Développements agrégation 2011

Sylvain Courte

Table des matières

1 Billard convexe

Ref : Rouvière largement modifié

THÉORÈME 1.1 *Soit Γ une courbe $\mathcal{C}^1$ du plan affine euclidien E, difféomorphe à un cercle et délimitant un domaine convexe. On peut réaliser le triangle comme trajectoire de billard dans D. (Autrement dit, il existe une trajectoire de billard fermée à trois rebonds).*

PREUVE.

Résumé : On va obtenir cette trajectoire de billard en cherchant le triangle inscrit de périmètre maximal qui existe par compacité. Avec le théorème des extrema liés, on montrera qu'un tel triangle maximal est nécessairement une trajectoire de billard.

Du point de vue du calcul différentiel, E est simplement $\mathbb{R}^2$. Mais on n'aura pas besoin de faire le choix d'un repère orthonormé pour les identifier en tant qu'espace affine euclidien.

Soit $f : \Gamma^3 \subset \mathbb{E}^3 \to \mathbb{R}$ la fonction périmètre définie par :

$$f(A, B, C) = AB + BC + CA$$

Comme Γ est compact ainsi que Γ^3 par Tychonoff (version triviale), et f est continue, f est majorée et atteint son maximum en un triplet (A, B, C). Ce triplet maximal est formé de points distincts car par inégalité triangulaire si $A = B$ par exemple, alors $AC + AC < AC + AM + MC$ dès que M n'est pas sur le segment $[A, C]$. (faire un dessin).

Γ^3 est une sous-variété $\mathcal{C}^1$ de E^3 car c'est un produit de sous-variétés $\mathbb{C}^1$ de E. La fonction f est $\mathbb{C}^\infty$ sur l'ouvert des triplets de points deux à deux distincts car c'est la restriction à une sous-variété d'une fonction $\mathbb{C}^\infty$ sur E^3. Le triplet (A, B, C) est dans cet ouvert donc (par le théorème des extrema liés) $\mathrm{d}f_{(A,B,C)}$ est nulle sur l'espace tangent à Γ^3 en (A, B, C). Regardons ce que cela signifie :

Quand B et C sont fixés, en posant $g(A) = f(A, B, C) = AB + BC + CA$. On a pour u vecteur tangent à Γ en A :

$$\mathrm{d}g_A(u) = < \frac{\vec{BA}}{BA} + \frac{\vec{CA}}{CA}, u >$$

Mais on a aussi :

$$\mathrm{d}g_A(u) = \mathrm{d}f_{(A,B,C)}(u, 0, 0) = 0$$

car $(u, 0, 0)$ est tangent à Γ^3 au point (A, B, C).

Ainsi $\frac{\vec{BA}}{BA} + \frac{\vec{CA}}{CA}$ est orthogonal à Γ, et c'est justement dire que c'est une réflexion sur un billard selon la loi de Descartes. (faire un dessin)

Le même raisonnement est valable aussi pour B et C, donc le triangle ABC est une trajectoire de billard à l'intérieur de Γ.

□

Remarques :

1. Ici courbe désigne "sous-variété de dimension 1".
2. En particulier c'est vrai pour un cercle, une ellipse, un polygônes avec les coins arrondis.
3. Le même raisonnement marche pour un polygones à n côtés. Mais rien n'assure que ce polygone n'est pas aplati (penser à un diamètre sur un disque qui réalise des trajectoires de périmètre maximal pour un nombre pair de côtés)

Leçons concernées : problème d'extremum, sous-variétés, application différentiables, problème d'angle et de distance, compacité.

2 Image de l'exponentielle

ref : exercice sur la page web de Denis Serre.

Théorème 2.1

$\exp : \mathcal{M}(n,\mathbb{C}) \to GL(n,\mathbb{C})$ *est surjective, non injective.*

$\exp(\mathcal{M}(n,\mathbb{R}))$ *est l'ensemble des carrés de matrices réelles.*

Preuve.

Non injectivité :

$\exp(2i\pi I_n) = \exp(0) = I_n$, donc exp n'est pas injective.

Surjectivité sur $\mathbb{C}$ *:*

idée : On veut faire une preuve par calcul différentiel en utilisant la connexité de $\mathrm{GL}(n,\mathbb{C})$*. Il est immédiat que* exp *est ouverte en* 0 *par inversion locale étant donné que* $\mathrm{d}\exp_0 = \mathrm{id}$*. On ne peut pas conclure de même aux autres points directement par propriété de groupes car* exp *n'est pas un morphisme de groupes. On peut faire marcher cette idée quand même car* exp *est un morphisme en restriction à de gros sous-espaces : les algèbres de polynômes en des matrices.*

Soit $A \in \mathcal{M}(n,\mathbb{C})$, l'algèbre des polynômes en A notée $\mathbb{C}[A]$ est en particulier un groupe additif. L'exponentielle est un morphisme de $\mathbb{C}[A]$ dans $\mathbb{C}[A]^* = \mathrm{GL}(n,\mathbb{C}) \cap \mathbb{C}[A]$. En effet, $\exp(M)$ est un polynôme en M car c'est une limite de polynômes en M lequel sous-espace vectoriel est fermé car $\mathcal{M}(n,\mathbb{C})$ est dimension finie.

$\mathrm{GL}(n,\mathbb{C})$ étant ouvert, son intersection avec $\mathbb{C}[A]$ est un ouvert de $\mathbb{C}[A]$. C'est aussi un connexe par la même preuve que pour la connexité de $\mathrm{GL}(n,\mathbb{C})$. Si M, N sont deux matrices le chemin $tM + (1-t)N$ rencontre peut-être des matrices non inversibles pour $t \in [0,1]$ mais si on passe par des t complexes, il n'y a plus de problème car on doit simplement éviter un nombre fini de valeurs vu que $\det(xM + (1-x)N)$ est un polynôme en x qui n'a donc qu'un nombre fini de racines.

L'application $\exp : \mathbb{C}[A] \to \mathbb{C}[A]^*$ est un morphisme de groupes et sa différentielle en 0 est l'identité, donc par inversion local elle est ouverte en 0. Par propriété de groupes, elle est alors ouverte en tous les points ; la translation dans $\mathbb{C}[A]$ et la multiplication dans $\mathbb{C}[A]^*$ étant des difféomorphismes. Toujours par propriété de groupes, l'image est fermée car ouverte (partition en les classes à gauche modulo le sous-groupe). Par connexité, c'est tout $\mathbb{C}[A]^*$, et cela montre donc que tout $B \in \mathrm{GL}(n,\mathbb{C})$ s'écrit $B = \exp(P(B))$ pour un $P \in \mathbb{C}[X]$.

Cas réel :

Pour le résultat réel, on remarque que $\exp(M/2)^2 = \exp(M)$ pour une inclusion. L'autre inclusion est conséquence du cas complexe en utilisant la conjugaison : pour $B \in GL(n,\mathbb{R})$,

$$B^2 = B\overline{B} = \exp(P(B))\exp(\overline{P}(\overline{B})) = \exp(P(B) + \overline{P}(B))$$

car $P(B)$ et $\overline{P}(B)$ commutent. □

Leçons concernées : exponentielle de matrices, polynômes d'endomorphismes, connexité, inversion locale, groupe linéaire.

3 Théorème de Hadamard

ref : Maison

THÉORÈME 3.1 (HADAMARD) *Soit $f : \tilde{M} \to M$ une application de classe $\mathcal{C}^2$ avec $\tilde{M} = M = \mathbb{R}^n$ munis de la norme euclidienne. On suppose qu'il existe $k > 0$ tel que :*

$$\forall x \in \tilde{M}, \forall v \ \in \mathbb{R}^n, \|\mathrm{d}f_x(v)\| \geq k\|v\|$$

Alors f est un $\mathcal{C}^2$-difféomorphisme global.

PREUVE. *Propriétés locales :*

La condition sur f implique en particulier que $\mathrm{d}f_x$ est injective donc est un isomorphisme (dim finie) en chaque point x. En effet,

$$\mathrm{d}f_x(v) = 0 \Rightarrow k\|v\| = 0 \Rightarrow v = 0 \text{ car } k \neq 0$$

Comme f est de classe $\mathcal{C}^1$, le théorème d'inversion locale montre que f est un difféomorphisme local. Il reste à montrer que f est injective et surjective pour avoir un difféomorphisme global de $\tilde{M}$ sur M.

On fixe un point x_0 dans M et on introduit sur M le champ de vecteur radial rentrant : $X(x) = -\vec{x_0x}$. C'est un champ linéaire autonome. Son flot φ^t est défini pour tout temps et on a :

$$\forall x \in M, \forall t \in \mathbb{R}, \quad \varphi^t(x) = x_0 + e^{-t}(x - x_0)$$

Comme f est un difféomorphisme local, on peut relever le champ X en un champ $\tilde{X}$ sur $\tilde{M}$ par la formule suivante :

$$\forall \tilde{x} \in \tilde{M}, \quad \tilde{X}(\tilde{x}) = (\mathrm{d}f_{\tilde{x}})^{-1}(X(f(\tilde{x})))$$

(C'est l'unique formule raisonnable que l'on peut écrire)

Le champ $\tilde{X}$ est moins régulier que X, il est seulement $\mathcal{C}^1$ car f est $\mathcal{C}^2$. L'existence et l'unicité locale des solutions est alors assurée par le théorème de Cauchy-Lipschitz, mais on peut éviter de l'invoquer ici (voir remarque ci-dessous).

Le flot $\tilde{\varphi}$ de $\tilde{X}$ est conjugué à celui de X :

$$\forall \tilde{x}, \forall t \text{ tel que le flot soit défini }, \quad f(\tilde{\varphi}^t(\tilde{x})) = \varphi^t(f(\tilde{x})) = x_0 + e^{-t}(f(\tilde{x}) - x_0)$$

En effet, en dérivant le membre de gauche, on s'aperçoit qu'il est solution de X et il vaut $f(\tilde{x})$ au temps 0.

Montrons que le champ $\tilde{X}$ est complet :

Soit $\tilde{x} \in \tilde{M}$. Regardons la longueur de l'orbite de x :

$\forall t$ tel que le flot soit défini :

$$\begin{aligned}
\|\tilde{\varphi}^t(\tilde{x}) - \tilde{x}\| \leq & \left| \int_0^t \|\frac{\mathrm{d}}{\mathrm{d}s}(\tilde{\varphi}^s(\tilde{x}))\| \mathrm{d}s \right| \\
\leq & \left| \int_0^t \|\tilde{X}(\tilde{\varphi}^s(\tilde{x}))\mathrm{d}s| \right| \| \\
\leq & \left| \int_0^t \|(\mathrm{d}f_{\tilde{\varphi}^s(\tilde{x})})^{-1}(X(f(\tilde{\varphi}^s(\tilde{x})))\| \mathrm{d}s \right| \\
\leq & \left| \int_0^t \frac{1}{k} e^{-s} \|f(\tilde{x}) - x_0\| \mathrm{d}s \right| \\
\leq & \frac{1}{k} \|f(\tilde{x}) - x_0\| |1 - e^{-t}|
\end{aligned}$$

Donc, en temps fini, les solutions de $\tilde{X}$ restent dans un compact. D'après le lemme de sortie de tout compact, les solutions sont définies sur $\mathbb{R}$ tout entier, autrement dit le champ $\tilde{X}$ est complet.

(Cela montre déjà la surjectivité de f puisque chaque point de M est de type $x_0+e^{-t}(x-x_0)$ pour $t \in \mathbb{R}$ et x dans un voisinage de x_0 où f est un difféomorphisme local, qui a au moins un relevé par f, à savoir $\varphi^t_{\tilde{X}}(\tilde{x})$ pour un relevé quelconque de x.)

Montrons que f est bijective :

On pose, pour $\tilde{x} \in \tilde{M}$, $W^s(\tilde{x}) = \{\tilde{y} \in \tilde{M} \quad | \quad \tilde{\varphi}^t(\tilde{y}) \xrightarrow[t\to+\infty]{} \tilde{x}\}$, on appelle cette partie la variété stable de $\tilde{x}$, mais c'est juste une terminologie. On va montrer que $\tilde{M}$ est l'union disjointe des $W^s(\tilde{x_0})$ pour $f(\tilde{x_0}) = x_0$. On montrera que les variétés stables sont ouvertes, ce qui, par connexité de $\tilde{M}$, implique qu'il n'y en a qu'une.

Soit $\tilde{x} \in \tilde{M}$. D'après le raisonnement mené pour montrer la complétude, l'orbite de $\tilde{x}$ pour les temps positifs reste dans un compact. Donc, on peut trouver une suite de temps (t_p) tendant vers $+\infty$ tel que la suite $(\tilde{\varphi}^{t_p})$ converge vers $\tilde{x_0}$ qui est nécessairement une préimage de x_0 par passage à la limite dans l'égalité liant les flots de $\tilde{X}$ et de X. En particulier x_0 a au moins un antécédent !

Mais $\tilde{x_0}$ a un voisinage positivement invariant par le flot : les boules de centre x_0 dans M sont invariantes par le flot, si on prend un rayon suffisamment petit, celle ci est difféomorphe via f^{-1} à un voisinage de $\tilde{x_0}$ car f est un difféomorphisme local en $\tilde{x_0}$. Donc, pour p assez grand, $(\tilde{\varphi}^{t_p})$ est dans ce voisinage de x_0 et y reste pour les temps $t \geq t_p$. On a donc

$$\tilde{M} = \bigsqcup_{f(\tilde{x_0})=x_0} W^s(\tilde{x_0})$$

Il reste à montrer que ces variétés stables sont ouvertes. Prenons $\tilde{x} \in W^s(\tilde{x_0})$ et $\tilde{y}$ proche de $\tilde{x}$. Comme précédemment, soit V un voisinage de $\tilde{x_0}$ invariant par le flot $\tilde{X}$ obtenu en relevant une petit boule euclidienne centrée en x_0. Il existe $T > 0$ tel que $\tilde{\varphi}^T(\tilde{x}) \in V$ et aussi pour les temps supérieurs. Par le théorème de dépendance continue des conditions initiales, si $\tilde{y}$ est suffisamment proche de $\tilde{x}$, on a aussi $\tilde{\varphi}^T(\tilde{y}) \in V$, et donc aussi pour les temps supérieurs car V est positivement invariant par le flot. Une fois rentré dans ce voisinage, la dynamique est celle du champ radial sur M, i.e., toute les orbites tendent vers $\tilde{x_0}$. Ainsi, $\tilde{\varphi}^t(\tilde{y}) \xrightarrow[t\to+\infty]{} \tilde{x_0}$ dès que $\tilde{y}$ est assez proche de $\tilde{x}$, c'est-à-dire, $W^s(\tilde{x_0})$ est ouvert.

Par connexité de M, il n'y a donc qu'une seule variété stable, et donc un unique antécédent de x_0 par f. Cela est vrai pour tout x_0 dans M. Donc f est bijective.

Finalement, f est un $\mathcal{C}^1$-difféomorphisme de $\tilde{M}$ sur M. Comme f est $\mathcal{C}^2$, sa réciproque l'est aussi, donc f est un $\mathcal{C}^2$-difféomorphisme. □

Remarques

1. C'est un exemple typique de résultat qui passe "du local au global" : les conditions sur f ne sont que locales. Les arguments de nature globale font intervenir compacité et connexité.
2. Le contexte naturel de ce théorème est l'application exponentielle sur une variété riemannienne à courbure négative. L'application f apparait dans ce contexte comme l'application exponentielle de l'espace tangent en un point dans la variété. Dans ce contexte, on a des informations "métriques" comme la condition du théorème qui apparaissent naturellement, et on veut en déduire un résultat global. Le résultat est le suivant : une variété riemannienne complète simplement connexe à courbure négative est difféomorphe à $\mathbb{R}^n$ via l'application exponentielle en un point quelconque.
3. Il faut penser $\tilde{M}$ comme "au-dessus" de M et f comme une *projection* de $\tilde{M}$ sur M. La *fibre* au dessus d'un point de M est simplement sa préimage par f.

