 0$ tel que :

$$\forall n \geq N, \forall p \geq 0, \quad \|u_{n+p} - u_n\|_{H^1}^2 \leq \varepsilon$$

I.e :

$$\forall n \geq N, \forall p \geq 0, \quad \|u_{n+p} - u_n\|_{L^2}^2 + \|u'_{n+p} - u'_n\|_{L^2}^2 \leq \varepsilon$$

En particulier, $(u_n)_n$ (resp. $(u'_n)_n$) est de Cauchy dans l'espace complet $L^2(I)$ donc y admet une limite $u \in L^2(I)$ (resp. $v \in L^2(I)$). Or :

$$\begin{aligned}
\forall \varphi \in \mathcal{C}_c^\infty(I), \quad \left|\int_I u'_n\varphi - \int_I u'\varphi\right| &= \left|\int_I u_n\varphi' - \int_I u\varphi'\right| \\
&\leq \int_I |u_n - u||\varphi'| \\
&\leq \|u_n - u\|_{L^2}\|\varphi'\|_{L^2} \text{ par Cauchy–Schwarz} \\
&\xrightarrow[n\to\infty]{} 0
\end{aligned}$$

Donc $\forall \varphi \in \mathcal{C}_c^\infty(I)$, $\int_I u'_n\varphi \xrightarrow[n\to\infty]{} \int_I u'\varphi$ (i.e $u'_n \rightharpoonup u'$ au sens des distributions). Cependant on montre de même que :

$$\forall \varphi \in \mathcal{C}_c^\infty(I), \quad \left|\int_I u'_n\varphi - \int_I v\varphi\right| \leq \|u'_n - v\|_{L^2}\|\varphi'\|_{L^2} \xrightarrow[n\to\infty]{} 0$$

De fait par unicité de la limite :

$$\forall \varphi \in \mathcal{C}_c^\infty(I), \quad \int_I (u' - v)\varphi = 0$$

Ce qui implique, par théorème de représentation de Riesz, que $u' = v$ p.p donc dans L^2.
In fine :

$$\|u_n - u\|_{H^1}^2 = \|u_n - u\|_{L^2}^2 + \|u'_n - u'\|_{L^2}^2 \xrightarrow[n\to\infty]{} 0$$

D'où le résultat.

(ii) – Commençons par démontrer que tout $u \in H^1(I)$ admet un représentant continu. Soit $y_0 \in I$. On définit $\tilde{u} \in \mathcal{C}(\overline{I})$ comme suit :

$$\tilde{u} : x \mapsto \int_{y_0}^x u'(t)dt$$

$\tilde{u}$ est bien continue car $u' \in L^2(I) \subset L^1_{\text{loc}}(I)$ (car I est borné). De plus :

$$\begin{aligned}
\forall \varphi \in \mathcal{C}_c^\infty(I), \quad \int_I \tilde{u}\varphi' &= \int_I \int_{y_0}^x u'(t)dt\varphi'(x)dx \\
&= \int_a^{y_0}\int_{y_0}^x u'(t)dt\varphi'(x)dx + \int_{y_0}^b\int_{y_0}^x u(t)dt\varphi'(x)dx \\
&= -\int_a^{y_0}\int_{y_0}^x u'(t)dt\varphi'(x)dx + \int_{y_0}^b\int_{y_0}^x u'(t)dt\varphi'(x)dx \\
&= -\int_a^{y_0} u'(t)dt\int_a^t \varphi'(x)dx + \int_{y_0}^b u'(t)dt\int_t^b \varphi'(x)dx \text{ par Fubini} \\
&= -\int_a^{y_0} u'(t)(\varphi(t) - 0)dt + \int_{y_0}^b u'(t)(0 - \varphi(t))dt \\
&= -\int_I u'\varphi
\end{aligned}$$

De fait $\tilde{u}' = u'$ et donc d'après le lemme 2.2, il existe $C \in \mathbb{R}$ tel que $u = \tilde{u} + C$ presque partout donc dans $H^1(I)$. $\bar{u} := \tilde{u} + C$ est bien un représentant continu de u.

– Notons $\mathcal{B}$ la boule unité fermée de $H^1(I)$. Alors, pour $u \in \mathcal{B}$ on a :

$$\begin{aligned}
\forall x \neq y \in I,\ |u(x) - u(y)| = |\bar{u}(x) - \bar{u}(y)|^2 &= \left| \int_y^x u'(t)dt \right| \\
&\leq \sqrt{|x-y|}\|u'\|_{L^2} \text{ par Cauchy–Schwarz} \\
&\leq \sqrt{|x-y|}\|u'\|_{H^1} \\
&\leq \sqrt{|x-y|}
\end{aligned}$$

Donc $\mathcal{B}$ est équicontinue dans $\mathcal{C}^0(\overline{I})$. De plus *(variation par rapport au Brézis)* :

$$\begin{aligned}
\forall x \in I,\ |u(x)| &= \left| \frac{1}{b-a} \int_a^b u(x)dy \right| \\
&= \left| \frac{1}{b-a} \int_a^b \left(\int_y^x u'(t)dt - u(y) \right) dt \right| \\
&\leq \frac{1}{b-a} \int_a^b \int_y^x |u'(t)|dtdy + \frac{1}{b-a} \int_I |u| \\
&\leq \frac{1}{b-a} \int_a^b \int_a^b |u'(t)|dtdy + \frac{1}{b-a} \int_I |u| \\
&= \int_a^b |u'(t)|dt + \frac{1}{b-a} \int_I |u| \\
&\leq \sqrt{b-a}\|u'\|_{L^2} + \frac{1}{\sqrt{b-a}}\|u\|_{L^2} \text{ par Cauchy–Schwarz} \\
&\leq \left(\sqrt{b-a} + \frac{1}{\sqrt{b-a}} \right) \|u\|_{H^1}
\end{aligned}$$

Donc $\mathcal{B}$ est bornée pour $\|.\|_\infty$. De fait, par théorème d'Ascoli, $\mathcal{B}$ est relativement compacte dans $\mathcal{C}^0(\overline{I})$, d'où le résultat.

(iii) La topologie L^2 étant plus faible que la topologie de la convergence uniforme, (iii) est une conséquence immédiate de (ii).

Détails supplémentaires :

– *Utilisation du théorème de représentation de Riesz.* Si $f \in L^2$ est telle que pour tout $\varphi \in \mathcal{C}_c^\infty$, $\int f\varphi = 0$ alors par densité la forme linéaire $\varphi \mapsto \int f\varphi$ est nulle. Le théorème de représentation de Riesz implique alors que $f = 0$ dans L^2 (donc presque partout).
– *Unicité de u'.* Si deux fonctions $g, h \in L^2$ vérifient que $\forall \varphi \in \mathcal{C}_c^\infty(I),\quad \int_I u\varphi' = -\int_I g\varphi = -\int_I g\varphi$ alors $\forall \varphi \in \mathcal{C}_c^\infty(I),\quad \int_I (g-h)\varphi = 0$ et donc $g = h$ presque partout.
– Soit $u \in L^1_{\text{loc}}(I)$. Alors pour $y_0 \in I$, $x\overline{I}$ et h tel que $x + h \in \overline{I}$ on a :

$$\left| \int_{y_0}^{x+h} u - \int_{y_0}^x u \right| = \left| \int_x^{x+h} u \right| \leq \int_x^{x+h} |u| \xrightarrow[h \to 0]{} 0 \text{ car } \forall \varepsilon \in [0,h],\ u \in L^1_{\text{loc}}(I)$$

Donc $x \mapsto \int_{y_0}^x u \in \mathcal{C}^0(\overline{I})$.
– On a fait usage du lemme suivant (cf. [Bre05], p.122–123) :

Lemme 2.2
Soit $f \in L^1_{\text{loc}}(I)$.
On suppose que :

$$\forall \varphi \in \mathcal{C}_c^\infty(I), \qquad \int_I f\varphi' = 0$$

Alors il existe $C \in v\mathbb{R}$ tel que $f = C$ presque partout. En particulier deux éléments de $H^1(I)$ de même dérivée diffèrent d'une constante.

Démonstration : Soit $\psi \in \mathcal{C}_c^\infty(I)$ d'intégrale 1 et soit $w \in \mathcal{C}_c^\infty(I)$. Alors la fonction $h := w - \psi \int_I w$ est dans $\mathcal{C}_c^\infty(I)$ et $\int_I h = \int_I w - 1 \times \int_I w = 0$ donc [3] h admet une primitive $\varphi \in \mathcal{C}_c^\infty(I)$ et donc :

$$0 = \int_I f\varphi' = \int_I f\left(w - \psi \int_I w\right)$$

I.e :

$$\begin{aligned}\forall w \in \mathcal{C}_c^\infty(I),\ 0 &= \int_I f\left(w - \psi \int_I w\right)\\ &= \int_I fw - \int_I \int_I w(x)f(y)\psi(y)dydx \text{ par Fubini}\\ &= \int_I w\left(f - \int_I f\psi\right)\end{aligned}$$

Et donc, $f = C := \int_I f\psi$ presque partout.

2.4 Estimations des grands écarts

Référence :
- [Les01], p. 16–20

Prérequis :
- formule de Stirling.

Proposition 2.4
Soit $p \in (0,1)$.
On considère une suite $(X_n)_{n\geq 1}$ de variables aléatoires i.i.d de loi $\mathcal{B}(p)$ et on pose :

$$\forall n \geq 1,\ S_n := \sum_{i=1}^n X_i \sim \mathcal{B}(n,p)$$

Pour $\varepsilon \in (0, 1-p)$ on définit également :

$$h_+(\varepsilon) := (p+\varepsilon)\ln\left(\frac{p+\varepsilon}{p}\right) + (1-p-\varepsilon)\ln\left(\frac{1-p-\varepsilon}{1-p}\right)$$

Alors :

(i) $h_+(\varepsilon) > 0$;

(ii)

$$\forall n \geq 1, \quad \mathbb{P}\left(\frac{S_n}{n} \geq p+\varepsilon\right) \leq e^{-nh_+(\varepsilon)}$$

(iii) cette inégalité est optimale, i.e :

$$\frac{1}{n}\ln\left(\mathbb{P}\left(\frac{S_n}{n} \geq p+\varepsilon\right)\right) \xrightarrow[n\to\infty]{} -h_+(\varepsilon)$$

Démonstration :

3. Il est clair que h admet une primitive dans $\mathcal{C}^\infty(I)$. La nullité de $\int_I h$ nous prouve que celle–ci est à support compact.

(i) et (ii) Soit $t > 0$. Alors :

$$\begin{aligned}
\mathbb{P}\left(\frac{S_n}{n} \geq p+\varepsilon\right) &= \mathbb{P}\left(e^{t(S_n-np-n\varepsilon)} \geq 1\right) \\
&\leq \mathbb{E}(e^{t(S_n-np-n\varepsilon)}) \text{ par inégalité de Markov} \\
&= e^{-nt(p+\varepsilon)}\mathbb{E}(e^{tS_n}) \\
&= e^{-nt(p+\varepsilon)} \sum_{k=0}^{\infty} e^{tk}\mathbb{P}(S_n = k) \text{ par lemme de transfert} \\
&= e^{-nt(p+\varepsilon)} \sum_{k=0}^{n} e^{tk} C_n^k p^k (1-p)^{n-k} \\
&= e^{-nt(p+\varepsilon)} \sum_{k=0}^{n} e^{tk} C_n^k p^k (1-p)^{n-k} \\
&= e^{-nt(p+\varepsilon)}(1-p+pe^t)^n \\
&= e^{-n(t(p+\varepsilon)-\ln(1-p+pe^t))}
\end{aligned}$$

Posons :

$$h := \sup_{t>0}(t(p+\varepsilon) - \ln(1-p+pe^t))$$

On a alors :

$$\mathbb{P}\left(\frac{S_n}{n} \geq p+\varepsilon\right) \leq e^{-nh}$$

On considère à présent la fonction $g : (t \in \mathbb{R}_+^*) \mapsto t(p+\varepsilon) - \ln(1-p+pe^t)$. Comme $g(0) = 0$, $h = \sup(g) \leq 0$. De plus $\forall t > 0$, $g'(t) = p + \varepsilon - \dfrac{pe^t}{1-p+pe^t}$ et donc $g'(0) = \varepsilon > 0$, ce qui implique que g est strictement croissante au voisinage de 0 et donc que $h > 0$. Enfin si on pose $t_0 := \ln\left(\dfrac{(p+\varepsilon)(1-p)}{p(1-p-\varepsilon)}\right)$ alors une rapide étude de fonction montre que $h = g(t_0) = h_+\varepsilon$, d'où les points (i) et (ii).

(iii) Par (ii) on a :

$$\frac{1}{n}\ln\left(\mathbb{P}\left(\frac{S_n}{n} \geq p+\varepsilon\right)\right) \leq -h_+(\varepsilon) \tag{2.4.1}$$

Nous allons donc tenter de minorer cette quantité. Pour $n \geq 1$ on pose $k_n := \lceil n(p+\varepsilon)\rceil$ et on remarque que $\mathbb{P}\left(\dfrac{S_n}{n} \geq p+\varepsilon\right) = \mathbb{P}(S_n \geq n(p+\varepsilon)) \geq \mathbb{P}(S_n = k_n) = C_n^{k_n}p^{k_n}(1-p)^{n-k_n}$. En appliquant la formule de Stirling à chacune[4] des factorielles présentes dans $C_n^{k_n}$ on trouve alors :

$$\mathbb{P}(S_n = k_n) \sim \frac{1}{\sqrt{2\pi}}\sqrt{\frac{n}{k_n(n-k_n)}}\left(\frac{np}{k_n}\right)^{k_n}\left(\frac{n(1-p)}{n-k_n}\right)^{n-k_n} \tag{2.4.2}$$

Or $k_n = n(p+\varepsilon) + o(n)$ et $n - k_n = n(1-p-\varepsilon) + o(n)$, donc $\mathbb{P}(S_n = k_n) \xrightarrow[n\to\infty]{} 0$, on peut passer au logarithme dans l'équivalent (2.4.2), d'où :

$$\frac{1}{n}\ln(\mathbb{P}(S_n = k_n)) \sim \frac{-1}{2n}\ln(2\pi) + \frac{1}{2n}\ln\left(\frac{n}{k_n(n-k_n)}\right) + \frac{1}{n}\ln\left(\left(\frac{np}{k_n}\right)^{k_n}\right) + \frac{1}{n}\ln\left(\left(\frac{n(1-p)}{n-k_n}\right)^{n-k_n}\right)$$

On sait que $\dfrac{n}{k_n(n-k_n)} \xrightarrow[n\to\infty]{} 0$. Remarquons ensuite que :

$$\begin{aligned}
\forall n \geq 1,\ \ln\left(\left(\frac{np}{k_n}\right)^{k_n}\right) = k_n\ln\left(\frac{np}{k_n}\right) &= n(p+\varepsilon)\ln\left(\frac{np}{k_n}\frac{p+\varepsilon}{p+\varepsilon}\right) + (k_n - n(p+\varepsilon))\ln\left(\frac{np}{k_n}\right) \\
&= n(p+\varepsilon)\ln\left(\frac{p}{p+\varepsilon}\right) + n(p+\varepsilon)\ln\left(\frac{n(p+\varepsilon)}{k_n}\right) + (k_n - n(p+\varepsilon))\ln\left(\frac{np}{k_n}\right)
\end{aligned}$$

4. J'aimerais que ce soit une mauvaise blague. J'aimerais tellement.

Ainsi, comme $(k_n - n(p+\varepsilon))_n$ est bornée (par 1) on obtient :

$$\frac{1}{n}\ln\left(\left(\frac{np}{k_n}\right)^{k_n}\right) \xrightarrow[n\to\infty]{} (p+\varepsilon)\ln\left(\frac{p}{p+\varepsilon}\right)$$

De même :

$$\frac{1}{n}\ln\left(\left(\frac{n(1-p)}{n-k_n}\right)^{n-k_n}\right) \xrightarrow[n\to\infty]{} (1-p-\varepsilon)\ln\left(\frac{1-p}{1-p-\varepsilon}\right)$$

Et donc in fine :

$$\frac{1}{n}\mathbb{P}(S_n = k_n) \xrightarrow[n\to\infty]{} -h_+(\varepsilon)$$

Ce qui implique , comme $\mathbb{P}\left(\frac{S_n}{n} \geq p+\varepsilon\right) \geq \mathbb{P}(S_n = k_n)$ que :

$$\liminf_{n\to\infty} \frac{1}{n}\ln\left(\mathbb{P}\left(\frac{S_n}{n} \geq p+\varepsilon\right)\right) \geq -h_+(\varepsilon) \tag{2.4.3}$$

Or par (2.4.1) :

$$\limsup_{n\to\infty} \frac{1}{n}\ln\left(\mathbb{P}\left(\frac{S_n}{n} \geq p+\varepsilon\right)\right) \leq -h_+(\varepsilon) \tag{2.4.4}$$

Et donc, en combinant (2.4.3) et (2.4.4) :

$$\frac{1}{n}\ln\left(\mathbb{P}\left(\frac{S_n}{n} \geq p+\varepsilon\right)\right) \xrightarrow[n\to\infty]{} -h_+(\varepsilon)$$

Détails supplémentaires :

– Rappelons la très divertissante *formule de Stirling* :

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

– Soient u et v deux suites de $\mathbb{R}_+^*$ convergeant vers une limite $\ell \neq 1$ telles que $u_n \sim v_n$. Montrons que $\ln(u_n) \sim \ln(v_n)$. Remarquons que comme $\lim_n v_n \neq 1$, il existe $N \geq 0$ tel que $\forall n \geq N$, $v_n \neq 1$. On peut alors écrire :

$$\forall n \geq N,\ \frac{\ln(u_n)}{\ln(v_n)} - 1 = \frac{\ln(u_n) - \ln(v_n)}{\ln(v_n)} = \frac{\ln\left(\frac{u_n}{v_n}\right)}{\ln(v_n)} \xrightarrow[n\to\infty]{} 0$$

D'où le résultat.

2.5 Inégalité isopérimétrique

Référence :

– [QZ95], p. 101–102 (alternativement [FGN12])

Prérequis :

– théorème de Jordan ;
– formule de Green–Riemann.

Proposition 2.5 (Inégalité isopérimétrique)
Soient $a, b \in \mathbb{R}$
Soit Γ une courbe de Jordan (i.e continue fermée simple) admettant un paramétrage $f : [a,b] \to \mathbb{C}$ de classe $\mathcal{C}^1$.
On note L la longueur de f et S l'aire enfermée à l'intérieur de la courbe.
Alors :

(i)

$$L^2 \geq 4\pi S$$

(ii) $L^2 = 4\pi S \Leftrightarrow f$ *définit un cercle parcouru une unique fois*

DÉMONSTRATION : D'après le théorème de Jordan, $\mathbb{C} \setminus \Gamma$ possède exactement deux composantes connexes, l'une (notée A) bornée et l'autre non. On a alors $S = \lambda(A)$. De plus, si on pose $f = x + iy$ et si f est orientée positivement [5] (i.e $\forall z \in A$, $\frac{1}{2i\pi} \int_a^b \frac{dt}{f(t) - z} = 1$) la formule de Green–Riemann s'écrit :

$$S = \frac{1}{2} \int_a^b x(t)y'(t) - y(t)x'(t)dt = \frac{1}{2}\mathrm{Im}\left(\int_a^b f'(s)\overline{f(s)}ds \right) \tag{2.5.1}$$

On peut supposer sans perdre de généralité que $L = 1$. De plus, quitte à remplacer f par $f \circ s^{-1}$, avec s une abscisse curviligne de la courbe, on peut supposer notre paramétrage normal, avec $a = 0$ et $b = 1$. Enfin, quitte à remplacer f par $f(1 - .)$, on peut supposer la courbe orientée positivement.

Puisque $f(0) = f(1)$, on peut prolonger f en une fonction 1–périodique et $\mathcal{C}^1$ par morceaux $f : \mathbb{R} \to \mathbb{C}$. Alors, pour $n \in \mathbb{Z}$ on peut définir le n–ième coefficient de Fourier de cette application comme suit :

$$c_n(f) := \int_0^1 f(s)e^{-2i\pi ns}ds$$

En outre, comme f est de classe $\mathcal{C}^1$ sur $[0, 1]$, $c_n(f') = 2i\pi n c_n(f)$. La formule de Parseval appliquée à f' (qui est bien L^2 car continue sur un compact) donne alors :

$$L = 1 = \int_0^1 |f'(s)|ds = \sum_{n=-\infty}^{\infty} |c_n(f')|^2 = \sum_{n=-\infty}^{\infty} 4\pi^2 |c_n(f)|^2$$

Comme f et f' sont L^2 elles sont sommes (au sens L^2) de leurs séries de Fourier. En particulier :

$$\int_0^1 f'(s)\overline{f(s)}ds = \sum_{n=-\infty}^{\infty} c_n(f')\overline{c_n(f)}$$

Ainsi, par la formule (2.5.1) :

$$S = \frac{1}{2}\mathrm{Im}\left(\int_0^1 f'(s)\overline{f(s)}ds \right) = \sum_{n=-\infty}^{\infty} \pi n |c_n(f)|^2$$

Ainsi :

$$L - 4\pi S = 4\pi^2 \sum_{n=-\infty}^{\infty} (n^2 - n)|c_n(f)|^2 \geq 0$$

D'où le (i). De plus, $\forall n \notin \{0, 1\}$, $n^2 - n > 0$ et donc dans le cas d'égalité, $c_n(f) = 0$ sauf pour $n = 0$ ou 1. Ainsi, $L = 4\pi S^2$ si et seulement si $\forall s \in [0, 1]$, $f(s) = c_0(f) + c_1(f)e^{2i\pi s}$, ce qui définit le cercle de centre $c_0(f)$ et de rayon $|c_1(f)|$.

Détails supplémentaires :

– La formule de Green–Riemann s'écrit, pour un ouvert Ω de $\mathbb{R}^2$:

$$\int\int_\Omega \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y} \right)(x, y)dxdy = \int_{\partial\Omega} (P(x, y)dx + Q(x, y))dy$$

En particulier, si on prend $Q : (x, y) \mapsto \frac{x}{2}$ et $P : (x, y) \mapsto -\frac{y}{2}$ et Ω l'intérieur de la courbe Γ on a $\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y} = 1$ et donc :

$$S := \int\int_\Omega dxdy = \int_{\partial\Omega} (P(x, y)dx + Q(x, y))dy = \frac{1}{2} \int_a^b x(t)y'(t) - y(t)x'(t)dt$$

5. Le théorème de Jordan nous indique que l'indice a pour valeur ± 1 à l'intérieur de la courbe.

2.6 Formule d'inversion de Fourier

Référence :
- [QZ07] p. 331–332

Pour $f \in \mathcal{S}(\mathbb{R})$ on définit sa transformée de Fourier comme suit :

$$\widehat{f}(t) := \int_{\mathbb{R}} e^{-itx} f(x)dx$$

Proposition 2.6
Soit $f \in \mathcal{S}(\mathbb{R})$.
Alors :

$$\forall x \in \mathbb{R}, \quad f(x) = \frac{1}{2\pi}\widehat{\widehat{f}}(-x) = \frac{1}{2\pi}\int_{\mathbb{R}} e^{itx}\widehat{f}(t)dt$$

Démonstration : Pour $\varepsilon > 0$ on pose $f_\varepsilon : t \mapsto e^{-\varepsilon t^2} e^{itx}\widehat{f}(t)$. Alors :
- les f_ε sont L^1 ;
- $f_\varepsilon(t) \xrightarrow[\varepsilon \to 0]{} e^{itx}\widehat{f}(t)$ presque partout sur $\mathbb{R}$;
- $|f_\varepsilon| \leq |\widehat{f}| \in L^1(\mathbb{R})$.

De fait, par théorème de convergence dominée on a :

$$\frac{1}{2\pi}\int_{\mathbb{R}} e^{-\varepsilon t^2} e^{itx}\widehat{f}(t) \xrightarrow[\varepsilon \to 0]{} \frac{1}{2\pi}\int_{\mathbb{R}} e^{itx}\widehat{f}(t)dt \tag{2.6.1}$$

Remarquons à présent à présent que pour tout $x \in \mathbb{R}$ on a :

$$\int_{\mathbb{R}}\int_{\mathbb{R}} |e^{it(x-y)}e^{-\varepsilon t^2} f(y)|dydt \leq \int_{\mathbb{R}} e^{-\varepsilon t^2}dt \int_{\mathbb{R}} |f(y)|dy < \infty$$

De fait, par théorème de Fubini–Tonelli on a :

$$\begin{aligned}
\frac{1}{2\pi}\int_{\mathbb{R}} e^{itx-\varepsilon t^2}\widehat{f}(t)dt &= \frac{1}{2\pi}\int_{\mathbb{R}}\int_{\mathbb{R}} e^{it(x-y)}e^{-\varepsilon t^2} f(y)dydt \\
&= \frac{1}{2\pi}\int_{\mathbb{R}}\int_{\mathbb{R}} e^{it(x-y)}e^{-\varepsilon t^2} f(y)|dtdy \\
&= \frac{1}{2\pi}\int_{\mathbb{R}} f(y)\int_{\mathbb{R}} e^{it(x-y)}e^{-\varepsilon t^2}dtdy \\
&= \frac{1}{2\pi}\frac{\sqrt{\pi}}{\sqrt{\varepsilon}}\int_{\mathbb{R}} f(y)e^{(y-x)^2/4\varepsilon}dy \text{ (cf. infra)} \\
&= \frac{1}{\sqrt{\pi}}\int_{\mathbb{R}} e^{-y^2} f(x+2\sqrt{\varepsilon}y)dy \text{ via } y \mapsto x+2\sqrt{\varepsilon}y)
\end{aligned}$$

Une nouvelle application du théorème de convergence dominée nous indique que :

$$\int_{\mathbb{R}} e^{-y^2} f(x+2\sqrt{\varepsilon}y)dy \xrightarrow[\varepsilon \to 0]{} \int_{\mathbb{R}} e^{-y^2}dy f(x) = \sqrt{\pi}f(x)$$

D'où le résultat via la relation (2.6.1).

Détails supplémentaires :
- Ce développement est trop court en l'état, il sera donc nécessaire de l'allonger le moins artificiellement possible. Le jour de mon oral d'agrégation, j'ai proposé en première partie la démonstration du fait que si $f \in \mathcal{S}(\mathbb{R})$ alors $\widehat{f} \in \mathcal{S}(\mathbb{R})$. On pourrait aussi inclure le calcul de l'intégrale de Gauss "généralisée" (cf. infra, ou alors la version avec prolongement analytique). Tous ces "petits" résultats se trouvent dans [QZ07] dans un voisinage de la page 330.
- Il nous reste à justifier le calcul de $\int_{\mathbb{R}} e^{it(x-y)}e^{-\varepsilon t^2}dt$. Posons :

$$I(x) = \int_{\mathbb{R}} e^{-itx}e^{-\varepsilon t^2}dt$$

Alors comme la fonction $(x,t) \mapsto e^{-itx}e^{-\varepsilon t^2}$ est $\mathcal{C}^1$ selon sa première variable, intégrable selon sa deuxième et que sa dérivée "en x" est dominée par $t \mapsto te^{-\varepsilon t^2}$ qui est intégrable on a, par théorème de dérivation sous le signe intégral que I est de classe $\mathcal{C}^1$ et que :

$$\begin{aligned}
I'(x) &= \int_{\mathbb{R}} \frac{d}{dx}(e^{-itx}e^{-\varepsilon t^2})dt \\
&= \int_{\mathbb{R}} (-it)e^{-itx}e^{-\varepsilon t^2}dt \\
&= -\frac{i}{2\varepsilon}\int_{\mathbb{R}} e^{-itx}\frac{d}{dt}(e^{-\varepsilon t^2})dt \\
&= \frac{i}{2\varepsilon}\int_{\mathbb{R}} \frac{d}{dt}(e^{-itx})e^{-\varepsilon t^2}dt \text{ en intégrant par parties} \\
&= \frac{i}{2\varepsilon}\int_{\mathbb{R}} (-ix)e^{-itx}e^{-\varepsilon t^2}dt \\
&= \frac{x}{2\varepsilon}I(x)
\end{aligned}$$

De fait $I(x) = I(0)e^{(x/2\varepsilon)/2}$. Or :

$$\begin{aligned}
I(0) &= \int_{\mathbb{R}} e^{-\varepsilon t^2}dt \\
&= \frac{1}{\sqrt{\varepsilon}}\int_{\mathbb{R}} e^{-t^2}dt \text{ via } t \mapsto \frac{t}{\sqrt{\varepsilon}} \\
&= \frac{\sqrt{\pi}}{\sqrt{\varepsilon}}
\end{aligned}$$

D'où :

$$\int_{\mathbb{R}} e^{it(x-y)}e^{-\varepsilon t^2}dt = I(y-x) = \frac{\sqrt{\pi}}{\sqrt{\varepsilon}}e^{(y-x)^2/4\varepsilon}$$

2.7 Formule sommatoire d'Euler–Maclaurin

Référence :
- [Gou08] p. 301–302

Prérequis :
- une certaine prédisposition aux calculs crades [6].

Proposition 2.7 (Euler–Maclaurin)
Soient $m, n \in \mathbb{Z}^2$ tels que $m < n$.
Soit $f \in \mathcal{C}^r([m,n],\mathbb{C})$ $(r \geq 1)$.
Alors :

$$\sum_{k=m}^{n} f(k) = \int_m^n f(t)dt + \frac{1}{2}(f(m)+f(n)) + \sum_{k=2}^{r}\frac{b_k}{k!}(f^{(k-1)}(n) - f^{(k-1)}(m)) + R_r \tag{2.7.1}$$

Où :

$$R_r := \frac{(-1)^{r+1}}{r!}\int_m^n \tilde{B}_r(t)dtf^{(r)}(t)dt$$

Démonstration : On démontre (2.7.1) par récurrence sur $r \geq 1$.
- $r = 1$. Fixons $m \leq l \leq n-1$ et remarquons que $\tilde{B_1} = B_1$ sur $(0,1)$ donc $\tilde{B_1} = B_1(. - k)$

6. Si vous aimez les exposants en pagaille, c'est un plus.

presque partout sur $[k,k+1]$ ergo :

$$\begin{aligned}\int_k^{k+1}\tilde{B_1}(t)f'(t)dt &= \int_k^{k+1}B_1(t-k)f'(t)dt\\ &= \int_0^1 B_1(t)f'(t+k)dt \text{ via } t\mapsto t+k\\ &= \int_0^1 (t-\frac{1}{2})f'(t+k)dt\\ &= \frac{f(k+1)+f(k)}{2}-\int_0^1 f(t+k)dt \text{ par parties}\\ &= \frac{f(k+1)+f(k)}{2}-\int_k^{k+1} f(t)dt\end{aligned}$$

En sommant sur k on obtient :

$$\begin{aligned}R_1 &= \sum_{k=m}^{n-1}\frac{f(k+1)+f(k)}{2}-\int_m^n f(t)dt\\ &= \sum_{k=m}^{n} f(k)-\frac{1}{2}(f(m)+f(n))-\int_m^n f(t)dt\end{aligned}$$

D'où le résultat.

– Supposons la propriété vraie au rang $r-1\geq 1$. Une fois n'est pas coutume, immobilisons *manu militari* un entier $m\leq k\leq n-1$. Alors, en suivant le même procédé que ci–avant [7] :

$$\begin{aligned}\frac{1}{(r-1)!}\int_k^{k+1}\tilde{B_{r-1}}(t)f^{(r-1)}(t) &= \frac{1}{r!}[B_r(t)f^{(r-1)}(t+k)]_0^1-\frac{1}{r!}\int_k^{k+1}\tilde{B_r}(t)f^{(r)}(t)dt\\ &= \frac{b_r}{r!}(f^{(r-1)}(k+1)-f^{(r-1)}(k))-\frac{1}{r!}\int_k^{k+1}\tilde{B_r}(t)f^{(r)}(t)dt\end{aligned}$$

On somme sur k puis on multiplie par $(-1)^r$, obtenant :

$$R_{r-1}=(-1)^r\frac{b_r}{r!}(f^{(r-1)}(n)-f^{(r-1)}(m))+R_r$$

Or, si r est pair $(-1)^r b_r=b_r$ et si r est impair c'est également vrai car $b_r=0$ (vu que $r\geq 2$). Donc, par hypothèse de récurrence :

$$\begin{aligned}\sum_{k=m}^{n} f(k) &= \int_m^n f(t)dt+\frac{1}{2}(f(m)+f(n))+\sum_{k=2}^{r-1}\frac{b_k}{k!}(f^{(k-1)}(n)-f^{(k-1)}(m))+R_{r-1}\\ &= \int_m^n f(t)dt+\frac{1}{2}(f(m)+f(n))+\sum_{k=2}^{r-1}\frac{b_k}{k!}(f^{(k-1)}(n)-f^{(k-1)}(m))+\frac{b_r}{r!}(f^{(r-1)}(n)-f^{(r-1)}(m))+R_r\\ &= \int_m^n f(t)dt+\frac{1}{2}(f(m)+f(n))+\sum_{k=2}^{r}\frac{b_k}{k!}(f^{(k-1)}(n)-f^{(k-1)}(m))+R_r\end{aligned}$$

D'où le résultat.

Détails supplémentaires :

– *Nombres de Bernoulli ([Gou08], p. 299).* On considère l'application suivante, définie sur $\mathbb{C}$:

$$f: z\mapsto\sum_{n=0}^{\infty}\frac{z^n}{(n+1)!}$$

Alors, pour tout $z\neq 0$ on a $f(z)=\dfrac{e^z-1}{z}$ et $f(0)=1\neq 0$ donc la fonction $\dfrac{1}{f}$ est développable en série entière sur un voisinage de 0, i.e il existe $r>0$ et une suite de nombres complexes

7. Changement de variable puis intégration par parties puis re–changement de variable, le tout en remarquant que $\tilde{B_r}=B_r$ presque partout sur $[0,1]$.

$(b_n)_n$ tels que :

$$\forall z \in \mathbb{C}^* \text{ tel que } |z| < r,\ \frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{b_n}{n!} z^n$$

Les complexes b_n sont appelés *nombres de Bernoulli.* On en déduit par produit de Cauchy que pour tout $z \in \mathbb{C}^*$ tel que $|z| < r$ et tout $x \in \mathbb{R}$ il existe une suite $(B_n(x))_n$ de nombres complexes tels que :

$$\frac{ze^{zx}}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n$$

Les polynômes $B_n \in \mathbb{C}[X]$ sont appelés *polynômes de Bernoulli.* On peut alors montrer les propriétés suivantes :
* si n est impair supérieur à 2 alors $b_n = 0$;
* $\forall n \geq 2,\ B_n(0) = B_n(1)$;
* on peut donc construire pour tout $n \geq 2$ une fonction $\tilde{B_n}$ continue 1–périodique sur $\mathbb{R}$ telle que $B_n = \tilde{B_n}$ sur $[0, 1)$;
* pour $n \geq 2$ on a $B_n' = nB_{n-1}$, ce qui permet de calculer les polynômes (et les nombres) de Bernoulli par récurrence :

i	B_n	b_n
0	1	1
1	$X - 1/2$	$-1/2$
2	$X^2 - X + 1/6$	$1/6$
3	$X^3 - (3/2)X^2 + (1/2)X$	0
4	$X^4 - 2X^3 + X^2 - 1/30$	$-1/30$

– En fait on peut définir les polynômes de Bernoulli comme l'unique suite de polynôme vérifiant $B_0 = 1$, $B_n' = nB_{n-1}$ et $\int_0^1 B_n = 0$, puis poser $b_n := B_n(0)$.