4. La preuve ci-dessus utilise des équations différentielles de façon contestable, la preuve naturelle utilise la théorie des revêtements, mais cette preuve est substantiellement la même (on relève des chemins au lieu de relever un champ de vecteur).
5. Le résultat reste vrai si on remplace $\mathbb{R}^n$ par un espace de Banach, mais dans ce cas il faut l'attribuer (semble-t-il) à Hadamard *et* Lévy. Celui-ci est dû seulement à Hadamard.
6. Si f est seulement $\mathcal{C}^1$, le résultat est encore vrai. La preuve fonctionne du début à la fin sauf pour montrer que les variétés stables sont ouvertes (du moins je n'arrive pas à le faire). Dans ce cas, $\tilde{X}$ est seulement continu, mais l'unicité des solutions ne pose pas de problème car on a unicité des solutions de X dans M. Les problèmes d'unicité de solutions sont toujours locaux (par connexité des intervalles de $\mathbb{R}$), et localement le champ $\tilde{X}$ a les mêmes solutions que X via f^{-1}. L'existence locale ne requiert pas Cauchy-Peano, car on peut tirer en arrière les solutions locales de X par f. On a besoin dans la preuve ci-dessus du caractère localement lipschitzien de $\tilde{X}$ seulement pour le théorème de dépendance continue des conditions initiales pour montrer que les variétés stables sont ouvertes.

Leçons concernées : étude qualitatives d'edo, connexité, applications différentiables, inversion locale, compacité.

4 Théorèmes de Sylow

ref : Perrin

THÉORÈME 4.1 (SYLOW) *Soit G un groupe de cardinal $n = p^\alpha m$ avec p premier, $\alpha \geq 1$ et m premier à p. On appelle p-sylow de G un sous-groupe de G de cardinal p^α.*

1. *G admet un p-sylow.*
2. *Les p-sylows de G sont tous conjugués.*
3. *Si n_p désigne le nombre de p-sylows de G. Ce nombre est contraint aux congruences suivantes :*
   (a) *$n_p = [G : N_G(S)]$, indice du normalisateur de n'importe quel p-sylow S, en particulier n_p divise n.*
   (b) *$n_p = 1 \pmod p$*
   (c) *n_p divise m*

PREUVE.

1. Le groupe $GL(n, \mathbb{F}_p)$ est de cardinal :

$$(p^n - 1)(p^n - p)...(p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}}(p^n - 1)(p^{n-1} - 1)...(p - 1)$$

   Le sous-groupe des matrices triangulaires supérieures avec des 1 sur la diagonale est de cardinal $p^{\frac{n(n-1)}{2}}$ (le nombre de coefficient dans le triangle supérieur strict). C'est donc un p-sylow de $GL(n, \mathbb{F}_p)$.
   On sait par ailleurs que tout groupe de cardinal n se réalise comme sous-groupe de $\mathfrak{S}_n$, lui même sous-groupe de $GL(n, K)$ pour n'importe quel corps K (via les matrices de permutations). Donc il suffit maintenant de voir qu'un sous-groupe d'un groupe admettant un p-sylow en admet un aussi. Pour cela, on va le chercher sous-forme de conjugué de ce p-sylow.
   Soit H un sous-groupe de G et S un p-sylow de G. Le groupe G agit naturellement sur G/S par translation. Le stabilisateur de la classe de 1 est S, et les autres stabilisateurs lui sont conjugués. Restreignons cette action à une action de H sur G/S. Celle-ci n'est a priori plus transitive. Les stabilisateurs sont les $H \cap gSg^{-1}$ pour $g \in G$. L'un de ces stabilisateurs est nécessairement un p-sylow de G. En effet, H agit sur G/S qui est un ensemble de cardinal premier à p car S est un p-sylow de G. L'ensemble G/S est partitionné en ses orbites sous l'action de H qui ne peuvent donc pas être toutes de cardinal divisibles par p. Cela signifie justement qu'un des stabilisateurs est de cardinal p^α, à savoir la puissance de p maximale pour un sous-groupe de H.
2. C'est une conséquence de la version forte de l'existence que l'on vient de montrer. Si S et S' sont deux p-sylows, il existe une conjugaison par $g \in G$ qui envoie S sur un p-sylow de S', c'est à dire S' tout entier.
3. D'après 2., G agit transitivement par conjugaison sur l'ensemble de ses p-sylows. Le stabilisateur d'un p-sylow pour cette action est exactement le normalisateur de ce p-sylow. En effet, c'est l'ensemble $Stab(S) = \{g \in G | gSg^{-1} = S\}$, c'est la définition du normalisateur de S dans G noté $N_G(S)$. En particulier, n_p divise n, l'ordre de G. Les autres congruences s'obtiennent en restreignant cette action par conjugaison sur l'ensemble des sylows à une action d'un sylow particulier. Cette fois, c'est une action d'un p-groupe, donc l'ensemble de ces points fixes à même cardinal modulo p que l'ensemble entier. C'est-à-dire, $n_p = \#\{S' | sS's^{-1} = S', \forall s \in S\} \pmod p$. On utilise l'argument de Frattini : Soit S'

différent de S, stable par conjugaison par les éléments de S. Le groupe P engendré par S et S' normalise S'. Mais ce groupe P a deux p-sylows distincts S et S' qui sont conjugués dans P par le point 2., ce qui est contradictoire. Donc S est le seul sylow dans l'ensemble ci-dessus, d'où $n_p = 1 \pmod p$. Le dernier point est conséquence du lemme de Gauss.

□

Applications

1. Un groupe d'ordre 63 n'est jamais simple. En effet, $63 = 9 \times 7$, il n'y a qu'un 7-sylow car n_7 divise 9 et $n_7 = 1 \pmod 7$ implique $n_7 = 1$. S'il existe un unique p-sylow dans un groupe il est distingué (même caractéristique), donc ce 7-sylow est distingué.
2. Un groupe d'ordre 255 n'est jamais simple. On a : $255 = 5 \times 51$. Le 51-sylow est unique donc distingué.
3. Construction d'un automorphisme non intérieur de $\mathfrak{S}_6$. Le groupe $\mathfrak{S}_5$ a six 5-sylows. Il faut compter les sous-groupes d'ordre 5 de $\mathfrak{S}_5$, ils sont engendrés par des 5-cycles qui figurent au nombre de 24. Chaque 5-sylow en contient 4 (+ l'identité), donc il y a $\frac{24}{4} = 6$, 5-sylows. Autre méthode, d'après le théorème de Sylow n_5 divise 24 et est congru à 1 modulo 5, donc $n_5 = 1$ ou 6. Mais 1 n'est pas possible le 5-sylow serait distingué

   L'action par conjugaison de $\mathfrak{S}_5$ sur ses 5-sylows est transitive d'après le théorème de Sylow. L'action est alors fidèle car le noyau de l'action est un sous-groupe distingué de $\mathfrak{S}_5$ qui est au moins d'indice 6 car l'action est transitive (donc l'image de l'action a au moins 6 permutations), et $\mathfrak{S}_5$ n'a que $\mathfrak{A}_5$ comme sous-groupe distingué qui lui est d'indice 2. On a donc trouvé un sous-groupe d'indice 6 de $\mathfrak{S}_6$ qui n'est conjugué à aucun des stabilisateurs des $i \in [|1, n|]$ puisqu'il agit transitivement. Ces deux actions inéquivalentes fournissent un automorphisme non intérieur de $\mathfrak{S}_6$. A revoir, ce n'est pas clair..

Leçons concernées : action de groupe,groupes finis, sous-groupe distingué, (groupe linéaire).

5 $\mathrm{SO}_0(1,2) \simeq \mathrm{PSL}(2,\mathbb{R})$

ref : Un peu Mneimné tome 0 + Maison

THÉORÈME 5.1 *Le groupe* $\mathrm{PSL}(2,\mathbb{R})$ *est isomorphe à la composante connexe de l'identité dans* $\mathrm{SO}(1,2)$*, notée* $\mathrm{SO}_0(1,2)$*.*

PREUVE.

det est une forme quadratique sur l'ensemble des matrices de trace nulle $\mathfrak{sl}(2,\mathbb{R})$. Cette forme quadratique est non dégénérée et de signature $(1,2)$:

$$\det \begin{pmatrix} x & y \\ z & -x \end{pmatrix} = -x^2 - yz = -x^2 + \frac{1}{4}((y-z)^2 - (y+z)^2))$$

Notons (E,q) cet espace quadratique de dimension 3, isomorphe à $(\mathbb{R}^3, x^2 - y^2 - z^2)$.

Le groupe $\mathrm{SL}(2,\mathbb{R})$ agit par conjugaison sur E car la trace est invariante par conjugaison et c'est une action par isométries car le déterminant est invariant par conjugaison.

Cela fournit donc un morphisme de groupes continu :

$$\Phi : \mathrm{SL}(2,\mathbb{R}) \to \mathrm{O}(E)$$

Comme $\mathrm{SL}(2,\mathbb{R})$ est connexe, l'image est un connexe qui contient l'identité, donc est incluse dans le sous-groupe $\mathrm{SO}_0(E)$.

Le noyau est formé de matrices qui commutent avec toutes les matrices de trace nulle donc ce sont des homothéties (toute droite étant droite stable d'une matrice de trace nulle, un telle application stabilise toutes les droites) , c'est donc $\{\pm \mathrm{id}\}$.

L'image est un sous-groupe connexe, si elle est ouverte elle est aussi fermée par propriété de groupes (partition en les classes à gauche modulo le sous-groupe), c'est donc la composante connexe du neutre. Il reste donc à montrer que l'image est ouverte. Il suffit que l'application soit ouverte en tous les points mais comme c'est un morphisme de groupes, il suffit que Φ est ouverte en id. En effet, si V voisinage de M dans $\mathrm{SL}(2,\mathbb{R})$, $M^{-1}V$ est un voisinage de I_2 et $\Phi(V) = \Phi(M)\Phi(M^{-1}V)$ est un voisinage de $\Phi(M)$ dans $\mathrm{SO}_0(E)$.

$\mathrm{SL}(2,\mathbb{R})$ est une sous-variété $\mathcal{C}^\infty$ de dimension 3 de $\mathcal{M}(2,\mathbb{R})$ car det est une submersion au dessus de 1. En effet, si $A \in \mathrm{SL}(2,\mathbb{R})$, $\mathrm{d}\det_A(H) = \mathrm{tr}({}^t\mathrm{com}(A)H)$ qui est une forme linéaire non nulle puisque $\mathrm{com}(A)$ est non nulle. L'espace tangent en id est le noyau de la trace.

$\mathrm{SO}(E)$ est une sous-variété $\mathcal{C}^\infty$ de dimension 3 de $\mathrm{End}(E)$.

Φ représente l'action par conjugaison, elle est donc définie sur $\mathrm{GL}(2,\mathbb{R})$. On va calculer sa différentielle sur $\mathrm{GL}(2,\mathbb{R})$ et obtenir celle sur $\mathrm{SL}(2,\mathbb{R})$ par restriction. On a $\Phi(A) : M \mapsto AMA^{-1}$, donc φ est $\mathcal{C}^1$ dans la variable A car l'inverse est $\mathcal{C}^1$ et la multiplication à gauche et à droite est $\mathcal{C}^1$. Calculons la différentielle en I_2.

$$\begin{aligned} \Phi(I_2+H) : M \mapsto (I_2+H)M(I_2+H)^{-1} &= M \mapsto (I_2+H)M(I_2-H-H\epsilon(H)) \\ &= M \mapsto HM - MH + (MH - HMH)\epsilon(H) \end{aligned}$$

Alors :

$$\|\Phi(I_2+H) - \Phi(I_2) - [M,.]\|_{op} \leq \|H\|\delta(\|H\|)$$

avec $\delta \underset{0}{\to} 0$.

Donc $\mathrm{d}\Phi_{I_2}(H) = (M \to HM - MH)$. Cette différentielle est injective (donc bijective) car si $HM = MH$ pour tout M dans $\mathfrak{sl}(2,\mathbb{R})$, comme précédemment, H est une homothétie de trace nulle, donc $H = 0$.

Ainsi, par le théorème d'inversion locale entre sous-variétés, Φ est ouverte au voisinage de I_2. Ainsi l'image est $\mathrm{SO}_0(1,2)$, d'où l'isomorphisme de groupe souhaité par passage au quotient $\tilde{\Phi} : \mathrm{PSL}(2,\mathbb{R}) \to \mathrm{SO}_0(E) \simeq (\mathrm{SO}_0(1,2))$.

En fait c'est un homéomorphisme : notons π la projection $\mathrm{PSL}(2,\mathbb{R}) \to \mathrm{SL}(2,\mathbb{R})$. Si U est un ouvert de $\mathrm{SO}_0(E)$, $p^{-1}(\tilde{\varphi}^{-1}(U)) = \varphi^{-1}(U)$ est ouvert, donc $\varphi(\tilde{U})$ est ouvert par définition de la topologie quotient. Si V ouvert de $\mathrm{PSL}(2,\mathbb{R})$, $\tilde{\varphi}(U) = \tilde{\varphi}(\pi(\pi^{-1}(V)) = \varphi(\pi^{-1}(V))$ est ouvert car $\pi^{-1}(V)$ est ouvert et φ est ouverte.

□

leçons concernées : action de groupe sur les espaces de matrices, groupe linéaire, sous-variétés, formes quadratiques réelles, inversion locale, applications différentiables

6 $H^1([0,1])$

ref : Allaire

THÉORÈME 6.1 *On pose* $H^1([0,1]) = \{u \in L^2([0,1]) \quad | \quad u' \in L^2([0,1])\}$*, la dérivée étant au sens des distributions.*

H^1 *est un espace de Hilbert, ses éléments sont des fonctions continues sur* $[0,1]$ *et l'injection* $H^1 \to C^0$ *est compacte.*

PREUVE. On munit H^1 du produit scalaire $< u, v >= \int uv + \int u'v'$. C'est clairement un produit scalaire. Si (u_n) est une suite de Cauchy de H^1, (u_n) et (u_n') sont en particulier de Cauchy dans L^2 donc converge vers u et v dans L^2 car L^2 est complet. Pour $\varphi \in \mathcal{D}(]0,1[)$, on a :

$$\int u_n' \varphi = -\int u_n \varphi'$$

On peut passer à la limite dans cette inégalité car la convergence dans L^2 est plus forte que celle dans $\mathcal{D}'$:

$$|\int_0^1 (u_n - u)\varphi| \leq \int_0^1 |u_n - u||\varphi| \leq \sqrt{\int |u_n - u|^2}\sqrt{|\varphi|^2}$$

par l'inégalité de Cauchy-Schwartz.

Cela donne donc pour tout $\varphi \in \mathcal{D}$:

$$\int v\varphi = -\int u\varphi'$$

c'est-à-dire $v = u'$. Donc $u_n \to u$ dans H^1.

LEMME 6.2 *Les fonctions de* H^1 *sont l'intégrale de leur dérivée : pour tout* x*,*

$$u(x) = u(0) + \int_0^x u'(y)\mathrm{d}y$$

Notons $w(x)$ le membre de droite, qui est bien définie car u' est L^1 par Cauchy-Schwartz. Il est aussi continu par la même inégalité :

$$|w(x) - w(y)| \leq \sqrt{|x-y|}\|u'\|_{L^2}$$

Calculons la dérivée de w au sens des distributions.

Pour $\varphi \in \mathcal{D}$, on a :

$$\begin{aligned} < w', \varphi > &= -\int_0^1 w\varphi' = -\int_0^1 u(0)\varphi' - \int_0^1 \int_0^x u'(y)\varphi'(x)\mathrm{d}y\mathrm{d}x \\ &= -\int_0^1 u'(y) \int_y^1 \varphi'(x)\mathrm{d}x\mathrm{d}y = \int_0^1 u'(y)\varphi(y)\mathrm{d}y \end{aligned}$$

Donc $w' = u'$. Deux distributions qui ont même dérivée diffèrent d'une constante. (Si $u' = 0$, u est nulle contre toutes les dérivées de fonctions de $\mathcal{D}$, c'est-à-dire toutes les fonctions d'intégrale nulle. C'est aussi le cas de la fonction constante égale à 1. Deux formes linéaires ayant même noyau sont proportionnelles, donc u est constante). Donc u est continue.

Passons à l'injection compacte.

Si (u_n) est bornée dans H^1 par $M > 0$. L'inégalité de Cauchy-Schwartz donne :

$$|u_n(x) - u_n(y)| \leq \sqrt{|x-y|}\|u_n'\|_{L^2} \leq M\sqrt{|x-y|}$$

ainsi que :

$$|u_n(x)| \leq K$$

La suite (u_n) est donc équicontinue car équihölderienne sur $[0,1]$ qui est compact et ponctuellement bornée. Par le théorème d'Ascoli, on peut extraire une sous-suite $(u_{\varphi(n)})$ qui converge uniformément vers u qui est continue.

□

Leçons concernées : dérivation au sens des distributions, compacité, espaces de hilbert, espaces de fonctions.

7 Inégalité isopérimétrique

ref : ZQ

THÉORÈME 7.1 *Soit Γ une courbe fermée simple de classe C^1 du plan euclidien $\mathbb{R}^2$. On pose $\mathcal{A} = \frac{1}{2}|\int_\Gamma x\mathrm{d}y - y\mathrm{d}x|$ (qui correspond à l'aire enfermée par Γ (via Jordan + Green-Riemann)). Alors on a l'inégalité dite isopérimétrique :*

$$\mathcal{A} \leq \frac{l^2}{4\pi}$$

avec égalité si et seulement si Γ est un cercle.

PREUVE.

Quitte à effectuer une dilatation de l'espace $(x, y) \mapsto (\delta x, \delta y)$ qui transforme l en δl et $\mathcal{A}$ en $\delta^2\mathcal{A}$, on peut supposer $l = 2\pi$. On se ramène donc à montrer que $\mathcal{A} \leq \pi$.

On paramètre Γ par longueur d'arc : $\gamma(s) = (x(s), y(s))$ est définie sur $[0, 2\pi]$, $\gamma(0) = \gamma(2\pi)$, de classe $\mathcal{C}^1$ et $\|\gamma'(s)\| = 1, \quad \forall s \in [0, 2\pi]$. On l'obtient à partir d'un paramétrage quelconque (une immersion) $f(t)$ en posant $s(t) = \int_0^t \|f'(u)\|\mathrm{d}u$. Alors s est $\mathcal{C}^1$, sa dérivée est strictement positive, c'est donc un $\mathcal{C}^1$- difféomorphisme sur son image et donc $s \mapsto f(t(s)))$ est un paramétrage par longueur d'arc. Quitte à parcourir Γ dans l'autre sens, on peut retirer les valeurs absolues dans la formule de l'aire.

On remarque, du fait que x et y sont périodiques que :

$$\mathcal{A} = \frac{1}{2}\int_0^{2\pi}(x(s)y'(s) - y(s)x'(s))\mathrm{d}s = \frac{1}{2i}\int_0^{2\pi}\overline{\gamma(s)}\gamma'(s)\mathrm{d}s = -i\pi < \gamma, \gamma' >$$

où le produit scalaire est le produit L^2 : $\int \overline{f}g\frac{\mathrm{d}t}{2\pi}$.

On développe γ en série de Fourier avec $c_n(\gamma) = \frac{1}{2\pi}f(s)e^{-ins}\mathrm{d}s$. Comme f est $\mathcal{C}^1$, on a $c_n(f') = inc_n(f)$ par intégration par parties. La formule de Parseval (γ et γ' sont L^2 car continues) donne alors :

$$\mathcal{A} = \pi\sum_{n\in\mathbb{Z}}|c_n(\gamma)|^2 n$$

Mais on a aussi : $\int_0^{2\pi}|\gamma'(s)|^2\mathrm{d}s = 2\pi$, ce qui donne d'après Parseval :

$$\sum_{n\in\mathbb{Z}} n^2|c_n(\gamma)|^2 = 1$$

L'inégalité $n \leq n^2$ donne alors $\mathcal{A} \leq \pi$.

Si on a égalité : $\mathcal{A} = \pi$, alors toutes les inégalités précédentes sont des égalités. En particulier, l'inégalité $n \leq n^2$ étant stricte pour $n \neq 0, 1$. Seuls c_0 et c_1 sont non nuls. Donc Γ est le cercle de centre c_0 et de rayon $|c_1| = 1$ car le paramétrage est à vitesse 1.

Réciproquement, pour un cercle on a bien l'égalité : $l^2 = (2\pi r)^2 = 4\pi\pi r^2 = 4\pi\mathcal{A}$. □

Leçons concernées : Séries de Fourier, étude métrique de courbes, méthode de calcul d'intégrales.

8 Formule des compléments

ref : Stein-Shakarchi : complex analysis

THÉORÈME 8.1 *On définit* Γ *sur* $]0,+\infty[$ *par* $\Gamma(s)=\int_0^{+\infty}t^{s-1}e^{-t}\mathrm{d}t$. *On a alors pour* $s\in]0,1[$,

$$\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin\pi s}$$

PREUVE.

Tout d'abord, Γ est bien définie pour $s>0$ car en 0 l'intégrande est équivalent à t^{s-1} qui est intégrable par le critère de Riemann et en $+\infty$ on a une décroissance exponentielle.

Réécrivons le membre de gauche :

$$\Gamma(s)\Gamma(1-s)=\int_0^{+\infty}(\int_0^{+\infty}u^{-s}e^{-u}\mathrm{d}u)t^{s-1}e^{-t}\mathrm{d}t=\int_0^{+\infty}\int_0^{+\infty}(vt)^{-s}e^{-vt}t^se^{-t}\mathrm{d}v\mathrm{d}t$$

en faisant le changement de variable $u=tv$.

D'où, par Fubini,

$$\Gamma(s)\Gamma(1-s)=\int\int\frac{e^{-(1+v)t}}{v^s}\mathrm{d}v\mathrm{d}t=\int_0^{+\infty}\frac{\mathrm{d}v}{(1+v)v^s}$$

En posant $a=1-s$, ce qui ne change pas le terme de gauche, on est donc ramené à calculer, pour $a\in]0,1[$:

$$\int_0^{+\infty}\frac{v^{a-1}}{1+v}\mathrm{d}v$$

On va utiliser le théorèmes des résidus : Tout d'abord, en posant $v=e^x$, qui est un $\mathcal{C}^1$-difféomorphisme de $\mathbb{R}$ dans $]0,+\infty[$ on se ramène à calculer :

$$I(a)=\int_{-\infty}^{+\infty}\frac{e^{ax}}{1+e^x}\mathrm{d}x$$

La fonction $f(z)=\frac{e^{az}}{1+e^z}$ est holomorphe sur $\mathbb{C}\setminus i\pi+2i\pi\mathbb{Z}$.

Calculons le résidu de f en $i\pi$.

$$(z-i\pi)f(z)=e^{az}\frac{z-i\pi}{e^z-e^{i\pi}}\xrightarrow[z\to i\pi]{}e^{ia\pi}e^{i\pi}=-e^{ia\pi}$$

On applique le théorème des résidus à f avec le contour Γ défini par le rectangle de sommets $-R,R,R+2i\pi,-R+2i\pi$ dans le demi-plan supérieur orienté dans le sens trigonométrique. Ce contour enferme seulement un pôle de f à savoir $i\pi$.

$$\int_\Gamma f(z)\mathrm{d}z=-2i\pi e^{ia\pi}$$

Calculons le membre de gauche morceaux par morceaux :

$$|\int_R^{R+2i\pi}f(z)\mathrm{d}z|=|\int_0^{2\pi}\frac{e^{a(R+i\theta)}}{1+e^{R+i\theta}}\mathrm{d}\theta|\le Ce^{(a-1)R}\xrightarrow[R\to+\infty]{}0$$

$$|\int_{-R}^{-R+2i\pi}f(z)\mathrm{d}z|=|\int_0^{2\pi}\frac{e^{a(-R+i\theta)}}{1+e^{-R+i\theta}}\mathrm{d}\theta|\le C'e^{-aR}\xrightarrow[R\to+\infty]{}0$$

$$\int_{R+2i\pi}^{R-2i\pi} f(z)\mathrm{d}z = \int_{R}^{-R} f(2i\pi + x)\mathrm{d}x = -e^{2i\pi a}\int_{-R}^{R} f(z)\mathrm{d}z$$

En passant à la limite quand $\mathbb{R}$ tend vers $+\infty$, on obtient, puisque f est intégrable sur $\mathbb{R}$:

$$I(a)(1 - e^{2i\pi a}) = -2i\pi e^{i\pi a}$$

D'où, en factorisant par l'arc-moitié :

$$I(a) = -2i\pi\frac{e^{i\pi a}}{1 - e^{2i\pi a}} = \frac{\pi}{\sin \pi a}$$

□

Leçons concernées : fonctions holomorphes, méthode de calcul d'intégrales.

9 Formule d'inversion de Fourier dans $\mathcal{S}$

ref : Stein-Shakarchi ou Zuily

THÉORÈME 9.1 *On définit la transformée de Fourier par* $\mathcal{F}(f)(\xi) = \hat{f}(\xi) = \int_{\mathbb{R}} f(x)e^{-2i\pi x\xi}\mathrm{d}\xi$.

Si $f \in \mathcal{S}(\mathbb{R})$ *alors* $\hat{f} \in \mathcal{S}(\mathbb{R})$.

On a la formule d'inversion $\hat{\hat{f}} = \check{f}$, *donc la transformée de Fourier est un automorphisme de* $\mathcal{S}(\mathbb{R})$.

PREUVE.

Transformée de Fourier d'une gaussienne :

Calculons la transformée de Fourier d'une gaussienne : $G_\delta(x) = e^{-\pi\delta x^2}$.

$$K_\delta(\xi) := \mathcal{F}(G_\delta)(\xi) = \int_{\mathbb{R}} e^{-\pi\delta x^2 - 2i\pi x\xi}\mathrm{d}x$$

On peut dériver sous le signe intégral car G_δ est dans $\mathcal{S}$, donc intégrable sur $\mathcal{R}$ contre tout polynôme. Dérivons :

$$K'_\delta(\xi) = \int_{\mathbb{R}} (-2i\pi x)e^{-\pi\delta x^2}e^{-2i\pi x\xi}\mathrm{d}x$$

Puis, intégrons par partie :

$$K'_\delta(\xi) = \frac{i}{\delta}[e^{-\pi\delta x^2}e^{-2i\pi x\xi}]_{-\infty}^{+\infty} - \frac{2\pi\xi}{\delta}\int_{\mathbb{R}} e^{-\pi\delta x^2}e^{-2i\pi x\xi}\mathrm{d}x = -\frac{2\pi\xi}{\delta}K_\delta(\xi)$$

K_δ vérifie donc une équation différentielle d'ordre 1, donc on peut expliciter la solution :

$$K_\delta(\xi) = K_\delta(0)e^{-\frac{\pi x^2}{\delta}}$$

La constante $K_\delta(0)$ est une intégrale de Gauss, que l'on peut calculer en passant en coordonnées polaires, on trouve :

$$K_\delta(0) = \frac{1}{\sqrt{\delta}}$$

Utilisation de la gaussienne :

En utilisant Fubini, on montre la formule de multiplication :

$$\int G_\delta \hat{f} = \int K_\delta f$$

Il reste à passer à la limite quand δ tend vers 0. Le terme de gauche ne pose pas de problème, il y a convergence simple vers $\hat{f}$ est dominée par $\hat{f}$ car G_δ est une gaussienne qui s'étale.

Pour le terme de droite on fait un changement d'échelle :

$$\int K_\delta f = \int_{\mathbb{R}} f(x)\frac{1}{\sqrt{\delta}}e^{-\frac{\pi x^2}{\delta}}\mathrm{d}x = \int_{\mathbb{R}} f(y\sqrt{\delta})e^{-\pi y^2}\mathrm{d}y$$

Par convergence dominée (par f qui est intégrable), ce terme tend vers $f(0)$ quand $\delta \to 0$.

On obtient donc :

$$f(0) = \int_{\mathbb{R}} \hat{f}(\xi)\mathrm{d}\xi$$

Translation :

Ensuite, il reste à faire une translation et utiliser le comportement de Fourier vis-à-vis d'elle : On pose $F(y) = f(x+y)$, puis on a, comme F est dans $\mathcal{S}$:

$$f(x) = F(0) = \int_{\mathbb{R}} \hat{F}(\xi)\mathrm{d}\xi = \int_{\mathbb{R}}\int_{\mathbb{R}} f(x+y)e^{-2i\pi y\xi}\mathrm{d}y\mathrm{d}\xi = \int_{\mathbb{R}} \hat{f}(\xi)e^{2i\pi x\xi}\mathrm{d}\xi$$

par changement de variable $u = x + y$.

□

Remarque : 1) il faut admettre les propriétés standards de $\mathcal{S}$ (invariance par translation..) et le fait que Fourier envoie $\mathcal{S}$ dans $\mathcal{S}$ (à mettre dans le plan).

2) On déduit facilement de ce résultat l'inversion de Fourier sur L^1 ainsi que le prolongement à L^2 (Plancherel). En effet, la formule de multiplication + la formule d'inversion montrent que $\mathcal{F}$ est une isométrie sur $\mathcal{S}$ muni de la norme L^2. On peut alors prolonger l'opérateur linéaire $\mathcal{F}$ à L^2 car celui-ci est complet et $\mathcal{S}$ y est dense. Cela reste une isométrie et la formule d'inversion $\hat{\hat{f}} = \check{f}$ est toujours valable. On a donc démontré Plancherel (pas si sûr ...). Pour la formule d'inversion sur L^1, cela provient de la continuité de $\mathcal{F}$ pour la norme L^1 sur $\mathcal{S}$ ainsi que la densité de $\mathcal{S}$ dans L^1.

Leçons concernées : méthodes de calcul d'intégrales, Intégrales à param, Fourier et convolution, Fourier dans $\mathcal{S}$ et $\mathcal{S}'$, $\mathcal{S}$ et $\mathcal{S}'$, (problème d'interversion de limites)

10 Lemme de Morse

ref : Rouvière

THÉORÈME 10.1 *Soit $f : \mathbb{R}^n \to \mathbb{R}$ de classe $\mathcal{C}^3$ telle que $f(0) = 0$, $\mathrm{d}f(0) = 0$ et $\mathrm{d}^2 f(0)$ soit non dégénérée de signature (p, q). Alors il existe θ un C^1-difféomorphisme d'un voisinage de 0 tel que*

$$f \circ \theta^{-1}(x_1, ..., x_n) = x_1^2 + ... + x_p^2 - x_{p+1}^2 - ... - x_{p+q}^2$$

PREUVE. En prenant une base orthogonale pour $\mathrm{d}^2 f(0)$ (c'est-à-dire par un changement de coordonnées linéaire inversible), on peut se ramener à $\mathrm{d}^2 f(0) = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$, ce que nous faisons. On applique la formule de Taylor à l'ordre 2 à f au voisinage de 0, c'est possible car f est de classe $\mathcal{C}^2$.

$$f(x) = \int_0^1 \mathrm{d}^2 f(tx)(x, x)\mathrm{d}t =^t xQ(x)x$$

où $Q(x) = \int_0^1 \mathrm{d}^2 f(tx)\mathrm{d}t$ est une fonction $\mathcal{C}^1$ (car f est $\mathcal{C}^3$ et par dérivation sous le signe intégral) d'un voisinage de 0 à valeurs dans $\mathrm{S}(n, \mathbb{R})$. On est conduit à étudier des familles paramétrées de formes quadratiques. On a le lemme suivant :