2.8 Formule sommatoire de Poisson

Référence :
– [Gou08], p.272–273

On adopte ici les conventions de notation suivantes :
◇ pour $f \in \mathcal{S}(\mathbb{R})$ on note $\widehat{f}$ sa transformée de Fourier définie sur $\mathbb{R}$ de la façon suivante :

$$\widehat{f} : \xi \mapsto \int_{\mathbb{R}} f(t) e^{-2i\pi\xi t} dt$$

◇ pour f continue 1–périodique sur $\mathbb{R}$ on note $(c_n(f))_{n\in\mathbb{Z}}$ la suite de ses coefficients de Fourier, définis comme suit :

$$\forall n \in \mathbb{Z},\ c_n(f) := \int_0^1 f(t) e^{-2i\pi nt} dt$$

Proposition 2.8 (Poisson)
Soit $f \in \mathcal{S}(\mathbb{R})$.
Alors la série $\sum_{(n\in\mathbb{Z})} f(. + n)$ converge normalement sur tout compact de $\mathbb{R}$ et :

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

Démonstration : On définit pour $n \in \mathbb{Z}$ l'application $f_n := f(. + n)$. Soit $K \geq 0$: alors, comme $f(x) = O\left(\frac{1}{n^2}\right)$, pour n assez grand (en valeur absolue) $\exists C > 0$, $\forall x \in [-K, K]$, $|f_n(x)| \leq \frac{C}{(x + n)^2} \leq \frac{C}{-K + |n|)^2}$.
Ainsi $\|f_n\|_{\infty,[-K,K]} = O(\frac{1}{n^2})$, d'où la convergence normale escomptée.

De la même façon on démontre que $\sum_{(n\in\mathbb{Z})} f'(. + n)$ converge normalement sur tout compact de $\mathbb{R}$ ($f' \in \mathcal{S}(\mathbb{R})$) donc l'application $F : x \mapsto \sum_{n\in\mathbb{Z}} f_n(x)$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}$ et vérifie :

$$\forall x \in \mathbb{R},\ F'(x) = \sum_{n=-\infty}^{\infty} f'(x + n)$$

Si $x \in \mathbb{R}$ et $N \geq 1$, alors :

$$\sum_{n=-N}^{N} f(x+n+1) = \sum_{n=-N+1}^{N+1} f(x+n)$$

En passant à la limite, on obtient que F est 1–périodique et alors :

$$\begin{aligned}
\forall N \in \mathbb{Z},\ c_N(F) := \int_0^1 \sum_{n=-\infty}^{\infty} f(x+n)e^{-2i\pi Nx}dx \\
&= \sum_{n=-\infty}^{\infty} \int_0^1 f(x+n)e^{-2i\pi Nx}dx \text{ par convergence uniforme} \\
&= \sum_{n=-\infty}^{\infty} \int_n^{n+1} f(x)e^{-2i\pi N(x-n)}dx \\
&= \sum_{n=-\infty}^{\infty} \underbrace{e^{2i\pi nN}}_{=1} \int_n^{n+1} f(x)e^{-2i\pi Nx}dx \\
&= \int_{\mathbb{R}} f(x)e^{-2i\pi Nx}dx \\
&= \widehat{f}(N)
\end{aligned}$$

Or F est de classe $\mathcal{C}^1$ et 1–périodique donc est la somme de sa série de Fourier, i.e :

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

D'où le résultat.

Corollaire 2.8.1
Soit $s > 0$. Alors :

$$\sum_{n=-\infty}^{\infty} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n=-\infty}^{\infty} e^{-\pi\frac{n^2}{s}}$$

Démonstration : On considère l'application $f : x \mapsto e^{-\alpha x^2} \in \mathcal{S}(\mathbb{R})$. Alors :

$$\begin{aligned}
\forall n \in \mathbb{Z},\ \widehat{f}(n) &= \int_{\mathbb{R}} e^{-\alpha t^2}e^{-2i\pi nt}dt \\
&= \frac{1}{\sqrt{\alpha}} \int_{\mathbb{R}} e^{-t^2}e^{-2i\pi n\frac{t}{\sqrt{\alpha}}}dt \text{ via } t \mapsto \frac{t}{\sqrt{\alpha}}
\end{aligned}$$

Posons à présent pour $x \in \mathbb{R}$ $I(x) := \int_{\mathbb{R}} e^{-t^2}e^{-2i\pi x\frac{t}{\sqrt{\alpha}}}dt$ (cf. [Gou08] p. 164–166). Alors par dérivation sous le signe somme I est de classe $\mathcal{C}^1$ sur $\mathbb{R}$ et :

$$\forall x \in \mathbb{R},\ I'(x) = \frac{2i\pi}{\sqrt{\alpha}} \int_{\mathbb{R}} te^{-t^2}e^{-2i\pi x\frac{t}{\sqrt{\alpha}}}dt$$

En intégrant par parties on trouve de plus que :

$$\forall x \in \mathbb{R},\ I(x) = \frac{\sqrt{\alpha}}{2i\pi x} \int_{\mathbb{R}} 2te^{-t^2}e^{-2i\pi x\frac{t}{\sqrt{\alpha}}}dt = \frac{\sqrt{\alpha}}{i\pi x}\frac{\sqrt{\alpha}}{2i\pi}I'(x) = -\frac{\alpha}{2x\pi^2}I'(x)$$

In fine :

$$I(x) = I(0)e^{-\dfrac{x^2\pi^2}{\alpha}} = \sqrt{\pi}e^{-\dfrac{x^2\pi^2}{\alpha}}$$

D'où :

$$\forall n \in \mathbb{Z},\ \widehat{f}(n) = \sqrt{\frac{\pi}{\alpha}}e^{-\dfrac{n^2\pi^2}{\alpha}}$$

La formule de Poisson appliquée en $x = 0$ à f avec $\alpha := \pi s$ nous livre alors le résultat.

Corollaire 2.8.2
Soit $N \geq 0$; on pose :

$$T_N := \sum_{n=-N}^{N} \delta_n \in \mathcal{S}'(\mathbb{R})$$

Alors la suite $(T_N)_N$ converge dans $\mathcal{S}'(\mathbb{R})$ vers une distribution $\delta_{\mathbb{Z}}$ qui vérifie la relation suivante :

$$\widehat{\delta_{\mathbb{Z}}} = \delta_{\mathbb{Z}}$$

DÉMONSTRATION : Soit $\varphi \in \mathcal{S}(\mathbb{R})$. Comme on vient de voir que la somme $\sum_{n\in\mathbb{Z}} \varphi(n)$ étant bien définie on a :

$$\langle T_N, \varphi\rangle \xrightarrow[N\to\infty]{} \langle \delta_{\mathbb{Z}}, \varphi\rangle := \sum_{n\in\mathbb{Z}} \varphi(n)$$

Vérifions que $\delta_{\mathbb{Z}}$ est bien une distribution tempérée. Si $f \in \mathcal{S}(\mathbb{R})$ on a :

$$\begin{aligned} |\langle \delta_{\mathbb{Z}}, f\rangle| &\leq \sum_{n\in\mathbb{Z}} |f(n)| \\ &= \sum_{n\in\mathbb{Z}^*} \frac{1}{n^2}|n^2 f(n)| + |f(0)| \\ &\leq \left(\sum_{n\in\mathbb{Z}^*} \frac{1}{n^2}\right) \|f\|_{2,0} + \|f\|_{0,0} \end{aligned}$$

Où les $\|.\|_{n,p} : f \mapsto \sup_{x\in\mathbb{R}} |x^n f^{(p)}(x)|$ sont les semi–normes définissant la topologie de $\mathcal{S}(\mathbb{R})$. Ainsi on a bien :

$$|\langle \delta_{\mathbb{Z}}, f\rangle| \leq \left(\frac{\pi^2}{3} + 1\right) \sup(\|f\|_{2,0}, \|f\|_{0,0})$$

D'où $\delta_{\mathbb{Z}} \in \mathcal{S}'(\mathbb{R})$. Enfin, la formule sommatoire de Poisson nous donne alors :

$$\begin{aligned} \forall f \in \mathcal{S}(\mathbb{R}), \quad \langle \widehat{\delta_{\mathbb{Z}}}, f\rangle &= \langle \delta_{\mathbb{Z}}, \widehat{f}\rangle \\ &= \sum_{n\in\mathbb{Z}} \widehat{f}(n) \\ &= \sum_{n\in\mathbb{Z}} f(n) \\ &= \langle \delta_{\mathbb{Z}}, f\rangle \end{aligned}$$

D'où le résultat.

Détails supplémentaires :
- On n'aura vraisemblablement le temps de n'exposer qu'un seul des corollaires. Je préfère pour ma part largement le second, qui est plus facile à mettre en contexte.
- *Détails de la majoration de $f(x+n)$.* Soit $x \in [-K, K]$ et soit $n \in \mathbb{Z}$ tel que $|n| \geq K+1$. Alors :
  * si $n \geq 0$ alors $x + n \geq -K + n = -K + |n|$;
  * si $x < 0$ alors $-x \in [-K, K]$ donc $(x+n)^2 = (-x-n)^2 = (-x+|n|)^2 \geq (-K+|n|)$ par le cas précédent $(-x \geq 0)$.
- *Intégrale de Gauss.* Il est clair que $x \mapsto e^{-x^2}$ est intégrable sur $\mathbb{R}$, nous nous intéresserons donc ici uniquement au calcul effectif de l'intégrale (cf. [Gou08], p. 163). On considère l'application suivante :

$$\begin{aligned} h : \mathbb{R}_+ \times [0,1] &\to \mathbb{R} \\ (x,t) &\mapsto \frac{e^{-(t^2+1)x^2}}{t^2+1} \end{aligned}$$

  On pose également $g := \int_0^1 h(., t)dt$. Alors :
  * pour (presque) tout $x \geq 0$, $h(x, .)$ est intégrable sur $[0,1]$;
  * pour tout $t \in [0,1]$, $h(., t)$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}_+$;

* pour (presque) tout $x \geq 0$, $\dfrac{\partial h}{\partial x}(x,.)$ est intégrable sur $[0,1]$.

Ainsi par théorème de dérivation sous le signe intégral, g est de classe $\mathcal{C}^1$ et :

$$\begin{aligned}\forall x \in \mathbb{R}_+,\ g'(x) &= -2x\int_0^1 e^{-(t^2+1)x^2}dt \\ &= -2xe^{-x^2}\int_0^1 e^{-(tx)^2}dt \\ &= -2e^{-x^2}\int_0^1 e^{-t^2}dt \text{ via } t \mapsto \frac{t}{x} \\ &= -2f'(x)f(x) \text{ où } f(x) := \int_0^x e^{-t^2}dt\end{aligned}$$

De fait :

$$\forall x \in \mathbb{R}_+,\ g(x) - g(0) = \int_0^x g(t)dt = -2\int_0^x f'(t)f(t)dt = -(f^2(x) - f^2(0))$$

Or $f^2(0) = 0$ et $g(0) = \int_0^1 \frac{1}{t^2+1}dt = \arctan(1) - \arctan(0) = \frac{\pi}{4} - 0$ d'où $g(x) = \frac{\pi}{4} - f^2(x)$.
Comme $0 \leq g(x) \leq e^{-x^2}\int_0^1 \frac{1}{1+t^2}dt$, $g(x) \xrightarrow[x\to\infty]{} 0$ et donc $f^2(x) \xrightarrow[x\to\infty]{} \frac{\pi}{4}$. f étant positive on en déduit finalement que $f(x) \xrightarrow[x\to\infty]{} \sqrt{\frac{\pi}{4}}$ et donc :

$$\int_0^\infty e^{-x^2}dx = \frac{\sqrt{\pi}}{2} d'o \int_{\mathbb{R}} e^{-x^2}dx = \sqrt{\pi} \text{ par parité}$$

2.9 Lemme de Borel

Référence :
- [Rou09], p. 359 – 360

Proposition 2.9 (Borel)
Soit $(a_k)_k \in \mathbb{R}^{\mathbb{N}}$.
Alors il existe $u \in \mathcal{C}^\infty(\mathbb{R})$ *telle que :*

$$\forall k \geq 0, \qquad u^{(k)}(0) = a_k$$

DÉMONSTRATION : Soit $f \in \mathcal{C}_c^\infty(\mathbb{R})$ telle que $f(x) = 1$ si $|x| \leq \frac{1}{2}$ et $\text{supp}(f) \subset (-1,1)$. On fixe une suite $(\lambda_k)_k$ de réels strictement positifs et on définit :

$$\forall k \geq 0, \qquad f_k : x \mapsto f(\lambda_k x)\frac{a_k}{k!}x^k$$

Cherchons à présent à faire converger $\sum f_k$ et ses dérivées.

Soit $m \in \mathbb{N}$. Alors, par formule de Leibniz :

$$\forall k \geq m, \forall x \in \mathbb{R}, \quad f_k^{(m)}(x) = a_k \sum_{p=0}^m C_m^p f^{(m-p)} \lambda_k^{m-p} \frac{x^{k-p}}{(k-p)!}$$

On pose [8] :

$$M_m := \max_{0 \leq k \leq m} \max_{x \in \mathbb{R}} |f^{(k)}(x)|$$

Pour $k \geq m$ et $x \in \mathbb{R}$ alors :
- si $|x| > \frac{1}{\lambda_k}$ alors $f^{(m)}(\lambda_k x) = 0$ (car $\text{supp}(f) \subset (-1,1)$) donc $f_k^{(m)}(x) = 0$;

8. Le deuxième "max" est bien un maximum car f est à support compact.

– sinon, i.e si $|x| \leq \frac{1}{\lambda_k}$:

$$\begin{aligned}
|f_k^{(m)}(x)| &\leq M_m|a_k| \sum_{p=0}^{m} C_m^p \lambda_k^{m-p} \frac{|x|^{k-p}}{(k-p)!} \\
&\leq M_m|a_k| \sum_{p=0}^{m} C_m^p \lambda_k^{m-p} \frac{\lambda_k^{p-k}}{(k-p)!} \\
&\leq M_m|a_k|\lambda_k^{m-k} \sum_{p=0}^{m} C_m^p \frac{1}{(k-p)!} \\
&\leq M_m|a_k|\lambda_k^{m-k} \frac{1}{(k-m)!} \sum_{p=0}^{m} C_m^p \\
&= \frac{2^m M_m|a_k|}{(k-m)!\lambda_k^{k-m}}
\end{aligned}$$

Ainsi, si on prend pour tout k $\lambda_k := \max(1, |a_k|)$ alors pour tous $(k, m) \in \mathbb{N}^2$ tels que $k \geq m+1$ on a $\lambda_k^{k-m} \geq \lambda_k \geq |a_k|$. Ainsi :

$$\forall m \in \mathbb{N},\ \forall k \geq m+1,\ \forall x \in \mathbb{R}, \qquad |f_k^{(m)}(x)| \leq \frac{2^m M_m}{(k-m)!}$$

D'où, comme les $f_k^{(m)}$ sont continues à support compact donc bornées :

$$\forall m \in \mathbb{N},\ \forall k \geq m+1, \qquad \|f_k^{(m)}\|_\infty \leq \frac{2^m M_m}{(k-m)!} \tag{2.9.1}$$

De fait, la série $\sum f_k^{(m)} = \sum_{(0\leq k\leq m)} f_k^{(m)} + \sum_{(k\geq m+1)} f_k^{(m)}$ converge normalement donc uniformément sur $\mathbb{R}$ et donc la fonction $u := \sum_{k=0}^{\infty} f_k$ est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$ et dérivable terme à terme. En particulier :

$$\forall m \in \mathbb{N}, \quad u^{(m)}(0) = \sum_{k=0}^{\infty} f_k^{(m)}(0) = a_k \text{ car } \forall k \in \mathbb{N},\ \forall x \in [-\lambda_k/2, \lambda_k/2], \quad f_k(x) = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!}$$

D'où le résultat.

Détails supplémentaires :

– On trouve dans [Rou09], p. 355 comment construire des fonctions plateau $\mathcal{C}^\infty$ à support compact. Pour $a < b < c < d$ on définit :

$$\psi : t \mapsto \begin{cases} e^{-1/t} \text{ si } t > 0 \\ 0 \text{ sinon} \end{cases} \in \mathcal{C}^\infty(\mathbb{R}) \ \ , \alpha : t \mapsto \psi(t)\psi(1-t) \text{ et } \beta : t \mapsto \frac{\int_0^t \alpha(s)ds}{\int_0^1 \alpha(s)ds}$$

Alors la fonction $f : x \mapsto \beta\left(\frac{x-a}{b-a}\right)\beta\left(\frac{d-x}{d-c}\right)$ est de classe $\mathcal{C}^\infty$, égale à 1 sur $[b, c]$ et à support contenu dans $[a, d]$.

2.10 Méthode de Newton

Référence :

– [Rou09], p. 152–155

Prérequis :

– formule de Taylor–Lagrange.

Soit $f : [c, d] \to \mathbb{R}$ une application de classe $\mathcal{C}^2$ $(c < d)$ telle que :

– $f(c) < 0 < f(d)$;
– $\forall x \in [c, d],\ f'(x) > 0$

f est continue, strictement croissante et $0 \in f((c,d))$ donc il existe un unique point $a \in (c,d)$ tel que $f(a) = 0$. On cherche à approcher a ; pour ce faire, on définit la fonction suivante :

$$\begin{aligned} F : [c,d] &\to \mathbb{R} \\ x &\mapsto x - \frac{f(x)}{f'(x)} \end{aligned}$$

On fixe ensuite $x_0 \in [c,d]$ et on pose, pour $n \geq 0$, $x_{n+1} := F(x_n)$. On a alors le résultat suivant :

Proposition 2.10
Il existe $\alpha > 0$ tel que si $x_0 \in [a-\alpha, a+\alpha]$, la suite $(x_n)_n$ converge de façon quadratique vers a ; i.e $(x_n)_n$ converge vers a et il existe $A > 0$ tel que :

$$\forall n \in \mathbb{N}, \quad |x_{n+1} - a| \leq C|x_n - a|^2$$

Démonstration : Commençons par remarquer que :

$$F(a) = a \text{ et } F'(a) = 1 - \frac{f'(a)^2 - f(a)f''(a)}{f'(a)^2} = 1 - 1 = 0$$

Soit $x \in [c,d]$. On a alors :

$$\begin{aligned} F(x) - a &= (x-a) - \frac{f(x) - f(a)}{f'(x)} \text{ car } f(a) = 0 \\ &= \frac{f(a) - f(x) - (a-x)f'(x)}{f'(x)} \end{aligned}$$

En appliquant la formule de Taylor–Lagrange à l'ordre 2 à f entre x et a (ou a et x) on obtient l'existence d'un point $z_x \in (x,a)$ ou (a,x) tel que :

$$f(a) - f(x) - (a-x)f'(x) = \frac{1}{2} f''(z_x)(a-x)^2$$

D'où :

$$F(x) - a = \frac{1}{2} \frac{f''(z_x)}{f'(x)} (x-a)^2 \tag{2.10.1}$$

Posons $C := \dfrac{\max_{[c,d]} |f''|}{2 \min_{[c,d]} |f'|}$. Alors on a :

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

Soit à présent α tel que $C\alpha < 1$ et $I := [a-\alpha, a+\alpha] \subset [c,d]$. Alors, si $x \in I$, $|F(x) - a| \leq C\alpha^2 < \alpha$ et donc I est stable par f. Ainsi, si $x_0 \in I$, tous les x_n seront dans I et :

$$\forall n \geq 0, \quad |x_{n+1} - a| = |F(x_n) - a| \leq C|x_n - a|^2$$

Et donc par récurrence :

$$\forall n \geq 0, \quad C|x_n - a|^2 \leq (C|x_0 - a|)^{2^n} \leq (C\alpha)^{2^n}$$

D'où le résultat comme $0 < C\alpha < 1$.

Proposition 2.11
On suppose à présent que $f'' > 0$.
Alors :
- *$I := [a,d]$ est stable par F ;*
- *si $x_0 \in I$, la suite $(x_n)_n$ est strictement décroissante ou constante et :*

$$\begin{cases} \forall n \geq 0, \quad 0 \leq x_{n+1} - a \leq C(x_n - a)^2 \\ x_{n+1} - a \sim_{n \to \infty} \dfrac{1}{2} \dfrac{f''(a)}{f'(a)} (x_n - a)^2 \text{ si } x_0 > a \end{cases}$$

Démonstration : Comme $f'' > 0$, f est strictement convexe sur (c, d). Si $x \in I$, $f'(x) > 0$ et $f(x) \geq 0$ donc :

$$F(x) \leq x \text{ avec inégalité stricte si } x > a \tag{2.10.2}$$

De plus, d'après (2.10.1) et comme la courbe de f est au dessus de ses tangentes, il existe $z_x \in [a, x]$ tel que :

$$F(x) - a = \frac{1}{2}\frac{f''(z_x)}{f'(x)}(x-a)^2 \geq 0 \text{ avec inégalité stricte si } x > a \tag{2.10.3}$$

Combinant (2.10.2) et (2.10.3) on obtient que I est stable par F et que si $x_0 \in (a, d]$, pour tout $n \geq 0$, $a < x_n \leq d$ et $(x_n)_n$ est strictement décroissante ; si $x_0 = a$, cette dernière suite est constante.

Dans tous les cas, $(x_n)_n$ admet une limite $\ell \in I$ (car décroissante et minorée) et par continuité $F(\ell) = \ell$ et donc $f(\ell) = 0$ d'où $\ell = a$. Comme précédemment [9] on montre que :

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

D'où la convergence quadratique de $(x_n)_n$ vers a.

Enfin, si $x_0 \in (a, d]$, les x_n sont tous dans $(a, d]$ et si note z_n les "z_{x_n}" provenant de la formule de Taylor–Lagrange on a :

$$\frac{x_{n+1} - a}{(x_n - a)^2} = \frac{1}{2}\frac{f''(z_n)}{f'(z_n)} \xrightarrow[n\to\infty]{} \frac{f''(a)}{f'(a)} \text{ car } a < z_n < x_n \text{ donc } z_n \xrightarrow[n\to\infty]{} a$$

D'où le résultat.

Détails supplémentaires :

– Rappelons la mirifique *formule de Taylor–Lagrange* :

Proposition 2.12 (Formule de Taylor–Lagrange)
Soit I un intervalle de $\mathbb{R}$.
Soit $f \in \mathcal{C}^{n+1}(I, \mathbb{R})$.
Soit $a \in I$.
Alors pour tout $x \in I$ il existe z strictement compris entra a et x (ou x et a) tel que :

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k + \frac{f^{(n+1)}(z)}{k!}(x-a)^{n+1}$$

2.11 Nombres normaux

Référence :
– [QZ07], p. 550–551

Soit $x \in [0, 1)$ et $r \geq 2$ un entier. On sait qu'alors x admet un unique développement propre en base r :

$$x = \sum_{n=1}^{\infty} \frac{\varepsilon_n(x)}{r^n}, \qquad \text{les } \varepsilon_n(x) \in \mathcal{A} := \{0, \ldots, r-1\}$$

Soit $k \geq 1$ et soit $b \in \mathcal{A}^k$. Alors on pose :

$$N_x(b, n) := \text{card}(\{i \in [n-k+1] \,|\, \varepsilon_i(x) = b_1, \ldots, \varepsilon_{i+k-1} = b_k\})$$

$N_x(b, n)$ correspond donc au nombre d'occurrences du motif b dans l'écriture de x en base r. On pose alors la définition suivante :

Définition 2.1 (Nombre normal)
Soit $x \in [0, 1)$.
Alors x est dit :

9. La minoration provient du fait que $x_n \in I$.

(i) r–normal, pour $r \geq 2$, si pour tout mot $b \in \mathcal{A}^k$ (où $\mathcal{A} := \{0, \ldots, r-1\}$) on a :

$$\frac{N_x(b,n)}{n} \xrightarrow[n\to\infty]{} \frac{1}{r^k}$$

(ii) normal si il est r–normal pour tout $r \geq 2$.

Un nombre normal est donc un nombre plein de bon sens, qui se comporte exactement comme on aimerait. Et il a raison. On se propose alors de démontrer le résultat suivant :

Proposition 2.13
Presque tout réel (au sens de Lebesgue) de $[0,1)$ (muni de sa tribu borélienne) est normal.

Démonstration : Soit $r \geq 2$ et posons[10] $\mathcal{A} := \{0, \ldots, r-1\}$. Pour $x \in [0,1)$, on note par[11] $(\varepsilon_n(x))_n$ le développement de x en base r. On remarque alors que ce procédé nous fournit une suite i.i.d de variables aléatoires : la suite $(\varepsilon_n)_n$, avec :

$$\forall b \in \mathcal{A}, \quad \mathbb{P}(\varepsilon_1 = b) = \mathbb{P}\left(\left[\frac{b}{r}, \frac{b+1}{r}\right)\right) = \frac{1}{r}$$

On définit également la variable aléatoire $N(b,n) : x \mapsto N_x(b,n)$.

Fixons à présent $b \in \mathcal{A}$ et posons, pour $j \in \mathbb{N}^*$, $X_j := 1_{\varepsilon_j = b}$. Alors les variables aléatoire X_j sont i.i.d de loi de Bernoulli de paramètre $\mathbb{E}(X_1) = \mathbb{P}(\varepsilon_1 = b) = \frac{1}{r}$. De fait, par loi forte des grands nombres on a :

$$\frac{N(b,n)}{n} = \frac{1}{n}\sum_{j=1}^{n} X_j \xrightarrow[n\to\infty]{\text{p.s}} \frac{1}{r}$$

Et donc le résultat est vrai pour b de longueur 1.

Si $b = (u,v) \in \mathcal{A}^2$, on modifie légèrement le procédé en posant $Y_j := 1_{\varepsilon_j = u, varepsilon_{j+1} = v}$. On a alors :

$$\frac{N(b,n)}{n} = \frac{1}{n}\sum_{j=1}^{n-1} Y_j$$

Cependant, les v.a Y_j, bien qu'étant identiquement distribuées de loi $\mathcal{B}\left(1, \frac{1}{r^2}\right)$, ne sont pas indépendantes. On contourne ce problème en remarquant que les suites $(Y_{2n+1})_{n\geq 0}$ et $(Y_{2n})_{n\geq 1}$ sont, elles, i.i.d. Une application double de la loi forte des grands nombres nous donne alors :

$$\frac{1}{n}\sum_{j=1}^{n} Y_{2j-1} \xrightarrow[n\to\infty]{\text{p.s}} \frac{1}{r^2} \quad \text{et} \quad \frac{1}{n}\sum_{j=1}^{n} Y_{2j} \xrightarrow[n\to\infty]{\text{p.s}} \frac{1}{r^2}$$

De fait :

$$\frac{1}{2n}\sum_{j=1}^{2n} Y_j = \frac{1}{2}\left(\frac{1}{n}\sum_{j=1}^{n} Y_{2j-1}\right) + \frac{1}{2}\left(\frac{1}{n}\sum_{j=1}^{n} Y_{2j}\right) \xrightarrow[n\to\infty]{\text{p.s}} \frac{1}{r^2} \tag{2.11.1}$$

Et :

$$\frac{1}{2n-1}\sum_{j=1}^{2n-1} Y_j = \frac{n}{2n-1}\left(\frac{1}{n}\sum_{j=1}^{n} Y_{2j-1}\right) + \frac{n}{2n-1}\left(\frac{1}{n}\sum_{j=1}^{n-1} Y_{2j}\right) \xrightarrow[n\to\infty]{\text{p.s}} \frac{1}{r^2} \tag{2.11.2}$$

En effet, le second membre converge comme on le souhaite car :

$$\frac{1}{n}\sum_{j=1}^{n-1} Y_{2j} = \frac{n}{n-1}\left(\frac{1}{n-1}\sum_{j=1}^{n-1} Y_{2j}\right)$$

En combinant (2.11.1) et (2.11.2) on obtient que :

$$\frac{1}{n}\sum_{j=1}^{n} Y_j \xrightarrow[n\to\infty]{\text{p.s}} \frac{1}{r^2}$$

10. À nouveau ...
11. Ô surprise !

In fine :

$$\frac{N(b,n)}{n} = \frac{1}{n}\sum_{j=1}^{n-1} Y_j = \frac{n-1}{n}\left(\frac{1}{n-1}\sum_{j=1}^{n-1} Y_j\right) \xrightarrow[n\to\infty]{\text{p.s}} \frac{1}{r^2}$$

En itérant ce procédé, on obtient le résultat suivant : pour tout b mot de longueur k sur $\mathcal{A}$, $\frac{N(b,n)}{n} \xrightarrow[n\to\infty]{\text{p.s}} \frac{1}{r^k}$. Presque tout réel de $[0,1)$ est donc r–normal.

Or si on note E (resp. E_r pour $r \geq 2$) l'ensemble des réels de $[0,1)$ normaux (resp. r–normaux) on a :

$$E = \bigcap_{r\geq 2} E_r$$

Cette intersection étant dénombrable on a, comme les $\mathbb{P}(E_r)$ sont égaux à 1, que $\mathbb{P}(E) = 1$. En effet,

$$\begin{aligned}
\mathbb{P}([0,1)\setminus E) &= \mathbb{P}\left([0,1)\setminus \bigcap_{r\geq 2} E_r\right) \\
&= \mathbb{P}\left(\bigcup_{r\geq 2}[0,1)\setminus E_r\right) \\
&\leq \sum_{r=2}^{\infty} \mathbb{P}([0,1)\setminus E_r) \\
&= 0
\end{aligned}$$

D'où le résultat.

2.12 Problème de la ruine du joueur

Référence :
- [Ouv00], p.394–398

Prérequis :
- décomposition de Doob ;
- premier théorème d'arrêt ;
- martingales équi–intégrables.

On considère le problème suivant : *un joueur compulsif joue à pile où face avec une pièce truquée. S'il obtient pile, la banque lui donne un euro et s'il obtient face il donne un euro à la banque. Le joueur étant compulsif il joue jusqu'à sa propre ruine ou celle de la banque.*

Modèle :

On note $a \in \mathbb{N}^*$ (resp. $b \in \mathbb{N}^*$) la fortune initiale du joueur (resp. de la banque) et p la probabilité d'obtenir pile en lançant la pièce. On se place alors sur un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$ et on se donne une suite $(Y_n)_n$ de variables aléatoires i.i.d de loi $p\delta_1 + q\delta_{-1}$ (avec bien entendu $q = 1-p$), la variable Y_n représentant l'impact de la n–ième partie sur le pécule du joueur. On peut alors modéliser sa fortune au bout n parties par le processus aléatoire suivant :

$$\forall n \geq 0,\ S_n := a + \sum_{j=1}^{n} Y_j$$

Si on pose $Y_0 := a$ les filtrations $(\sigma(S_i \,|\, 0 \leq i \leq n))_{n\in\mathbb{N}}$ et $(\sigma(Y_i \,|\, 0 \leq i \leq n))_{n\in\mathbb{N}}$ sont égales : notons les (la ?) $(\mathcal{A}_n)_n$. On définit enfin le temps d'arrêt T du jeu :

$$T := \inf\{n \geq 1 \,|\, S_n \in \{0, a+b\}\}$$

On cherche à calculer la probabilité $\rho := \mathbb{P}(S_T = a+b)$ de non–ruine du joueur, ainsi que la probabilité $\mathbb{P}(T < \infty)$ que la partie s'achève un jour et sa durée moyenne $\mathbb{E}(T)$ le cas échéant.

Étude :

– *Nature du processus S.*

$$\begin{aligned}\forall n \geq 1,\ \mathbb{E}(S_n|\mathcal{A}_{n-1}) &= a + \sum_{j=1}^{n} \mathbb{E}(Y_j|\mathcal{A}_{n-1}) \\ &= a + \sum_{j=1}^{n-1} \underbrace{\mathbb{E}(Y_j|\mathcal{A}_{n-1})}_{=Y_j \text{ car } Y_j \in m(\mathcal{A}_{n-1})} + \underbrace{\mathbb{E}(Y_n|\mathcal{A}_{n-1})}_{=Y_n \text{ car } Y_n \perp \mathcal{A}_{n-1}} \\ &= S_{n-1} + p - q\end{aligned}$$

De fait S est une martingale (resp. sous, sur) si $p = q = \dfrac{1}{2}$ (resp. $p > q$, $p < q$) intégrable.

– *Cas $p \neq q$.* Par exemple, supposons que $p > q$ (S est alors une sous–martingale). On définit le processus aléatoire suivant :

$$A_0 := 0 \text{ et } \forall n \in \mathbb{N}^*, \quad A_n - A_{n-1} := \mathbb{E}(S_n - S_{n-1}|\mathcal{A}_{n-1}) \text{i.e (par récurrence)} A_n = n(p-q)$$

Il est alors évident que $(A_n)_n$ est un processus croissant prévisible. Par décomposition de Doob [12] on a alors que $M := S - A$ est une martingale intégrable. Pour $n \geq 0$, le premier théorème d'arrêt appliqué à la martingale M et au temps d'arrêt borné $T \wedge n$ s'écrit alors :

$$\mathbb{E}(S_0) = \mathbb{E}(M_{T\wedge n}) \text{ i.e } a = \mathbb{E}(S_{T\wedge n}) - (p-q)\mathbb{E}(T \wedge n)$$

De fait comme $\mathbb{E}(S_{T\wedge n}) \leq a + b$ par construction on a :

$$0 \leq (p-q)\mathbb{E}(T \wedge n) \leq b \tag{2.12.1}$$

Commençons par remarquer que $T\wedge n \xrightarrow[n\to\infty]{} T$ p.s. En effet, sur $\{T = \infty\}$, $T\wedge n = n \xrightarrow[n\to\infty]{} \infty$ et si $\omega \in \{T < \infty\}$ il va exister $N \in \mathbb{N}$ tel que $\forall n \geq N$, $n \geq T(\omega)$ i.e $(T \wedge n)(\omega) = T(\omega)$ et donc $(T \wedge n)(\omega) \xrightarrow[n\to\infty]{} T(\omega)$, d'où le résultat.
La suite $(T \wedge n)$ étant croissante, positive, intégrable et convergeant vers T p.s, le théorème de Beppo–Levi nous affirme que $\limsup_{n\to\infty} \mathbb{E}(T \wedge n) = \mathbb{E}(T)$. En passant à la limite (sup) dans (2.12.1) on obtient alors que $T \in L^1$ ergo $\mathbb{P}(T < \infty) = 1$. De plus, pour tout $k, n \geq 1$, $S_{T\wedge n}1_{\{T=k\}} = S_{k\wedge n} = S_k$ pour n assez grand, i.e $S_{T\wedge n}1_{\{T=k\}} = S_T 1_{\{T=k\}}$ et donc $S_{T\wedge n} \xrightarrow[n\to\infty]{} S_T$ p.s.
En appliquant le théorème de convergence dominée (combiné à Beppo-Levi, cf supra) avec domination $0 \leq S_{T\wedge n} \leq a + b$ dans (2.12.1) on obtient [13] de fait :

$$0 \leq (p-q)\mathbb{E}(T) = \mathbb{E}(S_T) - a \tag{2.12.2}$$

Par définition de T on a également :

$$\mathbb{E}(S_T) = (a+b)\mathbb{P}(S_T = a+b) + 0\mathbb{P}(S_T = 0) = (a+b)\rho$$

D'où, via (2.12.2), $\mathbb{E}(T) = \dfrac{(a+b)\rho - a}{p-q}$.

Posons à présent $\forall n \geq 0$, $U_n := \left(\dfrac{q}{p}\right)^{S_n}$. Alors U est une martingale. En effet :

$$\begin{aligned}\forall n \geq 1,\ \mathbb{E}(U_n|\mathcal{A}_{n-1}) &= \mathbb{E}\left(\left(\frac{q}{p}\right)^{S_{n-1}}\left(\frac{q}{p}\right)^{Y_n}\middle|\mathcal{A}_{n-1}\right) \\ &= \left(\frac{q}{p}\right)^{S_{n-1}}\mathbb{E}\left(\left(\frac{q}{p}\right)^{Y_n}\middle|\mathcal{A}_{n-1}\right) \text{ car } \left(\frac{q}{p}\right)^{S_{n-1}} \in m(\mathcal{A}_{n-1}) \\ &= \left(\frac{q}{p}\right)^{S_{n-1}}\mathbb{E}\left(\left(\frac{q}{p}\right)^{Y_n}\right) \text{ car } \left(\frac{q}{p}\right)^{Y_n} \perp Ar_{n-1} \\ &= U_{n-1}\left(\frac{q}{p}p + \frac{p}{q}q\right) \\ &= U_{n-1}\end{aligned}$$

12. Le processus croissant prévisible dans cette dernière étant nécessairement le processus des accroissements.
13. En "passant à la limsup".

Comme $\frac{q}{p} < 1$, $\forall n \in \mathbb{N}$, $U_{T\wedge n} \in [0,1]$ et donc :

$$\forall a \geq 1, \int_{|U_{T\wedge n}|>a} |U_{T\wedge n}| d\mathbb{P} = 0$$

Ce qui signifie que la martingale arrêtée $U^T := (U_{T\wedge n})$ est équi–intégrable donc converge dans L^1 et $\mathbb{P}$–p.s vers une variable aléatoire X. Or $S_{T\wedge n} \xrightarrow[n\to\infty]{} S_T$ p.s donc on a nécessairement $X = U_T$. Remarquons à présent que :

$$\mathbb{E}(U_T) = \left(\frac{q}{p}\right)^0 \mathbb{P}(S_T = 0) + \left(\frac{q}{p}\right)^{a+b} \mathbb{P}(S_T = a+b)$$

I.e :

$$\mathbb{E}(U_T) = 1 - \rho + \left(\frac{q}{p}\right)^{a+b} \rho \tag{2.12.3}$$

En outre, par le premier théorème d'arret on a :

$$\forall n \in \mathbb{N}, \mathbb{E}(U_{T\wedge n}) = \mathbb{E}(U_0) = \left(\frac{q}{p}\right)^a$$

Et appliquant le théorème de convergence dominé à $U_{T\wedge n} \leq \left(\frac{q}{p}\right)^{a+b} \in L^1$ on obtient :

$$\mathbb{E}(U_T) = \left(\frac{q}{p}\right)^a$$

En utilisant les égalités (2.12.2) et (2.12.3) on obtient alors le résultat recherché :

$$\rho := \frac{1 - \left(\frac{q}{p}\right)^a}{1 - \left(\frac{q}{p}\right)^{a+b}} \text{ et } \mathbb{E}(T) = \frac{1}{p-q}\left((a+b)\frac{1 - \left(\frac{q}{p}\right)^a}{1 - \left(\frac{q}{p}\right)^{a+b}} - a\right)$$

– *Cas* $p = q = \frac{1}{2}$. Les Y_n étant L^∞, S est alors une martingale L^2. On définit un processus aléatoire B comme suit :

$$B_0 := 0 \text{ et } \forall n \geq 1, B_n - B_{n-1} := \mathbb{E}((S_n - S_{n-1})^2 | \mathcal{A}_{n-1}) = \mathbb{E}(Y_n^2 | \mathcal{A}_{n-1})$$

Le processus B est alors croissant prévisible et comme $Y_n^2 \perp \mathcal{A}_{n-1}$ alors $B_n - B_{n-1} = \mathbb{E}(Y_n^2) = p+q = 1$, d'où $\forall n \geq 0$, $B_n = n$.
Par décomposition de Doob, comme S^2 est une sous–martingale, le processus $(S_n^2 - n)_n$ est alors une martingale et on obtient en lui appliquant le premier théorème d'arrêt que :

$$\forall n \geq 0, \ a^2 = \mathbb{E}(S_0^2 - 0) = \mathbb{E}(S_{T\wedge n}^2 - T \wedge n) \tag{2.12.4}$$

Comme $S_{T\wedge n}^2 \leq (a+b)^2$ on a :

$$\mathbb{E}(T \wedge n) = \mathbb{E}(S_{T\wedge n}^2) - a^2 \leq (a+b)^2 - a^2$$

En procédant exactement comme dans le cas $p \neq q$ on montre (en utilisant Beppo–Levi) que $\limsup_n \mathbb{E}(T \wedge n) = \mathbb{E}(T)$ d'où par passage à la limite $\mathbb{E}(T) \leq (a+b)^2 - a^2$. De fait $T \in L^1$ et donc $\mathbb{P}(T < \infty) = 1$ ce qui nous permet, toujours de façon analogue au cas précédent, de conclure que $S_{T\wedge n} \xrightarrow[n\to\infty]{} S_T$. En appliquant le théorème de convergence dominée, avec domination $0 \leq S_{T\wedge n} \leq a+b$ on obtient que $(S_{T\wedge n})_n$ converge dans L^1 et L^2 vers S_T.
Par premier théorème d'arrêt on a également que $\mathbb{E}(S_{T\wedge n}) = \mathbb{E}(S_0) = a$ donc en passant à la limite on trouve $\mathbb{E}(S_T) = a$. Or $\mathbb{E}(S_T) = (a+b)\rho$ ergo :

$$\rho = \frac{a}{a+b}$$

Pour finir, remarquons que l'on peut à présent passer à la limite dans (2.12.4), obtenant :

$$\mathbb{E}(T) = \mathbb{E}(S_T^2) - a^2$$

Or :

$$\mathbb{E}(S_T^2) = (a+b)^2\rho = a(a+b)$$

D'où le résultat :

$$\mathbb{E}(T) = ab$$

Détails supplémentaires :

– *Motivation du choix de* U.Fixons $s > 0$ et posons $\forall n \geq 0,\, U_n := s^{S_n}$. Recherchons pour quelle(s) valeur(s) de s ce processus définit une martingale.

$$\begin{aligned}\forall n \geq 1,\ \mathbb{E}(U_n|\mathcal{A}_{n-1}) &= \mathbb{E}(s^{S_{n-1}}s^{Y_n}|\mathcal{A}_{n-1})\\ &= s^{S_{n-1}}\mathbb{E}(s^{Y_n}|\mathcal{A}_{n-1}) \text{ car } s^{S_{n-1}} \in m(\mathcal{A}_{n-1})\\ &= s^{S_{n-1}}\mathbb{E}(s^{Y_n}) \text{ car } s^{Y_n} \perp Ar_{n-1}\\ &= U_{n-1}\left(sp + \frac{1}{s}q\right)\end{aligned}$$

Or :

$$sp + \frac{1}{s}q = 1 \Leftrightarrow s^2p - s + q = 0 \Leftrightarrow s \in \left\{1, \frac{q}{p}\right\}$$

Si $s = 1$, la martingale U est remarquablement peu intéressante[14], tandis que so $s = \frac{q}{p}$ elle est non constante. On choisit donc $s := \frac{p}{q}$.

– *Rappel.* On dit qu'une famille $(X_i)_{i\in I}$ de v.a est équi–intégrable si :

$$\lim_{a\to\infty} \sup_{i\in I} \int_{|X_i|>a} |X_i| d\mathbb{P} = 0$$

2.13 Prolongement méromorphe de la fonction Γ d'Euler

Références :

– [BMP05], p. 82–83 et [QZ95] p. 305–306

Prérequis :

– holomorphie sous le signe intégral ;
– sommation méromorphe.

Proposition 2.14
On considère l'application définie (formellement) de la façon suivante :

$$\Gamma(z) := \int_0^\infty e^{-t}t^{z-1}dt$$

Alors :

(i) cette expression définit une fonction holomorphe de $\mathcal{P} := \{z \in \mathbb{C} \,|\, \Re(z) > 0\}$ *dans* $\mathbb{C}$ *;*

(ii) la fonction $\Gamma : \mathcal{P} \to \mathbb{C}$ *admet un prolongement méromorphe à* $\mathbb{C}$ *de pôles les entiers négatifs.*

Démonstration :

(i) ([QZ95]) On considère l'application suivante :

$$\begin{aligned} g : \mathcal{P} \times \mathbb{R}_+^* &\to \mathbb{C}\\ (z,t) &\mapsto e^{-t}t^{z-1}\end{aligned}$$

Alors :

– pour tout $t > 0$, l'application $g(.,t)$ est holomorphe de dérivée $\frac{\partial}{\partial z}(e^{-t}e^{(z-1)\ln(t)}) = \ln(t)g(.,t)$;

14. Mais d'une facilité d'étude assez déconcertante, vous en conviendrez.

– soit K un compact de $\mathcal{P}$. Posons $M := \max_{z\in K} \Re(z)$ et $\varepsilon := \min_{z\in K} \Re(z)$; comme $K \subset \mathcal{P}$ alors $\varepsilon > 0$. Alors, pour tout $z \in K$ et $t > 0$:
  * si $t \in (0,1)$, $|e^{-t}t^{z-1}| = |e^{-t}e^{(z-1)\ln(t)}| \leq t^{\varepsilon-1} = \dfrac{1}{t^{1-\varepsilon}}$;
  * si $t \geq 1$,$|e^{-t}t^{z-1}| = e^{-t}t^{\Re(z)-1} \leq e^{-t}t^{M-1} = o\left(\frac{1}{t^2}\right)$.

D'où le résultat par proposition 2.16 (cf. infra).

(ii) ([BMP05]) Soit $z \in \mathcal{P}$. Alors :

$$\Gamma(z) = \int_0^1 e^{-t}t^{z-1}dt + \int_1^\infty e^{-t}t^{z-1}dt$$

De plus, pour $t \in [0,1]$:

$$e^{-t}t^{z-1} = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} t^{n+z-1}$$

On souhaite appliquer le théorème de Fubini à la mesure produit des mesures de Lebesgue et de comptage et à la fonction $g : (n,t) \mapsto \dfrac{(-1)^n}{n!}t^{n+z-1}$. Pour ce faire il nous suffit de démontrer que g est intégrable, i.e que :

$$\int_0^1 \sum_{n=0}^{\infty} \left| \frac{(-1)^n}{n!} t^{n+z-1} \right| dt < \infty$$

Or si $t \in (0,1]$, $t^z = t^{\Re(z)}$ donc :

$$\sum_{n=0}^{\infty} \left| \frac{(-1)^n}{n!} t^{n+z-1} \right| = t^{\Re(z)-1} \sum_{n=0}^{\infty} \frac{t^n}{n!} = t^{\Re(z)-1}e^t$$

Comme $\Re(z) > 0$, $\Re(z) - 1 > -1$ donc $t \mapsto t^{\Re(z)-1}e^t$ est intégrable sur $(0,1]$ d'où le résultat par domination. De fait, par Fubini :

$$\begin{aligned}
\int_0^1 e^{-t}t^{z-1}dt &= \int_0^1 \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} t^{n+z-1}dt \\
&= \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} \int_0^1 t^{n+z-1}dt \\
&= \sum_{n=0}^{\infty} \frac{(-1)^n}{n!(z+n)}
\end{aligned}$$

Au final :

$$\forall z \in \mathcal{P}, \quad \Gamma(z) = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!(z+n)} + \int_1^\infty e^{-t}t^{z-1}dt$$

On définit ensuite la suite de fonctions $f_n : z \mapsto \dfrac{(-1)^n}{n!(z+n)}$. Alors :

– pour tout $n \geq 0$, f_n est méromorphe sur $\mathbb{C}$, de pôle (simple) $-n$;
– pour tout compact $K \subset\subset \mathbb{C}$, il existe $N \geq 0$ tel que $K \subset \overline{\mathcal{B}}(0,N)$. De fait, pour $n \geq N+1$, f_n n'a aucun pôle dans K et :

$$\forall z \in K,\ |z+n| = |n-(-z)| \geq |n - |z|| = n - |z| \geq n - N \text{ d'où } |f_n(z)| \leq \frac{1}{n!(n-N)}$$

  Ainsi $\|f\|_{\infty,K} \leq \dfrac{1}{n!(n-N)}$ et donc $\sum_{(n\geq N_K)} f_n$ converge normalement uniformément sur K.

Par la proposition 2.15 (cf. infra) l'application $f : z \mapsto \sum_{n=0}^\infty \dfrac{(-1)^n}{n!(z+n)}$ est donc méromorphe sur $\mathbb{C}$ et l'ensemble de ses pôles est $-\mathbb{N}$. En utilisant les mêmes majorations qu'au point (i) on montre que $z \mapsto \int_1^\infty e^{-t}t^{z-1}dt$ est holomorphe sur $\mathbb{C}$ (dans le cas $t \geq 1$ on n'a pas utilisé que $\Re(z) > 0$). Ainsi, Γ admet le prolongement méromorphe sur $\mathbb{C}$ suivant :

$$\Gamma : z \mapsto \sum_{n=0}^{\infty} \frac{(-1)^n}{n!(z+n)} + \int_1^\infty e^{-t}t^{z-1}dt$$

Détails supplémentaires :

– Soit $t > 0$. On rappelle que pour $z = x + iy \in \mathbb{C}$ on définit :

$$t^z := e^{x\ln(t)}e^{iy\ln(t)} =: t^x t^{iy}$$

– On rappelle le résultat suivant (cf. [BMP05]) :

Proposition 2.15
Soit $\mathcal{U}$ un ouvert de $\mathbb{C}$.
Soit $\sum f_n$ une série de fonctions méromorphes sur $\mathcal{U}$.
On suppose que pour tout compact $K \subset\subset \mathcal{U}$ il existe $N_K \geq 0$ tel que :
– pour tout $n \geq N_K$ f_n n'a aucun pôle dans K ;
– la série $\sum_{(n\geq N_K)} f_n$ converge uniformément sur K.
Alors :

(i) la fonction $\sum_{n=0}^{\infty} f_n$ ainsi définie est méromorphe sur $\mathcal{U}$, et l'ensemble de ses pôles est la réunion de ceux des f_n ;

(ii)

$$\left(\sum_{n=0}^{\infty} f_n\right)' = \sum_{n=0}^{\infty} f_n'$$

– On a fait usage de l'énoncé suivant du théorème d'holomorphie sous le signe intégral (cf. [QZ95], p. 301) :

Proposition 2.16
Soit $(X, \mathcal{A}, \mu)$ un espace mesuré.
Soit $\mathcal{U}$ un ouvert de $\mathbb{C}$.
Soit $f : \mathcal{U} \times X \to \mathbb{C}$ telle que :
– pour tout $z \in \mathcal{U}$, $f(z, .) \in L^1(X)$;
– pour presque tout $x \in X$, $f(., x)$ est holomorphe sur $\mathcal{U}$;
– pour tout compact K de $\mathcal{U}$ il existe $g \in L^1(X)$ positive telle que :

$$\forall z \in K, \ \ pp\ x \in X, \quad |f(z, x)| \leq g(x)$$

Alors :

(i) $F : z \mapsto \int_X f(z, x)d\mu(x)$ est holomorphe sur $\mathcal{U}$;

(ii)

$$\forall z \in \mathcal{U}, \quad F'(z) = \int_X \frac{\partial f}{\partial z}(z, x)d\mu(x)$$

2.14 Théorèmes d'Abel angulaire et taubérien faible

Référence :

– [Gou08], p. 252 – 254

Proposition 2.17 (Théorème d'Abel angulaire)
Soit $\sum a_n z^n$ une série entière de rayon de convergence supérieur ou égal à 1 et de somme f. Soit $\theta_0 \in \left[0, \frac{\pi}{2}\right[$. On pose :

$$\Delta_{\theta_0} := \{z \in \mathbb{C} \,|\, |z| < 1 \ \text{et}\ \exists \rho > 0, \varphi \in [-\theta_0, \theta_0],\ z = 1 - \rho e^{i\varphi}\}$$

On suppose que $\sum a_n$ converge.
Alors :

$$f(z) \xrightarrow[\substack{z\in\Delta_{\theta_0} \\ z\to 1}]{} \sum_{n=0}^{\infty} a_n$$

Démonstration : On adopte les conventions de notations suivantes :

$$S := \sum_{n=0}^{\infty} a_n,\ \forall n \geq 0,\ S_n := \sum_{k=0}^{n} a_k,\ R_n := S - S_n$$

Alors pour tout $z \in \mathbb{C}$ tel que $|z| < 1$ on a , comme[15] $a_n = R_{n-1} - R_n$:

$$\begin{aligned}
\forall N \geq 1,\ \sum_{n=0}^{N} a_n z^n - S_N &= \sum_{n=1}^{N} (R_{n-1} - R_n)(z^n - 1) \\
&= \sum_{n=0}^{N-1} R_n (z^{n+1} - 1) - \sum_{n=1}^{N} R_n (z^n - 1) \\
&= R_0(z-1) + \sum_{n=1}^{N-1} R_n z^{n+1} - \sum_{n=1}^{N-1} R_n - \sum_{n=1}^{N-1} R_n z^n + \sum_{n=1}^{N-1} R_n - R_N(Z^N - 1) \\
&= \sum_{n=0}^{N-1} R_n (z^{n+1} - z^n) - R_N(z^N - 1) \\
&= (z-1) \sum_{n=0}^{N-1} R_n z^n - R_N(z^N - 1)
\end{aligned}$$

Comme $\sum a_n$ converge, $R_N \xrightarrow[N \to \infty]{} 0$. De plus $\left(\sum_{n=0}^{N} a_n z^n - S_N\right)_N$ converge car $|z| < 1$ et donc $\left(\sum_{n=0}^{N-1} R_n z^n\right)_N$ converge ce qui entraîne, par passage à la limite :

$$f(z) - S = (z-1) \sum_{n=0}^{+\infty} R_n z^n \tag{2.14.1}$$

Fixons à présent $\varepsilon > 0$. Alors par convergence de $(R_n)_n$ vers 0 il existe $N \geq 1$ tel que $\forall n \geq N$, $|R_n| \leq \varepsilon$. Pour tout $z \in \mathbb{C}$ tel que $|z| < 1$ on a alors, par (2.14.1) :

$$|f(z) - S| \leq |z-1| \left| \sum_{n=0}^{N} R_n z^n \right| + \varepsilon |z-1| \sum_{n=N+1}^{\infty} |z|^n \tag{2.14.2}$$

$$\leq |z-1| \sum_{n=0}^{N} |R_n| + \varepsilon \frac{|z-1|}{1-|z|} \tag{2.14.3}$$

Soit à présent $z \in \Delta_{\theta_0}$: alors il existe $\rho > 0$ et $\varphi \in [-\theta_0, \theta_0]$ tels que $z = 1 - \rho e^{i\varphi}$ et donc $|z|^2 = 1 - 2\rho\cos(\varphi) + \rho^2$.

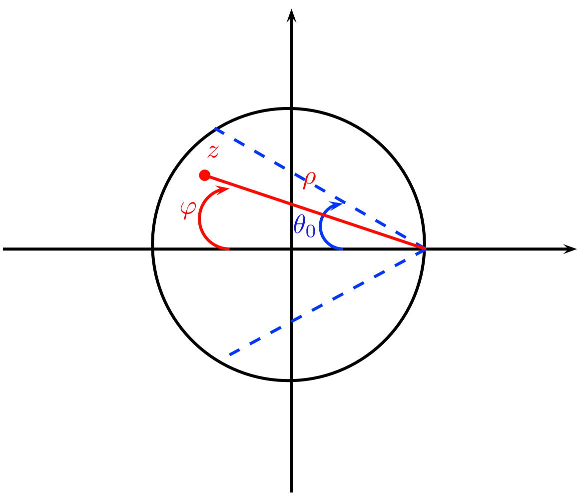


FIGURE 2.2 – Coordonnées dans Δ_{θ_0}.

15. Pour ceux qui voudraient briller en société, ce type de calcul s'appelle une transformée d'Abel.

Si on suppose $\rho \leq \cos(\theta_0)$ (ce qui a un sens puisque notre intention est de faire tendre z vers 1 dans Δ_{θ_0} alors :

$$\begin{aligned}\frac{|z-1|}{1-|z|} &= \frac{|z-1|}{1-|z|^2}(1+|z|)\\ &= \frac{\rho}{2\rho\cos(\varphi)-\rho}(1+|z|)\\ &\leq \frac{2}{2\cos(\varphi)-\rho}\\ &\leq \frac{2}{2\cos(\theta_0)-\cos(\theta_0)} \text{ car } \cos(\varphi)\geq\cos(\theta_0)\\ &= \frac{2}{\cos(\theta_0)}\end{aligned}$$

Finalement, si on se donne $\alpha_N > 0$ tel que $\alpha_N \sum_{n=0}^{N} |R_n| < \varepsilon$ et $z \in \Delta_{\theta_0}$ tel que $|z-1|^l eq \min(\alpha_N, \cos(\theta_0))$ on a, par (2.14.3) :

$$|f(z)-S| \leq \varepsilon + \varepsilon\frac{2}{\cos(\theta_0)}$$

D'où le résultat.

On poursuit ce développement avec une "semi–réciproque" du théorème d'Abel angulaire :

Proposition 2.18 (Théorème taubérien faible)
Soit $\sum a_n z^n$ une série entière de rayon de convergence 1 et de somme f.
On suppose que :
- $\exists S \in \mathbb{C}, \quad f(x) \xrightarrow[\substack{x\in(-1,1)\\ x\to 1}]{} S$;
- $a_n = o\left(\frac{1}{n}\right)$.

Alors la série $\sum a_n$ converge et on a :

$$\sum_{n=0}^{\infty} a_n = S$$

DÉMONSTRATION : On adopte la notation suivante :

$$\forall n \geq 0,\ S_n := \sum_{k=0}^{n} a_k$$

Alors, pour tout $n \in \mathbb{N}^*$ et $x \in (0,1)$:

$$S_n - f(x) = \sum_{k=1}^{n} a_k(1-x^k) - \sum_{k=n+1}^{\infty} a_k x^k$$

Or :

$$\forall k \geq 1, \quad (1-x^k) = (1-x)\sum_{i=0}^{k-1} x^i \leq (1-x)k \text{ car } x \leq 1$$

De fait [16], la suite $(ka_k)_k$ étant bornée car $a_k = o\left(\frac{1}{k}\right)$, on a :

$$\begin{aligned}|S_n - f(x)| &\leq (1-x)\sum_{k=1}^{n} k|a_k| + \sum_{k=n+1}^{\infty}\frac{k}{n}|a_k|x^k \quad (2.14.4)\\ &\leq (1-x)Mn + \frac{1}{n}\frac{1}{(1-x)}\sup_{k>n}(k|a_k|) \text{ où } M := \sup_{k\geq 1}(k|a_k|) \quad (2.14.5)\end{aligned}$$

16. La première majoration dans la seconde somme provenant du fait que si $k \geq n+1$ alors (!) $\frac{k}{n} \geq 1$.

Soit $0 < \varepsilon < 1$: alors d'après (2.14.5) :

$$\forall n \geq 1, \quad \left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| \leq M\varepsilon + \frac{1}{\varepsilon}\sup_{k>n}(k|a_k|)$$

La suite (ka_k) convergeant vers 0 il existe $N_0 \geq 1$ tel que $\sup_{k>N_0}(k|a_k|)$. Ainsi :

$$\forall n \geq N_0, \quad \left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| \leq M\varepsilon + \varepsilon \tag{2.14.6}$$

Or $f(x) \xrightarrow[\substack{x\in(-1,1)\\ x\to 1}]{} S$ donc il existe $N_1 \geq 1$ tel que :

$$\forall n \geq N_1, \quad \left|f\left(1 - \frac{\varepsilon}{n}\right) - S\right| \leq \varepsilon \tag{2.14.7}$$

En combinant (2.14.6) et (2.14.7) on obtient :

$$\begin{aligned}\forall n \geq \max(N_0, N_1), \quad |S_n - S| &\leq \left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| + \left|f\left(1 - \frac{\varepsilon}{n}\right) - S\right| \\ &\leq \varepsilon(M+2)\end{aligned}$$

D'où le résultat.

Détails supplémentaires :

- La réciproque du théorème d'Abel angulaire est fausse. En effet, la série $\sum(-1)^n z^n$ converge normalement sur le disque unité ouvert vers $z \mapsto \dfrac{1}{1+z}$ et :

$$\sum_{n=0}^{\infty}(-1)^n z^n \xrightarrow[z\to 1,\, |z|<1]{} \frac{1}{2} = \lim_{z\to 1,\, |z|<1} \frac{1}{1+z}$$

  Cependant, la série $\sum(-1)^n$ n'est pas convergente.

2.15 Théorème de Banach–Steinhaus

Référence :
- [Gou08], p.404–406

Prérequis :
- théorème de Baire.

Proposition 2.19 (Banach–Steinhaus)
Soit E un espace de Banach et F un e.v.n.
Soit $H \subset \mathcal{L}_c(E, F)$. Alors soit $(\|f\|)_{f\in H}$ est bornée, soit il existe $x \in E$ tel que $\sup_{f\in H} \|f(x)\| = \infty$.

Démonstration : Pour $k \in \mathbb{N}$ on définit l'ensemble suivant :

$$\Omega_k := \{x \in E \,|\, \sup_{f\in H} \|f(x)\| > k\} \subset E$$

Montrons que Ω_k est ouvert. Si $x_0 \in \Omega_k$, il existe $f \in H$ telle que $\|f(x_0)\| > k$ donc par continuité de f il existe $\rho > 0$ tel que $\forall x \in \mathcal{B}(x_0, \rho)$, $\|f(x)\| > k$ et donc $\mathcal{B}(x_0, \rho) \subset \Omega_k$ d'où le résultat.

Nous distinguons à présent deux cas.

- *Cas 1 : les Ω_k sont* tous *denses dans E.* E est un espace métrique complet donc un espace de Baire, aussi le théorème éponyme nous livre-t-il :

$$\overline{\bigcap_{k\in\mathbb{N}} \Omega_k} = E$$

  En particulier, $\cap_k \Omega_k \neq \emptyset$ et si l'on se donne $x \in \cap_k \Omega_k$ on a :

$$\sup_{f\in H} \|f(x)\| = \infty$$

- *Cas 2 : ¬ (cas 1).* Il existe donc $k \geq 0$ tel que Ω_k ne soit pas dense dans E, i.e il existe $x_0 \in E$ et $\rho > 0$ tels que $\mathcal{B}(x_0, \rho) \cap \Omega_k = \emptyset$. De fait $\forall x \in \mathcal{B}(x_0, \rho)$, $\sup_f \|f(x)\| \leq k$, ergo :

$$\begin{aligned}\forall x \in \mathcal{B}(0, \rho),\ \forall f \in H,\ \|f(x)\| &= \|f(x + x_0) - f(x_0)\| \\ &\leq \|f(x + x_0)\| + \|f(x)\| \\ &\leq 2k\end{aligned}$$

  Par continuité de f cette inégalité s'étend naturellement à $\overline{\mathcal{B}}(0, \rho)$. Soient donc $f \in H$ et $x \in E$ de norme 1. Alors :

$$\|f(x)\| = \frac{1}{\rho}\|f(\rho x)\| \leq \frac{2k}{\rho}$$

  D'où $\|f\| \leq \dfrac{2k}{\rho}$ et donc $(\|f\|)_{f \in H}$ est bornée, ce qui achève le théorème.

Corollaire 2.19.1
On note $\mathcal{C}_{2\pi}$ le $\mathbb{C}$−e.v des fonctions continues 2π−périodiques à valeurs complexes, que l'on munit de la norme $\|.\|_\infty$ usuelle.
Pour $f \in \mathcal{C}_{2\pi}$ on définit :

$$\forall n \in \mathbb{Z},\ c_n(f) := \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)e^{-int}dt \ \textit{et}\ \forall n \geq 0,\ S_n(f) : x \mapsto \sum_{k=-n}^{n} c_k(f)e^{ikx}$$

Alors il existe une fonction $f \in \mathcal{C}_{2\pi}$ telle que $(S_n(f)(0))_{n \geq 0})$ diverge. En particulier, f n'est pas somme de sa série de Fourier.

Démonstration : On commence par définir la forme linéaire suivante (pour $n \geq 1$) :

$$\begin{aligned}\ell_n : \mathcal{C}_{2\pi} &\to \mathbb{C} \\ f &\mapsto S_n(f)(0) = \sum_{k=-n}^{n} c_k(f)\end{aligned}$$

Alors ℓ_n est une forme linéaire continue sur $\mathcal{C}_{2\pi}$. En effet, si $f \in Cr_{2\pi}$ on a :

$$\begin{aligned}\ell_n(f) &= \sum_{k=-n}^{n} \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)e^{-ikt}dt \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\sum_{k=-n}^{n} e^{-ikt}dt \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)D_n(t)dt \text{ où } D_n : t \mapsto \sum_{k=-n}^{n} e^{-ikt} = \frac{\sin((n+1/2)t)}{\sin(t/2)}\end{aligned}$$

De fait :

$$|\ell_n(f)| \leq \frac{1}{2\pi}\int_{-\pi}^{\pi} |D_n(t)|dt\|f\|_\infty \text{ donc } \|\ell_n\| \leq \frac{1}{2\pi}\int_{-\pi}^{\pi} |D_n(t)|dt$$

On définit ensuite pour $\varepsilon > 0$ l'application suivante :

$$\begin{aligned}f_\varepsilon : \mathbb{R} &\to \mathbb{C} \\ x &\mapsto \frac{D_n(x)}{|D_n(x)| + \varepsilon}\end{aligned}$$

$\|f_\varepsilon\|_\infty \leq 1$ et par convergence dominée on a :

$$|\ell_n(f_\varepsilon)| \xrightarrow[\varepsilon \to 0]{} \frac{1}{2\pi}\int_{-\pi}^{\pi} |D_n(t)|dt$$

De fait $\|\ell_n\| = \dfrac{1}{2\pi}\int_{-\pi}^{\pi}|D_n(t)|dt$. En utilisant l'inégalité $|\sin(t/2)| \leq |t/2|$ on trouve alors :

$$\begin{aligned}
\|\ell_n\| &\geq \frac{1}{pi}\int_0^{\pi}\left|\frac{\sin((n+1/2)t)}{t/2}\right|dt \\
&= \frac{2}{\pi}\int_0^{(n+1/2)\pi}|\mathrm{sinc}(t)|dt \text{ via } t \mapsto \frac{2}{2n+1}t \\
&\xrightarrow[n\to\infty]{} \infty \text{ car } \int_0^{\infty}|\mathrm{sinc}(t)|dt \text{ diverge}
\end{aligned}$$

L'espace $(\mathcal{C}_{2\pi}, \|.\|_\infty)$ étant complet, le théorème de Banach–Steinhaus s'applique et implique qu'il existe $f \in \mathcal{C}_{2\pi}$ telle que :

$$\sup_{n\geq 0} S_n(f)(0) = \sup_{n\geq 0}\ell_n(f) = \infty$$

Donc $(S_n(f)(0))_n$ diverge.

Détails supplémentaires :

- *Sommons.* Soient $t \in \mathbb{R}$ et $n \geq 0$. Alors :

$$\begin{aligned}
\sum_{k=-n}^{n} e^{-ikt} &= \sum_{k=0}^{n} e^{ikt} + \sum_{k=0}^{n} e^{-ikt} \\
&= \frac{1-e^{i(n+1)t}}{1-e^{it}} + e^{-it}\frac{1-e^{-int}}{1-e^{-it}} \\
&= \frac{1-e^{i(n+1)t}}{1-e^{it}} + \frac{1-e^{-int}}{e^{it}-1} \\
&= \frac{e^{i(n+1)t}-e^{-int}}{e^{it}-1} \\
&= \frac{e^{it/2}}{e^{it/2}}\frac{e^{i(n+1/2)t}-e^{-i(n+1/2)t}}{e^{it/2}-e^{-it/2}} \\
&= \frac{\sin((n+1/2)t)}{\sin(t/2)}
\end{aligned}$$

- *Sinus cardinal.* Soit $n \geq 1$. Alors :

$$\int_{(n-1)\pi}^{n\pi}|\mathrm{sinc}(t)|dt \geq \frac{1}{n\pi}\int_{(n-1)\pi}^{n\pi}|\sin(t)|dt \text{ car } t \leq n\pi$$

  Or par périodicité :

$$\int_{(n-1)\pi}^{n\pi}|\sin(t)|dt = \int_0^{\pi}|\sin(t)|dt = \int_0^{\pi}\sin(t)dt = -(\cos(\pi)-\cos(0)) = 2$$

  D'où :

$$\int_0^{n\pi}|\mathrm{sinc}(t)|dt \geq \frac{2}{\pi}\sum_{k=1}^{n}\frac{1}{k}$$

  Et donc $\int_{\mathbb{R}_+}|\mathrm{sinc}|$ diverge.

2.16 Théorème de Bernstein

Référence :

- [QZ07] p. 518–519

Proposition 2.20 (Bernstein)
Soit $f \in \mathcal{C}^0([0,1],\mathbb{C})$.
On pose $\omega : (h \in [0,1]) \mapsto \sup\{|f(u)-f(v)| \mid |u-v| \leq h\}$.
Pour $n \geq 1$ on définit le n–ième polynôme de Bernstein de f :

$$B_n(f) : x \mapsto \sum_{k=0}^{n} C_n^k x^k (1-x)^{n-k} f\left(\frac{k}{n}\right)$$

Alors :

(*i*) *il existe* $C > 0$ *tel que* $\forall n \geq 1$, $\|f - B_n(f)\|_\infty \leq C\omega\left(\frac{1}{\sqrt{n}}\right)$ *; en particulier* $(Bn(f))_n$ *converge uniformément vers* f *sur* $[0,1]$ *;*

(*ii*) *l'inégalité précédente est optimale : il existe* $f \in \mathcal{C}^0([0,1],\mathbb{C})$ *lipschitzienne et* $\delta > 0$ *tels que* $\forall n \geq 1$, $\|f - B_n(f)\|_\infty \geq \frac{\delta}{\sqrt{n}}$.

Démonstration :

(*i*) Soit $x \in [0,1]$. On peut montrer (cf. infra) que pour tous $\lambda, h \geq 0$ tels que $\lambda h \in [0,1]$ on a $\omega(\lambda h) \leq (\lambda+1)\omega(h)$. De fait, si on se donne $(X_n)_{n\geq 1}$ une suite de variables de Bernoulli i.i.d de paramètre x et si on note pour $n \geq 1$ $S_n := \sum_{k=1}^n X_k$ on a :

$$\omega\left(\left|x - \frac{S_n}{n}\right|\right) \leq \left(\sqrt{n}\left|x - \frac{S_n}{n}\right| + 1\right)\omega\left(\frac{1}{\sqrt{n}}\right)$$

Remarquons ensuite que l'on a $\mathbb{E}(f(x)) = f(x)$ et que pour tout $n \geq 1$ $\mathbb{E}\left(f\left(\frac{S_n}{n}\right)\right) = B_n(f)(x)$ d'où :

$$\begin{aligned}
|f(x) - B_n(f)(x)| &= \left|\mathbb{E}\left(f(x) - f\left(\frac{S_n}{n}\right)\right)\right| \\
&\leq \mathbb{E}\left(\left|f(x) - f\left(\frac{S_n}{n}\right)\right|\right) \\
&\leq \mathbb{E}\left(\omega\left(\left|x - \frac{S_n}{n}\right|\right)\right) \\
&\leq \omega\left(\frac{1}{\sqrt{n}}\right)\mathbb{E}\left(\sqrt{n}\left|x - \frac{S_n}{n}\right| + 1\right)
\end{aligned}$$

Or :

$$\begin{aligned}
\mathbb{E}\left(\sqrt{n}\left|x - \frac{S_n}{n}\right| + 1\right) &= 1 + \sqrt{n}\mathbb{E}\left(\left|x - \frac{S_n}{n}\right|\right) \\
&\leq 1 + \sqrt{n}\left\|x - \frac{S_n}{n}\right\|_2 \quad \text{par inégalité de Hölder, où } \|X\|_2 = \sqrt{\mathbb{E}(|f|^2)}
\end{aligned}$$

De plus :

$$\begin{aligned}
\mathbb{E}\left(\left|x - \frac{S_n}{n}\right|^2\right) &= x^2 - 2\frac{x}{n}\mathbb{E}(S_n) + \frac{1}{n^2}\mathbb{E}(S_n^2) \\
&= x^2 - 2x^2 + \frac{1}{n^2}\left(\sum_{1\leq i\neq j\leq n}\mathbb{E}(X_i)\mathbb{E}(X_j) + \sum_{i=1}^n \mathbb{E}(X_i^2)\right) \\
&= -x^2 + \frac{n^2-n}{n^2}x^2 + \frac{1}{n^2}\sum_{i=1}^n x \\
&= \frac{x(1-x)}{n}
\end{aligned}$$

Ergo :

$$\mathbb{E}\left(\sqrt{n}\left|x - \frac{S_n}{n}\right| + 1\right) \leq 1 + \sqrt{n}\sqrt{\frac{x(1-x)}{n}} \leq \frac{3}{2}$$

Finalement :

$$\|f - B_n(f)\|_\infty \leq \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right)$$

(*ii*) On pose $f : x \mapsto \left|x - \frac{1}{2}\right|$. Alors, pour tous $u, v \in [0,1]$ on a $|f(u) - f(v)| \leq |u - v|$: f est 1–lipschitzienne et donc $\omega(h) \leq h$.