LEMME 10.2 *Soit $S_0 \in \mathrm{S}(n, \mathbb{R})$ une matrice symétrique inversible, il existe un voisinage ouvert V de S_0 dans $\mathrm{S}(n, \mathbb{R})$ et φ une application $\mathcal{C}^\infty$ de V dans $\mathrm{GL}(n, \mathbb{R})$ telle que :*

$$\forall S \in V, \quad {}^t\varphi(S)S_0\varphi(S) = S_0$$

PREUVE. On définit la fonction $\Psi : \mathrm{S}(n, \mathbb{R}) \times \mathcal{M}(n, \mathbb{R}) \to \mathrm{S}(n, \mathbb{R})$ par

$$\psi(S, M) =^t MSM$$

On remarque que Ψ est $\mathcal{C}^\infty$, que $\Psi(S_0, I_n) = S_0$ et que l'objet du lemme est d'étudier le niveau $\Psi^{-1}(S_0)$ au voisinage de (S_0, I_n). On cherche à exprimer M en fonction de S, il faut donc regarder la dérivée partielle par rapport à M :

$$L(H) = \frac{\partial \Psi}{\partial M}(S_0, I_n).H =^t HS_0 + S_0H$$

Le noyau de cette application linéaire $\mathcal{M}(n, \mathbb{R}) \to \mathrm{S}(n, \mathbb{R})$ est exactement $S_0^{-1}\,\mathrm{A}(n, \mathbb{R})$. En effet, $H \in \ker L$ si et seulement S_0H est antisymétrique. On prend alors un supplémentaire vectoriel du noyau, un choix évident est $H = S_0^{-1}\,\mathrm{S}(n, \mathbb{R})$. On restreint Ψ au sous-espace $\mathrm{S}(n, \mathbb{R}) \times H$ qui contient (S_0, I_n) car S_0 est symétrique. (On a pas besoin de translater H ce qu'on pouvait s'attendre à devoir faire). Ainsi on peut résoudre l'équation $\Psi(S, M) = S_0$ au voisinage de (S_0, I_n) par le théorème des fonctions implicites : Il existe une application φ de classe $\mathcal{C}^\infty$ d'un voisinage ouvert de S_0 dans $\mathrm{S}(n, \mathbb{R})$ dans $\mathrm{GL}(n, \mathbb{R})$ (quitte à restreindre) telle que

$$\Psi(S, \varphi(S)) =^t \varphi(S)S\varphi(S) = S_0$$

□

Revenons à l'expression de f, et utilisons le lemme avec $S_0 = Q(0)$:

$$f(x) =^t x^t\varphi(Q(x))^{-1}Q(0)\varphi(Q(x))^{-1}x$$

Il reste à voir que l'application $x \mapsto \theta(x) = \varphi(Q(x))^{-1}x$ est un $\mathcal{C}^1$-difféomorphisme d'un voisinage de 0. On applique cette fois le théorème d'inversion locale :

$$\theta(0+h) = \varphi(Q(h))^{-1}h = \varphi(Q(0)+o(1))^{-1}h = (I_n+o(1))^{-1}h = h+o(\|h\|)$$

Donc $\mathrm{d}\theta(0) = I_n$ est inversible et par inversion locale (θ est $\mathcal{C}^1$), θ est un $\mathcal{C}^1$-difféomorphisme. Ensuite, dans ces coordonnées on a bien :

$$f \circ \theta^{-1}(x) = {}^t x Q(0) x$$

□

Leçons concernées : Taylor, inversion locale, applications différentiables, matrices symétriques réelles, formes quadratiques réelles

11 Ellipsoïde de John

ref : FGN algèbre 3 pas mal modifié

THÉORÈME 11.1 *Soit K un compact contenant 0 dans son intérieur de l'espace euclidien standard $\mathbb{R}^n$. Il existe un unique ellipsoïde (centré en 0) contenant K qui soit de volume minimal.*

PREUVE. On entend par ellipsoïde la boule unité d'une forme quadratique définie positive. Les formes quadratiques sont identifiées aux matrices de $S(n,\mathbb{R})^{++}$ via $q(x) = {}^t xSx$. On note $\mathcal{E}(S) = \{x \in \mathbb{R}^n | {}^t xSx \leq 1\}$ la boule unité pour la forme quadratique associée à S.

Volume d'un ellipsoïde :

L'ellipsoïde $\mathcal{E}(S)$ est l'image de la boule unité euclidienne B par une affinité orthogonale. Pour $S \in \mathrm{S}(n,\mathbb{R})^{++}$, on note $S^{\frac{1}{2}}$ la racine carrée définie positive de S [1]. On a alors :

$$x \in \mathcal{E}(S) \Leftrightarrow {}^t xSx \leq 1 \Leftrightarrow S^{\frac{1}{2}}x \in B$$

Donc $vol(\mathcal{E}(S)) = \det(S)^{-\frac{1}{2}}\omega$ où ω est le volume de la boule unité B. [2]

Le problème se ramène donc à minimiser la fonction $\varphi(S) = \det(S)^{-\frac{1}{2}}$.

Existence du minimum :

On pose :

$$A = \{S \in \mathrm{S}(n,\mathbb{R})^{++} | K \subset \mathcal{E}(S)\}$$

A est non vide car K est compact, donc inclus dans une grande boule euclidienne par exemple.

A est bornée parce que moralement plus S est grand plus son ellipsoïde est petite et elle ne peut pas être trop petite si elle veut contenir un compact d'intérieur non vide. Détaillons ce point. On admet que $\|S\|_2 = \rho(S)$, il suffit donc de contrôler le rayon spectral. Il existe une boule $B(0,r)$ incluse dans K par hypothèse. Pour $S \in A$, comme S est diagonalisable et son rayon spectral est une valeur propre strictement positive $\lambda > 0$, soit e un vecteur propre unitaire pour λ. Le vecteur re est dans $B(0,r) \subset \mathcal{E}(S)$, donc ${}^t(re)Sre = \rho(S)r^2 \leq 1$, donc $\rho(S) \leq \frac{1}{r^2}$.

La fonction φ est minorée sur A par le volume de K qui est strictement positif car K est d'intérieur non vide. Elle admet donc une borne inférieure sur A, prenons donc une suite minimisante S_k, c'est-à-dire vérifiant :

$$\varphi(S_k) \xrightarrow[k\to+\infty]{} \inf_{S\in A} \varphi(S)$$

A étant bornée, on peut, d'après Heine-Borel, quitte à extraire extraire de S_k converge vers S. Il faut vérifier que S satisfait bien toutes les propriétés requises : L'inégalité ${}^t xS_k x \leq 1$ pour $x \in K$ passe bien à la limite, donc $\mathcal{E}(S)$ contient K. En effet, $\mathrm{S}(n,\mathbb{R})^+$ est fermé dans $\mathrm{S}(n,\mathbb{R})$ car les conditions ${}^t xSx \geq 0$ sont fermées. De plus $\varphi(S) \leq C < 0$, donc $\det(S) \geq C'$, et $S \in \mathrm{S}^{++}(n,\mathbb{R})$. De plus $\mathcal{E}(S)$ contient K car les inégalités pour $x \in K$, ${}^t xS_k x \leq 1$ passent bien à la limite.

Unicité du minimum :

L'ensemble A sur lequel on a minimisé φ est convexe car $\mathrm{S}(n,\mathbb{R})^{++}$ est convexe et les inégalités ${}^t xSx \leq 1$ pour $x \in K$ passent bien aux combinaisons convexes de S. Il suffit maintenant de montrer que φ est strictement convexe sur $\mathrm{S}(n,\mathbb{R})^{++}$, on procède par calcul différentiel en montrant que la différentielle seconde de φ est définie positive. Pour $S \in \mathrm{S}(n,\mathbb{R})^{++}$ et $H \in \mathrm{S}(n,\mathbb{R})$, on a :

1. Attention, dans cette notation se cache le théorème de diagonalisation en b.o.n. des endomorphismes symétriques.
2. il me semble ridicule ici d'utiliser l'intégrale de Lebesgue et le théorème du changement de variables.

$$\mathrm{d}_S\varphi(H) = -\frac{1}{2}\det(S)^{-\frac{3}{2}}\det(S)\operatorname{tr}(S^{-1}H) = -\frac{1}{2}\varphi(S)\operatorname{tr}(S^{-1}H)$$

Puis,

$$\begin{aligned}\mathrm{d}^2_S\varphi(H,H) &= -\frac{1}{2}(-\frac{1}{2}\varphi(S)\operatorname{tr}(S^{-1}H))\operatorname{tr}(S^{-1}H) - \frac{1}{2}\varphi(S)\operatorname{tr}(-S^{-1}HS^{-1}H)\\ &= \frac{1}{4}\varphi(S)((\operatorname{tr}(S^{-1}H))^2 + 2\operatorname{tr}(S^{-1}H)^2)\end{aligned}$$

Le terme $(\operatorname{tr}(S^{-1}H))^2$ est ≥ 0. La matrice $S^{-1}H$ est diagonalisable à valeurs propres réelles car elle est auto-adjointe pour le produit scalaire ${}^txSx$, donc son carré est de trace positive, et nulle seulement si $H = 0$.

On a donc montré que $\mathrm{d}^2\varphi_S$ est définie positive pour tout $S \in \mathrm{S}(n,\mathbb{R})^{++}$, d'où φ strictement convexe et l'unicité du minimum.

□

Remarques : il serait peut-être plus clair de travailler sur l'ensemble des formes quadratiques plutôt que sur les matrices symétriques.

Application : Tout sous-groupe compact G de $\mathrm{GL}(n,\mathbb{R})$ est conjugué à un sous-groupe de $\mathrm{O}(n,\mathbb{R})$. On prend l'union de tous les images de la boule unité euclidienne $\overline{B}(0,1)$ par les éléments de G. Cela fait un compact K d'intérieur non vide auquel on applique le théorème pour trouver un ellipsoïde $\mathcal{E}(S)$ minimal. Pour $g \in G$, on a par unicité les ellipsoïdes $g(\mathcal{E}(S))$, $\mathcal{E}(S)$ et $g^{-1}(\mathcal{E}(S))$ sont égaux, puisque ils contiennent tous $g(K) = K$ et l'un parmi $g(\mathcal{E}(S))$ et $g^{-1}(\mathcal{E}(S))$ est de volume minimal (suivant la position de $|\det g|$ par rapport à 1.) Donc G préserve l'ellipsoïde $\mathcal{E}(S)$, c'est donc un isométrie de ${}^txSx$. Un endomorphisme envoyant une base orthonormée euclidienne sur une base orthonormée de ${}^txSx$ conjugue alors G en un sous-groupe de $\mathrm{O}(n,\mathbb{R})$.

Leçons concernées : matrices symétriques réelles, formes quadratiques réelles, endomorphisme remarquable d'un espace euclidien, compacité, applications différentiables, problèmes d'extremum, convexité en analyse, (déterminant).

12 Théorème de Morgenstern

THÉORÈME 12.1 *L'espace $\mathcal{C}^\infty([0,1])$, muni de la topologie de la convergence uniforme de toutes les dérivées, contient un G_δ dense de fonctions analytiques nulle part*

ref : Dugundji PREUVE. On définit sur $\mathcal{C}^\infty$ la distance :

$$d(f,g) = \sum_{n=0}^{+\infty} \min(2^{-n}, \|f^{(n)} - g^{(n)}\|_\infty)$$

Cela fait de $\mathcal{C}^\infty$ un espace métrique complet.

Si une fonction $\mathcal{C}^\infty$ est analytique en un point a alors sa série de Taylor au point a a un rayon de convergence non nul, c'est-à-dire d'après la règle de Hadamard, $\sup_k \sqrt[k]{\frac{|f^{(k)}(a)|}{k!}} < \infty$. Il faut montrer que cette inégalité est rarement vérifié, posons alors, pour $a \in [0,1]$ et $c \in \mathbb{N}$:

$$T(a,c) = \{f \in \mathcal{C}^\infty | \forall k \geq 0, |f^{(k)}(a)| \leq k! c^k\}$$

Comme une fonction analytique en a l'est aussi sur un voisinage de a, elle est dans l'un des $T(a,c)$ pour $a \in \mathbb{Q} \cap [0,1]$.

Chaque $T(a,c)$ est fermé car les conditions sont fermées pour la topologie $\mathcal{C}^\infty$. Si $T(a,c)$ est d'intérieur vide, alors l'ensemble des fonctions analytiques quelque part est contenu dans une union dénombrable de fermés d'intérieur vide, qui est d'intérieur vide par le théorème de Baire (C^∞ étant complet). Par passage au complémentaire, l'ensemble des fonctions analytiques nulle part contient alors un G_δ dense. Il reste donc à montrer que $T(a,c)$ est d'intérieur vide. Prenons $f \in T(a,c)$, $\epsilon > 0$, $n \in \mathbb{N}^*$ et $b > 2$ et posons :

$$s(x) = f(x) + \epsilon b^{-n} \cos(b(x-a))$$

Il faut choisir les paramètres pour que s soit proche de f au sens de la distance d et pour que s ne vérifie pas les inégalités définissant $T(a,c)$.

$$|s^{(2n)}(a) - f^{(2n)}(a)| = \epsilon b^n$$

Pour $k \leq n$,

$$\|s^{(k)} - f^{(k)}\|_\infty \leq \epsilon b^{k-n}$$

Donc,

$$d(s,f) \leq \sum_{k=0}^{n-1} \epsilon b^{k-n} + \sum_{k=n}^{+\infty} 2^{-k} \leq \epsilon b^{-n} \frac{b^n - 1}{b-1} + 2^{-n+1} \leq \epsilon + 2^{-n+1}$$

il suffit maintenant d'ajuster les paramètres :

On prend n assez grand pour que $2^{-n+1} < \epsilon$, ainsi $s \in B(f, 2\epsilon)$. Puis b suffisamment grand pour que $\epsilon b^n > 2(2n)! c^{2n}$, ainsi par inégalité triangulaire, $|s^{(2n)}(a)| > (2n)! c^{2n}$, donc s n'est pas dans $T(a,c)$.

On a trouvé des fonctions n'appartenant pas à $T(a,c)$ arbitrairement proche de f, donc $T(a,c)$ est d'intérieur vide.

□

Leçons concernées : espace complet, séries entières, continuité et dérivabilité.

13 Théorèmes de Ceva et Menelaüs par les groupes

ref : Maison

THÉORÈME 13.1 *Soit ABC un triangle non aplati du plan affine $\mathcal{E}$. On prend trois points A', B' et C' respectivement sur les droites (BC), (CA) et (AB) et on pose $\mathcal{D}_A = (AA')$, $\mathcal{D}_B = (BB')$ et $\mathcal{D}_C = (CC')$.*

1. *(Menelaüs) : Les points A', B' et C' sont alignés si et seulement si*
$$\frac{\overline{A'B}}{\overline{A'C}}.\frac{\overline{B'C}}{\overline{B'A}}.\frac{\overline{C'A}}{\overline{C'B}} = 1$$
2. *(Ceva) : Les droites $\mathcal{D}_A$, $\mathcal{D}_B$ et $\mathcal{D}_C$ sont concourantes ou parallèles si et seulement si*
$$\frac{\overline{A'B}}{\overline{A'C}}.\frac{\overline{B'C}}{\overline{B'A}}.\frac{\overline{C'A}}{\overline{C'B}} = -1$$

Menelaüs :

Soit $h_{A\to B}$ l'homothétie-translation de centre C' envoyant A sur B, $h_{B\to C}$ et $h_{C\to A}$ définies de même. On a $h_{C\to A} \circ h_{B\to C} \circ h_{A\to B} = h'$ est une homothétie (c'est le groupe des homothéties-translations) de centre A car ce point est fixé par construction. L'application $h_{B\to C} \circ h_{A\to B}$ stabilise la droite $(A'C')$ puisque celle-ci passe par les deux centres des homothéties. Donc h' préserve la droite $(A'C')$ si et seulement si $h_{C\to A}$ préserve a droite $(A'C')$, c'est-à-dire si et seulement si A', B' et C' sont alignés.

Mais h' étant une homothétie de centre A, elle préserve la droite $(A'C')$ si et seulement si c'est l'identité, c'est-à-dire si et seulement si son rapport vaut 1.On trouve donc la condition :

$$\frac{\overline{A'B}}{\overline{A'C}}.\frac{\overline{B'C}}{\overline{B'A}}.\frac{\overline{C'A}}{\overline{C'B}} = 1$$

en utilisant la multiplicativité des rapports ($f \to \vec{f}$ est un morphisme de GA dans GL).

De Menelaüs à Ceva :

On trace les droites D_A, D_B et D_C, qui intersectent en A', B' et C' les côtés du triangle. On construit le point D' comme intersection de $(A'B')$ et de (AB).