Cependant, si $n \geq 1$:

$$\begin{aligned}
\|f - B_n(f)\|_\infty &\geq \left| f\left(\frac{1}{2}\right) - B_n(f)\left(\frac{1}{2}\right) \right| \\
&= \left| B_n(f)\left(\frac{1}{2}\right) \right) \\
&= \mathbb{E}\left(\left| \frac{S_n}{n} - \frac{1}{2} \right| \right) \text{ où l'on prend les } X_n \text{ de paramètre } \frac{1}{2} \\
&= \frac{1}{2n}\mathbb{E}(|2S_n - n|) \\
&= \frac{1}{2n}\mathbb{E}\left(\sum_{j=1}^n \varepsilon_j \right) \text{ où les } \varepsilon_j := 2X_j - 1 \text{ sont des variables de Rademacher i.i.d} \\
&\geq \frac{1}{2n\sqrt{e}} \left\| \sum_{j=1}^n \varepsilon_j \right\|_2 \text{ par inégalité de Khintchine}
\end{aligned}$$

Or :

$$\begin{aligned}
\mathbb{E}\left(\left(\sum_{j=1}^n \varepsilon_j \right)^2 \right) &= \left(\sum_{1 \leq i \neq j \leq n} \mathbb{E}(\varepsilon_i)\mathbb{E}(\varepsilon_j) + \sum_{i=1}^n \mathbb{E}(varepsilon_i^2) \right) \\
&= 0 + \sum_{i=1}^n 1
\end{aligned}$$

D'où :

$$\|f - B_n(f)\|_\infty \geq \frac{1}{2\sqrt{n}\sqrt{e}} \geq \frac{1}{2\sqrt{e}}\omega\left(\frac{1}{\sqrt{n}}\right)$$

D'où le résultat.

Détails supplémentaires :

- Soit $\lambda, h \geq 0$ tels que $\lambda h \in [0,1]$; montrons que $\omega(\lambda h) \leq (\lambda+1)\omega(h)$. Il est clair que ω est croissante et que pour tous h, k on a $\omega(h+k) \leq \omega(h) + \omega(k)$ donc par récurrence pour tout $k \in \mathbb{N}$ on a $\omega(kh) \leq k\omega(h)$. Si on pose $k := \lceil \lambda \rceil$ on a donc $\omega(\lambda h) \leq \omega(kh) \leq k\omega(h) \leq (\lambda+1)\omega(h)$.
- On trouve le résultat suivant dans [QZ07], p. 248 :

Proposition 2.21 (Khintchine)
Soit $r_1, \ldots, r_n$ des variables i.i.d de Rademacher (i.e valant ± 1 avec probabilité $\frac{1}{2}$).
Soit $f \in \langle r_1, \ldots, r_n \rangle_{\mathbb{R}}$.
Alors :

$$\|f\|_2 \leq \sqrt{e}\mathbb{E}(|f|)$$

Démonstration : On a alors $f = \sum_j a_j r_j$ et on peut supposer $\sum_j a_j^2 = \|f\|_2 = 1$. On pose :

$$g := \prod_{j=1}^n (1 + i a_j r_j)$$

Alors pour presque tout x :

$$\begin{aligned}
|g(x)| &= \prod_{j=1}^n \sqrt{1 + a_j^2 r_j^2(x)} \\
&= \prod_{j=1}^n \sqrt{1 + a_j^2} \text{ par Pythagore appliqué aux } r_j \\
&\leq \prod_{j=1}^n \sqrt{e^{a_j^2}} \\
&= \sqrt{e}
\end{aligned}$$

De fait $\|g\|_\infty \leq \sqrt{e}$. De plus pour $j \in [n]$ on a :

$$\begin{aligned}
\mathbb{E}(r_j g) &= \mathbb{E}\left(r_j(1+ia_jr_j)\prod_{k\neq j}(1+ia_kr_k)\right) \\
&= \mathbb{E}(r_j(1+ia_jr_j))\mathbb{E}\left(\prod_{k\neq j}(1+ia_kr_k)\right) \\
&= ia_j \prod_{k\neq j}\mathbb{E}\left(1+ia_kr_k\right)
\end{aligned}$$

car $\mathbb{E}(r_j)=0$ et $\mathbb{E}(r_j^2)=1=ia_j$

Or $\mathbb{E}(fg)=\sum_j a_j\mathbb{E}(r_jg)$ d'où $|\mathbb{E}(fg)|=1$. On conclut en remarquant que :

$$\mathbb{E}(|f|) \geq \frac{|\mathbb{E}(fg)|}{\|g\|_\infty}$$

2.17 Théorème de Brouwer en dimension 2

Références :
- [Rou09], p. 175 – 178 et/ou [GT96] p. 23–24

Prérequis :
- homotopie dans le plan complexe.

Proposition 2.22 (Brouwer)
Soit $\mathcal{B}$ la boule unité fermée de $\mathbb{R}^2$.
Alors toute application continue de $\mathcal{B}$ dans elle–même admet un point fixe.

Démonstration : Soit $F \in \mathcal{C}^0(\mathcal{B},\mathcal{B})$. Supposons que F n'admet aucun point fixe. Pour $x \in B$ on peut alors noter $G(x)$ le point d'intersection entre la demi–droite d'origine $F(x)$ passant par x et la sphère $\mathbb{S}^1$.

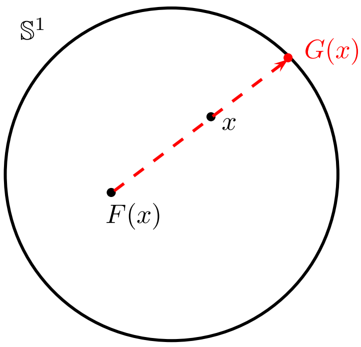


Figure 2.3 – Construction de la fonction G.

Fixons $x \in \mathcal{B}$. Le point $G(x) \in \mathbb{S}^1$ est alors caractérisée par le système d'équation suivant, d'inconnue $\lambda > 0$:

$$\begin{cases} G(x)-F(x)=\lambda(x-F(x)) \\ \|G(x)\|^2 = 1 \end{cases}$$

Ce système est équivalent à l'équation suivante :

$$\|\lambda(x-F(x))+F(x)\|^2-1=0 \tag{2.17.1}$$

Ce qui peut se réécrire – en développant – de la façon suivante :

$$P_x(\lambda)=0 \text{ avec } P_x = \|x-F(x)\|^2X^2+2\langle x-F(x),F(x)\rangle X+\|F(x)\|^2-1 \tag{2.17.2}$$

Remarquons que :

- $P_x(0) = \|F(x)\|^2 - 1 \leq 0$ car $F(x) \in \mathcal{B}$;
- $P_x(1) = \|x\|^2 - 1 \leq 0$ car $x \in \mathcal{B}$;
- $P_x(\lambda) \xrightarrow[n\to\pm\infty]{} \infty$.

De fait le polynôme du second degré P_x admet deux racines, l'une négative ou nulle et la seconde supérieure ou égale à un. Ces deux racines sont distinctes donc le discriminant de P_x est nécessairement strictement positif, i.e :

$$\Delta(x) := 4\langle x - F(x), F(x)\rangle^2 + 4\|x - F(x)\|^2(1 - \|F(x)\|^2) > 0$$

Si on suppose trouvée une solution λ de (2.17.2), il s'agit alors nécessairement de la racine strictement positif de P_x, i.e de :

$$\lambda(x) := \frac{-2\langle x - F(x), F(x)\rangle + \sqrt{\Delta(x)}}{2\|x - F(x)\|^2} = \frac{-\langle x - F(x), F(x)\rangle + \sqrt{\langle x - F(x), F(x)\rangle^2 + \|x - F(x)\|^2(1 - \|F(x)\|^2}}{\|x - F(x)\|^2}$$

Réciproquement on vérifie que $\lambda(x)$ est bien une solution strictement positive de (2.17.2) et donc $G(x) = \lambda(x)$. De plus si $x \in \mathbb{S}^1$, $P_x(1) = 0$ et donc $\lambda(x) = 1$ et comme $x \mapsto \lambda(x)$ est continue G l'est : on a construit une rétraction [17] de $\mathcal{B}$ sur $\mathbb{S}^1$.

✍ **Méthode 1 : par homotopie.**

Fixons à présent $s \in [0,1]$ et paramétrons le cercle de centre 0 et de rayon s par l'application suivante :

$$\begin{aligned} x_s : [0,1] &\to \mathcal{B} \\ t &\mapsto (s\cos(2\pi t), s\sin(2\pi t)) \end{aligned}$$

On peut alors définir un lacet [18] γ_s de $\mathcal{B}$ via $\gamma_s : t \mapsto G \circ x_s(t)$. En particulier, γ_0 est le lacet trivial en $G(0)$ et γ_1 parcoure $\mathbb{S}^1$ une fois dans le sens direct, i.e [19] $\forall t \in [0,1]$, $\gamma_1(t) = e^{2i\pi t}$. Alors :

$$\mathrm{Ind}_{\gamma_0}(0) := \frac{1}{2i\pi}\int_{\gamma_0}\frac{dz}{z} = \frac{1}{2i\pi}\int_0^1 \frac{\gamma_0'(t)}{\gamma_0(t)}dt = 0$$

Et :

$$\mathrm{Ind}_{\gamma_1}(0) := \frac{1}{2i\pi}\int_{\gamma_1}\frac{dz}{z} = \frac{1}{2i\pi}\int_0^1 \frac{2i\pi e^{2i\pi t}}{e^{2i\pi t}}dt = 1$$

On considère à présent l'application suivante :

$$\begin{aligned} \gamma : [0,1]\times[0,1] &\to \mathcal{B} \\ (s,t) &\mapsto \gamma_s(t) = G \circ x_s(t) \end{aligned}$$

Comme $G(0) \neq 0$ (car $0 \notin \mathbb{S}^1$), cette application est en fait à valeurs dans $\mathcal{B}\setminus\{0\}$, et transforme continûment γ_0 en γ_1 (car $s \mapsto x_s$ est continue) : ces deux lacets sont donc homotopes dans $\mathbb{C}\setminus\{0\}$ et donc $\mathrm{Ind}_{\gamma_0}(0) = \mathrm{Ind}_{\gamma_0}(1)$, ce qui est absurde. On en déduit qu'il ne peut exister de rétraction de $\mathcal{B}$ sur $\mathbb{S}^1$ et donc que F admet un point fixe.

✍ **Méthode 2 : autrement.**

On se base sur le résultat suivant :

Lemme 2.3
Soit K un compact étoilé *non vide de $\mathbb{C}$.*
On désigne par C_K (resp. E_K) le groupe multiplicatif $\mathcal{C}^0(K,\mathbb{C}^*)$ (resp. $\{e^g \mid g \in \mathcal{C}^0(K,\mathbb{C})\}$).
Alors $C_K = E_K$.

DÉMONSTRATION : On va montrer que E_K est la composante connexe de $x \mapsto 1$ dans $(C_K, \|.\|_\infty)$.

- Il est clair que $x \mapsto 1 = e^0$ est dans E_K.

17. I.e une application de $\mathcal{B}$ sur $\mathbb{S}^1$ induisant l'identité sur $\mathbb{S}^1$. Vous peinez à visualiser un truc pareil ? C'est normal, cela n'existe pas.
18. I.e un chemin continu fermé.
19. Si vous me pardonnez l'identification $\mathbb{R}^2 \cong \mathbb{C}$.

- Soit $f = e^g \in E_K$ et soit $\tilde{f} \in C_K$ telle que $\|\tilde{f} - f\|_\infty < \inf_K |f|$. Alors $\left\|\frac{\tilde{f}-f}{f}\right\|_\infty \leq \|\tilde{f}-f\|_\infty \times \frac{1}{\inf_K |f|} < 1$ i.e $\left\|\frac{\tilde{f}}{f} - 1\right\|_\infty < 1$ donc $\frac{\tilde{f}}{f}$ est à valeurs dans $\mathbb{C} \setminus \mathbb{R}_-$. On peut donc poser $h := L\left(\frac{\tilde{f}}{f}\right)$ (où L dénote la représentation principale du logarithme sur $\mathbb{C} \setminus \mathbb{R}_-$) et avoir $\frac{\tilde{f}}{f} = e^h$. De fait, $\tilde{f} = e^{g+h} \in E_K$: E_K est donc ouvert dans $(C_K, \|.\|_\infty)$.
- E_K est fermé car si G est un groupe topologique et que $H \leq G$ est ouvert, alors G/H est ouvert en tant que réunion de classes d'équivalence homéomorphes à H (prendre $G = C_K$ et $H = E_K$).
- E_K est connexe (par arcs) car si $f = e^g \in E_K$ alors $\gamma : (t \in [0,1]) \mapsto e^{tg}$ relie $x \mapsto 1$ à f dans E_K.

E_K est donc bien la composante connexe de $x \mapsto 1$ dans $(C_K, \|.\|_\infty)$. Quitte à homéomorpher tout ça, on peut supposer K étoilé par rapport à 0. Il est clair que $E_K \subset C_K$; fixons $f \in C_K$. Alors pour $t \in [0,1]$ l'application $z \mapsto f(tz)$ appartient à C_K et donc $t \mapsto f_t$ relie f à $z \mapsto f(0)$ dans C_K. Or $\mathbb{C}^*$ est connexe par arcs donc on peut y relier $f(0)$ à 1 ergo on peut relier f à $x \mapsto 1$ dans C_K d'où $f \in E_K$.

Revenons nous en à nos moutons (topologiques) : on a construit une rétraction G de $\mathcal{B}$ sur Ss^1. Comme G ne s'annule pas sur le compact[20] $\mathcal{B}$, $G \in C_{\mathcal{B}} = E_{\mathcal{B}}$ ergo il existe g continue telle que $G = e^g$. De plus, pour $z \in \mathbb{S}^1$ on a $-1 = \frac{G(z)}{G(-z)} = e^{g(z)-g(-z)}$. De fait, il existe $k(z) \in \mathbb{Z}$ tel que $g(z) - g(-z) = i\pi(2k(z)+1)$. k étant une application continue du connexe $\mathbb{S}^1$ à valeurs dans $\mathbb{Z}$ elle est constante donc $g - g(-.)$ l'est également. Or en tout $z \neq \pm 1$ on a $g(z) - g(-z) = L(G(z)) - L(G(-z)) = L(z) - L(-z)$ donc $g - g(-.)$ y est impaire, donc nulle car constante. Or $G \neq 1$ d'où la contradiction voulue.

On en déduit qu'il ne peut exister de rétraction de $\mathcal{B}$ sur $\mathbb{S}^1$ et donc que F admet un point fixe.

Détails supplémentaires :

- Une équivalence d'homotopie entre deux lacets κ et η partant d'un même point $x_0 \in \mathbb{C}$ — i.e vérifiant $\kappa(0) = \eta(0) = x_0$ — est[21] une application $f : [0,1]^2 \to \mathbb{C}$ telle que :
  (i) $f(0,.) = \kappa$ et $f(1,.) = \eta$;
  (ii) $\forall t \in [0,1]$, $f(.,t)$ est continue ;
  (iii) $\forall s \in [0,1]$, $f(s,.)$ est un lacet partant de x_0.

  Dans le cas de notre application γ, (i) et (ii) sont évidents et (iii) découle du fait que $\forall s \in [0,1]$, $\gamma_s(0) = G(x_s(0)) = G(0)$.

2.18 Théorème de Cauchy–Lipschitz global

Référence :
- [Rou09], p. 180–184

Proposition 2.23 (Cauchy–Lipschitz global)
Soit $m \geq 1$ et soit $\|.\|$ une norme sur $\mathbb{R}^m$.
Soit I un intervalle de $\mathbb{R}$.
Soit $f \in \mathcal{C}^0(I \times \mathbb{R}^m, \mathbb{R})$ globalement lipschitzienne selon la seconde variable, i.e :

$$\forall K \subset\subset I,\ \exists k > 0,\ \forall t \in I,\ \forall y, z \in \mathbb{R}^m, \quad \|f(t,y) - f(t,z)\| \leq k\|y - z\|$$

Soient $x \in \mathbb{R}^m$ et $t_0 \in I$.
On considère le problème de Cauchy suivant :

$$\left\{ \begin{array}{l} y' = f(.,y) \\ y(t_0) = x \end{array} \right. , \text{ d'inconnue } y \in E := \mathcal{C}^0(I, \mathbb{R}^m) \tag{2.18.1}$$

20. Saint Riesz, priez pour nous.
21. On se place ici dans le cas particulier du plan complexe. La définition se généralise très facilement à tout espace topologique.

Alors le problème (2.18.1) admet une unique solution globale.

DÉMONSTRATION : Pour $y \in E$ et $t \in I$ on pose :

$$F(y)(t) := x + \int_{t_0}^{t} f(s, y(s))ds$$

Remarquons que y est solution (globale) de (2.18.1) si et seulement si y est dérivable sur I et vérifie $y' = f(., y)$ et $y(t_0) = x$. Comme f est continue, y est alors nécessairement $\mathcal{C}^1$ et vérifie :

$$\forall t \in I, \qquad y(t) = x + \int_{t_0}^{t} f(s, y(s))ds = F(y)(t) \tag{2.18.2}$$

Réciproquement, si y est solution de (2.18.2) elle est dérivable et est solution de (2.18.1). On a donc ramené notre problème de Cauchy à une recherche de point fixe pour F sur E.

Commençons par supposer I compact. Soit alors k la constante de Lipschitz associée au compact I et soit $\ell := \sup(I) - \inf(I)$ la longueur de I. On munit E de la norme suivante :

$$\|.\|_k : y \mapsto \max_{t\in I}(e^{-k|t-t_0|}\|y(t)\|) = \|e^{-k|.-t_0|}y\|_\infty$$

On a alors :

$$\forall y \in E, \quad e^{-k\ell}\|y\|_\infty \leq \|y\|_k \leq \|y\|_\infty$$

De fait $\|.\|_k$ est équivalente $\|.\|_\infty$ sur E. En particulier, $(E, \|.\|_k)$ est un espace de Banach. De plus, comme F est continue l'application F envoie bien E sur lui–même. Également :

$$\forall y, z \in E, \forall t \leq t_0, \qquad F(y)(t) - F(z)(t) = \int_{t_0}^{t} f(s, y(s)) - f(s, z(s))ds$$

D'où :

$$\begin{aligned}
\forall y, z \in E, \forall t \leq t_0, \qquad e^{-k(t-t_0)}\|F(y)(t) - F(z)(t)\| &\leq e^{-k(t-t_0)} \int_{t_0}^{t} \|f(s, y(s)) - f(s, z(s))\|ds \\
&\leq e^{-k(t-t_0)} \int_{t_0}^{t} k\|y(s) - z(s)\|ds \\
&= e^{-k(t-t_0)} \int_{t_0}^{t} ke^{k(s-t_0)}(e^{-k(s-t_0)}\|y(s) - z(s)\|)ds \\
&\leq e^{-k(t-t_0)} \int_{t_0}^{t} ke^{k(s-t_0)}\|y - z\|_k ds \\
&= e^{-k(t-t_0)}\|y - z\|_k(e^{k(t-t_0)} - 1) \\
&= (1 - e^{-k(t-t_0)})\|y - z\|_k
\end{aligned}$$

On obtient exactement le même résultat pour $t \leq t_0$ en remplaçant $e^{-k(t-t_0)}$ par $e^{-k(t_0-t)}$, d'où :

$$\forall y, z \in E, \forall t \in I, \qquad e^{-k|t-t_0|}\|F(y)(t) - F(z)(t)\| \leq (1 - e^{-k|t-t_0|})\|y - z\|_k \leq (1 - e^{-k\ell})\|y - z\|_k$$

D'où, en "passant au max[22]" en t :

$$\forall y, z \in E, \qquad \|F(y) - F(z)\|_k \leq (1 - e^{-k\ell})\|y - z\|_k$$

F est donc contractante $(0 < 1 - e^{-k\ell} < 1)$ donc, par théorème du point fixe de Picard, admet un unique point fixe, ce qui résout notre problème.

Si on ne suppose plus I compact, on peut trouver une suite croissante d'intervalles compacts I_j, $j \in \mathbb{N}$ tels que :

$$I = \bigcup_{j\in\mathbb{N}} I_j \text{ et } \forall j \in \mathbb{N},\ t_0 \in I_j$$

Pour $j \in \mathbb{N}$ on note y_j la (cf. supra) solution de (2.18.1) sur I_j. Alors si y est solution de (2.18.1) sur I, par unicité sur les I_j on a nécessairement $y_{|I_j} = y_j$. Inversement, toujours par unicité sur les I_j, on peut "recoller" les y_j, i.e l'application $y : (t \in I_j) \mapsto y_j(t)$ est bien définie et dérivable. Elle est également solution de (2.18.1) sur I par exhaustivité de $(I_j)_j$ dans I, d'où le résultat.

22. À consommer avec modération.

Détails supplémentaires :

- Une $f : \mathbb{R}^m \to \mathbb{R}^m$ linéaire continue vérifie les hypothèses de ce théorème quitte à l'identifier à $(t, y) \mapsto f(y)$. On a alors une constante de Lipschitz "globale en t", à savoir la norme subordonnée (à $\|.\|$) de f :

$$\forall t \in I, \forall y, z \in \mathbb{R}^m, \quad \|f(t,y) - f(t,z)\| \leq \|f\| \|y - z\|$$

- Rappelons le résultat suivant :

Proposition 2.24 (Picard)
Soit E un espace de Banach.
Soit F un evn.
Soit A un fermé de E.
Soit $f \in \mathcal{C}(A, F)$ contractante, i.e telle que :

$$\exists 0 < k < 1, \forall x, y \in A, \quad \|f(x) - f(y)\| \leq k\|x - y|$$

Alors f admet un unique point fixe.
Démonstration : L'unicité est claire : en effet, si x et y sont deux points fixes distincts de f on a :

$$\|x - y\| = \|f(x) - f(y)\| \leq k\|x - y\| < \|x - y\|$$

D'où contradiction.
Pour démontrer l'existence, commençons par fixer $x_0 \in A$. Pour $n \geq 0$ on pose $x_{n+1} = f(x_n)$. Alors :

$$\begin{aligned}\forall n \in \mathbb{N}^*, \quad \|x_{n+1} - x_n\| &= \|f(x_n) - f(x_{n-1})\| \\ &\leq k\|x_n - x_{n-1}\| \\ &\vdots \quad \text{(par récurrence)} \\ &\leq k^n \|x_1 - x_0\|\end{aligned}$$

De fait :

$$\begin{aligned}\forall n, p \in \mathbb{N}, \quad \|x_{n+p} - x_n\| &= \left\| x_{n+p} - \sum_{i=1}^{p-1} x_{n+i} + \sum_{i=1}^{p-1} x_{n+i} - x_n \right\| \\ &\leq \sum_{i=0}^{p-1} \|x_{n+i+1} - x_{n+i}\| \\ &\leq \sum_{i=0}^{p-1} k^{n+i} \|x_1 - x_0\| \\ &= k^n \|x_1 - x_0\| \sum_{k=0}^{p-1} k^i \\ &\leq k^n \|x_1 - x_0\| \sum_{k=0}^{+\infty} k^i \text{ la série } \sum k^i \text{ convergeant car } 0 < k < 1 \\ &= \frac{k^n}{1-k} \|x_1 - x_0\| \\ &\xrightarrow[n \to \infty]{} 0\end{aligned}$$

La dernière majoration étant indépendante de p, la suite $(x_n)_n$ est de Cauchy dans l'espace complet [23] A donc y converge vers un certain $x \in A$. En passant à la limite (par continuité – séquentielle – de f) dans la relation $x_{n+1} = f(x_n)$ on obtient que x est un point fixe de f d'où le résultat.

23. Car fermé dans le complet E.

2.19 Théorème de Fischer–Riesz

Référence :
- [Bre05], p. 57–58

Proposition 2.25 (Fischer–Riesz)
Soit Ω *un ouvert de* $\mathbb{R}^d$, $d \geq 1$.
Soit $p \in [1, \infty]$.
Alors :

(i) $L^p(\Omega)$ *est un espace de Banach ;*

(ii) de toute suite convergente dans $L^p(\Omega)$ *on peut extraire une suite convergeant presque partout sur* Ω.

Démonstration :
- *Cas* $p = \infty$. Soit $(f_n)_n$ une suite de Cauchy dans $L^\infty(\Omega)$. Alors $\forall k \geq 1$, $\exists N_k \geq 0$ tel que :
$$\forall n \geq N_k,\ \forall q \geq 0,\ \|f_{n+q} - f_n\|_\infty \leq \frac{1}{k}$$
De fait il existe un ensemble négligeable $E_k \subset \Omega$ tel que :
$$\forall n \geq N_k,\ \forall q \geq 0,\ \forall x \notin E_k,\ |f_{n+q}(x) - f_n(x)| \leq \frac{1}{k} \tag{2.19.1}$$
Ainsi, pour tout x n'appartenant pas à l'ensemble négligeable $E := \cup_k E_k$, la suite $(f_n(x))_n$ est de Cauchy dans $\mathbb{R}$ donc converge vers un réel $f(x)$. De plus, en faisant tendre q vers l'infini dans (2.19.1) on obtient :
$$\forall x \notin E,\ \forall n \geq N_k,\ |f(x) - f_n(x)| \leq \frac{1}{k}$$
De fait, la fonction f ainsi définie[24] est dans L^∞ (ce qui prouve le point (ii) étant donné que toute suite convergente est de Cauchy) et $\forall n \geq N_k$, $\|f_n - f\|_\infty \leq \frac{1}{k}$, ce qui signifie que $f_n \xrightarrow[n\to\infty]{L^\infty} f$, ce qui prouve le point (i).
- *Cas* $p < \infty$. Soit $(f_n)_n$ une suite de Cauchy dans L^p. Comme toute de suite de Cauchy admettant une valeur d'adhérence converge, il nous suffit d'extraire de cette dernière une suite convergente pour prouver le point (i). Commençons par remarquer que :
$$\exists \varphi : \mathbb{N} \to \mathbb{N} \text{ strictement croissante telle que } \forall n \geq 1,\ \|f_{\varphi(n+1)} - f_{\varphi(n)}\|_p \leq \frac{1}{2^n} \tag{2.19.2}$$
On pose ensuite, pour $n \geq 0$:
$$g_n : x \mapsto \sum_{k=1}^{n} |f_{\varphi(k+1)}(x) - f_{\varphi(k)}(x)|$$
Alors $g_n \in L^p(\Omega)$ (comme somme de fonctions L^p) et par inégalité triangulaire :
$$\|g_n\|_p \leq \sum_{k=1}^{n} \|f_{\varphi(k+1)} - f_{\varphi(k)}\|_p \leq \sum_{k=1}^{n} \frac{1}{2^k} \leq \sum_{k=1}^{\infty} \frac{1}{2^k} = 1$$
De fait la suite de fonctions $(g_n)_n$ est croissante et bornée en norme L^p donc par théorème de Beppo–Levi, il existe $g \in L^p(\Omega)$ tel que $g_n \xrightarrow[n\to\infty]{} g$ presque partout. Ainsi, pour presque tout $x \in \Omega$ on a :
$$\begin{aligned}\forall n \geq 2, \forall q \geq 0,\ |f_{\varphi(n+q)}(x) - f_{\varphi(n)}(x)| &= \left| f_{\varphi(n+q)}(x) - \sum_{k=1}^{q-1} f_{\varphi(n+k)}(x) + \sum_{k=1}^{q-1} f_{\varphi(n+k)}(x) - f_{\varphi(n)}(x) \right| \\ &\leq \sum_{k=1}^{q} |f_{\varphi(n+k)}(x) - f_{\varphi(n+k-1)}(x)| \\ &= g_{n+q}(x) - g_{n-1}(x) \\ &\leq g(x) - g_{n-1}(x) \xrightarrow[n\to\infty]{} 0\end{aligned}$$

24. Comme on travaille dans un espace L on peut (doit !) se contenter de la définir presque partout.

Ainsi (la majoration étant indépendante de q) la suite $(f_\varphi(n))_x$ est de Cauchy dans $\mathbb{R}$ donc converge vers un réel $f(x)$. Comme pour presque tout $x \in \Omega$ on a $|f(x) - f_\varphi(n)(x)| \leq g(x)$ $(n \geq 2)$ la fonction f ainsi définie est bien dans L^p, ce qui au passage prouve le point (ii) car toute suite convergente est de Cauchy.
In fine les $f_{\varphi(n)}$ sont dans L^p, convergent presque partout vers $f \in L^p$ et subissent l'intenable domination $|f_{\varphi(n)(x)}| \leq |f(x)| + |g(x)|$ (avec $|f| + |g| \in L^p$) presque partout. Vous l'aurez deviné, notre salut va provenir du théorème de convergence dominée qui nous permet de conclure que $f_{\varphi(n)} \xrightarrow[n\to\infty]{L^p} f$.
La suite de Cauchy $(f_n)_n$ admet donc une valeur d'adhérence f dans $L^p(\Omega)$ donc converge vers cette dernière, ce qui prouve le point (i) et achève le théorème (tout du moins sa preuve).

Détails supplémentaires :

- On peut ajouter au point (ii) que la sous–suite en question est dominée par $h \in L^p$. En effet, il suffit de poser $h = |f| + |g|$ (dans le cas $p < \infty$) ou $h = 1 + |f|$ (dans le cas $p = \infty$).
- *Démonstration du point* (2.19.2). Construisons φ par récurrence. Comme $(f_n)_n$ est de Cauchy, il existe $N_1 \geq 0$ tel que :

$$\forall n \geq N_1,\ \forall q \geq 0,\ \|f_{n+q} - f_n\|_p \leq \frac{1}{2}$$

On pose $\varphi(1) := N_1$.
Supposons à présent φ construite jusqu'au rang $n \geq 1$. Alors, toujours comme $(f_n)_n$ est de Cauchy, il existe N_{n+1} tel que :

$$\forall n \geq N_{n+1},\ \forall q \geq 0,\ \|f_{n+q} - f_n\|_p \leq \frac{1}{2^{n+1}}$$

Quitte à aller un peu plus loin que prévu, on peut supposer $N_{n+1} > \varphi(n)$ et il nous suffit alors de poser $\varphi(n+1) := N_{n+1}$ pour conclure.

2.20 Théorème de Montel

Références :

- [Rud98], p. 329 et [QZ95], p. 157

Prérequis :

- théorème d'Ascoli ;
- formule de Cauchy.

Proposition 2.26 (Montel)
Soit Ω un ouvert de $\mathbb{C}$.
Soit $\mathcal{F} \subset \mathcal{H}(\Omega)$ une famille uniformément bornée sur tout compact (de $\mathbb{C}$) inclus dans Ω, i.e :

$$\forall K \subset\subset \Omega,\ \exists M(K) > 0,\ \forall f \in \mathcal{F},\ \forall z \in K, \quad |f(z)| \leq M(K)$$

Alors de toute suite d'éléments de $\mathcal{F}$ on peut extraire une suite convergeant uniformément sur tout compact inclus dans Ω.

Démonstration : Soit $(K_n)_n$ une suite de compacts inclus dans Ω tels que (cf. infra) :

$$\Omega = \bigcup_{n=0}^{\infty} K_n \text{ et } \forall n \geq 0,\ K_n \subset \overset{\circ}{K}_{n+1}$$

De par cette dernière relation, on peut trouver une suite $(\delta_n)_n \in \mathbb{R}_+^{\mathbb{N}}$ telle que :

$$\forall n \geq 0,\ \forall z \in K_n,\ \mathcal{B}(z, 2\delta_n) \subset K_{n+1}$$

Soit $n \in \mathbb{N}$ et soient $x, y \in K_n$ tels que $|x - y| < \delta_n$. Si on note γ le cercle de centre x et de rayon $2\delta_n$ orienté positivement, alors par formule de Cauchy :

$$\begin{aligned} f(x) - f(y) &= \frac{1}{2i\pi} \int_\gamma f(\xi) \left(\frac{1}{\xi - x} - \frac{1}{\xi - y} \right) d\xi \\ &= \frac{x - y}{2i\pi} \int_\gamma \frac{f(\xi)}{(\xi - x)(\xi - y)} d\xi \end{aligned}$$

Pour tout ξ dans l'image de γ, $|\xi - x| = 2\delta_n$ et $|\xi - y| > \delta_n$. Ainsi :

$$\forall f \in \mathcal{F}, \forall x, y \in K_n \text{ tels que } |x-y| < \delta_n, \quad |f(x) - f(y)| \leq \frac{M(K_{n+1}}{\delta_n}|x-y|$$

Donc $\mathcal{F}_n := \{f_{|K_n} \,|\, f \in \mathcal{F}\}$ est équicontinue et uniformément bornée donc par théorème d'Ascoli relativement compacte dans $\mathcal{C}(K_n)$. De fait, de toute suite $(f_k)_k \in \mathcal{F}_n^{\mathbb{N}} \subset \overline{\mathcal{F}_n}^{\mathbb{N}}$ on peut extraire une suite convergeant uniformément sur K_n. Un procédé d'extraction diagonale permet alors de conclure. En effet, on fabrique ainsi une extraction $(f_{\varphi_1 \circ \ldots \circ \varphi_k(k)})_k$ convergeant sur tous les K_n et si K est un compact inclus dans Ω, $K \subset \cup_n \overset{\circ}{K}_n$. Cette dernière expression formant un recouvrement ouvert du compact K on peut extraire un recouvrement fini ce qui signifie par croissance de $(\overset{\circ}{K}_n)_n$ qu'il existe n tel que $K \subset \overset{\circ}{K}_n \subset K_n$, d'où le résultat.

Corollaire 2.26.1 ([QZ95], p. 157)
Soit Ω un ouvert convexe borné de $\mathbb{C}$.
Soit $a \in \Omega$.
Soit $f \in \mathcal{H}(\Omega)$ telle que $f(a) = a$ et $|f'(a)| < 1$.
Alors on peut extraire de $(f^n)_n$ un sous–suite convergeant uniformément vers a sur tout compact inclus dans Ω (où $f^n = \underbrace{f \circ \ldots \circ f}_{n \text{ fois}}$).

DÉMONSTRATION : Soit $\lambda \in (0,1)$ et soit $r > 0$ tel que $\overline{\mathcal{B}}(a,r) \subset \Omega$ et que $\forall z \in \overline{\mathcal{B}}(a,r)$, $|f'(z)| \leq \lambda$ (tout ceci est possible par continuité de f'). Par inégalité des accroissements finis on a alors :

$$\forall z \in \overline{\mathcal{B}}(a,r), \quad |f(z) - a| \leq \lambda |z-a|$$

On montre alors par récurrence que :

$$\forall n \geq 1, \forall z \in \overline{\mathcal{B}}(a,r), \quad |f^n(z) - a| \leq \lambda^n |z-a| \leq \lambda^n r$$

De fait, $A := \{f^n \,|\, n \geq 1\}$ est uniformément bornée sur tout compact de Ω, et donc par théorème de Montel il existe une sous–suite de $(f^n)_n$ qui converge uniformément sur tout compact inclus dans Ω vers une fonction $g \in \mathcal{H}(\Omega)$ constante égale à a sur $\overline{\mathcal{B}}(a,r)$. Ω étant connexe, le théorème de prolongement analytique impose que g soit égale à a sur tout Ω, d'où le résultat.

Détails supplémentaires :
- Pour construire la suite $(K_n)_n$ on peut procéder comme suit (cf. [Rud98], p. 311) : on compactifie $\mathbb{C}$ en la sphère de Riemann $\mathbb{S}^2$ et on pose

$$\forall n \geq 0, \quad V_n := \{z \in \mathbb{C} \,|\, |z| > n\} \bigcup \bigcup_{a \notin \Omega} \mathcal{B}\left(a, \frac{1}{n}\right)$$

  On montre ensuite que $K_n := \mathbb{S}^2 \setminus V_n$ convient (on peut tenter de s'en convaincre par un dessin).

2.21 Théorème des quatre sommets

Référence :
- [FGN12], p. 335–336

Proposition 2.27 (Théorème des quatre sommets)
On considère un arc paramétré $\mathcal{C}^3$ τ–périodique, correspondant à un courbe fermée simple, défini comme suit :

$$\begin{aligned} M : \mathbb{R} &\to \mathbb{R}^2 \\ s &\mapsto (x(s), y(s)) \end{aligned}$$

On suppose que :

– le paramétrage M est normal ;
– la courbure γ de l'arc est positive.
Alors γ admet au moins 4 points critiques sur chaque période.

DÉMONSTRATION : Comme M est $\mathcal{C}^3$, sa tangente unitaire T et sa normale unitaire N sont de classe $\mathcal{C}^2$ et γ est de classe $\mathcal{C}^1$. Ces deux fonctions sont de plus τ–périodiques donc on a :

$$\int_0^\tau \gamma'(s)ds = \gamma(\tau) - \gamma(0) = 0 \tag{2.21.1}$$

Par intégration par parties on a de plus (toujours par périodicité) :

$$\begin{aligned}\int_0^\tau \gamma'(s)M(s)ds &= \underbrace{[\gamma(s)M(s)]_0^\tau}_{=0} - \int_0^\tau \gamma(s)T(s)ds \\ &= \int_0^\tau \frac{dN}{ds}(s)ds \\ &= 0\end{aligned}$$

I.e :

$$\int_0^\tau x(s)\gamma'(s)ds = \int_0^\tau y(s)\gamma'(s)ds = 0 \tag{2.21.2}$$

Comme γ est continue τ–périodique, elle admet au moins un maximum et un minimum sur chaque période en lesquels qui sont également des points critiques. On peut donc supposer que γ admet deux points critiques s_1, s_2 tels que $s_1 < s_2 < s_1 + \tau$. De plus, si γ est constante le résultat est trivial donc on peut supposer $\gamma' \neq 0$.

Supposons qu'il s'agisse des seuls points critiques de γ sur $[s_1, s_1+\tau)$. Alors par (2.21.1), γ' ne peut être de signe constant sur $[s_1, s_1+\tau)$ (car elle serait dans ce cas nulle). De fait, γ' a des signes opposés sur (s_1, s_2) et $(s_2, s_1+\tau)$. De plus, comme la courbe définie par M délimite un convexe, les ensembles $M([s_1, s_2])$ et $M([s_2, s_1+\tau])$ sont situé de part et d'autre de la droite[25] $(M(s_1)M(s_2))$ (cf. figure 2.4). Si on suppose donnée une équation $ax + by + c = 0$ de cette dernière, la fonction $f : s \mapsto (ax(s) + by(s) + c)\gamma'(s)$ doit donc être de signe constant sur $[s_1, s_1 + \tau)$. Or on sait par (2.21.1) et (2.21.2) que $\int_{s_1}^{s_1+\tau} f(s)ds = 0$,d'où $f = 0$ ce qui est absurde car alors $M((s_1, s_2))$ et $M((s_2, s_1 + \tau))$ seraient inclus dans la droite $(M(s_1)M(s_2))$ et donc l'arc tout entier le serait.

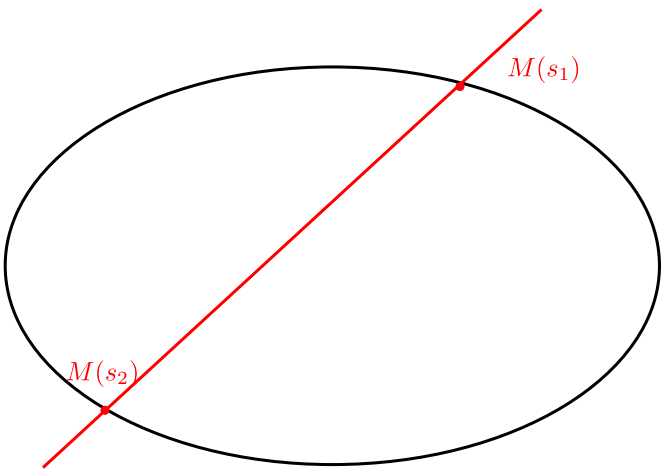


FIGURE 2.4 – Droite $(M(s_1)M(s_2))$

γ' admet donc un troisième point critique s_3 dans $[s_1, s_1 + \tau)$ et on peut supposer, quitte à remplacer (s_1, s_2) par $(s_2, s_1 + \tau)$ que l'on a $s_1 < s_3 < s_2 < s_1 + \tau$. Enfin, par symétrie, on peut

25. $M(s_1) \neq M(s_2)$ car γ est non constante.

supposer que s_1 correspond au minimum de γ et s_2 à son maximum. Si on suppose que ce sont le seuls points critiques de γ' sur $[s_1, s_1+\tau)$ alors γ' est de signe constant sur (s_1, s_3), (s_3, s_2) et $(s_2, s_1+\tau)$. De plus, par "extremalité" de s_1 et s_2 les variations de γ' sont nécessairement les suivantes :

s	s_1		s_3		s_2		$s_1+\tau$
$\gamma'(s)$	0	>0	0	>0	0	<0	

De fait γ' est positive sur (s_1, s_2) et négative sur $(s_2, s_1+\tau)$, chose impossible comme on l'a démontré précédemment. D'où le résultat.

Chapitre 3

Les inclassables

3.1 Composantes connexes des formes quadratiques non dégénérées

Référence :
- [FGN10], p. 214–215

Proposition 3.1 *Soit $(E, \|.\|)$ un $\mathbb{R}$–e.v de dimension finie $n \geq 1$.*
On munit l'ensemble $Q(E)$ de la norme $N : q \mapsto \sup \|x\| = 1|q(x)|$. Soit $\Omega(E)$ l'ensemble des formes quadratiques non dégénérées sur E.
Alors :

(i) $\Omega(E)$ est un ouvert de $Q(E)$;

(ii) pour tout $q \in Q(E)$, il existe un réel $k > 0$ tel que si $q' \in Q(E)$ et $N(q - q') < k$ alors q et q' ont même signature ;

(ii) les composantes connexes de $\Omega(E)$ sont les ensembles $\Omega_i(E)$ constitués des formes quadratiques (non dégénérées) de signature $(i, n - i)$ pour $i \in \{0, \dots n\}$.

Démonstration :

(i) une fois choisie une base de E on a un isomorphisme $Q(E) \cong S_n(\mathbb{R})$ et $\Omega(E) \cong S_n(\mathbb{R}) \cap GL_n(\mathbb{R})$ d'où le résultat.

(ii) Soit $q \in Q(E)$ de signature (r, s). Comme q est non dégénérée on a $r + s = n$, de fait si on considère une base q–orthogonale $(e_1, \dots e_r, f_1, \dots, f_s)$ convenablement ordonnée (i.e $q(e_i) = 1$ et $q(f_j) = -1$) on obtient un s–e.v $F := \langle e_1, \dots, e_r\rangle$ (resp. $G := \langle f_1, \dots, f_s\rangle$) de E tel que $q_{|_F}$ (resp. $q_{|_F}$) soit définie positive (resp. définie négative), avec en "bonus" $E = F \oplus G$. $q_{|_F}$ est définie positive donc $\sqrt{q}$ constitue une norme euclidienne sur F, qui est donc équivalente à $\|.\|$. En particulier, il existe $k_1 > 0$ tel que :

$$\forall x \in F,\ \sqrt{q}(x) \geq k_1\|x\| \text{ d'où } q(x) \geq k_1^2\|x\|^2$$

En raisonnant de même avec la norme euclidienne (sur G) $\sqrt{-q}$ on obtient l'existence de $k_2 > 0$ tel que :

$$\forall x \in G,\ q(x) \leq -k_2^2\|x\|^2$$

Si on pose $k := \min(k_1^2, k_2^2)$ on a alors :

$$\forall x \in F,\ q(x) \geq k\|x\|^2 \text{ et } \forall x \in G,\ q(x) \leq -k\|x\|^2$$

Pour tout $q' \in Q$ tel que $N(q - q') < k$ on a :

$$\forall x \neq 0,\ |q(x) - q'(x)| \leq N(q - q')\|x\|^2 < k\|x\|^2$$

Donc :

$$q(x) - q'(x) < k\|x\|^2 \text{ et } q'(x) - q(x) < k\|x\|^2$$

De fait :
- si $x \in F \setminus \{0\}$ on a :

$$q'(x) > q(x) - k\|x\|^2 \geq 0$$

– si $x \in G \setminus \{0\}$ on a :

$$q'(x) < q(x) + k\|x\|^2 \leq 0$$

Donc q' est définie positive (resp. définie négative) sur F (resp. G) donc a même signature que q.

(iii) Il est clair que les $\Omega_i(E)$ forment une partition de $\Omega(E)$. Ils sont de plus ouverts par (ii). Ils ne nous reste plus qu'à montrer qu'ils sont connexes, ce que nous traitons matriciellement ($\Omega(E)$ étant homéomorphe à $GL_n(\mathbb{R}) \cap S_n(\mathbb{R})$) : soient $A, B \in GL_n(\mathbb{R}) \cap S_n(\mathbb{R})$ de signature $(i, n-i)$. Alors, par théorème spectral il existe $P, Q \in O_n(\mathbb{R})$ telles que $A =^t PD_iP$ et $B =^t QD_iQ$ où $D_i := \text{diag}(\underbrace{1 \ldots 1}_{i}, \underbrace{-1 \ldots -1}_{n-i})$. Quitte à changer en son opposée la première ligne de P et/ou Q on peut supposer $P, Q \in GL_n^+(\mathbb{R})$ qui est connexe par arc ; donc, si γ y relier P à Q $\delta : t \mapsto^t \gamma(t)D_i\gamma(t)$ relie A à B dans $GL_n(\mathbb{R}) \cap S_n(\mathbb{R})$ d'où le résultat.

Détails supplémentaires :

– $GL_n^+(\mathbb{R})$ *est connexe par arcs.* On utilise la décomposition polaire.

3.2 Ellipsoïde de John–Loewner

Référence :

– [FGN10], p. 229–231

Proposition 3.2

Soit $K \subset\subset \mathbb{R}^n$ d'intérieur non vide.

Alors il existe un unique ellipsoïde de volume minimal contenant K.

Démonstration : On sait qu'un ellipsoïde (plein) centré en l'origine admet une équation de la forme $q(x) \leq 1$, avec $q \in Q_{++}$. De fait, on peut associer à toute forme quadratique définie positive q un ellipsoïde $\mathcal{E}_q := \{x \in \mathbb{R}^n \,|\, q(x) \leq 1\}$.

Soit donc $q \in Q_{++}$. Alors, par théorème spectral, il existe une b.o.n $\mathcal{B} := (e_1, \ldots, e_n)$ de $\mathbb{R}^n$ telle que si l'on pose $a_i = q(e_i)$ on ait :

$$\forall x = \sum_{i=1}^{n} x_i e_i \in \mathbb{R}^n, \; q(x) = \sum_{i=1}^{n} a_i x_i^2$$

Si on note V_q le volume de l'ellipsoïde $\mathcal{E}_q$ on a alors :

$$V_q = \int_{a_1x_1^2+\ldots+a_nx_n^2 \leq 1} dx_1 \ldots dx_n = \int_{\mathbb{R}^n} \prod_{i=1}^{n} \chi_{\{a_ix_i^2 \leq 1\}} dx_1 \ldots dx_n$$

Par le changement de variable ($\mathcal{C}^1$–difféomorphisme) $\varphi : x \mapsto (\frac{x_1}{\sqrt{a_1}}, \ldots, \frac{x_n}{\sqrt{a_n}})$ on a :

$$V_q = \int_{\mathbb{R}^n} \prod_{i=1}^{n} \chi_{\{x_i^2 \leq 1\}} |\text{Jac}(\varphi)| dx_1 \ldots dx_n = \frac{1}{\sqrt{a_1 \ldots a_n}} \int_{x_1^2+\ldots+x_n^2 \leq 1} dx_1 \ldots dx_n$$

Remarquons de plus que si $\mathcal{B}_1$ est une b.o.n de $\mathbb{R}^n$ quelconque et si on note $S := \text{mat}_{\mathcal{B}_1}(q)$ on a, par changement de base pour les formes quadratiques, qu'il existe $P \in GL_n(\mathbb{R})$ telle que :

$$S = P\text{mat}_{\mathcal{B}}(q)^tP = P\text{Diag}(a_1, \ldots, a_n)^tP$$

Comme $\mathcal{B}$ et $\mathcal{B}_1$ sont orthonormées on a de plus que $P \in O_n(\mathbb{R})$. De facto, $D(q) := \det(S) = a_1 \ldots a_n$ ne dépend que de q. Si on note V_0 le volume de la boule unité (euclidienne) de $\mathbb{R}^n$ on a finalement :

$$V_q = \frac{V_0}{\sqrt{D(q)}}$$

On se ramène donc à montrer qu'il existe un unique $q \in Q_{++}$ tel que :

(i) $D(q)$ soit maximal ;

(ii) $\forall x \in K,\ q(x) \leq 1$.

On munit l'espace vectoriel Q de la norme $N : q \mapsto \sup_{\|x\| \leq 1} |q(x)|$ et on cherche à maximiser D sur l'ensemble suivant :

$$A := \{q \in Q_+ \mid \forall x \in K,\ q(x) \leq 1\}$$

Démontrons que A est une partie convexe compacte non vide de Q.

- K est compact donc borné par un certain $M > 0$. De fait, la forme quadratique $q : x \mapsto \dfrac{\|x\|^2}{M^2}$ est dans A donc $A \neq \emptyset$.
- Soient $q, q' \in A$ et soit $\lambda \in [0,1]$. Alors il est clair que $\lambda q + (1-\lambda)q' \in Q_+$. De plus, si $x \in K$ on a :
$$\lambda q(x) + (1-\lambda)q'(x) \leq \lambda + (1-\lambda) = 1$$
Donc A est convexe.
- Soit $(q_n)_n \in A^{\mathbb{N}}$ une suite convergeant dans Q vers une forme quadratique q. Alors, pour tout $x \in \mathbb{R}^n$, on a :
$$\forall n \geq 0,\ |q_n(x) - q(x)| \leq N(q_n - q)\|x\| \xrightarrow[n\to\infty]{} 0$$
Donc par passages à la limite $q \in Q_+$ (considérer $q_n(x) \geq 0$) et $\forall x \in K,\ q(x) \leq 1$. Donc $q \in A$ donc A est fermée.
De plus, comme K est d'intérieur non vide, il existe $a \in K$ et $r > 0$ tels que $\overline{\mathcal{B}}(a,r) \subset K$. Ainsi, si $q \in A$ et $x \in \overline{\mathcal{B}}(0,r)$ alors $q(a+x) \leq 1$. De plus, $q(-a) = q(a) \leq 1$. Ainsi, par inégalité de Minkowski :
$$\sqrt{q(x)} = \sqrt{q(x+a-a)} \leq \sqrt{q(x+a)} + \sqrt{q(-a)} \leq 2$$
Ainsi $q(x) \leq 4$. In fine, si $x \in \overline{\mathcal{B}}(0,1)$ on a :
$$0 \leq q(x) = \frac{1}{r^2}q(rx) \leq \frac{4}{r^2}$$
Donc $N(q) \leq \dfrac{4}{r^2}$. A est un donc un sous–ensemble fermé et borné de l'espace vectoriel de dimension finie Q : il est compact.

Le déterminant étant continu, l'application $D : q \mapsto D(q)$ l'est également. Comme A est compact, D y est bornée et atteint son maximum en un certain $q_0 \in A$. De plus, comme $x \mapsto \dfrac{\|x\|^2}{M^2} \in A$, on a nécessairement $D(q_0) > 0$ et donc $q_0 \in Q_{++}$. D'où l'existence de l'ellipsoïde recherché (il suffit de prendre $\mathcal{E}_{q_0}$).

Supposons à présent qu'il existe $q \in A$ distincte de q_0 telle $D(q) = D(q_0)$. Posons $S := \mathrm{mat}_{\mathcal{B}_c}(q)$ et $S_0 := \mathrm{mat}_{\mathcal{B}_c}(q_0)$, où $\mathcal{B}_c$ désigne la base canonique de $\mathbb{R}^n$. Comme A est convexe, $\dfrac{q+q_0}{2} \in A$ et par log–concavité du déterminant sur $S_n^{++}(\mathbb{R})$ on a :

$$D\left(\frac{q+q_0}{2}\right) = \det\left(\frac{1}{2}(S+S_0)\right) > \sqrt{\det(S)}\sqrt{\det(S_0)} = \det(S_0) \geq D(q_0)$$

Ce qui contredit la maximalité de $D(q_0)$ et termine donc la preuve.

Détails supplémentaires :

- *Log–concavité du déterminant sur* $S_n^{++}(\mathbb{R})$. On se propose de montrer que l'application ϕ suivante est logarithmiquement concave, i.e que $\ln \circ \phi$ est concave (cf. [FGN10], p. 222–223) :
$$\begin{aligned} \phi : S_n^{++}(\mathbb{R}) &\to \mathbb{R} \\ A &\mapsto \det(A) \end{aligned}$$
Cela revient donc à montrer que :
$$\forall \alpha, \beta \in \mathbb{R}_+ \text{ tels que } \alpha + \beta = 1,\ \forall A, B \in S_n^{++}(\mathbb{R}), \quad \det(\alpha A + \beta B) \geq \det(A)^\alpha \det(B)^\beta$$
Par théorème de pseudo–réduction simultanée des formes quadratiques, on sait qu'il existe $P \in GL_n(\mathbb{R})$ et $D = \mathrm{Diag}(\lambda_1, \dots, \lambda_n)$ telles que $A = {}^tPP$ et $B = {}^tPDP$. Comme B est définie positive, on a de plus que les λ_i sont strictement positifs. De plus :
$$\left\{\begin{array}{lcll} \det(A)^\alpha \det(B)^\beta & = & (\det(P)^2)^\alpha (\det(P)^2 \det(D))^\beta & = \det(P)^2 \det(D)^\beta \\ \det(\alpha A + \beta B) & = & \det(P)^2 \det(\alpha I_n + \beta D) & \end{array}\right. \tag{3.2.1}$$

Le logarithme étant concave, on a également :

$$\forall i \in [n],\ \ln(\alpha + \beta\lambda_i) \geq \alpha \ln(1) + \beta \ln(\lambda_i) = \beta \ln(\lambda_i)$$

En sommant ces inégalités on obtient :

$$\sum_{i=1}^{n} \ln(\alpha + \beta\lambda_i) \geq \beta \sum_{i=1}^{n} \ln(\lambda_i)$$

I.e :

$$\ln\left(\prod_{i=1}^{n}(\alpha + \beta\lambda_i)\right) \geq \ln\left(\left(\prod_{i=1}^{n}\lambda_i\right)^{\beta}\right)$$

Donc par croissance du logarithme :

$$\underbrace{\prod_{i=1}^{n}(\alpha + \beta\lambda_i)}_{=\det(\alpha I_n + \beta D)} \geq \left(\underbrace{\prod_{i=1}^{n}\lambda_i}_{=\det(D)}\right)^{\beta}$$

Ce qui conclut la preuve (utiliser (3.2.1)).

- On rappelle qu'il y a une correspondance bijective entre $S_n(\mathbb{R})$ et l'ensemble des formes bilinéaires symétriques sur $\mathbb{R}^n \times \mathbb{R}^n$ via $A \mapsto ((x, y) \mapsto \langle Ax, y\rangle)$.
- *Un ellipsoïde (plein) centré en l'origine admet une équation de la forme $q(x) \leq 1$, avec $q \in Q_{++}$.* En effet, un tel ellipsoïde admet dans un repère ad hoc une équation de la forme :

$$\sum_{i=1}^{n} \frac{x_i^2}{a_i^2} \leq 1$$

Il suffit alors de remarquer que $q : x \mapsto \sum \dfrac{x_i^2}{R^2 a_i^2} \in Q_{++}$.

3.3 Équation de Hill–Mathieu

Référence :

- [QZ95], p. 401–403

On considère l'équation différentielle linéaire du second ordre suivante :

$$y'' + qy = 0 \text{ où } q \in \mathcal{C}^1_{\pi-\mathrm{per}}(\mathbb{R}, \mathbb{R}) \text{ est paire} \tag{3.3.1}$$

Notons $W \subset \mathcal{C}^2(\mathbb{R}, \mathbb{C})$ l'ensemble des solutions complexes de (3.3.1) et considérons l'endomorphisme suivant :

$$\begin{aligned} u : \mathcal{C}^2(\mathbb{R}, \mathbb{C}) &\to \mathcal{C}^2(\mathbb{R}, \mathbb{C}) \\ y &\mapsto y(. + \pi) \end{aligned}$$

Alors, si $y \in W$ on a :

$$0 = \underbrace{y(. + \pi)''}_{=y''(.+\pi)} + q(. + \pi)y(. + \pi) = y(. + \pi)'' + qy(. + \pi)$$

Donc W est un s–e.v u–stable de $\mathcal{C}^2(\mathbb{R}, \mathbb{C})$. Or W est un s–e.v de dimension 2 de $\mathcal{C}^2(\mathbb{R}, \mathbb{C})$ dont une base est donnée par $(y_1, y_2) \in W^2 \cap \mathcal{C}^2(\mathbb{R}, \mathbb{R})$ vérifiant $y_1(0) = 1$, $y_1'(0) = 0$, $y_2(0) = 0$ et $y_2'(0) = 1$. De fait l'endomorphisme induit par u sur W peut–être identifié à sa matrice dans la base (y_1, y_2), soit $A := \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.

Or $u(y_1) = Ay_1 = ay_1 + by_2 = y_1(. + \pi)$ et donc, par évaluation en 0, $y_1(\pi) = a$. De plus, on obtient en dérivant que $y_1'(. + \pi) = ay_1' + by_2'$. Évaluée en 0 cette égalité donne $b = y_1'(\pi)$. En se livrant aux mêmes exactions sur y_2 on obtient :

$$A = \begin{pmatrix} y_1(\pi) & y_2(\pi) \\ y_1'(\pi) & y_2'(\pi) \end{pmatrix}$$

Proposition 3.3
On pose $T := \mathrm{Tr}(A) = y_1(\pi) + y_2'(\pi)$. *Alors :*
(i) *si* $|T| < 2$, *toutes les solutions de (3.3.1) sont bornées ;*
(ii) *si* $|T| = 2$, *(3.3.1) possède une solution non nulle bornée ;*
(iii) $|T| = 2 \Leftrightarrow y_1'(\pi) \times y_2(\pi) = 0$ *;*
(iv) *si* $|T| > 2$ *alors toutes les solutions non nulles de (3.3.1) sont non bornées.*

Démonstration : Commençons par remarquer que si on note $W(y_1, y_2)$ le wronskien de (y_1, y_2) on a :

$$\begin{aligned} W(y_1,y_2)' &= (y_1y_2' - y_1'y_2)' \\ &= y_1'y_2' + (-qy_2)y_1 - (-qy_1)y_2 - y_1'y_2' \\ &= 0 \end{aligned}$$

Or $W(y_1, y_2)(0) = 1$ donc $W(y_1, y_2) = 1$ d'où $\det(A) = W(y_1, y_2)(\pi) = 1$. In fine on a :

$$\chi_A = X^2 - TX + 1 \in \mathbb{R}[X]$$

De fait, le discriminant de ce polynôme est $\Delta = T^2 - 4$.

(i) Dans ce cas on a $\Delta < 0$ et donc χ_A admet deux racines simples complexes conjuguées $\rho, \bar{\rho}$. Comme A est alors diagonalisable, il existe une base (u, v) de W formés de vecteurs propres de A, i.e $u(. + \pi) = \rho u$ et $v(. + \pi) = \bar{\rho} v$. Par relations coefficients–racines, $\rho\bar{\rho} = 1$ donc $|\rho| = |\bar{\rho}| = 1$ et donc $|u|$ et $|v|$ sont continues π–périodiques donc bornées. Par linéarité, tout élément de W est borné.

(ii) On a $T = \pm 2$, donc $\Delta = 0$ i.e χ_A admet une racine réelle double, qui est nécessairement ± 1 par relations coefficients–racines. Ceci signifie qu'il existe $u \in W \setminus \{0\}$ tel que $u(. + \pi) = \pm u$. De fait, $|u|$ est continue π–périodique donc bornée.

(iii) Commençons par remarquer que comme $\chi_A(A) = 0$ on a $A + A^{-1} = TI_2$. De plus, on peut montrer en utilisant l'unicité dans Cauchy–Lipschitz que y_1 (resp. y_2) est paire (resp. impaire) d'où, comme u^{-1} est l'endomorphisme $y \mapsto y(. - \pi)$:

$$A^{-1} = \begin{pmatrix} y_1(-\pi) & y_2(-\pi) \\ y_1'(-\pi) & y_2'(-\pi) \end{pmatrix} = \begin{pmatrix} a & -c \\ -b & d \end{pmatrix}$$

D'où :

$$\begin{pmatrix} 2a & 0 \\ 0 & 2d \end{pmatrix} = \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix}$$

Donc $a = d$ et de fait :

$$\begin{aligned} T = \pm 2 &\Leftrightarrow a = d = \pm 1 \\ &\Leftrightarrow bc = 0 \text{ car } ad - bc = 1 \end{aligned}$$

(iv) Si $|T| > 2$ alors χ_A admet deux racines réelles r et $r' = r^{-1}$ (car $rr^{prime} = 1$), avec $|r| > 1$ (quitte à intervertir les deux racines). De fait A est diagonalisables et si on se donne (u, v) une base de W formée de vecteurs propres de A alors toute solution non nulle de (3.3.1) s'écrit sous la forme $y = \alpha u + \beta v$ avec $(\alpha, \beta) \neq (0, 0)$.
– Si $\alpha \neq 0$ alors si on fixe x tel que $u(x) \neq 0$ on a :

$$\begin{aligned} y(x + n\pi) &= \alpha r^n u(x) + br^{-n} v(x) \\ &\sim_{n\to\infty} \alpha r^n u(x) \\ &\xrightarrow[n\to\infty]{} \infty \end{aligned}$$

Donc y est non bornée.
– Si $\alpha = 0$ alors $\beta \neq 0$ et si on fixe x n'annulant pas v on a :

$$\begin{aligned} y(x + n\pi) &= br^{-n} v(x) \\ &\sim_{n\to-\infty} br^{-n} v(x) \\ &\xrightarrow[n\to-\infty]{} \infty \end{aligned}$$

Et donc y n'est toujours pas bornée, d'où le résultat.

3.4 Le développement vide

Référence :
- aucune.

Proposition 3.4

Démonstration :

3.5 Lemme de Morse

Référence :
- [Rou09], p. 354–355

Prérequis :
- loi d'inertie de Sylvester ;

Lemme 3.1
Soit $A_0 \in S_n(\mathbb{R}) \cap GL_n(\mathbb{R})$.
Alors il existe $V \in \mathcal{V}_{S_n(\mathbb{R})}(A_0)$ et $\phi \in \mathcal{C}^1(V, GL_n(\mathbb{R}))$ tels que :

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

Démonstration : On considère l'application suivante :

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

φ est de classe $\mathcal{C}^1$ (car polynomiale[1]) et si $H \in \mathcal{M}_n(\mathbb{R})$ on a (en munissant $\mathcal{M}_n(\mathbb{R})$ d'une norme subordonnée $\|.\|$) :

$$\begin{aligned}\varphi(I_n + H) - \varphi(I_n) &= {}^tHA_0 + A_0H + {}^tHA_0H\\ &= {}^t(A_0H) + A_0H + \|H\|\varepsilon(H) \text{ où } \varepsilon(H) \xrightarrow[H\to 0]{} 0\end{aligned}$$

De fait, on a $d\varphi(I_n)(H) = {}^t(A_0H) + A_0H$. Cette applications est clairement surjective car $\forall A \in S_n(\mathbb{R}), A = d\varphi(I_n)\left(\frac{1}{2}A_0^{-1}A\right)$ et $\ker(d\varphi(I_n)) = \{H \in \mathcal{M}_n(\mathbb{R}) \,|\, A_0H \in \mathcal{A}_n(\mathbb{R})\}$. Or $\mathcal{M}_n(\mathbb{R}) = S_n(\mathbb{R}) \oplus \mathcal{A}_n(\mathbb{R})$ donc si on pose $F := \{H \in \mathcal{M}_n(\mathbb{R}) \,|\, A_0H \in S_n(\mathbb{R})\}$ on a :

$$\mathcal{M}_n(\mathbb{R}) = F \oplus \ker(d\varphi(I_n))$$

Si on note $\psi : F \to S_n(\mathbb{R})$ la restriction de φ à F on a $\ker(d\psi(I_n)) = \ker(d\varphi(I_n)) \cap F = \{0\}$ donc $d\psi(I_n)$ est bijective. Par théorème d'inversion locale on a alors l'existence d'un ouvert $\mathcal{U} \in \mathcal{V}_F(I_n)$ (que l'on peut, quitte à les intersecter, supposer inclus dans l'ouvert $GL_n(\mathbb{R})$) tel que ψ réalise un $\mathcal{C}^1$–difféomorphisme entre $\mathcal{U}$ et $V := \psi(\mathcal{U})$. De fait, V est un voisinage (ouvert) de $A_0 = \psi(I_n)$ dans $S_n(\mathbb{R})$ et :

$$\forall A \in V, \qquad A = {}^t\psi^{-1}(A)A_0\psi^{-1}(A)$$

D'où le résultat en posant $\phi := \psi^{-1}$.

Proposition 3.5 (Morse)
Soit $\mathcal{U} \subset \mathbb{R}^n$ un ouvert contenant 0.
Soit $f \in \mathcal{C}^3(\mathcal{U}, \mathbb{R})$.
On suppose que :
- *$df(0) = 0$;*
- *$d^2f(0)$ est non dégénérée de signature $(p, n-p)$.*

1. Oui, je sais.

Alors il existe un $\mathcal{C}^1$–difféomorphisme φ entre deux voisinages de 0 dans $\mathbb{R}^n$ tel que :

(i) $\varphi(0) = 0$;

(ii) pour x dans le premier des deux voisinages suscités, on a, en posant $u = \varphi(x)$:

$$f(x) - f(0) = u_1^2 + \ldots + u_p^2 - u_{p+1}^2 - \ldots - u_n^2$$

Démonstration : Soit x au voisinage de 0. Alors, par formule de Taylor avec reste intégral, $f(x) - f(0) = {}^t x Q(x) x$, où $Q(x)$ est la matrice symétrique inversible (car $d^2 f(0)$ est non dégénérée) $\int_0^1 (1-t) d^2 f(tx) dt$. Q définit alors une applications $\mathcal{C}^1$ au voisinages de 0. Par le lemme 3.1, comme $Q(0) \in S_n(\mathbb{R}) \cap GL_n(\mathbb{R})$, il existe alors une matrice $M(x) \in GL_n(\mathbb{R})$, avec $x \mapsto M(x)$ de classe $\mathcal{C}^1$ au voisinage de l'origine, telle que :

$$Q(x) = {}^t M(x) Q(0) M(x)$$

Ainsi, si on pose $y := M(x)x$ on a :

$$f(x) - f(0) = {}^t y Q(0) y$$

Or $Q(0) = \dfrac{1}{2} d^2 f(0)$ est de signature $(p, n-p)$ donc par loi d'inertie de Sylvester il existe un changement de base $A \in GL_n(\mathbb{R})$ tel que, si on pose $u := A^{-1} y$:

$$\begin{aligned} {}^t y Q(0) y &= {}^t u\, {}^t A Q(0) A u \\ &= u_1^2 + \ldots + u_p^2 - u_{p+1}^2 - \ldots - u_n^2 \end{aligned}$$

Enfin, comme $x \mapsto u := A^{-1} M(x) x$ a pour différentielle en l'origine $A^{-1} M(0) \in GL_n(\mathbb{R})$, il réalise par théorème d'inversion locale un $\mathcal{C}^1$–difféomorphisme entre deux voisinages de l'unité, d'où le résultat.

Détails supplémentaires :

– Rappelons l'hilarante formule de Taylor avec reste intégral : si f est de classe $\mathcal{C}^{k+1}$ sur un ouvert $\mathcal{U}$ de $\mathbb{R}^n$ alors pour tous $a, h \in \mathcal{U}$ tels que $[a, a+h] \subset \mathcal{U}$ on a [2] :

$$f(a+h) = f(a) + \sum_{i=1}^{k} \frac{1}{i!} d^i f(a)(h)^i + \int_0^1 \frac{(1-t)^k}{k!} d^{k+1} f(a+th)(h)^{k+1} dt$$

3.6 Méthode du gradient à pas optimal

Référence :

– [HU98], p. 66–69

Prérequis :

– inégalité de Kantorovitch.

Soit $A \in S_n^{++}(\mathbb{R})$.
Soit $b \in \mathbb{R}^n$.
Soit $c \in \mathbb{R}$.
On considère l'application suivante :

$$\begin{aligned} f : \mathbb{R}^n &\to \mathbb{R} \\ x &\mapsto \frac{1}{2}\langle Ax, x\rangle + \langle b, x\rangle \end{aligned}$$

☞ *On cherche à minimiser f sur $\mathbb{R}^n$* ; en effet on a $Ax = -b \Leftrightarrow x = \min(f)$.