On écrit le théorème de Menelaüs dans le triangle ABC avec les points A', B' et D' :

$$\frac{\overline{A'B}}{\overline{A'C}}.\frac{\overline{B'C}}{\overline{B'A}}.\frac{\overline{D'A}}{\overline{D'B}} = 1$$

Pour passer au résultat de Ceva, à savoir

$$\frac{\overline{A'B}}{\overline{A'C}}.\frac{\overline{B'C}}{\overline{B'A}}.\frac{\overline{C'A}}{\overline{C'B}} = -1$$

il faut examiner le terme :

$$\frac{\overline{D'A}}{\overline{D'B}}\frac{\overline{C'B}}{\overline{C'A}}$$

En fait, c'est le birapport $[A, B, C', D']$.

Il faut et il suffit de montrer que ce birapport vaut -1 si et seulement si les droites D_A, D_B et D_C sont concourantes.

Ce sont des notions projectives, on transforme la figure en envoyant la droite CD' à l'infini, ainsi le quadrilatère $ABA'B'$ devient un parallélogramme, les droites D_B et D_A se coupent au milieu des diagonales et la droite D_C étant parallèle aux côtés (AB') et $(A'B)$, elle concourt avec les diagonales si et seulement si $[A, B, C', D'] = \frac{\overline{C'A}}{\overline{C'B}} = -1$.

Leçons concernées : groupes en géométrie.

14 $\mathbb{C}[X,Y]/(X^2+Y^2-1)$ principal

ref : Ortiz, FG alg 1.

THÉORÈME 14.1 *L'anneau quotient $\mathbb{C}[X,Y]/(X^2+Y^2-1)$ est principal.*

PREUVE.
Démarche :
On va se ramener par deux isomorphismes successifs à un anneau plus simple : $\mathbb{C}[U,\frac{1}{U}]$ pour lequel on a le lemme suivant :

LEMME 14.2 *Soient A et B sont des anneaux intègres tels que $A \subset B \subset Frac(A)$. Si A est principal, alors B l'est aussi.*

PREUVE. Soit J un idéal de B. L'intersection de J avec A est un idéal de A qui est engendré par un élément a puisque A est principal. Montrons que a engendre en fait J tout entier.

Soit $b \in J$. On écrit $b = \frac{p}{q}$ avec p et q dans A, premiers entre eux. On a $p = bq \in J \cap A$, donc $p = ac$ avec $c \in A$. Il reste à montrer que $\frac{1}{q}$ appartient à B. Comme p et q sont premiers entre eux dans A qui est principal, on a une relation de Bézout qui les lie : $up + vq = 1$ avec $u, v \in A$.

D'où $pbq + vq = 1$, puis $q(pb + v) = 1$, donc $\frac{1}{q} \in B$. □

L'anneau $\mathbb{C}[U]$ est principal et son corps des fractions $\mathbb{C}(U)$ contient bien $\mathbb{C}[U,\frac{1}{U}]$, donc le lemme s'applique et ce dernier anneau est bien principal.

Montrons un premier isomorphisme :

$$\mathbb{C}[X,Y]/(X^2+Y^2-1) \simeq \mathbb{C}[U,V]/(UV-1)$$

Il faut penser à U et V comme z et $\overline{z}$ pour $z = X + iY$ pour poser :

Par propriété universelle de l'anneau $\mathbb{C}[U,V]$, il existe un (unique) morphisme

$$\Psi : \mathbb{C}[U,V] \to \mathbb{C}[X,Y]/(X^2+Y^2-1)$$

vérifiant $\Psi(U) = X + iY$ et $\Psi(V) = X - iY$. Il passe au quotient en un morphisme

$$\tilde{\Psi} : \mathbb{C}[U,V]/(UV-1) \to \mathbb{C}[X,Y]/(X^2+Y^2-1)$$

car $\Psi(U)\Psi(V) - 1 = (X+iY)(X-iY) - 1 = X^2 + Y^2 - 1 = 0$.

De même, par propriété universelle de $\mathbb{C}[X,Y]$, il existe un (unique) morphisme

$$\Phi : \mathbb{C}[X,Y] \to \mathbb{C}[U,V]/(UV-1)$$

vérifiant $\Phi(X) = \frac{U+V}{2}$ et $\Phi(Y) = \frac{U-V}{2i}$. Il passe au quotient en un morphisme

$$\tilde{\Phi} : \mathbb{C}[X,Y]/(X^2+Y^2-1) \to \mathbb{C}[U,V]/(UV-1)$$

car $\Phi(X)^2 + \Phi(Y)^2 - 1 = (\frac{U+V}{2})^2 + (\frac{U-V}{2i})^2 - 1 = UV - 1 = 0$.

On vérifie que $\tilde{\Psi} \circ \tilde{\Phi} = \mathrm{id}$ et $\tilde{\Phi} \circ \tilde{\Psi} = \mathrm{id}$. Il suffit de le faire sur les générateurs et alors c'est immédiat, on l'a construit pour.

Montrons un deuxième isomorphisme :

$$\mathbb{C}[U,V]/(UV-1) \simeq \mathbb{C}[U,\frac{1}{U}]$$

Par propriété universelle de l'anneau $\mathbb{C}[U,V]$, on a un morphisme

$$\Theta : \mathbb{C}[U,V] \to \mathbb{C}[U, \frac{1}{U}]$$

tel que $\Theta(U) = U$ et $\Theta(V) = \frac{1}{U}$. Ce morphisme est surjectif car l'image contient les deux générateurs U et $\frac{1}{U}$.

Cherchons le noyau de Θ. L'idéal $(UV-1)$ est dans le noyau car $U\frac{1}{U}-1=0$. Réciproquement si $P \in \ker\Theta$, Considérons P dans $\mathbb{C}(U)[V]$ et faisons une division euclidienne ce qui est justifié car $\mathbb{C}(U)$ est un corps donc $\mathbb{C}(U)[V]$ est euclidien.

$$P = (UV-1)Q + R$$

avec $R \in \mathbb{C}(U)$ et $Q \in C(U)[V]$. En multipliant par le ppcm A des dénominateurs des fractions rationnelles en U, on trouve :

$$AP = (UV-1)AQ + AR$$

avec $AQ \in \mathbb{C}[U][V]$ et $AR \in \mathbb{C}[U]$. En appliquant Θ, on trouve $A(T)R(T) = 0$, puis $R = 0$ car $A \neq 0$ dans $\mathbb{C}[T]$. Comme $UV-1$ est irréductible dans $\mathbb{C}[U,V]$ car primitif et de degré 1 dans l'anneau isomorphe $\mathbb{C}[U][V]$, par le lemme de Gauss $UV-1$ divisant AP doit diviser P (car A est de degré 0 en V). Ainsi $P \in (UV-1)$.

□

Leçons concernées : algèbre de polynômes en plusieurs indéterminées, anneaux principaux.

15 Conique passant par 5 points

Référence : Eiden, p.52-53

THÉORÈME 15.1 *Par 5 points distincts A, B, C, D et E d'un plan affine $\mathcal{E}$ passe une conique. Elle est unique si et seulement si 4 points quelconques parmi ces 5 sont non alignés.*

Cette conique définie par 5 points est non dégénérée si et seulement si 3 points quelconques parmi ces 5 sont non alignés.

PREUVE. Si les 5 points sont alignés, on peut prendre la droite et une autre droite quelconque, cela donne une infinité de coniques qui conviennent. Sinon, on peut supposer par exemple que A, B et C forment une base affine du plan. Notons (X, Y, Z) les coordonnées barycentriques dans cette base. L'équation d'une conique $\mathcal{C}$ passant par A, B et C (c'est-à-dire circonscrite au triangle ABC) est de la forme :

$$pYZ + qXZ + rXY = 0$$

En effet, les termes en X^2, Y^2 et Z^2 s'annulent si on impose que les points $A = (1, 0, 0)$, $B = (0, 1, 0)$ et $C = (0, 0, 1)$ satisfassent l'équation.

Notons (x_1, y_1, z_1) et (x_2, y_2, z_2) des coordonnées barycentriques de D et E. La conique $\mathcal{C}$ passe par D et E si et seulement si

$$py_1z_1 + qz_1x_1 + rx_1y_1 = 0$$
$$py_2z_2 + qz_2x_2 + rx_2y_2 = 0$$

Ce système est de rang ≤ 2, donc a toujours des solutions (p, q, r) non nulles (au moins une droite vectorielle de solution), d'où l'existence d'une conique dans tous les cas.

Il y a plusieurs coniques qui conviennent si et seulement si le système ci-dessus est de rang ≤ 1. C'est le cas exactement quand les déterminants extraits de taille 2 sont tous nuls.

Ces déterminants sont, au signe près,

$$z_1z_2\begin{vmatrix}0 & x_1 & x_2\\ 0 & y_1 & y_2\\ 1 & z_1 & z_2\end{vmatrix}, \quad y_1y_2\begin{vmatrix}0 & x_1 & x_2\\ 1 & y_1 & y_2\\ 0 & z_1 & z_2\end{vmatrix} \quad \text{et} \quad x_1x_2\begin{vmatrix}1 & x_1 & x_2\\ 0 & y_1 & y_2\\ 0 & z_1 & z_2\end{vmatrix}$$

Dans le cas général où D, E, ne figurent sur aucune des droites (AB), (BC) et (CA), c'est-à-dire quand $x_1y_1z_1x_2y_2z_2 \neq 0$, le système est de rang < 2 si et seulement si la droite (DE) contient A, B et C (les déterminants exprimant l'alignement de $D, E, A..$) ce qui est impossible puisque A, B, C forment une base affine.

Si le système est de rang < 2, et par exemple $D \in (AB)$ et les trois déterminants sont nuls ce qui donne pour les coordonnées : $z_1 = 0$, $x_1y_1 \neq 0$ et $y_1z_2 = 0$, c'est-à-dire $z_2 = 0$, donc E est aussi sur la droite (AB). On trouve donc 4 points alignés.

Réciproquement, si 4 points sont alignés, on a une infinité de coniques en prenant les unions de deux droites, dont l'une est fixée et l'autre doit seulement passer par un point. D'où le premier point du théorème.

Pour le second point, il faut revenir à la définition : une conique est non dégénérée si et seulement si la forme quadratique à 3 variables qui la définit en coordonnées barycentriques est non dégénérée.

Ecrivons la matrice de la forme quadratique :

$$\begin{pmatrix}0 & r & q\\ r & 0 & p\\ q & p & 0\end{pmatrix}$$

Son déterminant est pqr. On se place sous les hypothèses précédentes où la conique est définie de manière unique par les 5 points.

On peut alors dire que cette conique est non dégénérée si et seulement si $pqr = 0$.

Si $pqr = 0$, par exemple $p = 0$ et l'équation de la conique est $qXZ + rXY = 0$, c'est-à-dire $X(qZ + rY) = 0$ qui définit l'union de deux droites, sur lesquelles on ne peut placer 5 points sans que 3 parmi ces 5 soient alignés.

Réciproquement, si 3 points parmi les 5 sont alignés, alors la conique est l'union de deux droites (par unicité) qui est bien une conique dégénérée. En effet, son équation est de la forme $\varphi(X, Y, Z)\psi(X, Y, Z) = 0$ où φ est ψ sont deux formes linéaires. On écrit :

$$\varphi\psi = \frac{1}{4}((\varphi + \psi)^2 - (\varphi - \psi)^2)$$

ce qui montre que la forme quadratique $\varphi\psi$ est de rang ≤ 2. □

THÉORÈME 15.2 *Deux coniques distinctes du plan affine s'intersectent en au plus* 4 *points ou alors elles contiennent une droite commune.*

PREUVE.

Si elles s'intersectent en au moins 5 points, par l'unicité dans le théorème précédent, 4 points quelconques parmi ces 5 sont forcément alignés, donc ils sont tous alignés. Une conique passant par 3 points alignés contient la droite : en effet, si c'est la droite, on a gagné, sinon elle contient au moins deux points à l'extérieur, et on obtient ainsi 5 points qui définissent une unique conique d'après le théorème précédent, par unicité c'est l'union de deux droites. □

Remarque : On a supposé implicitement que le corps de base a une infinité d'éléments. On ne s'est pas intéressé aux coniques vide ou réduites à un point qui sont difficiles à définir par 5 points !

Leçons concernées : coniques, barycentres, déterminants, formes quadratiques, systèmes linéaires, utilisation de la dimension.

16 Théorème de Cauchy-Peano

ref : Demailly

THÉORÈME 16.1 *Soit U ouvert de $\mathbb{R}^n$ et X un champ de vecteurs continu sur U. Alors en tout point y_0, il existe $T > 0$ et une solution définie sur $[-T, T]$ qui passe par y_0 en $t = 0$.*

PREUVE.

On va construire des solutions approchées en suivant le schéma d'Euler explicite. En prenant des pas de temps de plus en plus petit, on aura une suite de solutions approchées dont on pourra extraire une sous-suite convergente par Ascoli.

Cylindre de sécurité :

X est continu en y_0, donc bornée au voisinage de x_0. Soit $M > 0$ et $r > 0$ tel que $\|X(x)\| \leq M$ pour $x \in B = \overline{B}(y_0, r)$. Posons $T = \frac{r}{M}$, alors moralement les solutions qui partent de y_0 reste dans la boule B pour $|t| \leq T$. On précisera cela dans le cas des solutions approchées que l'on va construire maintenant.

Construction de solutions approchées par schéma d'Euler explicite :

On prend pour $N > 0$, le pas de temps $h = \frac{T}{N}$ et on construit par récurrence la suite $(y_i)_{i=0...N}$ en posant :

$$y_0 = y_0 \text{ et } y_i = y_{i-1} + hX(y_{i-1}) \text{ pour } i = 1...N$$

On définit ensuite la fonction $y : [0, T] \to U$ affine par morceaux vérifiant $y(\frac{i}{N}) = y_i$.

La fonction y reste dans la boule B. Montrons le par récurrence :

$$\forall i \in \{0, \ldots, N\}, \|y_i - y_0\| \leq \frac{ir}{N}$$

C'est clair pour 0, si c'est vrai pour i, on écrit :

$$\|y_{i+1} - y_0\| \leq \|y_{i+1} - y_i\| + \|y_i - y_0\| \leq \|X(y_i)\|h + \frac{ir}{N} \leq \frac{(i+1)r}{N}$$

Cela prouve par récurrence que $y(t) \in B(y_0, r)$, $\forall t \in [0, T]$.

Montrons maintenant que y est M-lipschitzienne.

En effet, pour $0 \leq t \leq t' \leq T$, il existe $i \leq j$ tel que $(i-1)h < t \leq ih \leq jh \leq t' < (j+1)h$ et on peut écrire :

$$\begin{aligned} \|y(t) - y(t')\| &\leq \|y(t) - y_i\| + \|y_i - y_{i+1}\| + ... + \|y_j - y(t')\| \\ &\leq M(ih - t) + M((i+1)h - ih) + ... + M(t' - jh) \\ &= M(t' - t) \end{aligned}$$

En particulier pour $t = 0$ et $t' \in [0, T]$, on a $y(t') \in B$.

Convergence des solutions approchées :

On pose $\omega_X(\eta) = \sup\{\|X(y) - X(y')\| \quad | \quad y, y' \in B \text{ et } \|y - y'\| \leq \eta\}$ la module de continuité du champ X. Par le théorème de Heine, X est uniformément continue sur B qui est compacte, donc $\omega_X(\eta) \xrightarrow[\eta \to 0]{} 0$.

Montrons l'estimation, pour $t \geq 0$:

$$\|y(t) - (y_0 + \int_0^t X(y(s))\mathrm{d}s)\| \leq \omega_X(Mh)t$$

Il existe i tel que $ih \leq t < (i+1)h$, découpons alors :

$$\begin{aligned}\|y(t) - (y_0 + \int_0^t X(y(s))\mathrm{d}s)\| &\leq \|y(t) - y(ih) - \int_{ih}^t X(y(s))\mathrm{d}s\| + ... \\ &+\|y(ih) - y((i-1)h) - \int_{(i-1)h}^{ih} X(y(s))\mathrm{d}s\| \\ &+ ... + \|y(h) - y_0 - \int_0^h X(y(s))\mathrm{d}s\| \\ &\leq \omega_X(hM)(t - ih) + ... + \omega_X(hM)(ih - (i-1)h) + ... + \omega_X(hM)h \\ &\leq \omega_X(hM)t\end{aligned}$$

Extraction par compacité :

Pour N variant, on obtient une suite de fonctions (y_N) de $[0, T]$ dans B, qui est équilipschitzienne et va d'un compact dans un autre. Donc par le théorème d'Ascoli, on peut extraire une sous-suite de $y_{\varphi(n)}$ qui converge uniformément vers une fonction continue y. On peut passer à la limite dans l'estimation précédente, par convergence uniforme pour obtenir pour tout $t \in [0, T]$:

$$y(t) = y_0 + \int_0^t X(y(s))\mathrm{d}s$$

En dérivant, on obtient que y est solution de l'équation différentielle.

On construit de même une solution sur $[-T, 0]$ et elles se recollent en une solution sur $[-T, T]$ car les dérivées à droite et à gauche en 0 coïncident avec $X(y_0)$. □

Remarque : On peut supposer le champ autonome quitte à considérer le champ $\tilde{X}(t, x) = (1, X(t, x))$ qui est autonome sur $\mathbb{R} \times \mathbb{R}^n$ avec la même régularité (continue). Pour Cauchy-Lipschitz, le champ non autonome est plus général car on peut faire une hypothèse de régularité plus faible par rapport au temps que par rapport à la variable d'espace.

Leçons concernées : compacité, equa diff etudes qualitatives, méthodes approchées intégrale equa diff, suites et séries de fonctions.

17 L^p est complet

ref : Rudin

THÉORÈME 17.1 *Soit $(X, \mathcal{A}, \mu)$ un espace mesuré. Pour $1 \leq p \leq +\infty$, l'espace vectoriel normé $L^p(X, \mathcal{A}, \mu)$ est complet. De plus, de toute suite convergente dans L^p, on peut extraire une sous-suite qui converge presque partout.*

PREUVE.

Cas $p = \infty$:

Soit (f_n) une suite de Cauchy de L^∞. L'idée est la suivante : $(f_n(x))$ est une suite de Cauchy pour presque tout x, donc converge dans $\mathbb{R}$ qui est complet. Un passage à la limite dans l'inégalité de Cauchy donne la convergence uniforme de (f_n). On choisit tout d'abord des représentants de chaque f_n qu'on appellera encore f_n. Soit $A_k = \{x \text{ tel que } |f_k(x)| > \|f_k\|_\infty\}$ et $B_{n,m} = \{x \text{ tel que } |f_n(x) - f_m(x)| > \|f_n - f_m\|_\infty\}$. Ces ensembles sont de mesure nulle par définition des sup essentiels. Notons E la réunion (dénombrable) de tous ces ensembles, qui est donc encore de mesure nulle. Pour $x \notin E$, $(f_n(x))$ est une suite de Cauchy de $\mathbb{R}$ donc converge vers un réel noté $f(x)$. Cela définit f mesurable bornée sur le complémentaire de E, on l'étend par 0 sur E. Donc $f \in L^\infty$ et la suite (f_n) converge alors uniformément vers f sur le complémentaire de E. Donc $f_n \to f$ dans L^∞. Le deuxième point est clair sans avoir besoin d'extraire.

Cas $p < \infty$:

Soit (f_n) une suite de Cauchy de L^p. De même, on choisit des représentants et on les identifie à f_n. On peut construire une sous-suite (f_{n_i}) vérifiant :

$$\|f_{n_{i+1}} - f_{n_i}\|_p \leq 2^{-i}$$

Posons alors :

$$g_k = \sum_{i=1}^{k} |f_{n_{i+1}} - f_{n_i}| \text{ et } g = \sum_{i=1}^{\infty} |f_{n_{i+1}} - f_{n_i}|$$

Ce sont des fonctions à valeurs dans $[0, +\infty]$. L'inégalité triangulaire montre que :

$$\|g_k\|_p \leq \sum_i 2^{-i} \leq 1$$

Le lemme de Fatou ou le théorème de convergence monotone donne ensuite $\|g\|_p \leq 1$.

En particulier cela montre que ces fonctions sont finies presque partout et donc pour presque tout x, la série $\sum f_{n_{i+1}}(x) - f_{n_i}(x)$ converge absolument. Comme $\mathbb{R}$ est complet, cette série converge et comme c'est une série télescopique, cela signifie que $f_{n_i}(x)$ converge vers la somme de la série noté $f(x)$. Cela définit f presque partout, puis on complète par 0. On a ainsi montré le deuxième point. Il reste à montrer que f est dans L^p et que (f_n) converge vers f pour la norme L^p. Revenons au fait que (f_n) est de Cauchy :

$$\forall \epsilon > 0, \exists N, \forall n, m \geq N, \int |f_n - f_m|^p < \epsilon^p$$

En prenant $n = n_i$, on a par le lemme de Fatou :

$$\int |f - f_m|^p \leq \liminf \int |f_{n_i} - f_m|^p < \epsilon^p$$

En particulier, par inégalité triangulaire f est dans L^p, et $f_n \to f$ dans L^p.

□

Leçons concernées : espaces L^p, espaces complets, suite et séries de fonctions intégrables.

18 Formes quadratiques sur $\mathbb{F}_q$

ref : Perrin

THÉORÈME 18.1 *Soit E un espace vectoriel de dimension finie sur un corps fini $\mathbb{F}_q$ de caractéristique différente de 2. Soit q une forme quadratique sur E. Pour $a \in \mathbb{F}_q$ qui n'est pas un carré, il existe une base dans laquelle la matrice de q est de la forme* $\mathrm{diag}(0,\dots,0,1,\dots,1)$ *ou* $\mathrm{diag}(0,\dots,0,1,\dots,1,a)$.

PREUVE.

On peut supposer q non dégénérée :

Si q est dégénérée, elle a un noyau N. On prend un supplémentaire quelconque H de N et la restriction de q à H est alors non dégénérée. En choisissant une base adaptée à la décomposition orthogonale $E = N \oplus H$, on a une matrice diagonale par blocs avec un bloc nul et un bloc non dégénéré.

Cas de la dimension 2 : heuristique + carrés dans $\mathbb{F}_q$

En dimension 2, dans une base orthogonale la matrice de q est de la forme $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Pour mettre un 1 en haut à gauche, il faut donc trouver un couple $(x,y) \neq (0,0)$ tel que $ax^2 + by^2 = 1$. Comme le cardinal du corps est fini, on va montrer l'existence abstraite de solutions en dénombrant les carrés.

LEMME 18.2 *L'ensemble des carrés non nuls $\mathbb{F}_q^{*2}$ est d'indice 2 dans le groupe $\mathbb{F}_q^*$: pour $a \in F_q^*$ non carré, on a $\mathbb{F}_q^* = F_q^{*2} \cup aF_q^{*2}$. Le nombre de carrés dans $\mathbb{F}_q$ est donc $\frac{q+1}{2}$. Pour $a, b \neq 0$, l'équation $ax^2 + by^2 = 1$ a toujours des solutions $(x,y) \neq (0,0)$.*

PREUVE. On a un morphisme de groupes multiplicatifs $\mathbb{F}_q^* \to \mathbb{F}_q^*$ donné par l'élévation au carré. Son noyau est le sous-groupe $\{\pm 1\}$ qui est d'ordre 2 car on est en caractéristique différente de 2. L'ensemble des carrés non nuls qui est l'image de ce morphisme est donc un sous-groupe d'indice 2. Il y a donc $\frac{q-1}{2}$ carrés non nuls, en y ajoutant 0, on trouve $\frac{q+1}{2}$. Les parties $\{\frac{1-by^2}{a}$ pour $y \in F_q\}$ et $\{x^2$ pour $x \in \mathbb{F}_q\}$ sont de cardinal $\frac{q+1}{2}$, dans un ensemble de cardinal q, donc doivent s'intersecter pour un couple (x,y) qui est forcément différent de $(0,0)$ qui n'est pas solution de l'équation. □

Récurrence : $n = 1$: Pour $x \in E \setminus 0$, $q(x)$ est ou non un carré. Quitte à multiplier x par un scalaire non nul, on se ramène à $q(x) = 1$ ou a.

$n \geq 2$: On prend un plan non isotrope P dans E engendré par un vecteur non isotrope e et un vecteur non isotrope f dans l'hyperplan orthogonal au premier. Dans la base (e,f), q s'écrit $ax^2 + by^2$ avec $a, b \neq 0$ et le lemme permet alors de trouver un vecteur $v = xe + yf$ non nul tel que $q(v) = 1$. L'orthogonal de v est alors un supplémentaire qui est non isotrope pour q auquel on peut appliquer l'hypothèse de récurrence.

Il reste à vérifier que les deux formes de matrices non dégénérées sont non congruentes. C'est à cause de l'invariance du discriminant : le déterminant d'une matrice symétrique est invariant par congruence modulo les carrés. On fabrique alors un invariant d'équivalence pour les formes quadratiques non dégénérées par $\det(q) \in K^*/K^{*2}$. □

Leçons concernées : corps finis, formes quadratiques.

19 Théorème de l'application ouverte

Ref : brézis

THÉORÈME 19.1 *Soit E et F des espaces vectoriels normés et $T : E \to F$ une application linéaire. Elle est ouverte si et seulement si elle est ouverte en 0. Dans ce cas, elle est surjective.*

Réciproquement si elle est surjective elle est ouverte si on suppose en plus que E et F sont complets.

PREUVE. Si elle est ouverte en 0, alors pour $x \in E$, et V un voisinage de x, $V - x$ est un voisinage de 0 et $T(V) = T(V - x) + T(x)$ est encore un voisinage de 0. Si T est ouverte, son image contient une boule ouverte centrée en 0 ainsi que ses images par homothétie, donc tout l'espace F.

Supposons maintenant E et F complets et T continue surjective. Montrons que T est ouverte. *On va d'abord utiliser la complétude à l'arrivée via le théorème de Baire.*

Par surjectivité on a :

$$F = \bigcup_{n=0}^{+\infty} n\overline{T(B(0,1))}$$

Les $n\overline{T(B(0,1))}$ sont fermés donc ne peuvent pas être tous d'intérieur vide par Baire. Ainsi $\overline{T(B(0,1))}$ contient une boule ouverte $B(y_0, 4c)$ avec $c > 0$. Comme $y_0 \in \overline{T(B(0,1))}$, par addition $B(0, 4c) \subset \overline{T(B(0,1))} + \overline{T(B(0,1))} \subset 2\overline{T(B(0,1))}$ par convexité de $\overline{T(B(0,1))}$. D'où $B(0, 2c) \subset \overline{T(B(0,1))}$.

On va maintenant montrer que $B(0, c) \subset T(B(0, 1))$ en utilisant la complétude de E.

Prenons $y \in F$ avec $\|y\| \leq c$ et cherchons $x \in B(0, 1)$ tel que $Tx = y$. On va obtenir cet élément x comme limite d'une suite de Cauchy que l'on construit grâce au point précédent :

$$\forall \epsilon > 0, \exists z \in E \text{ avec } \|z\| \leq \frac{1}{2} \text{ et } \|y - Tz\| \leq \epsilon$$

Pour $\epsilon = \frac{c}{2}$, on trouve z_1 vérifiant $\|z_1\| \leq \frac{1}{2}$ et $\|y - Tz_1\| \leq \frac{c}{2}$. On recommence avec $y - Tz_1$ et $\epsilon = \frac{c}{4}$. On construit ainsi une suite z_n et $x_n = z_1 + \cdots + z_n$ vérifiant $\|z_n\| \leq \frac{1}{2^n}$ et $\|y - Tx_n\| \leq \frac{c}{2^n}$. La suite (x_n) est donc de Cauchy dans E qui est complet donc converge vers un élément $x \in B(0, 1)$. Par continuité de T, on a alors $Tx = y$.

On a donc montré que $B(0, c) \subset T(B(0, 1))$, c'est-à-dire que T est une application ouverte. □

Leçons concernées : espaces complet, evn.

20 Entiers de Gauss et théorème des deux carrés

ref : Perrin

THÉORÈME 20.1 *1. L'anneau $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{N}\}$ est euclidien pour le stathme $N(a + ib) = a^2 + b^2$.*

2. Soit p un nombre premier. Alors p est somme de deux carrés si et seulement si $p = 2$ ou $p = 1 \mod 4$.

PREUVE. idée : $a^2 + b^2 = (a + ib)(a - ib)$. D'où le lien entre somme de deux carrés et irréductibles de $\mathbb{Z}[i]$.

$\mathbb{Z}[i]$ est euclidien :

Soit $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i] \setminus \{0\}$. Il existe $q \in \mathbb{Z}[i]$ tel que $r' = \frac{z}{w} - q$ soit de norme inférieure à $\frac{1}{\sqrt{2}}$. Alors $z = wq + wr'$ avec $N(wr') \leq \frac{N(w)}{\sqrt{2}} < N(w)$. On a donc bien une division euclidienne.

Inversibles de $\mathbb{Z}[i]$: Les inversibles sont de norme 1 car $zz' = 1 \Rightarrow N(z)N(z') = 1$ dans $\mathbb{Z}$, donc $N(z) = N(z') = 1$. On vérifie réciproquement que les entiers de Gauss de norme 1 à savoir $\{1, -1, i, -i\}$ sont inversibles.

Nombres premiers et irréductibles de $\mathbb{Z}[i]$ Notons Σ l'ensemble des nombres premiers somme de deux carrés.

LEMME 20.2 *$p \in \Sigma \Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$.*

PREUVE. Si $p = a^2 + b^2$ alors $a \neq 0$ et $b \neq 0$ et $p = (a + ib)(a - ib)$ avec $(a + ib)$ et $(a - ib)$ non inversibles.

Réciproquement, si p est réductible, il s'écrit $p = zz'$ avec z, z' non inversibles. Donc $N(p) = p^2 = N(z)N(z')$, puis $N(z) = N(z') = p$ car p est premier. Ainsi p est la norme d'un élément, c'est-à-dire une somme de deux carrés. □

Réduction modulo p :

Par factorialité de $\mathbb{Z}[i]$, p réductible $\Leftrightarrow$ (p) non premier dans $\mathbb{Z}[i] \Leftrightarrow \mathbb{Z}[i]/(p)$ non intègre.

Regardons quand cela se produit.

On a l'isomorphisme $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(X^2 + 1)$. En effet, par propriété universelle de l'anneau des polynômes, on a un morphisme surjectif $\varphi : \mathbb{Z}[X] \to \mathbb{Z}[i]$ défini de manière unique par $\varphi(X) = i$. Son noyau contient clairement l'idéal $(X^2 + 1)$. Réciproquement, si $P \in \ker \varphi$, par division euclidienne unitaire dans $\mathbb{Z}[X]$, il existe Q, R tel que $P = (X^2 + 1)Q + R$ avec $\deg(R) \leq 1$. Et $R(i) = 0$ implique $R = 0$ car R est de degré ≤ 1. Le théorème d'isomorphisme donne alors l'isomorphisme souhaité.

Ce même théorème permet d'intervertir l'ordre des quotients :

$$\mathbb{Z}[i]/(p) = \mathbb{Z}[X]/(p, X^2 + 1) = \mathbb{F}_p[X]/(X^2 + 1)$$

Ce dernier anneau est intègre si et seulement si $(X^2 + 1)$ est irréductible si et seulement si il n'a pas de racines car c'est un polynôme de degré 2.

On obtient donc, p réductible dans $\mathbb{Z}[i]$ si et seulement si -1 est un carré dans $\mathbb{F}_p$.

-1 est-t-il un carré dans $\mathbb{F}_p$? :

Si $p = 2$, tous les éléments sont des carrés, car $x \to x^2$ (Frobenius) est un morphisme de corps, donc injectif est bijectif par cardinal.