2. Comme il est d'usage dans le monde enchanté du calcul différentiel, on note $(h)^i$ le i–uplet (de vecteurs) $\underbrace{(h, \ldots, h)}_{i \text{ fois}}$.

f est strictement convexe et coercive définie sur un fermé, donc il existe un unique $\overline{x} \in \mathbb{R}^n$ minimisant f. De plus, comme f est différentiable, $\overline{x}$ est l'unique solution de l'équation $\nabla f(x) = 0$. Or :

$$\begin{aligned} \forall x, h \in \mathbb{R}^n, \quad df(x)(h) &= \frac{1}{2}(\langle Ax, h\rangle + \langle Ah, x\rangle) + \langle b, h\rangle \\ &= \langle Ax + b, h\rangle \text{ car } A \text{ est symétrique} \end{aligned}$$

Donc $\nabla f(x) = Ax + b$ d'où :

$$\overline{x} = -A^{-1}b \text{ et } \overline{f} := f(\overline{x}) = -\frac{1}{2}\langle A^{-1}b, b\rangle + c$$

On se propose à présent d'étudier l'algorithme de minimisation suivant :

Algorithme 3.1 (Gradient à pas optimal)
Soit $x_0 \in \mathbb{R}^n$.
On cherche à approcher $\overline{x}$ à l'aide de la suite récurrente $(x_k)_k$ construite comme suit : pour $k \geq 0$ on pose $x_{k+1} := x_k + t_k d_k$, où :

$$\begin{cases} d_k := -\nabla f(x_k) \\ t_k \text{ est l'unique réel minimisant } t \mapsto f(x_k + td_k) \text{ sur } \mathbb{R} \end{cases}$$

Dans toute la suite on fait l'hypothèse suivante :

$$\forall k \geq 0, \quad d_k = -\nabla f(x_k) \neq 0 \tag{3.6.1}$$

Cette hypothèse est justifiée par le fait qu'elle est équivalente au fait que $\forall k \geq 0$, $f(x_k) > \overline{f}$. Ainsi, si (3.6.1) n'est pas vérifiée l'algorithme converge en temps fini.

Vérifions tout d'abord que $(t_k)_k$ est bien définie. Pour $k \geq 0$ et $t \in \mathbb{R}$ on a :

$$f(x_k + td_k) = f(x_k) + \frac{1}{2}t^2\langle Ad_k, d_k\rangle + t\langle Ax_k + b, d_k\rangle$$

Une brève étude de fonction nous montre alors que sous l'hypothèse (3.6.1) cette fonction est minimisée en un unique point t_k vérifiant :

$$t_k := \frac{\|d_k\|^2}{\langle Ad_k, d_k\rangle} \tag{3.6.2}$$

De plus :

$$\begin{aligned} \forall k \geq 0,\ d_{k+1} &= -\nabla f(x_{k+1}) \\ &= -(Ax_{k+1} + b) \\ &= -A_k x_k - b - t_k A d_k \\ &= d_k - t_k A d_k \end{aligned}$$

D'où, d'après (3.6.2) :

$$\forall k \geq 0,\ \langle d_{k+1}, d_k\rangle = \langle d_k, d_k\rangle - t_k\langle Ad_k d_{,k}\rangle = 0 \tag{3.6.3}$$

De plus :

$$\begin{aligned} \forall k \geq 0,\ f(x_{k+1}) &= f(x_k + t_k d_k) \\ &= f(x_k) + \frac{1}{2}t_k^2\langle Ad_k, d_k\rangle + t_k\langle Ax_k + b, d_k\rangle \end{aligned}$$

$$\begin{aligned} & f(x_k) + \frac{1}{2}t_k^2\langle Ad_k, d_k\rangle + t_k(-\|d_k\|^2) \text{ d'après (3.6.3)} \\ &= f(x_k) + \frac{1}{2}\frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle} - \frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle} \\ &= f(x_k) - \frac{1}{2}\frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle} \end{aligned}$$

De fait :

$$\begin{aligned}\forall k \geq 0,\ f(x_{k+1}) - \overline{f} &= f(x_k) - \frac{1}{2}\frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle} - \overline{f} \\ &= (f(x_k) - \overline{f})\left(1 - \frac{1}{2f(x_k) - \overline{f})}\frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle}\right)\end{aligned}$$

De plus, sous l'hypothèse (3.6.1), on a :

$$\begin{aligned}\langle A^{-1}d_k, d_k\rangle &= \langle A^{-1}(Ax_k + b), Ax_k + b\rangle \\ &= 2\left(\frac{1}{2}\langle Ax_k, x_k\rangle + \langle b, x_k\rangle + \frac{1}{2}\langle A^{-1}b, b\rangle\right) \\ &= 2(f(x_k) - \overline{f}) \text{ car } \frac{1}{2}\langle A^{-1}b, b\rangle = c - \overline{f}\end{aligned}$$

Et donc :

$$\forall k \geq 0,\ f(x_{k+1}) - \overline{f} = (f(x_k) - \overline{f})\left(1 - \frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle\langle A^{-1}d_k, d_k\rangle}\right) \tag{3.6.4}$$

Notons $\lambda_1 \geq \ldots \geq \lambda_n$ les valeurs propres de A et posons la quantité suivante, appelée conditionnement de A :

$$c_2(A) := \frac{\lambda_1}{\lambda_n}$$

Par inégalité de Kantorovitch (lemme 3.2, cf. infra) on a alors :

$$\begin{aligned}\frac{\|d_k\|^4}{\langle Ad_k, d_k\rangle\langle A^{-1}d_k, d_k\rangle} &\geq 4\left(\sqrt{c_2(A)} + \frac{1}{\sqrt{c_2(A)}}\right)^{-2} \\ &= 4\frac{c_2(A)}{(1 + c_2(A))^2}\end{aligned}$$

En appliquant cette minoration à l'équation (3.6.4) on obtient :

$$\begin{aligned}\forall k \geq 0,\ f(x_{k+1}) - \overline{f} &\leq (f(x_k) - \overline{f})\left(1 - 4\frac{c_2(A)}{(1 + c_2(A))^2}\right) \\ &= (f(x_k) - \overline{f})\left(\frac{1 + 2c_2(A) + c_2(A)^2}{(1 + c_2(A))^2} - 4\frac{c_2(A)}{(1 + c_2(A))^2}\right) \\ &= (f(x_k) - \overline{f})\left(\frac{1 - 2c_2(A) + c_2(A)^2}{(1 + c_2(A))^2}\right) \\ &= (f(x_k) - \overline{f})\left(\frac{c_2(A) - 1}{c_2(A) + 1}\right)^2\end{aligned}$$

On montre alors par récurrence que :

$$\forall k \geq 0,\ f(x_k) - \overline{f} \leq (f(x_0) - \overline{f})\left(\frac{c_2(A) - 1}{c_2(A) + 1}\right)^{2k} \tag{3.6.5}$$

En outre :

$$\begin{aligned}\forall k \geq 0,\ f(x_k) - \overline{f} &= \frac{1}{2}\langle Ax_k, x_k\rangle + \langle b, x_k\rangle + c - f(\overline{x}) \\ &= \frac{1}{2}\langle A(x_k - \overline{x}), x_k - \overline{x}\rangle \\ &\geq \frac{1}{2}\lambda_n\|x_k - \overline{x}\|^2 \text{ car } \lambda_n = \inf_{x \neq 0}\frac{\langle Ax, x\rangle}{\|x\|^2}\end{aligned}$$

In fine :

$$\forall k \geq 0, \quad \|x_k - \overline{x}\| \leq \sqrt{2\frac{f(x_0) - \overline{f}}{\lambda_n}}\left(\frac{c_2(A) - 1}{c_2(A) + 1}\right)^k \tag{3.6.6}$$

En conclusion il apparaît que si $c_2(A)$ est proche de 1 la méthode converge rapidement, alors que dans le cas contraire elle converge très lentement.

Détails supplémentaires :

- *f est strictement convexe.* La matrice hessienne de f est A, qui est définie positive.
- *f est coercive.* Soit $x \in \mathbb{R}^n$. Alors :

$$\begin{aligned}|f(x)| &= |\frac{1}{2}\langle Ax, x\rangle + \langle b, x\rangle + c| \\ &\geq |\frac{1}{2}\langle Ax, x\rangle + \langle b, x\rangle| \\ &\geq \frac{1}{2}|\langle Ax, x\rangle| - |\langle b, x\rangle| \\ &\geq \frac{1}{2}|\langle Ax, x\rangle| - \|b\|\|x\| \\ &\geq \frac{1}{2}\lambda_n\|x\|^2 - \|b\|\|x\| \\ &\xrightarrow[\|x\|\to\infty]{} \infty\end{aligned}$$

- On rappelle le lemme suivant :

  Lemme 3.2 (Inégalité de Kantorovitch)
  Soit $A \in S_n^{++}(\mathbb{R})$ de valeurs propres $\lambda_1 \geq \ldots \geq \lambda_n > 0$.
  Soit $x \in \mathbb{R}^n$.
  Alors :

$$\langle Ax, x\rangle\langle A^{-1}x, x\rangle \leq \frac{1}{4}\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^2 \|x\|^4$$

3.7 Nombres de Bell

Référence :

- [FGN07], p. 14–16

Proposition 3.6
Pour $n \geq 0$ on note B_n le nombre[3] de partitions distinctes de l'ensemble $[n]$.
Alors :

(i) la série entière $\sum \frac{B_n}{n!}z^n$ a un rayon de convergence $R > 0$ et sa somme f vérifie :

$$\forall z \in (-R, R), \quad f(z) = e^{e^z - 1}$$

(ii) pour tout $k \in \mathbb{N}$ on a :

$$B_k = \frac{1}{e}\sum_{n=0}^{\infty}\frac{n^k}{n!}$$

Démonstration :

(i) Soit $n \geq 0$. Pour $0 \leq k \leq n$, on note E_k l'ensemble des partitions de $[n+1]$ telle que le "morceau[4]" contenant $n+1$ soit de cardinal $k+1$. Pour construire une telle partition, il suffit de choisir la classe de $n+1$ (choix de k éléments dans $[n]$) puis de partitionner les $n+1-(k+1) = n-k$ entiers restants, d'où $\text{card}(E_k) = C_n^k B_{n-k}$.
De plus, il est clair que $\{E_0, \ldots, E_n\}$ est une partition de l'ensemble des partitions de $[n+1]$ et donc :

$$B_{n+1} = \sum_{k=0}^{n}\text{card}(E_k) = \sum_{k=0}^{n}C_n^k B_{n-k} = \sum_{k=0}^{n}C_n^k B_k \text{ car } C_n^{n-k} = C_n^k \tag{3.7.1}$$

Démontrons par récurrence sur $n \geq 0$ que $\forall n \in \mathbb{N},\ B_n \leq n!$.

- $n = 0$. Trivial.

3. Notons que la seule partition de $\emptyset$ étant $\{\emptyset\}$, on a $B_0 = 1$.
4. Il faut bien que je m'amuse de temps en temps ...

– Supposons la propriété vraie au rang $n \geq 0$. Alors :

$$\begin{aligned} B_{n+1} &= \sum_{k=0}^{n} C_n^k B_k \\ &\leq \sum_{k=0}^{n} C_n^k k! \\ &= n! \sum_{k=0}^{n} \underbrace{\frac{1}{(n-k)!}}_{\leq 1} \\ &\leq (n+1)! \end{aligned}$$

D'où l'hérédité.

De fait, pour tout $n \in \mathbb{N}$ et $z \in \mathbb{C}$, $0 \leq \dfrac{B_n}{n!}|z|^n \leq |z|^k$ donc R est supérieur ou égal au rayon de convergence de la série géométrique, à savoir 1. En particulier, R est strictement positif. Soit à présent $z \in (-R, R)$. Alors, par un changement d'indice :

$$f(z) = 1 + \sum_{n=0}^{\infty} \frac{B_{n+1}}{(n+1)!} z^{n+1}$$

Par théorème de dérivation terme à terme pour les séries entières on obtient :

$$\begin{aligned} f'(z) &= \sum_{n=0}^{\infty} \frac{B_{n+1}}{n!} z^n \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \left(\sum_{k=0}^{n} C_n^k B_k \right) z^n \text{ par (3.7.1)} \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \frac{B_k}{k!} \frac{1}{(n-k)!} \right) z^n \end{aligned}$$

On reconnaît dans cette dernière expression le produit de Cauchy des séries $\Sigma \frac{z^n}{n!}$ et $\sum \frac{B_n}{n!} z^n$, toutes deux de rayon de convergence supérieur ou égal à R. De fait :

$$\forall z \in (-R, R), \quad f'(z) = f(z) \sum_{n=0}^{\infty} \frac{z^n}{n!} = f(z) e^z \tag{3.7.2}$$

Résolvant (3.7.2) on trouve que :

$$\exists C \in \mathbb{R}, \forall z \in (-R, R), \quad f(z) = C e^{e^z}$$

Or $f(0) = 1$ donc $C = e^{-1}$ d'où :

$$f(z) = \frac{1}{e} e^{e^z} = e^{e^z - 1}$$

(ii) Soit $z \in \mathbb{C}$. Alors :

$$e^{e^z} = \sum_{n=0}^{\infty} \frac{e^{nz}}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{\infty} \frac{(nz)^k}{k!}$$

On considère donc la série double[5] $\sum_{(n,k)} u_{n,k}$ où $\forall n, k \in \mathbb{N}$, $u_{n,k} := \dfrac{(nz)^k}{n!k!}$. Alors, pour tout $n \geq 0$, la série $\sum_{(k)} |u_{n,k}|$ converge et :

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

5. Vous préféreriez que je vous parle de mesure de comptage sur $\mathbb{N}^2$? ... Là. Faites ce que l'on vous dit et il n'y aura pas de blessé.

De fait, $\sum_{(n)} \sum_{k=0}^{\infty} |u_{n,k}|$ converge. Par théorème de Fubini pour les séries doubles, $\sum_{(n,k)} u_{n,k}$ converge et :

$$\sum_{n=0}^{\infty}\sum_{k=0}^{\infty} u_{n,k} = \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} u_{n,k}$$

I.e :

$$\begin{aligned}
f(z) &= \frac{1}{e}e^{e^z} \\
&= \frac{1}{e}\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{(nz)^k}{n!k!} \\
&= \sum_{k=0}^{\infty}\sum_{n=0}^{\infty}\frac{(nz)^k}{n!k!} \\
&= \sum_{k=0}^{\infty}\frac{1}{e}\left(\sum_{n=0}^{\infty}\frac{n^k}{n!}\right)\frac{z^k}{k!}
\end{aligned}$$

Et donc, par unicité du développement en série entière de f sur $(-R, R)$:

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

Détails supplémentaires :

– L'expression de B_k trouvée en (ii) et les calculs menés lors de la démonstration de ce dernier point montrent que R est en fait égal à $+\infty$.

3.8 Sous–groupes compacts de $GL_n(\mathbb{R})$

Référence :
– [Ale99], p. 141 et 160–162

Prérequis :
– théorème de Caratheodory.

Lemme 3.3
Soit V un espace vectoriel de dimension finie muni d'une norme euclidienne $\|.\|$.
Soit K un compact convexe de V.
Soit $\mathcal{G}$ un sous–groupe compact de $GL(V)$ tel que :

$$\forall u \in \mathcal{G}, \quad u(K) \subset K$$

Alors il existe $a \in K$ tel que :

$$\forall u \in \mathcal{G}, \quad u(a) = a$$

Démonstration : Commençons par montrer que si $v \in \mathcal{L}(V)$ vérifie $v(K) \subset K$, alors v admet un point fixe sur K. Fixons $x_0 \in K$ et posons pour $k \geq 1$:

$$x_k := \frac{1}{k+1}\sum_{i=0}^{k} v^i(x_0)$$

Comme K est convexe et stable par u il est clair que $\forall k \geq 0$, $x_k \in K$ et donc d'après le théorème de Bolzano–Weierstrass, il existe $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $(x_\varphi(k))_k$ converge vers un point $a \in K$. Or :

$$\begin{aligned}
\forall k \geq 0,\ v(x_k) &= v\left(\frac{1}{k+1}\sum_{i=0}^{k} v^i(x_0)\right) \\
&= \frac{1}{k+1}\sum_{i=0}^{k} v^{i+1}(x_0) \\
&= x_k + \frac{1}{k+1}(v^{k+1}(x_0) - x_0)
\end{aligned}$$

Or $\dfrac{1}{k+1}(v^{k+1}(x_0)-x_0) \xrightarrow[k\to\infty]{} 0$ car $(v^{k+1}(x_0)-x_0)_k$ est bornée par compacité de K et continuité de v donc en passant à la limite on obtient que $v\ v(a)=a$.

Remarquons ensuite que $\mathcal{G}$ agit naturellement sur V via $u.x := u(x)$. De plus comme $\mathcal{G}$ est compact, l'orbite $\mathcal{G}.x$ d'un élément $x \in V$ sous cette action est compacte ce qui nous permet de définir l'application suivante :

$$\begin{aligned} \nu : V &\to \mathbb{R}_+ \\ x &\mapsto \max_{u\in\mathcal{G}} \|u(x)\| \end{aligned}$$

On montre alors que comme $\mathcal{G} \leq GL(V)$ ν est une norme sur V constante sur les orbites sous l'action de $\mathcal{G}$. De plus si on se donne $x, y \in V$ et $u_0 \in \mathcal{G}$ tel que $\nu(x+y) = \|u_0(x+y)\|$. Alors :

$$\begin{aligned} \nu(x+y) &= \|u_0(x+y)\| \\ &\leq \|u_0(x)\| + \|u_0(y)\| \\ &\leq \nu(x) + \nu(y) \end{aligned}$$

Si on se place dans le cas d'égalité on a alors $\|u_0(x)+u_0(y)\| = \|u_0(x)\| + \|u_0(y)\|$ et donc il existe $\lambda \geq 0$ tel que $u_0(x) = \lambda u_0(y)$ et donc $x = \lambda y$.

Pour $u \in \mathcal{G}$ on considère à présent l'ensemble suivant :

$$F_u := \{x \in K \mid u(x) = x\}$$

Cet ensemble est un fermé non vide de K. De fait, si on suppose que $\cap_{u\in\mathcal{G}} F_u = \emptyset$ alors la propriété de Borel–Lebesgue impose l'existence de $u_1, \ldots, u_p \in K$ tels que $\cap_{i=1}^p F_{u_i} = \emptyset$. Posons alors :

$$v := \frac{1}{p}\sum_{i=1}^p u_i \in \mathcal{L}(V)$$

Alors, par convexité et $\mathcal{G}$–stabilité de K, $v(K) \subset K$ et donc il existe $a \in K$ tel que $v(a) = a$. On a alors :

$$\begin{aligned} \nu(v(a)) &= \nu\left(\frac{1}{p}\sum_{i=1}^p u_i(a) \in \mathcal{L}(V)\right) \\ &\leq \frac{1}{p}\sum_{i=1}^p \nu(u_i(a)) \\ &= \frac{1}{p}\sum_{i=1}^p \nu(a) \\ &= \nu(a) \end{aligned}$$

Les $u_i(a)$ sont donc positivement liés (i.e il existe $a_1, \ldots, a_{p-1} \geq 0$ tels que $u_1(a) = a_1 u_2(a) = \ldots = a_{p-1}u_p(a)$) et comme ils sont de même norme (pour ν) ils sont égaux. On a donc nécessairement $u_i(a) = a$ pour tout $i \in [p]$, ce qui contredit notre hypothèse et conclut la preuve.

Proposition 3.7
Soit G un sous–groupe compact de $GL_n(\mathbb{R})$.
Alors il existe une forme quadratique q définie positive sur $\mathbb{R}^n$ telle que $G \subset \mathcal{O}(q)$

Démonstration : On munit G d'une nouvelle structure de groupe $(G, \diamond)$ définie comme suit : $\forall A, B \in G,\ A \diamond B := BA$ et on considère l'application suivante :

$$\begin{aligned} \rho : (G,\diamond) &\to GL(S_n(\mathbb{R})) \\ A &\mapsto (S \mapsto {}^t ASA) \end{aligned}$$

On vérifie aisément que G est bien définie (on a même $\rho(A)^{-1} = \rho(A^{-1})$) et qu'il s'agit d'un morphisme de groupes[6]. De plus ρ est une application continue car égale à la restriction de la

6. ***Attention :*** n'oublions pas que nous avons modifié la structure de G !

composée $b \circ d$ à G où $b : (A, B) \mapsto (S \mapsto {}^tASB)$ est une application bilinéaire de $\mathcal{M}_n(\mathbb{R})^2$ dans $\mathcal{L}(S_n(\mathbb{R}), \mathcal{M}_n(\mathbb{R}))$ (continue par dimension finie) et où $d : A \mapsto (A, A)$ se passe de commentaires.

Posons $H := \{ {}^tMM \mid M \in G\}$. On vérifie aisément que K est un compact non vide du convexe $S_n(\mathbb{R})$ et donc par théorème de Caratheodory $K := \mathrm{conv}(H)$ est un compact convexe non vide de $S_n(\mathbb{R})$. De plus, $\mathcal{G} := \rho(G)$ est un sous–groupe (car ρ est un morphisme de groupes) compact (car ρ est continue et G compact) de $GL(S_n(\mathbb{R}))$. Enfin, si $A \in G$ et $M \in G$ on a :

$$\rho(A)({}^tMM) = {}^tA{}^tMMA = {}^t(AM)(AM) \in K$$

Comme $\rho(A)$ est linéaire donc conserve les combinaisons convexes on a bien $\rho(A)(K) \subset K$ et donc K est G–stable.

On applique alors le lemme 3.3 qui nous donne l'existence de $S \in K$ tel que pour tout $A \in G$ on ait $\rho(A)(S) = S$, i.e ${}^tASA = S$. Comme de plus $K \subset S_n^+ + (\mathbb{R})$ on a bien $G \subset \mathcal{O}(q)$ où $q : x \mapsto {}^txSx$ est une forme quadratique définie positive.

Détails supplémentaires :

- *Cas où le groupe G est fini.* On définit le produit scalaire suivant sur $\mathbb{R}^n$:

$$\Phi : (x, y) \mapsto \frac{1}{|G|} \sum_{A \in G} \langle Ax, Ay\rangle$$

  Il est alors clair, la translation à droite par un élément donné de G étant bijective, que toute matrice de G est orthogonale pour Φ.
- *Cas d'égalité pour ν.* Le lemme suivant nous permet de conclure :

  Lemme 3.4
  Soient $x, y \in V$ tels que $\|x + y\| = \|x\| + \|y\|$.
  Alors il existe $\lambda \geq 0$ tel que $x = \lambda y$ (ou $y = \lambda x$).
  DÉMONSTRATION : Plaçons nous dans le cas où $\|x\| = \|y\| = 1$. Alors $\|x + y\| = 2$ par hypothèse et on a également $\|x + y\|^2 = 2 + 2\langle x, y\rangle$ donc $\langle x, y\rangle = 1 = \|x\|\|y\|$: on se trouve dans le cas d'égalité de l'inégalité de Cauchy–Schwarz. De fait, il existe $t \geq 0$ tel que $x = ty$ et comme $\|x\| = \|y\|$ on a nécessairement $t \in \{-1, 1\}$. Cependant, si $t = -1$ alors $\langle x, y\rangle = -1$, ce qui est absurde d'où $x = y$.
  Dans le cas général, pour x et y non nuls[7] On applique alors la proposition précédente à $\frac{x}{\|x\|}$ et $\frac{y}{\|y\|}$, ce qui nous livre le résultat pieds et poings liés avec $\lambda = \frac{\|x\|}{\|y\|}$.

3.9 Théorème des extrema liés

Référence :

- [Gou08], p. 317 et 327

Proposition 3.8 (Extrema liés)
Soit $\mathcal{U} \subset \mathbb{R}^n$ un ouvert.
Soient $g_1, \ldots, g_r \in \mathcal{C}^1(\mathcal{U}, \mathbb{R})$.
On considère l'ensemble suivant :

$$\Gamma := \{x \in \mathcal{U} \mid \forall i \in [r],\, g_i(x) = 0\}$$

On suppose que :

- *$f_{|\Gamma}$ admet un extremum relatif en $a \in \Gamma$;*
- *la famille $(dg_i(a))_{1 \leq i \leq r}$ est libre dans $(\mathbb{R}^n)^*$.*

Alors il existe $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$ (appelés multiplicateurs de Lagrange) tels que :

$$df(a) = \sum_{i=1}^{r} \lambda_i dg_i(a)$$

7. La preuve dans le cas où l'un est nul est laissée en exercice au lecteur. Ne me remerciez pas.

Démonstration : On pose $s := n-r$ et on identifie $\mathbb{R}^n$ au produit cartésien $\mathbb{R}^s \times \mathbb{R}^r$. On utilisera de fait la notation $(x,y) = (x_1,\ldots,x_s,y_1,\ldots,y_r)$ pour les éléments de $\mathbb{R}^n$. Posons également $(\alpha,\beta) := a$ (via l'identification précitée). On rappelle que :

$$\forall h \in \mathbb{R}^n,\ \forall i \in [r],\ dg_i(a)(h) = \sum_{j=1}^{s} \frac{\partial g_i}{x_j}(a)h + \sum_{j=1}^{r} \frac{\partial g_i}{y_j}(a)h$$

Comme la famille $(dg_i(a))_{1\leq i\leq r}$ est libre, on a donc :

$$\operatorname{rg}(M) = r,\ \text{où } M := \begin{pmatrix} \frac{\partial g_1}{\partial x_1}(a) & \ldots & \frac{\partial g_1}{\partial x_s}(a) & \frac{\partial g_1}{\partial y_1}(a) & \ldots & \frac{\partial g_1}{\partial y_r}(a) \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial g_r}{\partial x_1}(a) & \ldots & \frac{\partial g_r}{\partial x_s}(a) & \frac{\partial g_r}{\partial y_1}(a) & \ldots & \frac{\partial g_r}{\partial y_r}(a) \end{pmatrix} \in \mathcal{M}_{r,n}(\mathbb{R})$$

Comme le rang de M est la taille de sa plus petite matrice sous–matrice carrée inversible, on peut supposer, quitte à renuméroter les variables[8] que :

$$\det\left(\frac{\partial g_i}{\partial y_j}(a)\right)_{i,j\in[r]} \neq 0$$

Ce qui peut se reformuler, en posant $g := (g_1,\ldots,g_r)$ par :

$$D_y g(a) \text{ est inversible}$$

On peut donc appliquer le théorème des fonctions implicites à g au voisinage de $a = (\alpha,\beta)$, obtenant de facto l'existence de deux voisinages ouverts $\mathcal{U}' \in \mathcal{V}_{\mathbb{R}^s}(\alpha)$ et $\Omega \in \mathcal{V}_{\mathbb{R}^r}(\beta)$ et d'une application $\varphi := (\varphi_1,\ldots,\varphi_r) : \mathcal{U}' \to \mathbb{R}^r$ de classe $\mathcal{C}^1$ telle que :

$$\left\{\begin{array}{l} g(x,y) = 0 \\ x \in \mathcal{U}' \\ y \in \Omega \end{array}\right. \Leftrightarrow y = \varphi(x) \tag{3.9.1}$$

En d'autres termes, les éléments de $\Gamma \cap (\mathcal{U}' \times \Omega)$ sont de la forme $(x,\varphi(x))$. En particulier, on a nécessairement $\beta = \varphi(\alpha)$. Posons à présent :

$$\begin{aligned} h : \mathcal{U}' &\to \mathbb{R} \\ x &\mapsto f(x,\varphi(x)) \end{aligned}$$

Comme $h(\alpha) = f(a)$ et que $\forall x \in \mathcal{U}'$, $(x,\varphi(x)) \in \Gamma$, h admet un extremum local en α (car f admet un extremum local sur Γ en a). De fait :

$$\begin{aligned} \forall i \in [s],\ 0 = \frac{\partial h}{\partial x_i}(\alpha) &= \frac{\partial}{\partial x_i}(f\circ\psi)(\alpha) \text{ où } \psi := (\psi_1,\ldots,\psi_n) : x \mapsto (x,\varphi(x)) \text{ (i.e } \psi = (\mathrm{id}_{\mathbb{R}^s},\varphi)) \\ &= \sum_{i=1}^{s} \frac{\partial f}{\partial x_j}(\psi(\alpha))\frac{\partial \psi_j}{\partial x_i}(\alpha) + \sum_{i=1}^{s} \frac{\partial f}{\partial y_j}(\psi(\alpha))\frac{\partial \psi_{s+j}}{\partial x_i}(\alpha) \end{aligned}$$

En remarquant que $\forall j \in [s]$, $\dfrac{\partial \psi_j}{\partial x_i} = \delta_{i,j}$, que $\forall j \in [r]$, $\dfrac{\partial \psi_{s+j}}{\partial x_i} = \dfrac{\partial \varphi_j}{\partial x_i}$ et que $a = \psi(\alpha)$ on obtient :

$$\forall i \in [s],\quad \sum_{j=1}^{r} \frac{\partial f}{\partial y_j}(a)\frac{\partial \varphi_j}{\partial x_i}(\alpha) + \frac{\partial f}{\partial x_i}(a) = 0 \tag{3.9.2}$$

De plus, $g\circ\psi$ est nulle sur $\mathcal{U}'$ donc pour tout $k \in [n]$ c'est également le cas pour $g_k\circ\psi$, ergo (par un calcul similaire) :

$$\forall i \in [s],\quad 0 = \frac{\partial g_k\circ\psi}{\partial x_i}(\alpha) = \sum_{j=1}^{r} \frac{\partial g_k}{\partial y_j}(a)\frac{\partial \varphi_j}{\partial x_i}(\alpha) + \frac{\partial g_k}{\partial x_i}(a) = 0 \tag{3.9.3}$$

8. Un peu de foi que diable !

On se donne la matrice suivante :

$$A := \begin{pmatrix} \frac{\partial f}{\partial x_1}(a) & \dots & \frac{\partial f}{\partial x_s}(a) & \frac{\partial f}{\partial y_1}(a) & \dots & \frac{\partial f}{\partial y_r}(a) \\ \frac{\partial g_1}{\partial x_1}(a) & \dots & \frac{\partial g_1}{\partial x_s}(a) & \frac{\partial g_1}{\partial y_1}(a) & \dots & \frac{\partial g_1}{\partial y_r}(a) \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial g_r}{\partial x_1}(a) & \dots & \frac{\partial g_r}{\partial x_s}(a) & \frac{\partial g_r}{\partial y_1}(a) & \dots & \frac{\partial g_r}{\partial y_r}(a) \end{pmatrix} \in \mathcal{M}_{r+1,n}(\mathbb{R})$$

D'après les relation (3.9.2) et (3.9.3) les s premières colonnes de A sont combinaisons linéaires de ses r dernières, ergo $\mathrm{rg}(A) \leq r$. Comme $\mathrm{rg}(A) = \mathrm{rg}({}^tA)$, on en déduit que les $r+1$ premières lignes de A sont liées, i.e qu'il existe $\mu_0, \dots, \mu_r \in \mathbb{R}$ non tous nuls tels que :

$$\mu_0 df(a) + \sum_{i=1}^{r} \mu_i dg_i(a) = 0$$

Or $(dg_i(a))_{i\in[r]}$ est libre donc $\mu_0 \neq 0$ (car sinon tous les μ_i devraient l'être). On obtient alors le résultat en posant $\lambda_0 := 1$ et $\forall i \in [r]$, $\lambda_i := -\frac{\mu_i}{\mu_0}$.

Détails supplémentaires :

– Comme la famille $(dg_i(a))_{1\leq i\leq r}$ est libre dans $(\mathbb{R}^n)^*$, il y a unicité des multiplicateurs de Lagrange.

3.10 Théorème de Rothstein–Trager

Référence :

– [SP99], p. 153–155

Proposition 3.9 (Rothstein–Trager)
Soient $P, Q \in \mathbb{Q}[X]$ premiers entre eux tels que $\deg(P) < \deg(Q)$.
On suppose de plus Q unitaire et sans facteur carré.
Soit $\mathbb{K}/\mathbb{Q}$ une extension dans laquelle on puisse écrire[9] *:*

$$\int \frac{P}{Q} = \sum_{i=1}^{n} c_i \ln(P_i) \tag{3.10.1}$$

Quitte à regrouper, on peut supposer les $c_i \in \mathbb{K}^*$ deux à deux distincts. La nature de Q nous permet également[10] *de supposer les P_i unitaires sans facteurs carrés, non constants*[11] *et premiers entre eux* deux à deux.
Alors :

(i) pour tout $i \in [n]$ on a :

$$P_i = (P - c_iQ') \wedge Q$$

(ii) les c_i sont exactement les racines du polynôme suivant :

$$R(Y) := \mathrm{Res}_X(P - YQ', Q) \in \mathbb{K}[Y]$$

DÉMONSTRATION :

(i) Commençons par poser, pour $i \in [n]$:

$$U_i := \prod_{j\neq i} P_j$$

9. On a existence d'une telle extension par théorème de décomposition en éléments simples.
10. Toujours par décomposition en éléments simples.
11. car $\deg(P) < \deg(Q)$.

Ensuite, si on dérive (formellement) la relation (3.10.1) on obtient :

$$\frac{P}{Q} = \sum_{i=1}^{n} c_i \frac{P_i'}{P_i}$$

D'où :

$$P \prod_{j=1}^{n} P_j = Q \sum_{j=1}^{n} c_j P_j' U_j$$

On déduit de cette dernière relation que, dans $\mathbb{K}[X]$:

$$Q \mid \prod_{i=1}^{n} P_i \text{ et } \forall i \in [n], \quad P_i \mid \sum_{j=1}^{n} c_j P_j' U_j$$

Soit $i \in [n]$; alors pour tous les $j \neq i$, $P_i | U_j$ et donc on déduit de la seconde relation ci–avant que :

$$P_i \mid c_i Q P_i' U_i$$

Or P_i est sans facteur carré donc $P_i \wedge P_i' = 1$. En sus, $P_i \wedge P_j = 1$ si $j \neq 1$ donc $P_i \wedge U_i = 1$: le théorème de Gauss nous permet alors de conclure que $P_i | Q$, ergo (comme les P_i sont premiers entre eux *deux à deux*) :

$$\prod_{i=1}^{n} P_i \mid Q$$

Les polynômes $\prod_{i=1}^{n} P_i$ et Q sont donc unitaires associés, d'où in fine :

$$Q = \prod_{i=1}^{n} P_i$$

Soit $i \in [n]$; on se propose à présent de démontrer que $P_i | P - c_i Q'$. On déduit du résultat que l'on vient de démontrer sur Q que :

$$Q' = \sum_{j=1}^{n} P_j' U_j$$

Ergo :

$$\begin{aligned} P - c_i Q' &= \sum_{j=1}^{n} c_j P_j' U_j - c_i \sum_{j=1}^{n} P_j' U_j \\ &= \sum_{j=1}^{n} (c_j - c_i) P_j' U_j \end{aligned}$$

Or la quantité $(c_i - c_j) P_j' U_j$ est nulle si $i = j$ et divisible par P_i sinon d'où le résultat attendu :

$$P_i \mid P - c_i Q'$$

Remarquons à présent que, si $i \in [n]$:

$$\begin{aligned} (P - c_i Q') \wedge Q &= (P - c_i Q') \wedge \prod_{j=1}^{n} P_j \\ &= \prod_{j=1}^{n} ((P - c_i Q') \wedge P_j) \text{ car les } P_j \text{ sont premiers entre eux deux à deux} \end{aligned}$$

Or, si $j \neq i$:

$$\begin{aligned} (P - c_i Q') \wedge P_j &= \left(\sum_{k=1}^{n} (c_k - c_i) P_k' U_k \right) \wedge P_j \\ &= (c_j - c_i) P_j' U_j \wedge P_j \text{ car } P_j \text{ divise les termes pour} \\ &= 1 \text{ car } P_j' \wedge P_j = U_j \wedge P_j = 1 \end{aligned}$$

D'où :

$$\begin{aligned}(P - c_iQ') \wedge Q &= (P - c_iQ') \wedge P_i \\ &= P_i \text{ car } P_i \mid P - c_iQ'\end{aligned}$$

(ii) On déduit du point (i) que pour tout $i \in [n]$ c_i est tel que $P - c_iQ'$ et Q ont un pgcd non trivial ; il est de fait racine du résultant R.
Réciproquement, si c est une racine de R dans une extension $\mathbb{L}/\mathbb{K}$, alors $S := (P-cQ')\wedge Q \in \mathbb{L}[X]$ est de degré strictement positif. Si on se donne T un facteur irréductible de S dans $\mathbb{L}[X]$ on a alors :

$$T \mid P - cQ' \text{ et } T \mid Q$$

Comme $Q = \prod_i P_i$ avec les P_i premiers entre eux deux à deux, T doit alors nécessairement diviser un et un seul des P_i, soit P_{i_0}. Mais :

$$P - cQ' = \sum_{i=1}^{n}(c_i - c)P_i'U_i$$

Comme T divise P_{i_0} donc tous les U_i pour $i \neq i_0$ et que $T|P - cQ'$ on a alors :

$$T \mid (c_{i_0} - c)P_{i_0}'U_{i_0}$$

Mais $T \nmid U_{i_0}$, ainsi si on suppose que c est distinct de tous les c_i on trouve $T|P_{i_0}'$ et donc P_{i_0} admet un facteur carré, ce qui est absurde et, accessoirement, conclut la preuve.