Si $p > 2$, x est un carré dans $\mathbb{F}_p$ si et seulement si $x^{\frac{p-1}{2}} = 1$. En effet, si $x = y^2$, $x^{\frac{p-1}{2}} = y^{p-1} = 1$ car $\mathbb{F}_p^*$ est d'ordre $p-1$. Il y a $\frac{p-1}{2}$ carrés non nuls, car le noyau du frobenius est d'ordre 2, qui sont tous racines de l'équation $X^{\frac{p-1}{2}} = 1$ de degré $\frac{p-1}{2}$. Par cardinal, on a l'équivalence souhaitée.

La condition est donc : $p \in \Sigma \Leftrightarrow p = 2$ ou $p = 1 \mod 4$. □

Leçons concernées : Anneaux principaux, nombres premiers.

21 Equation diophantienne et série génératrice

ref : Chambert-Loir

THÉORÈME 21.1 *Soient $\alpha_1, \ldots, \alpha_m \in N^*$ premiers entre eux dans leur ensemble. On pose $p(n) = \text{card}\{(x_1, \ldots, x_m) \in (\mathbb{N}^*)^n \quad | \quad \sum_i \alpha_i x_i = n\}$. On a l'équivalent :*

$$p(n) \sim \frac{n^{m-1}}{\alpha_1 \ldots \alpha_m (m-1)!}$$

PREUVE. On pose la série formelle génératrice $G(X) = \sum_{n \leq 0} p(n) X^n$. On va reconnaitre un produit de Cauchy :

$$G(X) = \sum_{n \geq 0} (\sum_{\alpha_1 x_1 + \cdots + \alpha_m x_m = n} 1) X^n = \sum_{n \geq 0} (\sum_{i_1 + \cdots + i_m = n} b_{i_1} \ldots b_{i_m}) X^n$$

où on a posé $b_{i_k} = 1$ si $\alpha_k | i_k$ et 0 sinon. D'où :

$$G(X) = \prod_{i=1}^{m} (\sum_{k \geq 0} b_{i_k} X^{i_k}) = \prod_{i=1}^{m} \sum_{k \geq 0} X^{k \alpha_i} = \prod_{i=1}^{m} \frac{1}{1 - X^{\alpha_i}}$$

On est ramené à étudier cette fraction rationnelle. Ses pôles sont des racines de l'unité et 1 est le seule pôle d'ordre maximal puisque les α_i sont premiers entre eux dans leur ensemble. En effet, si $\zeta^{\alpha_i} = 1$ pour tout i, par Bézout ζ vaut 1.

La décomposition de G en éléments simples s'écrit donc :

$$G(X) = \frac{A}{(1-X)^m} + B(X)$$

où $A \in \mathbb{C}$, $B \in \mathbb{C}(X)$ où les pôles de B sont d'ordre strictement inférieur à m.

Par dérivation successive du développement $\frac{1}{1-X} = \sum_{n \geq 0} X^n$ on a :

$$\frac{1}{(a-X)^m} = \frac{1}{a^m (m-1)!} \sum_{n \geq 0} (n+1) \ldots (n+m-1) (\frac{X}{a})^n$$

Le terme général de cette série formelle est équivalent à :

$$\frac{n^{m-1}}{(m-1)! a^{m-n}}$$

Le terme du développement correspondant au pôle 1 domine donc asymptotiquement sur les autres car son ordre m est strictement plus grand. On a donc l'équivalent :

$$p(n) \sim \frac{A n^{m-1}}{(m-1)!}$$

Il reste à déterminer le coefficient A.

En multipliant par $(1-X)^m$, on obtient :

$$G(X)(1-X)^m = A + B(X)(1-X)^m$$

Les deux membres sont des fractions rationnelles dont 1 n'est pas un pôle, on peut donc les évaluer en 1. Le terme $B(X)(1-X)^m$ vaut 0 en 1 et le terme de gauche se calcule :

$$G(X)(1-X)^m = \prod_{i=1}^{m} \frac{1-X}{1-X^{\alpha_i}} = \prod_{i=1}^{m} \frac{1}{1 + X + \cdots + X^{\alpha_i - 1}}$$

En évaluant en 1, cela donne $A = \frac{1}{\alpha_1 \dots \alpha_m}$ et l'équivalent souhaité :

$$p(n) \sim \frac{n^{m-1}}{\alpha_1 \dots \alpha_m (m-1)!}$$

□

22 $\mathrm{SO}(3,\mathbb{R})$ est simple

ref : FGN algèbre 3

THÉORÈME 22.1 *Le groupe* $\mathrm{SO}(3,\mathbb{R})$ *est simple.*

PREUVE. idée : On va utiliser de façon cruciale une partie génératrice de $\mathrm{SO}(3,\mathbb{R})$: les renversements (= rotations d'angle π, en dimension 3), ainsi que la connexité de $\mathrm{SO}(3,\mathbb{R})$ (conséquence de la connexité par arcs : on relie une rotation à l'identité en diminuant son angle jusqu'à 0.)

Les renversements sont tous conjugués car $\mathrm{SO}(3,\mathbb{R})$ agit transitivement sur les axes et une conjugaison envoie l'axe d'une rotation sur l'axe de le rotation conjuguée.

La fonction $\theta : \mathrm{SO}(3,\mathbb{R}) \to [0,\pi]$ est continue, on peut l'exprimer analytiquement comme $\theta(g) = \cos^{-1}(\frac{\mathrm{tr}\, g-1}{2})$.

Si H est un sous-groupe distingué de $\mathrm{SO}(3,\mathbb{R})$ et $H \neq \mathrm{id}$. Il suffit de montrer que H contient un renversement pour en déduire que c'est $\mathrm{SO}(3,\mathbb{R})$ tout entier. La première chose à remarquer est que l'on peut se ramener à H connexe en regardant H^0, la composante connexe de id dans H, qui est elle aussi distinguée et non réduite à id. En effet, :

H^0 est un sous-groupe de H car l'application

$$H^0 \times H^0 \to H : (g,h) \mapsto gh^{-1}$$

est continue ; son image est un connexe de H contenant id, donc est incluse dans H^0.

H^0 est distingué dans $\mathrm{SO}(3,\mathbb{R})$ car l'application

$$H^0 \times \mathrm{SO}(3,\mathbb{R}) \to H : (g,h) = hgh^{-1}$$

est continue ; son image est un connexe de H contenant id, donc est incluse dans H^0.

Les composantes connexes de chaque éléments de H dans H diffèrent d'un homéomorphisme global de $\mathrm{SO}(3,\mathbb{R})$ donné par l'action par translation dans le groupe. Il suffit donc de montrer que la composant connexe de $h \in H$, $h \neq \mathrm{id}$ dans H est non réduite à h. Pour cela prenons une rotation $g \in \mathrm{SO}(3,\mathbb{R})$ qui ne préserve pas l'axe Δ de h. Alors ghg^{-1} est d'axe $g(\Delta) \neq \Delta$, $ghg^{-1} \in H$ car H distingué et enfin enjoignant g à id, on voit que ghg^{-1} est dans la composante connexe de h dans H.

Finalement, H^0 est un sous-groupe distingué, connexe, on réduit à id, de $\mathrm{SO}(3,\mathbb{R})$. Montrons qu'un tel sous-groupe contient nécessairement un renversement et on aura terminé.

Revenons à la fonction angle : $\theta(H^0)$ est un connexe de $[0,\pi]$ contenant 0 et non réduit à $\{0\}$, c'est donc un intervalle qui contient en tout cas $[0,\alpha[$ pour $\alpha > 0$ assez petit. En particulier, il existe une rotation ρ d'angle π/n pour $n > \frac{\pi}{\alpha}$ dans le groupe H^0, ainsi ρ^n est bien un renversement contenu dans H^0. □

Leçons concernées : connexité, sous-groupes distingués, endomorphismes remarquables d'un espace euclidien, parties génératrices de groupe.

23 Automorphismes de $\mathfrak{S}_n$

ref : Perrin

THÉORÈME 23.1 *Pour $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont intérieurs.*

idée : Un automorphisme de $\mathfrak{S}_n$ préserve seulement les propriétés algébriques (ordre des éléments, commutation) mais pas les propriétés géométriques liées à l'action naturelle sur $\{1, \dots, n\}$ (décomposition en cycle). Pour des raisons de cardinal, quand $n \neq 6$, les propriétés géométriques seront aussi conservées.

Les transpositions engendrent $\mathfrak{S}_n$ et on a le lemme suivant :

LEMME 23.2 *Si un automorphisme envoie transpositions sur transpositions, il est intérieur.*

PREUVE. □

Soit Φ un automorphisme de $\mathfrak{S}_n$, comme il envoie classes de conjugaison sur classes de conjugaison, il envoie les transpositions sur une classe de conjugaison constituée d'éléments d'ordre 2. Il faut donc calculer le cardinal des classes de conjugaison pour obtenir une obstruction.

LEMME 23.3 *Soit $\mathcal{O}$ une classe de conjugaison dans $\mathfrak{S}_n$, elle correspond à une décomposition en cycles à supports disjoints $\{1, \dots, n\} = I_1 \sqcup \cdots \sqcup I_k$. Dans cette décomposition on note k_i le nombre de cycles de longueur i. Alors :*

$$\mathrm{card}(\mathcal{O}) = \frac{n!}{\prod_{i=1}^{n} k_i! i^{k_i}}$$

PREUVE. Le groupe $\mathfrak{S}_n$ agit transitivement sur 0 par conjugaison car c'est une orbite de l'action. On peut donc calculer son cardinal en connaissant un stabilisateur via la formule :

$$\mathrm{card}(\mathcal{O}) = \frac{\mathrm{card}(\mathfrak{S}_n)}{\mathrm{card}(\mathrm{Stab})}$$

Les stabilisateurs sont tous conjugués, donc ont même cardinaux. La formule de conjugaison :

$$\sigma(a_1, \dots, a_i)\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_i))$$

montre que l'égalité $\sigma\tau\sigma^{-1}$ pour $\tau \in \mathcal{O}$ et $\sigma \in \mathfrak{S}_n$ implique que σ permute les cycles de même longueur et et réalise une permutation cyclique sur chaque chacun. Il y a donc i possibilités pour ces permutations cycliques sur chaque cycle de longueur i et on a k_i tels cycles, d'où :

$$\mathrm{card}(\mathrm{Stab}) = \prod_{i=1}^{n} k_i! i^{k_i}$$

Puis,

$$\mathrm{card}(\mathcal{O}) = \frac{n!}{\prod_{i=1}^{n} k_i! i^{k_i}}$$

Les classes de conjugaison constituées d'éléments d'ordre 2 sont les classes de produits de k transpositions. D'après le lemme si φ n'est pas intérieur, on doit avoir égalité pour un certain $k \geq 2$ (donc si $n \geq 4$) du cardinal des transpositions et de celui des produits de k transpositions :

$$\binom{n}{2} = \frac{n!}{2^k k!(n-2k)!}$$

Manipulons cette égalité pour lui faire cracher $n = 6$:

$$\binom{n}{2} = \frac{n!}{2^k k!(n-2k)!} \Leftrightarrow (n-2)! = 2^{k-1}k!(n-2k)!$$
$$\Leftrightarrow \frac{(n-2)!}{2^{k-1}k!(n-2k)!} = 1$$
$$\Leftrightarrow \frac{\binom{n-2}{2k-2}(2k-2)!}{2^{k-1}k!} = 1$$
$$\Leftrightarrow \frac{\binom{n-2}{2k-2}(2k-3)(2k-5)\dots 1}{k} = 1$$

Cette dernière égalité parait difficile à réaliser pour k grand, en effet : si $k > 3$, alors $(2k-3) > k$ et l'inégalité ci-dessus est fausse.

Reste à examiner les cas $k = 2$ ou 3.

Pour $k = 2$, l'égalité est équivalente à :

$$\frac{\binom{n-2}{2}}{2} = 1 \Leftrightarrow (n-2)(n-3) = 4$$

qui est impossible car deux entiers consécutifs ne peuvent pas être pairs tous les deux.

Pour $k = 3$, on trouve la condition :

$$\binom{n-2}{4} = 1$$

qui implique $n = 6$.

□

Leçons concernées : actions de groupe, groupe de permutations, partie génératrice de groupe, groupe fini, dénombrement.

24 Théorème de Kakutani et Massera

ref : Gonnord-Tosel les deux

THÉORÈME 24.1 (KAKUTANI) *Soit E un espace vectoriel normé et K un compact convexe non vide de E. Toute application affine continue $T : E \to E$ stabilisant K admet un point fixe dans K.*

PREUVE. L'idée est d'itérer un point du compact sous l'application T et de regarder les moyennes de Cesaro de cette suite $(T^n(a))$.

Pour $a \in K$, on pose donc :

$$x_n = \frac{1}{n+1} \sum_{k=0}^{n} T^k(a)$$

Comme K est stable par T, $T^k(a) \in K$ pour tout $k \geq 0$ et par convexité de K les barycentres à coefficients positifs de ces points sont dans K et c'est le cas des x_n.

Comme K est compact, quitte à extraire, on peut supposer que (x_n) converge vers $x \in K$. Il reste à montrer que x est un point fixe de T.

Estimons pour cela la différence $\|T(x) - x\|$:

$$\begin{aligned} T(x_n) - x_n &= T(\frac{1}{n+1} \sum_{k=0}^{n} T^k(a)) - \frac{1}{n+1} \sum_{k=0}^{n} T^k(a) \\ &= \frac{1}{n+1} \sum_{k=0}^{n} T^{k+1}(a) - \frac{1}{n+1} \sum_{k=0}^{n} T^k(a) \quad \text{car } T \text{ est affine} \\ &= \frac{1}{n+1}(T^{n+1}(a) - a) \end{aligned}$$

Or $\|T^{n+1}(a) - a\|$ est bornée par le diamètre de K, donc $\|T(x_n) - x_n\|$ tend vers 0.

On découpe pour finir :

$$\|T(x) - x\| \leq \|T(x) - T(x_n)\| + \|T(x_n) - x_n\| + \|x_n - x\|$$

où $\|x_n - x\| \xrightarrow[n\to\infty]{} 0$ et $\|T(x) - T(x_n)\| \xrightarrow[n\to\infty]{} 0$ par continuité de T. D'où x est un point fixe de T.

□

Un exemple d'application affine apparait dans la méthode de la variation de la constante dans les équations différentielles linéaires. L'application du théorème précédent dans ce cadre donne lieu au théorème suivant.

COROLLAIRE 24.2 (MASSERA) *Soit $T > 0$, $A : \mathbb{R} \to \mathcal{M}(n, \mathbb{R})$ et $b : \mathbb{R} \to \mathbb{R}^n$ deux applications continues et T-périodiques.*

Si l'équation différentielle linéaire $x' = Ax + b$ admet une solution bornée sur $\mathbb{R}$, alors elle admet une solution T-périodique.

Le flot de l'équation différentielle est défini pour tout temps d'après un théorème fondamental des équations différentielles linéaires, notons $\varphi^t(x_0)$ la valeur en t de la solution valant x_0 en 0 (attention le champ n'est pas autonome, on fait un choix arbitraire dans $\mathbb{Z}/t\mathbb{Z}$).

La méthode de la variation de la constante s'exprime ainsi en faisant intervenir la résolvante :

On note $R(t) \in \mathcal{M}(n, \mathbb{R})$ la solution du système linéaire sans second membre :

$$R'(t) = A(t)R(t) \quad \text{et} \quad R(0) = I_n$$

On a alors :

$$\varphi^t(x_0) = R(t)x_0 + \int_0^t R(t)R(s)^{-1}b(s)\mathrm{d}s$$

Pour tout temps t, φ^t est une application affine. Un point périodique de période T correspond à un point fixe de φ^T, il reste à trouver un compact convenable où appliquer le théorème de Kakutani.

Soit $x = \varphi(x_0)$ la solution bornée donnée par l'hypothèse et posons :

$$X = \{x(nT) = \varphi^{nT}(x_0) | n \in \mathbb{Z}\}$$

X est borné.

Comme le champ est T-périodique, on a une propriété de flot plus faible que pour un champ autonome :

$$\varphi^{t+T}(a) = \varphi^t \circ \varphi^T(a)$$

En effet, on vérifie qu'elles ont même dérivée et coïncident en 0, puis on utilise l'unicité des solutions.