3.11 Théorème de Von Neumann

Références :
- [GT98], p. 83–84

Soit G un sous–groupe fermé de $GL_n(\mathbb{R})$. On pose :

$$\mathcal{L}_G := \{m \in \mathcal{M}_n(\mathbb{R}) \,|\, \forall t \in \mathbb{R},\, e^{tm} \in G\}$$

Alors $\mathcal{L}_G$ est un s–e.v de $\mathcal{M}_n(\mathbb{R})$ (cf. infra) donc y admet un supplémentaire, soit M.

Lemme 3.5
Il n'existe aucune suite $(m_k)_k \in (M \setminus \{0\})^{\mathbb{N}}$ convergeant vers 0 telle que $\forall k \geq 0,\ e^{m_k} \in G$.

Démonstration : Si il existe une suite $(m_k)_k \in (M\setminus\{0\})^{\mathbb{N}}$ convergeant vers 0 telle que $\forall k \geq 0, e^{m_k} \in G$, alors on peut la suite définie $\varepsilon_k := \dfrac{m_k}{\|m_k\|}$ est incluse dans un compact donc (quitte à extraire) converge vers un élément ε unitaire de M.

Soit $t \in \mathbb{R}$; on remarque que :

$$e^{t\varepsilon} = \lim_{k\to\infty} e^{t\varepsilon_k}$$

Or pour tout $k \geq 0$, on peut écrire $\dfrac{t}{\|m_k\|} = \lambda_k + \mu_k$ où $\lambda_k \in \mathbb{Z}$ et $|\mu_k| \leq \frac{1}{2}$. On a alors :

$$e^{t\varepsilon_k} = \underbrace{e^{\lambda_k m_k}}_{\in G}\ \underbrace{e^{\mu_k m_k}}_{\xrightarrow[k\to\infty]{} 1}$$

De fait, comme G est fermé, $e^{t\varepsilon} \in G$, ce qui est absurde car alors $\varepsilon \in \mathcal{L}_G \cap M \setminus \{0\}$.

Proposition 3.10 (Von Neumann)
Tout sous–groupe fermé de $GL_n(\mathbb{R})$ est une sous–variété de $GL_n(\mathbb{R})$.

Démonstration : Soit G un tel groupe. Commençons par remarquer que comme $h \mapsto gh$ est de classe $\mathcal{C}^\infty$ pour tout $g \in G$, il nous suffit de montrer qu'il existe un voisinage de I_n dans G difféomorphe à un ouvert d'un espace vectoriel de dimension finie.

- Supposons $\mathcal{L}_G = \{0\}$. Alors, d'après le lemme 3.5, 0 est un point isolé de $L(G)$ (cf. infra) donc que I_n est isolé dans G. Par structure ($\mathcal{C}^\infty$) de groupe, G est donc discret (ce qui implique que c'est une sous–variété).
- Supposons à présent $\mathcal{L}(G) \neq \{0\}$. L'application exp : $\mathcal{M}_n(\mathbb{R}) \to GL_n(\mathbb{R})$ est de classe $\mathcal{C}^\infty$ et on a $d\exp(0) = \mathrm{id}_{\mathcal{M}_n(\mathbb{R})} \neq 0$. De fait, par inversion locale, il existe un voisinage ouvert U de 0 dans $\mathcal{M}_n(\mathbb{R})$ tel que $W := \exp(U)$ soit un ouvert de $GL_n(\mathbb{R})$ et que exp : $U \to W$ soit un $\mathcal{C}^\infty$–difféomorphisme ; et donc, quitte à restreindre U, exp : $U \cap \mathcal{L}_G \to W \cap G$ l'est également. On a donc un difféomorphisme entre un voisinage de I_n dans G et un ouvert de $\mathcal{L}_G$ d'où le résultat.

Détails supplémentaires :

- *Logarithme matriciel.* Si $m \in \mathcal{M}_n(\mathbb{R})$ vérifie $\|m\| < 1$ on peut définir de façon $\mathcal{C}^\infty$ un "logarithme" de $I_n + m$ comme suit :

$$L(I_n + m) := \sum_{k=0}^{\infty} (-1)^k \frac{m^{k+1}}{k+1}$$

  On a alors $e^{L(I_n+m)} = I_n + m$.
- *$\mathcal{L}_G$ est un s–e.v de $\mathcal{M}_n(\mathbb{R})$.* Le seul point technique est la stabilité additive qui découle de la relation suivante :

$$\forall a, b \in \mathcal{M}_n(\mathbb{R}), \qquad \left(e^{a/k} e^{b/k}\right)^k \xrightarrow[k\to\infty]{} e^{a+b} \tag{3.11.1}$$

  Cette relation découle elle–même du fait que comme $e^{a/k}e^{b/k} == I_n + \frac{a+b}{k} + o\left(\frac{1}{k}\right)$ on a :

$$\begin{aligned}\left(e^{a/k} e^{b/k}\right)^k &= e^{kL\left(e^{a/k}e^{b/k}\right)} \\ &= e^{kL\left(I_n + \frac{a+b}{k} + o\left(\frac{1}{k}\right)\right)} \\ &\xrightarrow[k\to\infty]{} e^{a+b} \text{ car } L(I_n + m) = m + o(m)\end{aligned}$$

Chapitre 4

Développements coupés au montage

4.1 Formule sommatoire d'Euler–Maclaurin (variante)

Référence :
- [Mé06], p. 538–539

On commence par définir par récurrence une suite numérique, dite des nombres de Bernoulli :

$$B_0 := 1 \text{ et } \forall n \geq 1, \sum_{k=0}^{n} C_{n+1}^{k} B_k = 0$$

On définit ensuite une suite $(B_n(X))_n \in \mathbb{Q}[X]^{\mathbb{N}}$, dite des polynômes de Bernoulli, comme suit :

$$B_0(X) = 1 \text{ et } \forall n \geq 1,\ B_n'(X) = nB_{n-1}(X),\ \text{ avec } B_n(0) = B_n$$

On peut alors démontrer (cf. infra) que $B_n(0) = B_n(1)$, ce qui permet de définir à partir du polynôme B_n une application $\tilde{B_n} \in \mathcal{C}^0_{1-\mathrm{per}}(\mathbb{R}_+) \cap \mathcal{C}^\infty_{\mathrm{pm}}(\mathbb{R}_+)$.

Proposition 4.1 (Euler–Maclaurin)
Soient $k, n \geq 1$.
Soit $f \in \mathcal{C}^k(\mathbb{R}_+, \mathbb{R})$.
Alors :

$$\sum_{j=1}^{n} f(j) = \int_0^n f(t)dt + \frac{1}{2}(f(n)+f(0)) + \sum_{i=2}^{k}(-1)^i \frac{B_i}{i!}(f^{(i-1)}(n) - f^{(i-1)}(0)) + \frac{(-1)^{k-1}}{k!}\int_0^n \tilde{B_k}(t) f^{(k)}(t)dt$$

Démonstration : On va commencer raisonner par "récurrence finie" pour démontrer la propriété suivante : *pour tout $j \in [k]$ on a la formule suivante :*

$$\frac{1}{2}(f(1)+f(0)) = \int_0^1 f(t)dt + \sum_{i=2}^{j} \frac{(}{-}1)^i B_i i!(f^{(i-1)}(1) - f^{(i-1)}(0)) + \frac{(-1)^{j-1}}{j!}\int_0^1 \tilde{B_j}(t) f^{(j)}(t)dt \tag{4.1.1}$$

- $j = 1$. Remarquons que $\tilde{B_1}'$ est constante égale à 1 ce qui signifie que :

$$\begin{aligned}\int_0^1 f(t)dt &= \int_0^1 \tilde{B_1}'(t) f(t)dt \\ &= [\tilde{B_1}(t) f(t)]_0^1 - \int_0^1 \tilde{B_1}(t) f'(t)dt \text{ par intégration par parties} \\ &= \frac{1}{2}(f(1)+f(0)) - \int_0^1 \tilde{B_1}(t) f'(t)dt\end{aligned}$$

On a donc bien la formule pour $j = 1$ (car $B_1 = 1$) :

$$\frac{1}{2}(f(1)+f(0)) = \int_0^1 f(t)dt + \int_0^1 \tilde{B_1}(t) f'(t)dt$$

– Supposons la propriété validée pour $2 \leq j \leq k-1$. Comme $\tilde{B}'_{j+1} = (j+1)\tilde{B}_j$, on a :

$$\begin{aligned}\int_0^1 \tilde{B}_j(t) f^{(j)}(t)dt &= \frac{1}{j+1}\int_0^1 \tilde{B}'_{j+1}(t) f^{(j)}(t)dt \\ &= \frac{1}{j+1}\left([\tilde{B}_{j+1}(t)f^{(j)}(t)]_0^1 - \int_0^1 \tilde{B}_{j+1}(t)f^{(j+1)}(t)dt\right) \text{ par intégration par parties} \\ &= \frac{1}{j+1}\left(B_{j+1}(f^{(j)}(1) - f^{(j)}(0)) - \int_0^1 \tilde{B}_{j+1}(t)f^{(j+1)}(t)dt\right)\end{aligned}$$

Ainsi par hypothèse de récurrence :

$$\begin{aligned}\frac{1}{2}(f(1)+f(0)) &= \int_0^1 f(t)dt + \sum_{i=2}^{j}(-1)^i\frac{B_i}{i!}(f^{(i-1)}(1) - f^{(i-1)}(0)) + \frac{(-1)^{j-1}}{j!}\int_0^1 \tilde{B}_j(t)f^{(j)}(t)dt \\ &= \int_0^1 f(t)dt + \sum_{i=2}^{j}(-1)^i\frac{B_i}{i!}(f^{(i-1)}(1) - f^{(i-1)}(0)) \\ &\quad + \frac{(-1)^{j-1}}{j!}\left(\frac{1}{j+1}\left(B_{j+1}(f^{(j)}(1) - f^{(j)}(0)) - \int_0^1 \tilde{B}_{j+1}(t)f^{(j+1)}(t)dt\right)\right) \\ &= \int_0^1 f(t)dt + \sum_{i=2}^{j}(-1)^i\frac{B_i}{i!}(f^{(i-1)}(1) - f^{(j)}(0)) + (-1)^{j+1}\frac{B_{j+1}}{(j+1)!}(f^{(j)}(1) - f^{(j)}(0)) \\ &\quad + \frac{(-1)^j}{(j+1)!}\int_0^1 \tilde{B}_{j+1}(t)f^{(j+1)}(t)dt\end{aligned}$$

D'où le résultat.

La formule (4.1.1) appliquée à $j = k$ donne alors :

$$\frac{1}{2}(f(1)+f(0)) = \int_0^1 f(t)dt + \sum_{i=2}^{k}(-1)^i\frac{B_i}{i!}(f^{(i-1)}(1) - f^{(i-1)}(0)) + \frac{(-1)^{k-1}}{k!}\int_0^1 \tilde{B}_k(t)f^{(k)}(t)dt \tag{4.1.2}$$

Appliquons à présent cette formule (4.1.2) aux fonctions $g_j : t \mapsto f(t+j-1)$, pour $j \in [n]$ et remarquons que $\forall t \in \mathbb{R}_+$, $\forall i \in [k]$, $g_j^{(i)}(t) = f(i)(t+j-1)$. De fait :

$$\int_0^1 \tilde{B}_k(t)g^{(k)}(t)dt = \int_0^1 \tilde{B}_k(t)f^{(k)}(t+j-1)dt = \int_{j-1}^{j} \tilde{B}_k(t)f^{(k)}(t)dt \text{ car } \tilde{B}_k \text{ est 1–périodique}$$

De même :

$$\int_0^1 g_j(t)dt = \int_{j-1}^{j} f(t)dt$$

On obtient alors :

$$\frac{1}{2}(f(j)+f(j-1)) = \int_{j-1}^{j} f(t)dt + \sum_{i=2}^{k}(-1)^i\frac{B_i}{i!}(f^{(i-1)}(j) - f^{(i-1)}(j-1)) + \frac{(-1)^{k-1}}{k!}\int_{j-1}^{j} \tilde{B}_k(t)f^{(k)}(t)dt$$

En sommant cette dernière relation pour $j \in [n]$ on obtient :

$$\frac{1}{2}\left(\sum_{j=1}^{n} f(j) + \sum_{j=0}^{n-1} f(j)\right) = \int_0^1 f(t)dt + \sum_{j=1}^{n}\sum_{i=2}^{k}(-1)^i\frac{B_i}{i!}(f^{(i-1)}(j) - f^{(i-1)}(j-1)) + \frac{(-1)^{k-1}}{k!}\int_0^n \tilde{B}_k(t)f^{(k)}(t)dt$$

Remarquons dans un premier temps que :

$$\frac{1}{2}\left(\sum_{j=1}^{n} f(j) + \sum_{j=0}^{n-1} f(j)\right) = \sum_{j=1}^{n} f(j) - \frac{1}{2}(f(n)+f(0))$$

De plus :

$$\sum_{j=1}^{n}\sum_{i=2}^{k}(-1)^i\frac{B_i}{i!}(f^{(i-1)}(j)-f^{(i-1)}(j-1)) = \sum_{i=2}^{k}(-1)^i\frac{B_i}{i!}\sum_{j=1}^{n} f^{(i-1)}(j)-f^{(i-1)}(j-1)$$
$$= \sum_{i=2}^{k}(-1)^i\frac{B_i}{i!}(f^{(i-1)}(n)-f^{(i-1)}(0))$$

D'où le résultat voulu :

$$\sum_{j=1}^{n} f(j) = \int_0^n f(t)dt+\frac{1}{2}(f(n)+f(0))+\sum_{i=2}^{k}(-1)^i\frac{B_i}{i!}(f^{(i-1)}(n)-f^{(i-1)}(0))+\frac{(-1)^{k-1}}{k!}\int_0^n \tilde{B}_k(t)f^{(k)}(t)dt$$

Détails supplémentaires :

- On trouve les coquilles suivantes dans [Mé06] :
  * dans l'avant dernière formule "displayée" p. 538 il faut lire :

$$\frac{1}{2}(f(1)+f(0)) = \underbrace{\int_0^1 f(t)dt +}_{\text{ajouter}} \quad \sum_{i=2}^{k}\frac{(-1)^iB_i}{i!}(f^{(i-1)}(1)-f^{(i-1)}(0))+S_k$$

  * dans la première formule "displayée" p. 539 il faut lire :

$$\int_0^1 \tilde{B}_k(t)f^{(k)}(t+j-1)dt = \int_{j-1}^{j} \tilde{B}_k(t)f^{(k)}(\underbrace{\quad t \quad}_{\text{et non } t+j-1})dt$$

- On peut calculer les polynômes et les nombres de Bernoulli de proche en proche. Le tableau ci–dessous en répertorie les premières valeurs (cf. [Mé06], p.167) :

i	$B_i(X)$	B_i
0	1	1
1	$X-1/2$	$-1/2$
2	$X^2-X+1/6$	$1/6$
3	$X^3-(3/2)X^2+(1/2)X$	0
4	$X^4-2X^3+X^2-1/30$	$-1/30$

  De plus on montre facilement que si $n \geq 3$ est impair alors $B_n = 0$.
- $B_n(0) = B_n(1)$. Démontrons par récurrence sur $n \geq 0$ que :

$$B_n(X) = \sum_{i=0}^{n} C_n^i B_{n-i}X^i$$

  Si $n = 0$ la propriété est triviale car $B_0(X) = B_0$. Si on suppose la propriété vraie au rang $n \geq 0$ alors :

$$B'_{n+1}(X) = (n+1)B_n(X)$$
$$= (n+1)\sum_{i=0}^{n} C_n^i B_{n-i}X^i$$
$$= \sum_{i=0}^{n} B_{n-i}\frac{n!}{i!(n-i)!}(n+1)X^i$$
$$= \sum_{i=0}^{n} B_{n-i}\frac{(n+1)!}{i!(n-i)!}X^i$$

Ergo :

$$\begin{aligned}
B_{n+1}(X) &= B_{n+1}(0) + \sum_{i=0}^{n} B_{n-i} \frac{(n+1)!}{i!(n-i)!} \frac{1}{i+1} X^{i+1} \\
&= B_{n+1} + \sum_{i=0}^{n} B_{n-i} \frac{(n+1)!}{(i+1)!(n-i)!} X^{i+1} \\
&= B_{n+1} + \sum_{i=0}^{n} B_{n-i} \frac{(n+1)!}{(i+1)!(n+1-(i+1))!} X^{i+1} \\
&= B_{n+1} + \sum_{i=1}^{n} B_{n+1-i} C_{n+1}^{i} X^{i} \\
&= \sum_{i=1}^{n+1} B_{n+1-i} C_{n+1}^{i} X^{i}
\end{aligned}$$

D'où le résultat. Ainsi :

$$\begin{aligned}
B_n(1) &= \sum_{i=0}^{n} C_n^i B_{n-i} \\
&= \sum_{k=0}^{n} B_k C_n^{n-k} \\
&= \sum_{k=0}^{n} B_k \frac{n!}{(n-k)!(n-(n-k))!} \\
&= \sum_{k=0}^{n} B_k \frac{n!}{(n-k)!k!} \\
&= \sum_{k=0}^{n} B_k C_n^k \\
&= B_n \text{ car } \sum_{k=0}^{n-1} C_n^k B_k = 0
\end{aligned}$$

Donc on a bien $B_n(1) = B_n = B_n(0)$.

- Pour mieux comprendre l'hérédité dans la "récurrence finie", détaillons le cas $j = 2$. Comme $\tilde{B_2}' = 2\tilde{B}_1$ le cas $j = 1$ nous donne :

$$\begin{aligned}
\frac{1}{2}(f(1) + f(0)) &= \int_0^1 f(t)dt + \frac{1}{2} \int_0^1 \tilde{B_2}'(t) f'(t)dt \\
&= \int_0^1 f(t)dt + \frac{1}{2} \left([\tilde{B}_2(t) f'(t)]_0^1 - \int_0^1 \tilde{B}_2(t) f''(t)dt \right) \text{ par intégration par parties} \\
&= \int_0^1 f(t)dt + \frac{B_2}{2!}(f'(1) - f'(0)) + \frac{-1}{2!} \int_0^1 \tilde{B}_2(t) f''(t)dt
\end{aligned}$$

Ce qui constitue le résultat pour $j = 2$.

4.2 Théorème de Helly

Référence :

- [FGN09b], p. 166

Lemme 4.1 ([FGN09b], p. 166, 163 et 165)
Soit E un sous–ensemble dénombrable de $\mathbb{R}$.
Soit $(f_n)_n$ une suite de fonctions de E dans $\mathbb{R}$ telles que :

$$\forall x \in E, \forall n \geq 0, \quad |f_n(x)| \leq 1$$

Alors $(f_n)_n$ admet une sois suite convergeant simplement sur E.

DÉMONSTRATION : Soit $(r_p)_{p\in\mathbb{N}}$ une énumération de E. On va appliquer ici le procédé d'extraction diagonale de Cantor.

Commençons par démontrer par récurrence l'existence d'une suite $(\varphi_p)_p$ de fonctions strictement croissantes de $\mathbb{N}$ dans $\mathbb{N}$ telle que :

$$\forall p \in \mathbb{N},\, \forall 0 \leq k \leq p, \quad (f_{\varphi_0\circ\ldots\circ\varphi_p(n)}(r_k))_n \text{ converge}$$

- $p = 0$. Par hypothèse, la suite $(f_n(r_0))$ est bornée d'où le résultat par théorème de Bolzano–Weierstrass.
- *Supposons la propriété vérifiée pour* $p \geq 0$. On extrait par théorème de Bolzano–Weierstrass une sous suite convergente $(f_{\varphi_0\circ\ldots\circ\varphi_{p+1}(n)}(r_{p+1}))_n$ de la suite bornée $(f_{\varphi_0\circ\ldots\circ\varphi_p(n)}(r_p))_n$. De plus, si $k \leq p$ la suite $(f_{\varphi_0\circ\ldots\circ\varphi_{p+1}(n)}(r_k))_n$ est extraite de $(f_{\varphi_0\circ\ldots\circ\varphi_k(n)}(r_k))_n$ car $\varphi_{k+1}\circ\ldots\circ\varphi_{p+1}$ est strictement croissante, donc converge.

Définissons l'application suivante :

$$\begin{aligned}\psi : \mathbb{N} &\to \mathbb{N}\\ n &\mapsto \varphi_0\circ\ldots\circ\varphi_n(n)\end{aligned}$$

Alors :

$$\begin{aligned}\forall n \geq 0, \psi(n+1) &= \varphi_0\circ\ldots\circ\varphi_n(\varphi_{n+1}(n+1))\\ &> \varphi_0\circ\ldots\circ\varphi_n(\varphi_{n+1}(n)) \text{ car } \varphi_{n+1}(n+1) > \varphi_{n+1}(n)\\ &\geq \varphi_0\circ\ldots\circ\varphi_n(n)\end{aligned}$$

La dernière inégalité provient du fait que si $g : \mathbb{N} \to \mathbb{N}$ est strictement croissante on peut montrer par récurrence que $g \geq \mathrm{id}_{\mathbb{N}}$. Ainsi $\psi(n+1) > \psi(n)$ donc ψ est strictement croissante. De plus, pour tout $p \geq 0$, $(f_{\psi(n)}(r_p))_{n\geq p}$ est extraite de la suite convergente $(f_{\varphi_0\circ\ldots\circ\varphi_p(n)}(r_p))_{n\geq p}$ (car $n \mapsto \varphi_{p+1}\circ\ldots\circ\varphi_n(n)$ est strictement croissante[1]) donc converge. De fait $(f_{\psi(n)}(r_p))_{n\geq 0}$ converge et donc $(f_{\psi(n)})_{n\geq 0}$ converge simplement sur E.

Proposition 4.2 (Helly)
Soit $(f_n)_n$ une suite de fonctions croissantes de $\mathbb{R}$ dans $[-1,1]$.
Alors $(f_n)_n$ admet une sois suite convergeant simplement sur $\mathbb{R}$.

DÉMONSTRATION : En appliquant le lemme 4.1 à $E \leftarrow \mathbb{Q}$ on obtient l'existence d'une extraction ψ telle que $(f_{\psi(n)})_n$ converge simplement sur $\mathbb{Q}$ vers une fonction f, qui est alors nécessairement croissante sur $\mathbb{Q}$. Notons $D := \{x \in \mathbb{R} \,|\, f(x-) < f(x+)\}$, où $f(x+) := \lim_{h\to 0,\, h\in\mathbb{Q}_+} f(x+h)$ et $f(x-) = \lim_{h\to 0,\, h\in\mathbb{Q}_+} f(x-h)$ sont bien définis par croissance de f.

Si $x \notin D$ alors $f(x-) = f(x+) =: \ell$ (car f est croissante sur $\mathbb{Q}$ donc $f(x-) \leq f(x+)$). Si on fixe $\varepsilon > 0$, il existe $\eta > 0$ tel que pour tout $t \in [x-\eta, x+\eta]\cap\mathbb{Q}$, $|f(t)-\ell| \leq \varepsilon$. Fixons $\alpha \in [x-\eta, x]\cap\mathbb{Q}$ et $\beta \in [x, x+\eta]\cap\mathbb{Q}$; alors :

$$\forall n \geq 0, \quad f_{\psi(n)}(\alpha) \leq f_{\psi(n)}(x) \leq f_{\psi(n)}(\beta)$$

Or par convergence simple de $(f_{\psi(n)})_n$ vers f sur $\mathbb{Q}$ et croissance de cette dernière, il existe $N \geq 0$ tel que :

$$\forall n \geq N, \quad f_{\psi(n)}(\beta) \leq f(\beta) + \varepsilon \text{ et } f_{\psi(n)}(\alpha) \geq f(\alpha) - \varepsilon$$

De fait :

$$\forall n \geq N, \quad \ell - 2\varepsilon \leq f(\alpha) - \varepsilon \leq f_{\psi(n)}(x) \leq f(\beta) + \varepsilon \leq \ell + 2\varepsilon$$

D'où $f_{\psi(n)}(x) \xrightarrow[n\to\infty]{} \ell$. En posant $f(x) := \ell$ on a donc la convergence simple de $(f_{\psi(n)})_n$ vers f sur $\mathbb{R} \to D$.

Si $x \in D$, il existe $q_x \in [f(x-), f(x+)]\cap\mathbb{Q}$. De plus si pour $(x,y) \in D^2$ $q_x = q_y$, $[f(x-), f(x+)]\cap[f(y-), f(y+)] \neq \emptyset$ alors par croissance de f $f(x-) = f(y-)$ et $f(x+) = f(y+)$ donc $y = x$, ce qui prouve que $x \mapsto q_x$ est injective, donc D est dénombrable. On obtient alors le résultat en appliquant le lemme 4.1 à la suite $(f_{\psi(n)})_n$ et à l'ensemble dénombrable D.

1. Même démonstration que pour ψ.

4.3 Théorème de Liapounov

Référence :

- [Rou09], p. 138–143

Proposition 4.3
Soit $f \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}^n)$ *telle que :*

- $f(0) = 0$;
- $\mathrm{Sp}(df(0)) \subset \{\Re < 0\}$.

Soit $x \in \mathbb{R}^n$.
On considère le problème de Cauchy suivant :

$$\left\{ \begin{array}{l} y' = f(y) \\ y(0) = x \end{array} \right. , \text{ d'inconnue } y \in \mathcal{C}^1(\mathbb{R}_+, \mathbb{R}^n) \tag{4.3.1}$$

Alors 0 *est un point d'équilibre attractif de (4.3.1), i.e il existe* $V \in \mathcal{V}_{\mathbb{R}^n}(0)$ *tel que pour* $x \in V$ *la solutions* y *de (4.3.1) converge exponentiellement vers* 0 *à l'infini, i.e :*

$$\exists K_x, a_x > 0, \, \forall t \in \mathbb{R}_+, \quad \|y(t)\| \leq K_x e^{-a_x t}$$

Démonstration : On pose $A := df(0)$ et on note $\lambda_1, \ldots, \lambda_k$ les valeurs propres *distinctes* de A. Alors, si $\chi_A = (-1)^n \prod_{j=1}^k (X - \lambda_j)^{m_j}$, le lemme des noyaux s'écrit :

$$\mathbb{C}^n = \bigoplus_{j=1}^{k} \ker((A - \lambda_j I_n)^{m_j})$$

De fait [2], x s'écrit de façon unique comme $x_1 + \ldots + x_k$, les $x_j \in E_j := \ker((A - \lambda_j I_n)^{m_j})$. Alors les E_j sont A–stables et :

$$\begin{aligned} \forall j \in [k], \forall t \in \mathbb{R}, \, e^{tA} x_j &= e^{t\lambda_j I_n} e^{t(A - \lambda_j I_n)} x_j \\ &= e^{t\lambda_j} e^{t(A - \lambda_j I_n)} x_j \\ &= e^{t\lambda_j} \left(\sum_{p=0}^{\infty} \frac{t^p}{p!} (A - \lambda_j I_n)^p \right) x_j \\ &= e^{t\lambda_j} \left(\sum_{p=0}^{m_j - 1} \frac{t^p}{p!} (A - \lambda_j I_n)^p \right) x_j \text{ car } x_j \in E_j \end{aligned}$$

Si on note $\|.\|$ la norme induit par le produit scalaire canonique $\langle ., . \rangle$ sur $\mathbb{R}^n$, on a alors :

$$\begin{aligned} \forall j \in [k], \forall t \in \mathbb{R}, \, \|e^{tA} x_j\| &= \left\| e^{t\lambda_j} \left(\sum_{p=0}^{m_j - 1} \frac{t^p}{p!} (A - \lambda_j I_n)^p \right) x_j \right\| \\ &\leq e^{t\Re(\lambda_j)} C_j (1 + |t|)^{m_j - 1} \|x_j\| \text{ où } C_j := \max_{0 \leq p < m_j} \|A - \lambda_j I_n\|^p \\ &\leq C_0 e^{t\Re(\lambda_j)} (1 + |t|)^{n-1} \|x_j\| \text{ où } C_0 := \max_{1 \leq j \leq k} \left(C_j \frac{(1 + |t|)^{n-1} \|x_j\|}{(1 + |t|)^{m_j - 1} \|x_j\|} \right) \end{aligned}$$

D'où :

$$\begin{aligned} \forall t \in \mathbb{R}, \, \|e^{tA} x\| &\leq \sum_{j=1}^{k} \|e^{tA} x_j\| \\ &\leq C_0 (1 + |t|)^{n-1} \left(\sum_{j=1}^{k} e^{t\Re(\lambda_j)} \right) \max_{1 \leq j \leq k} \|x_j\| \\ &\leq\leq C_0 (1 + |t|)^{n-1} \left(\sum_{j=1}^{k} e^{t\Re(\lambda_j)} \right) \|x\| \end{aligned}$$

2. Quitte à identifier $\mathbb{R}^n$ à un s-e.v de $\mathbb{C}^n$.

Et donc :

$$\exists P \in \mathbb{C}[X], \quad \forall t \in \mathbb{R},\ \|e^{tA}x\| \leq P(|t|)\left(\sum_{j=1}^{k} e^{t\Re(\lambda_j)}\right)\|x\| \tag{4.3.2}$$

On considère le linéarisé en 0 de (4.3.1) :

$$\begin{cases} z' = df(0)(y) = Ay \\ z(0) = x \end{cases}, \text{ d'inconnue } z \in \mathcal{C}^1(\mathbb{R}_+, \mathbb{R}^n) \tag{4.3.3}$$

(4.3.3) admet pour unique solution globale la fonction $z : t \mapsto e^{tA}x$. De plus, comme les valeurs propres de A sont de partie réelle strictement négative, il existe $a > 0$ tel que $\forall j \in [k]$, $\Re(\lambda_j) < -a$. De fait on peut majorer $t \mapsto P(|t|)\left(\sum_{j=1}^{k} e^{t\Re(\lambda_j)}\right)e^{at}$ sur $\mathbb{R}_+$ par une constante $C > 0$. L'équation (4.3.2) nous donne alors :

$$\forall t \geq 0, \quad \|z(t)\| \leq Ce^{-at}\|x\|$$

Et donc 0 est un point d'équilibre attractif pour (4.3.3).

On considère à présent l'application suivante :

$$\begin{aligned} b : \mathbb{R}^n \times \mathbb{R}^n &\to \mathbb{R} \\ (x, y) &\mapsto \int_0^{\infty} \langle e^{tA}x, e^{tA}y\rangle dt \end{aligned}$$

Alors b est bien définie car :

$$\begin{aligned} \forall t \geq 0,\ \forall x, y \in \mathbb{R}^n,\ |\langle e^{tA}x, e^{tA}y\rangle| &\leq \|e^{tA}x\|\|e^{tA}y\| \text{ par Cauchy–Schwarz} \\ &\leq C^2e^{-2at}\|x\|\|y\| \end{aligned}$$

Il s'agit de plus d'une forme bilinéaire symétrique : notons donc q la forme quadratique associée. Alors :

$$\forall x \in \mathbb{R}^n,\ q(x) = \int_0^{\infty} \|e^{tA}x\|^2 dt \geq 0$$

Comme $e^{tA} \in GL_n(\mathbb{R})$, q est également définie positive par théorème de nullité de l'intégrale pour une fonction positive.

On a alors, pour $x \in \mathbb{R}^n$:

$$\begin{aligned} \langle \nabla q(x), Ax\rangle &= dq(x)(Ax) \\ &= \int_0^{\infty} 2\langle e^{tA}x, e^{tA}Ax\rangle dt \\ &= \int_0^{\infty} \frac{d}{dt}(\langle e^{tA}x, e^{tA}x\rangle dt \\ &= \lim_{T\to\infty} \left[\|e^{tA}x\|^2\right]_0^T \end{aligned}$$

I.e[3] :

$$\langle \nabla q(x), Ax\rangle = -\|x\|^2 \tag{4.3.4}$$

Revenons en à nos moutons différentiels. Le théorème de Cauchy–Lipschitz nous affirme qu'il existe une unique solution maximale y de (4.3.1), définie sur un intervalle de la forme $I := [0, \alpha)$, avec $\alpha \in (0, \infty)$. Alors :

$$\begin{aligned} \frac{d}{dt}q(y) &= dq(y)(y') \\ &= 2b(y, y') \\ &= 2b(y, Ay) + 2b(y, r(y)) \text{ où } r(y) := f(y) - Ay \\ &= -\|y\|^2 + 2b(y, r(y)) \end{aligned}$$

Or, par inégalité de Cauchy–Schwarz $|b(y, r(y)| \leq \sqrt{q(y)}\sqrt{q(r(y))}$. De plus, $r(y) = f(y) - f(0) - df(0)(y)$ (car $f(0) = 0$) ce qui implique, par définition de la différentielle $df(0)$ et continuité de $v \mapsto \sqrt{q(r(v))}$ que :

$$\forall \varepsilon > 0, \exists \alpha > 0,\ (q(y) \leq \alpha) \Rightarrow (\sqrt{q(r(y))} \leq \varepsilon\sqrt{q(y)})$$

3. Les amateurs remarquerons que q est donc une fonction de Liapounov pour (4.3.3).

Et donc sous ces conditions $2b(y, r(y)) \leq 2\varepsilon q(y)$.

L'espace $\mathbb{R}^n$ étant de dimension finie, les normes $\|.\|$ et $\sqrt{q}$ (q est définie positive) sont équivalentes et donc $\exists K > 0$, $Kq(y) \leq \|y\|^2$ d'où si on prend $\beta \leq K - 2\varepsilon$ et $q(y) \leq \alpha$:

$$\frac{d}{dt}q(y) \leq -\beta q(y)$$

Supposons à présent que $q(x) \leq \alpha$. Alors, pour tout $t \geq 0$, $q(y(t)) < \alpha$. En effet, dans le cas contraire, si on pose $t_0 := \inf\{t > 0 \,|\, q(y(t)) = \alpha\}$ on a :

$$(q \circ y)'(t_0) \leq -\beta q(y(t_0)) = -\beta\alpha < 0$$

Donc il existe un $t \leq t_0$ tel que $q(y(t)) < \alpha$, ce qui contredit la minimalité de t_0. Ainsi, on a bien :

$$\forall t \geq 0, \quad \frac{d}{dt}q(y(t)) \leq -\beta q(y(t))$$

Et donc :

$$\forall t \geq 0, \quad \frac{d}{dt}(e^{\beta t}q(y(t))) = e^{\beta t}((q \circ y)'(t) + \beta q(y(t))) \leq 0$$

La fonction $t \mapsto e^{\beta t}q(y(t))$ est donc décroissante sur $\mathbb{R}_+$ ce qui entraîne :

$$\forall t \geq 0, \quad e^{\beta t}q(y(t)) \leq e^{\beta \times 0}q(y(0)) = q(x)$$

D'où :

$$\forall t \geq 0, \quad q(y(t)) \leq e^{-\beta t}q(x)$$

D'où le résultat par équivalence entre $\|.\|$ et $\sqrt{q}$.

Détails supplémentaires :

- *Différentielle de q.* Soient $x, y \in \mathbb{R}^n$ et $t \in \mathbb{R}$. Alors :

$$q(x + ty) = q(x) + 2tb(x, y) + t^2q(y)$$

De fait :

$$\frac{d}{dt}(q(x + ty)) = 2b(x, y) + 2tq(y)$$

In fine [4] :

$$dq(x)(y) = \frac{d}{dt}(q(x + ty))\bigg|_{t=0} = 2b(x, y)$$

4.4 Théorème de Stone–Weierstrass

Référence :

- [QZ95], p. 342–345

Proposition 4.4 (Stone–Weierstrass)
Soit Ω un ouvert de $\mathbb{R}^n$.
Soit $K \subset\subset \Omega$.
Soit $f \in \mathcal{C}^0(\Omega, \mathbb{R})$.
Alors il existe une suite de polynômes [5] convergeant uniformément vers f sur K.

Démonstration : On munit $\mathbb{R}^n$ de sa norme euclidienne canonique $\|.\|$. Soit $\theta \in \mathcal{C}_c^\infty(\Omega)$ égale à 1 sur K. Dans toute la suite on considérera que la fonction θf est définie sur $\mathbb{R}^n$ entier en la prolongeant par 0, le prolongement restant clairement continu. Soit $K' := K - \mathrm{supp}(\theta)$. On considère l'application suivante :

$$\begin{aligned} \rho : \mathbb{R}^n &\to \mathbb{R} \\ x &\mapsto \frac{1}{\sqrt{\pi}^n}e^{-\|x\|^2} \end{aligned}$$

4. On peut retrouver "plus rapidement" ce résultat en se souvenant de l'expression de la différentielle d'une forme multilinéaire.
5. À n indéterminées.

Alors :

$$\begin{aligned}\int_{\mathbb{R}^n}\rho &= \frac{1}{\sqrt{\pi^n}}\int_{\mathbb{R}^n}\prod_{i=1}^n e^{-x_i^2}dx_1\dots dx_n\\ &= \frac{1}{\sqrt{\pi^n}}\int_{\mathbb{R}} e^{-x_1^2}\int_{\mathbb{R}} e^{-x_2^2}\dots\int_{\mathbb{R}} e^{-x_n^2}dx_n\dots dx_1 \text{ par Fubini}\\ &= \frac{1}{\sqrt{\pi^n}}(\sqrt{\pi})^n\\ &= 1\end{aligned}$$

Pour $m\in\mathbb{N}$ on définit également deux applications sur $\mathbb{R}^n$:

$$\rho_m : x\mapsto m^n\rho(mx) \text{ et } P_m : x\mapsto \frac{1}{\sqrt{\pi^n}}\sum_{j=0}^{m^3-1}\frac{(-1)^j\|x\|^{2j}}{j!}$$

Soient $z\in K'$ et $m\geq 0$. Alors :

$$\begin{aligned}m^{n+1}(\rho(mz)-P_m(mz)) &= \left(e^{-\|mz\|^2}-\sum_{j=0}^{m^3-1}\frac{(-1)^j\|mz\|^{2j}}{j!}\right)\\ &= \frac{m^{n+1}}{\sqrt{\pi^n}}\left(\sum_{j=0}^{\infty}\frac{(-1)^j m^{2j}\|z\|^{2j}}{j!}-\sum_{j=0}^{m^3-1}\frac{(-1)^j m^{2j}\|z\|^{2j}}{j!}\right)\\ &= \frac{m^{n+1}}{\sqrt{\pi^n}}\sum_{j=m^3}^{\infty}\frac{(-1)^j m^{2j}\|z\|^{2j}}{j!}\end{aligned}$$

Comme K' est compact (car K et $\operatorname{supp}\theta$ le sont), il est borné par un certain $R>0$. Ainsi :

$$\begin{aligned}m^{n+1}|\rho(mz)-P_m(mz)| &\leq \frac{m^{n+1}}{\sqrt{\pi^n}}\sum_{j=m^3}^{\infty}\frac{m^{2j}\|z\|^{2j}}{j!}\\ &\leq \frac{m^{n+1}}{\sqrt{\pi^n}}\sum_{j=m^3}^{\infty}\frac{(Rm)^{2j}}{j!}\\ &\leq \frac{1}{\sqrt{\pi^n}}\sum_{j=m^3}^{\infty}\frac{R^{2j}}{j!}j^{2j/3}j^{(n+1)/3} \text{ car } \forall j\geq m^3,\ m\leq j^{1/3}\\ &\leq \frac{1}{\sqrt{\pi^n}}\sum_{j=m^3}^{\infty}\frac{R^{2j}}{j!}j^{2j/3+(n+1)/3}\end{aligned}$$

Posons, pour $j\geq 0$, $\alpha_j := \dfrac{R^{2j}}{j!}j^{2/3+(n+1)/3}$. Alors :

$$\begin{aligned}\frac{\alpha_{j+1}}{\alpha_j} &= \frac{R^{2j+2}(j+1)^{2(j+1)/3+(n+1)/3}j!}{R^{2j}j^{2j/3+(n+1)/3}(j+1)!}\\ &= R^2\left(1+\frac{1}{j}\right)^{\frac{2}{3}j}\left(1+\frac{1}{j}\right)^{\frac{1}{3}(n+1)}\frac{1}{j+1}\\ &\xrightarrow[j\to\infty]{} 0 \text{ car } \left(1+\frac{1}{j}\right)^{\frac{2}{3}j} = e^{\frac{2}{3}j\ln\left(1+\frac{1}{j}\right)}\sim e^{\frac{2}{3}}\end{aligned}$$

Par règle de d'Alembert, la série $\sigma\alpha_j$ converge (absolument), donc son reste converge vers 0. De fait $m^{n+1}|\rho(mz)-P_m(mz)|\xrightarrow[m\to\infty]{} 0$ et donc il existe $m_0\in\mathbb{N}^*$ tel que :

$$\forall m\geq m_0,\ \forall z\in K',\quad m^{n+1}|\rho(mz)-P_m(mz)|\leq 1, \text{ donc } m^n|\rho(mz)-P_m(mz)|\leq\frac{1}{m}$$

In fine, par minimalité du supremum :

$$\forall m\geq m_0,\qquad \sup_{z\in K'}\left(m^n|\rho(mz)-P_m(mz)|\right)\leq\frac{1}{m} \tag{4.4.1}$$

Soient $m \geq m_0$ et $x \in K$. Alors :

$$\begin{aligned}
(\rho(m.) - P_m(m.)) * \theta f(x) &= \int_{\mathbb{R}^n} (\rho(m(x-y)) - P_m(m(x-y)))\theta(y)f(y)dy \\
&= \int_{\mathrm{supp}\theta} (\rho(m(x-y)) - P_m(m(x-y)))\theta(y)f(y)dy \\
&= \int_{K'} (\rho(my) - P_m(my))\theta(x-y)f(x-y)dy \text{ via } y \mapsto x-y \text{ et car } K' = K - \mathrm{supp}(\theta) \\
&= \int_{\mathbb{R}^n} (\rho(my) - P_m(my))1_{K'}(y)\theta(x-y)f(x-y)dy \\
&= (\rho(m.) - P_m(m.))1_{K'} * \theta f(x) \text{ par commutativité de la convolution}
\end{aligned}$$

De plus :

$$\begin{aligned}
m^n|(\rho(m.) - P_m(m.))1_{K'} * \theta f(x)| &\leq m^n \|(\rho(m.) - P_m(m.))1_{K'}\|_\infty \|\theta f\|_1 \\
&\leq \frac{1}{m}\|\theta f\|_1 \text{ par (4.4.1)}
\end{aligned}$$

Ergo :

$$\forall m \geq m_0, \qquad \sup_{x \in K}\left(m^n \left|\int_{\mathbb{R}^n} (\rho(m(x-y)) - P_m(m(x-y)))\theta(y)f(y)dy\right|\right) \leq \frac{1}{m}\|\theta f\|_1 \tag{4.4.2}$$

On fixe à nouveau $m \geq m_0$ et $x \in K$. On a :

$$\begin{aligned}
\rho_m * \theta f(x) - f(x) &= \int_{\mathbb{R}^n} m^n \rho(mz)\theta(x-z)f(x-z)dz - f(x) \\
&= \int_{\mathbb{R}^n} \rho(z)\theta\left(x - \frac{z}{m}\right) f\left(x - \frac{z}{m}\right) dz - f(x) \text{ via le changement de variable} z \mapsto \frac{z}{m} \text{ de jacobien } \frac{1}{m} \\
&= \int_{\mathbb{R}^n} \rho(z)(\theta f)\left(x - \frac{z}{m}\right) dz - \int_{\mathbb{R}^n} \rho(z)\theta(x)f(x)dz \text{ car } \int_{\mathbb{R}^n} \rho = 1 \text{ et } \theta(x) = 1 \\
&= \int_{\mathbb{R}^n} \rho(z)\left((\theta f)\left(x - \frac{z}{m}\right) - (\theta f)(x)\right) dz
\end{aligned}$$

Soit $\varepsilon > 0$ et soit $R_0 > 0$ choisi tel que :

$$\frac{1}{\sqrt{\pi^n}} e^{-\frac{1}{2}R_0^2}\left(\int_{\mathbb{R}^n} e^{-\frac{1}{2}\|y\|^2}dy\right) 2\sup_{x \in \Omega}|\theta f| \leq \frac{\varepsilon}{4}$$

Notez que $\sup_{x \in \Omega}|\theta f| = \sup_{x \in \mathbb{R}^n}|\theta f|$. Alors :

–

$$\begin{aligned}
\left|\int_{\|z\| \geq R_0} \rho(z)\left((\theta f)\left(x - \frac{z}{m}\right) - (\theta f)(x)\right) dz\right| &\leq 2\sup_{x \in \Omega}|\theta f| \int_{\|z\| \geq R_0} \frac{1}{\sqrt{\pi^n}} e^{-\|z\|^2}dz \\
&= 2\sup_{x \in \Omega}|\theta f| \int_{\|z\| \geq R_0} \frac{1}{\sqrt{\pi^n}} e^{-\frac{1}{2}\|z\|^2} e^{-\frac{1}{2}\|z\|^2}dz \\
&\leq e^{-\frac{1}{2}R_0^2} 2\sup_{x \in \Omega}|\theta f| \int_{\mathbb{R}^n} \frac{1}{\sqrt{\pi^n}} e^{-\frac{1}{2}\|z\|^2}dz \\
&\leq \frac{\varepsilon}{4}
\end{aligned}$$

– θf est continue à support compact donc uniformément continue (théorème de Heine). De fait, il existe $\delta > 0$ tel que pour tous $x, x' \in \mathrm{supp}(\theta)$ tels que $\|x - x\|' \leq \delta$ alors $|\theta f(x) - \theta f(x')| \leq \frac{\varepsilon}{4}$. Ainsi, si $m \in \mathbb{N}$ est tel que $\frac{R_0}{m} \leq \delta$ on a :

$$\forall z \in \overline{\mathcal{B}}(0, R_0), \qquad \left\|\left(x - \frac{z}{m}\right) - x\right\| = \frac{\|z\|}{m} \leq \delta$$

Ergo :

$$\begin{aligned}\left|\int_{\|z\|\le R_0}\rho(z)\left((\theta f)\left(x-\frac{z}{m}\right)-(\theta f)(x)\right)dz\right| &\le \frac{1}{\sqrt{\pi^n}}\int_{\|z\|\le R_0}e^{-\|z\|^2}\left|\theta f\left(x-\frac{z}{m}\right)-\theta f(x)\right|dz\\ &\le \frac{\varepsilon}{4}\frac{1}{\sqrt{\pi^n}}\int_{\|z\|\le R_0}e^{-\|z\|^2}dz\\ &\le \frac{\varepsilon}{4}\end{aligned}$$

In fine, si on pose $m_1 := \lfloor \frac{R_0}{\delta} \rfloor$ on a :

$$\forall m\ge m_1,\qquad \sup_{x\in K}|\rho_m*\theta f(x)-f(x)|\le\frac{\varepsilon}{2} \tag{4.4.3}$$

Ainsi, en combinant (4.4.2) et (4.4.3) on obtient que :

$$\begin{aligned}\forall m\ge\max(m_0,m_1),\quad \sup_{x\in K}|m^nP(m.)*\theta f(x)-f(x)| &\le \sup_{x\in K}|m^n(\rho(m.)-P(m.))*\theta f(x)|+\sup_{x\in K}|\rho_m*\theta f(x)-f(x)|\\ &\le \frac{1}{m}\|\theta f\|_1+\frac{\varepsilon}{2}\end{aligned}$$

Et donc la suite de polynômes $(Q_m)_m := (m^nP_m(m.)*\theta f)_m$ converge uniformément vers f sur K.

Détails supplémentaires :

– *La convolée d'un polynôme avec une fonction intégrable est un polynôme.* Nous nous contenterons [6] ici de la preuve en dimension 1. Si $f\in L^1(K)$ (avec $K\subset\subset\mathbb{R}$) et $P := \sum_{k=0}^d a_kX^k\in\mathbb{R}[X]$ alors :

$$\begin{aligned}\forall x\in\mathbb{R},\quad P*f(x) &= \int_K\sum_{k=0}^d a_k(x-y)^kf(y)dy\\ &= \int_K\sum_{k=0}^d a_k\sum_{j=0}^k C_k^jx^jy^{k-j}f(y)dy\\ &= \sum_{k=0}^d a_k\sum_{j=0}^k C_k^j\left(\int_K y^{k-j}f(y)dy\right)x^j\\ &= \sum_{j=0}^d\sum_{k=j}^d a_kC_k^j\left(\int_K y^{k-j}f(y)dy\right)x^j\end{aligned}$$

D'où le résultat.

4.5 Théorème de Sylow

Référence :

– [Per96] ; p. 18–20

Soit G un groupe fini de cardinal $n\ge1$. On suppose qu'il existe un nombre premier p et deux entiers $\alpha, m\ge1$ tels que $n=p^\alpha m$, avec $p\nmid m$.

Lemme 4.2
Soit $H\le G$.
Soit S un p–Sylow de G.
Alors il existe $a\in G$ tel que $H_a := aSa^{-1}\cap H$ soit un p–Sylow de H.

6. Les amateurs de multi–indices trouverons certainement très distrayant d'écrire ces calculs en dimension quelconque. Penser toutefois à remplacer $P\in\mathbb{R}[X]$ par $\mathbb{R}[X_1,\dots,X_n]$.

Démonstration : G agit sur G/S par translation à gauche et :

$$\begin{aligned}\forall a, g \in G,\ g.(aS) = as &\Leftrightarrow \forall s \in S,\ \exists s' \in S,\ gas = as' \\ &\Leftrightarrow \forall s \in S,\ \exists s' \in S,\ g = as's^{-1}a^{-1} \\ &\Leftrightarrow g \in aSa^{-1}\end{aligned}$$

On a donc $\forall a, g \in G$, $\mathrm{Stab}_G(aS) = aSa^{-1}$. Or H agit sur G/S par restriction et $\mathrm{Stab}_H(aS) = \mathrm{Stab}_G(aS) \cap H = H_a$ est un sous–groupe de $\mathrm{Stab}_G(aS)$, d'où $|H_a| \,|\, |aSa^{-1}| = |S| = p^\alpha$. De fait, par primalité, $p \,|\, |H_a|$.
Or $|H_a| = \dfrac{|H|}{(H : H_a)}$ donc il nous suffit de trouver $a \in G$ tel que $(H : H_a) \wedge p = 1$.

Si on note $\omega(aS)$ l'orbite d'un élément aS de G/S sous l'action de H, l'application $g \mapsto g.aS$ et la propriété universelle du quotient nous indiquent que $(H : H_a) = |H/H_a| = |\omega(aS)|$. De fait, si p divisait tous les indices $(H : H_a)$, on aurait par la formule des classes que p divise $m = |G/S|$, ce qui est impossible, d'où le résultat.

Proposition 4.5 (Sylow)
On note $c_p \geq 0$ le nombre de p–Sylow de G.
Alors :

(i) pour tout p-groupe $H \leq G$, il existe un p–Sylow de G contenant H (et donc $c_p \geq 1$) ;
(ii) les p–Sylow de G sont tous conjugués (et donc $c_p | n$), en particulier si S est un p–Sylow de G et si $S \lhd G$ alors S est l'unique p–Sylow de G ;
(iii) $c_p \equiv 1[p]$ (et donc $c_p | m$).

Démonstration :

(i) On a l'injection suivante (où $(e_1, \ldots, e_n)$ désigne la base canonique de $\mathbb{F}_p^n$) :

$$\begin{aligned}\mathfrak{S}_n &\hookrightarrow GL_n(\mathbb{F}_p) \\ \sigma &\mapsto (u_\sigma : e_i \mapsto e_{\sigma(i)})\end{aligned}$$

Ainsi, d'après le théorème de Cayley (proposition 4.6) et la propriété universelle du quotient, on peut identifier G à un sous groupe de $GL_n(\mathbb{F}_p)$. Or $GL_n(\mathbb{F}_p)$ possède un p–Sylow (les matrices triangulaires supérieures "strictes", cf. infra) donc d'après le lemme 4.2, G aussi : notons le S.

Toujours d'après le lemme 4.2, comme H est un sous–groupe de G, il existe $a \in G$ tel que H_a soit un p–Sylow de H. Or H est également un p–groupe et donc son unique p–Sylow est lui–même, ergo $H_a = H$, ce qui implique que $H \subset aSa^{-1}$, qui est un p–Sylow [7].

(ii) On procède comme pour le point (i) en imposant à H d'être un p–Sylow. On obtient bien alors que pour tout p–Sylow S de G, il existe $a \in G$ tel que $H \subset aSa^{-1}$. Or $|H| = p^\alpha = |S| = |aSa^{-1}|$ donc $H = aSa^{-1}$ est conjugué à S.

(iii) Notons X l'ensemble des p–Sylow de G. On sait que G agit sur X par conjugaison et si $S \in X$, cette action en induit une de S sur X. D'après le lemme 4.3 on a donc $|X| \equiv |X^S|[p]$. Il est de plus clair que $S \in X^S$.

Soit $T \in X^S$, i.e $\forall s \in S$, $sTs^{-1} = T$. On considère le sous–groupe N de G engendré par S et T ; alors $S \leq N$ et $T \leq N$ sont deux p–Sylow de N. Cependant il est clair que $T \lhd N$ et donc par le point (ii) $T = S$. In fine $X^S = \{S\}$ et donc $c_p = |X| \equiv 1[p]$.

Détails supplémentaires :

– *$GL_n(\mathbb{F}_p)$ admet un p-Sylow* (cf. [Per96], p.15). Commençons par remarquer que :

$$\forall A \in \mathcal{M}_n(\mathbb{F}_p), \quad A \in GL_n(\mathbb{F}_p) \Leftrightarrow (Ae_1, \ldots, Ae_n) \text{ est une base de } \mathbb{F}_p^n$$

$GL_n(\mathbb{F}_p)$ est de facto équipotent à l'ensemble des bases de $\mathbb{F}_p^n$. Or pour se donner une telle base $(a_1, \ldots, a_n)$, on dispose de $p^n - 1$ choix pour a_1 (on choisit $a_1 \in \mathbb{F}_p^n \setminus \{0\}$, de $p^n - p$ choix pour a_2 (on choisit $a_2 \notin \langle a_1 \rangle$) et de manière générale de $p^n - p^{i-1}$ choix pour a_i, $i \in [n]$ (on choisit $a_i \notin \langle a_1, \ldots, a_{i-1} \rangle$). In fine :

$$|GL_n(\mathbb{F}_p)| = \prod_{k=0}^{n-1} (p^n - p^k)$$

7. La conjugaison conservant les cardinaux, le conjugué d'un p–Sylow est un p–Sylow de G.

On a donc $|GL_n(\mathbb{F}_p)| = p^{n(n-1)/2}m$, avec $p \nmid m$. On considère alors le sous–groupe de $GL_n(\mathbb{F}_p)$ constitué des matrices triangulaires supérieures "strictes" :

$$P := \{A \in GL_n(\mathbb{F}_p) \,|\, \forall i,j \in [n],\ a_{i,j} = 0 \text{ si } i > j,\ a_{i,i} = n\} \leq GL_n(\mathbb{F}_p)$$

Alors $|P| = p^{n(n-1)/2}$ (on "choisit" exactement $\frac{n(n-1)}{2}$ coefficients de chaque matrice) donc P est un p–Sylow de $GL_n(\mathbb{F}_p)$.

- On trouve le résultat suivant dans [Per96], p.15 :

Proposition 4.6 (Cayley)
Soit G un groupe fini de cardinal $n \geq 1$.
Alors G est isomorphe à un sous–groupe de $\mathfrak{S}_n$.
Démonstration : G agit sur lui–même par translation à gauche donc il existe un morphisme de groupes de G dans $\mathfrak{S}(G) \cong \mathfrak{S}_n$. Ce morphisme est de plus injectif car si $g,h \in G$ $(\forall x \in G,\ g.x = h.x) \Rightarrow (g = h)$. On conclut par propriété universelle du quotient.

- Le lemme suivant est démontré dans [Per96], p.17 :

Lemme 4.3
Soit G un p–groupe.
Soit X un G–ensemble fini.
Alors :

$$|X| \equiv |X^G| [p]$$

Démonstration : D'après la formule des classes :

$$|X| = |X^G| + \sum |\omega(x)|$$

Où la somme compte une fois chaque orbite non triviale. De fait, chacun de ces $|\omega(x)|$ est strictement supérieur à 1 et divise $|G|$ donc $p||\omega(x)|$, d'où le résultat.

- *Une application classique : il n'existe pas de groupe simple d'ordre 63.* Soit G un groupe d'ordre $63 = 3^2 \times 7$. Alors $c_7 \equiv 1[7]$ et $c_7|9$ donc $c_7 = 1$: G admet un unique 7–Sylow qui est donc distingué.

4.6 Théorème de Tietze

Référence :
- [QZ95], p. 198–199

Lemme 4.4 ([QZ95], p. 197)
Soient E, F deux espaces de Banach.
Soit $T \in \mathcal{L}_c(E,F)$.
On suppose que T est presque surjective, i.e qu'il existe $\alpha \in (0,1)$ et $C > 0$ tels que :

$$\forall y \in \overline{\mathcal{B}}_F(0,1),\ \exists x \in \overline{\mathcal{B}}_E(0,C), \quad \|y - T(x)\| \leq \alpha$$

Alors T est surjectif. Plus précisément :

$$\forall y \in \overline{\mathcal{B}}_F(0,1),\ \exists x \in \overline{\mathcal{B}}_E\left(0, \frac{C}{1-\alpha}\right), \quad y = T(x)$$

Démonstration : Soit $y \in \overline{\mathcal{B}}_F(0,1)$. On construit par récurrence sur $n \geq 1$ une suite $(x_n)_{n\geq 1}$ telle que :

$$\forall n \geq 1, \qquad x_n \in \overline{\mathcal{B}}_E(0,C) \text{ et } \left\| y - \sum_{i=1}^{n} \alpha^{i-1} T(x_i) \right\| \leq \alpha^n$$

- $n = 1$. Découle de la presque surjectivité.
- Supposons la suite construite jusqu'au rang $n \geq 1$. Alors $\frac{y - \sum_{i=1}^n \alpha^{i-1} T(x_i)}{\alpha^n} \in \overline{\mathcal{B}}_F(0,1)$ donc il existe $x_{n+1} \in \overline{\mathcal{B}}_E(0,C)$ tel que $\left\| \frac{y - \sum_{i=1}^n \alpha^{i-1} T(x_i)}{\alpha^n} - T(x_{n+1}) \right\| \leq \alpha$ et donc :

$$\left\| y - \sum_{i=1}^{n+1} \alpha^{i-1} T(x_i) \right\| \leq \alpha^{n+1}$$

D'où le résultat.

De plus, pour tout $n \geq$, $\|\alpha^{n-1}x_n\| \leq \alpha^{n-1}C$. Comme $0 < \alpha < 1$, la série $\sigma\alpha^{n-1}x_n$ converge alors absolument (série géométrique) donc converge car E est un espace de Banach. On peut donc poser $x := \sum_{n=1}^{\infty} \alpha^{n-1}x_n \in E$ et alors :

$$\|x\| \leq \sum_{n=1}^{\infty} \alpha^{n-1}\|x_n\| \leq C\sum_{n=1}^{\infty} \alpha^{n-1} = \frac{C}{1-\alpha}$$

Et, si $N \geq 1$:

$$\left\| y - T\left(\sum_{n=1}^{N} \alpha^{n-1}x_n\right)\right\| \leq \alpha^N \xrightarrow[N\to\infty]{} 0$$

Donc, par continuité de T :

$$\|y - T(x)\| = \lim_{N\to\infty} \left\| y - T\left(\sum_{n=1}^{N} \alpha^{n-1}x_n\right)\right\| = 0$$

Proposition 4.7 (Tietze)
Soit (X, d) un espace métrique.
Soit $Y \subset X$ un fermé.
Soit $g_0 \in \mathcal{C}^0(Y, \mathbb{R})$.
Alors g_0 admet un prolongement continu f_0 à X.

Démonstration : On définit un opérateur $T \in \mathcal{L}_c(\mathcal{C}_b^0(X, \mathbb{R}), \mathcal{C}_b^0(y, \mathbb{R}))$ comme suit :

$$T : f \mapsto f_{|_Y}$$

Soit $g \in \mathcal{C}_b^0(Y, \mathbb{R})$ telle que $\|g\|_\infty \leq 1$ (i.e g comprise entre -1 et 1). On pose :

$$Y^+ := \left\{x \in Y \,\middle|\, \frac{1}{3} \leq g(x) \leq 1\right\} \text{ et } Y^- := \left\{x \in Y \,\middle|\, -1 \leq g(x) \leq -\frac{1}{3}\right\}$$

On définit alors une application $f \in \mathcal{C}_b^0(X, \mathbb{R})$ de la façon suivante :

$$f : x \mapsto \frac{1}{3}\frac{d(x, Y^-) - d(x, Y^+)}{d(x, Y^-) + d(x, Y^+)}$$

Il est clair $(d(x, Y^-) - d(x, Y^+) \leq d(x, Y^-) + d(x, Y^+))$ que $\|f\|_\infty \leq 1$. On distingue alors, pour $x \in Y$, 3 cas.

- *Cas 1 :* $x \in Y^+$. Alors $g(x) - f(x) = g(x) - \frac{1}{3} \in \left[0, \frac{2}{3}\right]$.
- *Cas 2 :* $x \in Y^-$. Alors $g(x) - f(x) = g(x) + \frac{1}{3} \in \left[-\frac{2}{3}, 0\right]$.
- *Cas 3 :* $\neg$*(cas 1* $\vee$ *cas 2).* Alors $|g(x) - f(x)| \leq |g(x)| + |f(x)| \leq \frac{1}{3} + \frac{1}{3} = \frac{2}{3}$.

In fine, on a bien $\|T(f) - g\|_\infty \leq \frac{2}{3}$: T est presque surjectif avec $\alpha = \frac{1}{3}$ et $C = \frac{2}{3}$.

D'après le lemme 4.4, pour tout g dans la boule unité fermée de $(\mathcal{C}_b^0(Y, \mathbb{R}), \|.\|_\infty$ il existe $f \in \mathcal{C}_b^0(X, \mathbb{R})$ de norme inférieure ou égale à $\frac{2/3}{1-1/3} = 1$ telle que $g = f_{|_Y}$, i.e g admet un prolongement continu à X de norme inférieure ou égale à 1.

Soit à présent g dans la boule unité *ouverte* de $(\mathcal{C}_b^0(Y, \mathbb{R}), \|.\|_\infty$. On vient de montrer que g admet un prolongement h dans la boule unité de $(\mathcal{C}_b^0(X, \mathbb{R}), \|.\|_\infty$ et on souhaite montrer qu'il existe h dans la boule unité *ouverte* de $(\mathcal{C}_b^0(X, \mathbb{R}), \|.\|_\infty)$ tel que $g = f_{|_Y}$.

- Si $\|h\|_\infty < 1$, $f := h$ convient.
- Sinon, on pose $Z := \{x \in X \mid |h(x)| = 1\}$. Par hypothèse, $\overline{Y \cap Z} = Y \cap Z = \emptyset$ donc on peut poser :

$$u : X \to \mathbb{R}_+$$
$$x \mapsto \frac{d(x, z)}{d(x, y) + d(x, z)}$$

  Posons $f := u \times h$. Alors :
  * si $x \in Y$, $f(x) = 1 \times g(x) = g(x)$;
  * sinon, $|u(x)| \leq 1$ donc $|f(x)| \leq 1$ et si $|h(x)| = 1$ alors $u(x) = 0$ donc $f(x)0$.
  De fait, $\|f\|_\infty\| < 1$ et $g = f_{|_Y}$.

Enfin, soit ϕ un homéomorphisme de $\mathbb{R}$ sur $(-1, 1)$ (par exemple $u \mapsto \frac{2}{\pi}\arctan(u)$). On vient de montrer que l'on peut prolonger $g := \phi \circ g_0$ en $f : X \mapsto (-1, 1)$: de fait, $f_0 := \phi^{-1} \circ f$ convient.

Notations

On a fait usage dans le présent document des notations suivantes :

- $\diamond$ $[n]$ désigne l'ensemble $\{1, \ldots, n\}$ pour $n \in \mathbb{N}^*$;
- $\diamond$ $|A|$ désigne le cardinal d'un ensemble fini A ;
- $\diamond$ $K \subset\subset E$ signifie que l'ensemble K est une partie compacte de l'espace topologique E ou à l'occasion –cela sera précisé– un compact inclus dans une partie E d'un espace topologique F ;
- $\diamond$ Q — ou $Q(E)$ — (respectivement Q_+, Q_{++}) désigne l'ensemble des formes quadratiques (resp. positives, définies positives) sur un espace vectoriel donné E ;
- $\diamond$ si $P \in \mathbb{A}[X]$ (avec $\mathbb{A}$ un anneau), on note $c(P)$ le contenu de P, i.e le pgcd (s'il existe) de ses coefficients ;
- $\diamond$ si $\mathbb{K}$ est un corps, on note $\mu_n(\mathbb{K})$ (resp. $\mu_n^*(\mathbb{K})$) l'ensemble des racines (resp. des racines primitives) de l'unité sur $\mathbb{K}$;
- $\diamond$ si E est un espace topologique et si $x \in E$, on note $\mathcal{V}_E(x)$ l'ensemble des voisinages de x dans E ;
- $\diamond$ si $(\Omega, \mathcal{A})$ est un espace mesurable, on note $m(\mathcal{A})$ l'ensemble des fonctions $\mathcal{A}$–mesurables sur Ω ;
- $\diamond$ si X et Y sont deux variables aléatoires indépendantes, on notera $X \perp Y$;
- $\diamond$ il nous arrivera d'utiliser la notation $x \wedge y$ (resp. $x \vee y$) pour l'objet $\inf(x, y)$ (resp. $\sup(x, y)$) ou $\mathrm{pgcd}(x, y)$ (resp. $\mathrm{ppcm}(x, y)$), selon les circonstances ;
- $\diamond$ si E est un espace métrique et $(x, r) \in E \times \mathbb{R}_+$ on notera $\mathcal{B}(x, r)$ (resp. $\overline{\mathcal{B}}(x, r)$) la boule ouverte (resp. fermée) de centre x et de rayon r, en particularisant au besoin en écrivant "$\mathcal{B}_E(x, r)$" ;
- $\diamond$ si Ω est un ouvert du plan complexe, on note $\mathcal{H}(\Omega)$ l'anneau des fonctions holomorphes de Ω dans $\mathbb{C}$;
- $\diamond$ selon les circonstances, la notation $\langle A \rangle$ désignera le sous–groupe ou le s-e.v engendré par l'ensemble A dans un certain groupe ou e.v. Dans ce dernier cas on pourra particulariser le corps de base $\mathbb{K}$ en notant $\langle A \rangle_{\mathbb{K}}$;
- $\diamond$ si $a, b, c, d \in \mathbb{P}^1(\mathbb{C})$, on notera $[a, b, c, d]$ le birapport de ce quadruplet, à savoir l'image de d par l'unique homographie envoyant a à l'infini, b sur 0 et c sur 1 ;
- $\diamond$ si $\mathbb{A}$ est un anneau, on notera $\mathbb{A}^\times$ (resp. $\mathbb{A}^*$) l'ensemble des inversibles de $\mathbb{A}$ (resp. $\mathbb{A} \setminus \{0\}$).

Bibliographie

[Ale99] Michel Alessandri. *Thèmes de géométrie.* Dunod, 1999.

[Art91] Michael Artin. *Algebra.* Prentice-Hall, 1991.

[BMP05] Vincent Beck, Jérôme Malick, and Gabriel Peyré. *Objectif Agrégation (2e édition).* H & K, 2005.

[Bre05] Haim Brezis. *Analyse fonctionelle.* Dunod, 2005.

[Car89] Jean-Claude Carrega. *Théorie des corps : la règle et le compas.* Hermann, 1989.

[FG97] Serge Francinou and Hervé Gianella. *Exercices de mathématiques pour l'agrégation, Algèbre 1.* Masson, 1997.

[FGN07] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X - ENS, Algèbre 1 (2e édition).* Cassini, 2007.

[FGN09a] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X - ENS, Algèbre 2 (2e édition).* Cassini, 2009.

[FGN09b] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X - ENS, Analyse 2 (2e édition).* Cassini, 2009.

[FGN10] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X - ENS, Algèbre 3.* Cassini, 2010.

[FGN12] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X - ENS, Analyse 4.* Cassini, 2012.

[Gou94] Xavier Gourdon. *Algèbre.* Ellipses, 1994.

[Gou08] Xavier Gourdon. *Analyse (2e édition).* Ellipses, 2008.

[GT96] Stéphane Gonnord and Nicolas Tosel. *Topologie et analyse fonctionnelle.* Ellipses, 1996.

[GT98] Stéphane Gonnord and Nicolas Tosel. *Calcul différentiel.* Ellipses, 1998.

[HU98] Jean-Baptiste Hiriart-Urruty. *Optimisation et analyse convexe.* Presses Universitaires de France, 1998.

[Les01] Emmanuel Lesigne. *Pile ou face.* Ellipses, 2001.

[MT97] Rached Mneimné and Frédéric Testard. *Introduction à la théorie des groupes de Lie classiques.* Hermann, 1997.

[Mé06] Jean-Yves Mérindol. *Nombres et algèbre.* EDP Sciences, 2006.

[Ouv00] Jean-Yves Ouvrard. *Probabilités 2.* Cassini, 2000.

[Per96] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.

[Pey04] Gabriel Peyré. *L'algèbre discrète de la transformée de Fourier.* Ellipses, 2004.

[QZ95] Hervé Queffélec and Claude Zuily. *Éléments d'analyse pour l'agrégation.* Masson, 1995.

[QZ07] Hervé Queffélec and Claude Zuily. *Éléments d'analyse pour l'agrégation (3e édition).* Dunod, 2007.

[Rou09] François Rouvière. *Petit guide du calcul différentiel à l'usage de la licence et de l'agrégation (3e édition).* Cassini, 2009.

[Rud98] Walter Rudin. *Analyse réelle et complexe (3e édition).* Dunod, 1998.

[Ser95] Jean-Pierre Serre. *Cours d'arithmétique.* Presses Universitaires de France, 1995.

[Ser98] Jean-Pierre Serre. *Représentations linéaires des groupes finis.* Hermann, 1998.

[SP99] Philippe Saux-Picart. *Cours de calcul formel : algorithmes fondamentaux.* Ellipses, 1999.

[Szp09] Aviva Szpirglas. *Mathématiques L3.* Pearson Education, 2009.

[Zui02] Claude Zuily. *Éléments de distribution et d'équations aux dérivées partielles.* Dunod, 2002.