En particulier, φ^T stabilise X :

$$\varphi^T(\varphi^{nT}(x_0)) = \varphi^{(n+1)T}(x_0) \in X$$

Comme φ^T est affine, elle stabilise $\mathrm{conv}(X)$. De plus P est continue donc stabilise $\overline{\mathrm{conv}(X)}$ qui est un convexe compact (car fermé borné dans $\mathbb{R}^n$) non vide.

Par le théorème de Kakutani, φ^T admet un point fixe, c'est-à-dire le champ affine a une solution périodique.

Leçons concernées : points fixes, equa diff linéaire, utilisation de la convexité en analyse.

25 Générateurs de Isom(E)

ref : maison + FGN algèbre 3

THÉORÈME 25.1 *Soit E un espace affine euclidien de direction $\vec{E}$. Soit $f \in \mathrm{Isom}(E)$, on note $r_f = \mathrm{rg}(\vec{f} - \vec{\mathrm{id}})$ alors*
- *Si f admet un point fixe, elle est le produit de r_f réflexions mais pas moins.*
- *Si f n'a pas de point fixe, elle est le produit de $r_f + 2$ réflexions mais pas moins.*

PREUVE. On va traiter la partie linéaire qui est une isométrie vectorielle de la direction $\vec{E}$ puis utiliser la forme canonique des isométries affines.

Si $f = \sigma_1 \circ \cdots \circ \sigma_r$ alors $\vec{f} = \vec{\sigma_1} \circ \cdots \circ \vec{\sigma_r}$, on s'intéresse donc au cas vectoriel :

PROPOSITION 25.2 *Toute isométrie vectorielle f d'un espace euclidien E est le produit de $r_f = \mathrm{rg}(f - \mathrm{id})$ réflexions, mais pas moins.*

PREUVE. Si $f = \sigma_1 \circ \cdots \circ \sigma_r$ où les σ_i sont des réflexions d'hyperplans respectifs H_i. Alors :

$$\bigcap_{i=1}^{r} H_i \subset \ker(f - \mathrm{id})$$

Mais, $\dim \bigcap_{i=1}^{r} H_i \geq n - r$, donc $n - r \leq n - r_f$, puis $r \geq r_f$. Cela montre que l'on ne peut pas faire mieux que le résultat annoncé.

L'existence d'une telle décomposition en produit de r_f réflexions se démontre par récurrence sur r_f.

Si $r_f = 0$, alors f est bien le produit de 0 réflexions (qui, par convention, est l'identité). Si c'est vrai pour $r_f = r \geq 0$, prenons le cas de $r_f = r + 1$ et composons par une réflexion pour augmenter la dimension du sous-espace des vecteurs invariants. On a la décomposition stable :

$$E = \ker(f - \mathrm{id}) \oplus \ker(f - \mathrm{id})^{\perp}$$

Pour $y \in \ker(f - \mathrm{id})^{\perp}$, on a $f(y) \neq y$, et si $H = <f(y) - y>^{\perp}$ est l'hyperplan médiateur de y et $f(y)$, et σ la réflexion par rapport à H alors $\sigma \circ f$ admet le sous-espace $\ker(f - \mathrm{id}) \oplus <y>$ parmi ces vecteurs invariants car $\ker(f - \mathrm{id}) \subset H$, donc par récurrence, c'est un produit de moins de $r_f - 1$ réflexions, on trouve donc que f est produit de r_f réflexions. □

Dans le cas où f a au moins un point fixe, on vectorialise l'espace affine E en un point fixe a, et f s'identifie alors à sa partie linéaire et la proposition donne directement le résultat.

Dans le cas où f n'a pas de point fixe, on peut toujours écrire : $f = t_{\vec{u}} \circ g$ avec g isométrie admettant un point fixe, on compose par une translation de vecteur $A\vec{f(A)}$ avec A quelconque. Comme on peut écrire une translation comme produit de 2 réflexions, on a l'existence d'une décomposition en produit de $r_f + 2$ réflexions. On cherche à montrer l'optimalité de cette borne. Le raisonnement sur la partie linéaire donne $r \geq r_f$. On peut exclure $r = r_f + 1$ en regardant l'orientation : f et g préservent ou renversent l'orientation en même temps, mais g est produit de r réflexions par le cas précédent, donc f ne peut pas être produit de $r + 1$ réflexions. Il reste à exclure le cas $r = r_f$ pour terminer.

Supposons par l'absurde $f = \sigma_1 \circ \cdots \circ \sigma_{r_f}$, alors comme précédemment on a :

$$\bigcap_{i=1}^{r_f} \vec{H_i} = \ker(\vec{f} - \vec{\mathrm{id}})$$

En effet, par dimension, c'est maintenant une égalité. Les hyperplans affines sont alors en position générale et leur intersection est non vide. En effet, on peut le voir par exemple par dualité,

dans un repère affine, $\cap H_i$ est l'ensemble des solutions d'un système linéaire à n inconnues avec second membre, et de rang r, donc admet un sous-espace affine de dimension $n-r$ de solutions. En particulier $\cap_i H_i$ est non vide, mais $\cap H_i \subset Fix(f)$, et on avait supposé que f n'a pas de point fixe, contradiction. $\square$

26 Table des caractères et simplicité du groupe

Ref : Peyré

idée : On cherche à trouver les sous-groupes distingués d'un groupe à partir de sa table des caractères. On va montrer qu'ils apparaissent tous dans la table des caractères, cela nous donnera en particulier un critère de simplicité pour un groupe.

La première remarque est que les noyaux des représentations irréductibles apparaissent sur la table des caractères, en particulier on voit lesquelles sont fidèles.

LEMME 26.1 *Soit (V, ρ) une représentation d'un groupe fini G (pas nécessairement irréductible). Alors :*

$$\ker(\rho) = \{g \in G \quad | \quad \chi(g) = \chi(1)\}$$

PREUVE. Tout repose sur le fait que les $\rho(g)$ sont diagonalisables et leurs valeurs propres sont de module 1. Notons n le cardinal du groupe, par le théorème de Lagrange, on a pour tout g : $\rho(g)^n = \mathrm{id}$. L'endomorphisme $\rho(g)$ est donc annulé par le polynôme $X^n - 1$ qui est scindé à racines simples sur $\mathbb{C}$. La trace est donnée par la somme des valeurs propres, qui sont des racines de l'unité en nombre $\chi(1)$: la dimension de V. L'inégalité triangulaire ainsi que son cas d'égalité montre que $|\chi(g)| \leq \chi(1)$ avec égalité si et seulement si $\rho(g)$ est une homothétie (une seule valeur propre). En particulier, $\chi(g) = \chi(1)$ si et seulement si $\rho(g) = \mathrm{id}$. □

Maintenant, montrons que tout sous-groupe distingué apparait dans la table :

THÉORÈME 26.2 *Soit G un groupe fini et $(\chi_i)_{i=1\ldots r}$ ses caractères irréductibles. Les sous-groupes distingués de G sont exactement les*

$$\bigcap_{i \in I} \ker \chi_i \quad \textit{pour } I \subset \{1, \ldots, r\}$$

PREUVE. Chaque $\ker \chi_i$ est le noyau d'une représentation donc est un sous-groupe distingué. De plus l'intersection de sous-groupes distingués est encore un sous-groupe distingué, donc cela montre un sens du théorème.

Réciproquement, prenons N un sous-groupe distingué de G et on cherche à écrire N en fonction de représentations de G, ce sont celles de G/N qui vont apparaître.

Soit $(V, \tilde{\rho})$ la représentation régulière du groupe G/N, c'est une représentation fidèle. On l'étend en une représentation de G via la projection $G \to G/N$, notée (V, ρ) et son noyau est exactement N. Décomposons (V, ρ) en somme directe des représentations irréductibles de G :

$$V = \bigoplus_{i=1}^{r} a_i V_i$$

où $a_i \in \mathbb{N}$ est le nombre de fois que V_i apparait dans la représentation V. Le noyau de ρ est l'intersection des noyaux des ρ_i, en effet, $\rho(g)$ agit trivialement sur V si et seulement si il agit trivialement sur chacun des sous-espaces V_i. On a donc :

$$N = \bigcap_{i | a_i \neq 0} \ker \rho_i$$

□

COROLLAIRE 26.3 *Un groupe est simple si et seulement si $\forall i \neq 1, \forall g \neq 1, \chi_i(g) \neq \chi_i(1)$*

PREUVE. S'il existe $g \neq 1$, $i \neq 1$ tel que $\chi_i(g) = \chi_i(1)$, alors la représentation χ_i a un noyau non réduit à l'identité, non égal à tout le groupe car $i \neq 1$, et un noyau est toujours distingué.

Réciproquement, le groupe a un sous-groupe distingué non trivial N. D'après le théorème, il s'écrit $N = \cap_{i \in I} \ker \chi_i$ avec $I \neq \{1\}$, tout élément $g \in N$, $g \neq 1$, vérifie $\chi_i(g) = \chi_i(1)$ pour tout $i \in I$ et en particulier pour un certain $i \neq 1$. □

Si le temps le permet, montrer sur la table des caractères de $\mathfrak{S}_4$, les sous groupes distingués à savoir V_4 et $\mathfrak{A}_4$ avec l'inclusion $V_4 \subset \mathfrak{A}_4$.

Leçons concernées : rep, rep de petit cardinal, sous-groupes distingués et quotients.

27 Théorème ergodique de Von-Neumann

Ref : Beck

THÉORÈME 27.1 *Soit H un espace de Hilbert, T un endomorphisme continu de norme ≤ 1 et p est la projection orthogonale sur* $\ker(T-\mathrm{id})$ *(qui est fermé). On pose* $T_n = \frac{1}{n+1}\sum_{k=1}^{n} T^k$. *Alors pour tout* $x \in H$,

$$T_n(x) \xrightarrow[n\to+\infty]{} p(x)$$

PREUVE. idée : Pour $x \in \ker(T-\mathrm{id})$, le résultat est clair, il suffit donc de regarder ce qu'il se passe sur l'orthogonal de $\ker(T-\mathrm{id})$.

Tout d'abord, $\ker(T-\mathrm{id})$ est fermé car c'est le noyau d'un endomorphisme continu. Par le théorème de projection sur un convexe fermé et ses corollaires, on a la décomposition orthogonale :

$$H = \ker(T-\mathrm{id}) \oplus \ker(T-\mathrm{id})^{\perp}$$

Identifions cet orthogonal, on procède en deux temps :
Tout d'abord, on a toujours pour u continu, $\ker(u)^{\perp} = \overline{\mathrm{im}\, u^*}$. En effet, on a :

$$x \in \ker u \Leftrightarrow \forall y, < u(x), y >= 0 \Leftrightarrow < x, u^*(y) >= 0 \Leftrightarrow x \in (\mathrm{im}\, u^*)^{\perp}$$

Puis en passant à l'orthogonal, puisque $F^{\perp\perp} = \overline{F}$, on obtient :

$$\ker(u)^{\perp} = (\mathrm{im}\, u^*)^{\perp\perp} = \overline{\mathrm{im}\, u^*}$$

Ensuite, comme $\|T\| \leq 1$, on a aussi : $\ker(T-\mathrm{id}) = \ker(T^*-\mathrm{id})$ qui donne en passant à l'orthogonal, $\overline{\mathrm{im}(T^*-\mathrm{id})} = \overline{\mathrm{im}(T-\mathrm{id})}$. Montrons ce point :

$$Tx = x \Leftrightarrow < Tx, x >= \|x\|^2 \Leftrightarrow < x, T$$

En effet, le sens direct est clair et l'autre sens provient du cas d'égalité dans Cauchy-Schwarz :

$$\|x\|^2 =< Tx, x >\leq \|T\|\|x\|^2 \leq \|x\|^2$$

Donc, $Tx = \lambda x$ avec $\lambda \geq 0$, et comme $\|T\| \leq 1$, on a $\lambda = 1$.
On a donc montré la décomposition orthogonale :

$$H = \ker(T-\mathrm{id}) \oplus \overline{\mathrm{im}(T-\mathrm{id})}$$

Pour $z = Tx - x$, il y a téléscopage :

$$T_n(z) = \frac{1}{n+1}(T^{n+1}(h) - h) \xrightarrow[n\to\infty]{} 0$$

Pour $y \in \overline{\mathrm{im}(T-\mathrm{id})}$ et $\epsilon > 0$, $\exists z \in \mathrm{im}(T-\mathrm{id})$ tel que $\|y-z\| \leq \epsilon$, d'où :

$$\|T_n(y)\| \leq \|T_n(y) - T_n(z)\| + \|T_n(z)\| \leq \|T_n\|\ \|y-z\| + \|T_n(z)\| \leq 2\epsilon$$

pour n assez grand. Et on a bien $p(y) = 0$ d'après la décomposition orthogonale.

□

COROLLAIRE 27.2 *Soit* $\alpha \in \mathbb{R} \setminus 2\pi\mathbb{Q}$, *alors pour tout* $f \in L^2(\mathbb{R}/2\pi\mathbb{Z})$,

$$\frac{1}{n+1}\sum f(.+k\alpha) \xrightarrow[n\to+\infty]{} c_0(f) = \frac{1}{2\pi}\int_0^{2\pi} f(x)\mathrm{d}x$$

PREUVE. Soit l'opérateur $T : L^2(\mathbb{R}/2\pi\mathbb{Z}) \to L^2(\mathbb{R}/2\pi\mathbb{Z})$ défini par $T(f)(x) = f(x+\alpha)$. Il est clairement continu de norme 1, cherchons ses vecteurs invariants : Les constantes sont invariantes et réciproquement, si $f(. + \alpha) = f(.)$, cela donne une relation sur les coefficients de Fourier de $f : c_n(f) = e^{in\alpha}c_n(f)$. Comme $e^{in\alpha} \neq 1$ pour tout $n \neq 0$, on a $f = c_0$ qui est bien une constante.

Par le théorème, la somme de Cesaro converge pour tout f vers la projection sur la droite vectorielle des constantes, c'est-à-dire vers $c_0(f)$. □

Leçons concernées : Hilbert, applications linéaires continues.

28 Algorithme de décomposition de Dunford

Ref : Risler

THÉORÈME 28.1 *Soit $A \in \mathcal{M}(n,\mathbb{C})$, $P = \prod_{\lambda \in spec(A)}(X-\lambda)$. On construit la suite :*

$$A_0 = 0, \quad A_{k+1} = A_k - P(A_k)P'(A_k)^{-1}$$

La suite est bien définie et stationne en D matrice diagonalisable qui est un polynôme en A, et telle que $A-D$ est nilpotente.

PREUVE.

idée : la partie diagonalisable de A est un polynôme en A et son polynôme minimal est P. Dans le sous-espace $\mathbb{C}[A]$, une matrice annulé par P est diagonalisable avec des valeurs propres incluses dans celle de A. On s'inspire de la méthode de Newton pour trouver un zéro de P dans $\mathbb{C}[A]$, on tombe alors sur D.

LEMME 28.2 *Soit $U \in \mathrm{GL}(n,\mathbb{C})$, N nilpotente et $NU = UN$, alors $U - N \in \mathrm{GL}(n,\mathbb{C})$.*

PREUVE. On écrit :

$$I_n = I_n - (U^{-1}N)^n = (I_n - U^{-1}N)(I_n + \cdots + (U^{-1}N)^{n-1})$$

Donc $I_n - U^{-1}N$ est inversible et $U-N$ également. □

1ère étape :

$$A_k \in \mathbb{C}[A], \exists B_k \in \mathbb{C}[X] | P(A_k) = P(A)^{2^k} B_k(A) \text{ et } P'(A_k) \in \mathrm{GL}(n,\mathbb{C})$$

Par récurrence sur k :

Pour $k=0$, $A_0 = A \in \mathbb{C}[A]$, $P(A_0) = A$ et comme $P \wedge P' = 1$, par Bezout, $UP + VP' = 1$ et en évaluant en A, on trouve : $V(A)P'(A) = I_n - U(A)P(A)$. Or $U(A)P(A)$ est nilpotente car $\chi_A | P^n$. Donc $P'(A) \in \mathrm{GL}(n,\mathbb{C})$ par le lemme précédent et on sait aussi que c'est un polynôme en A (il suffit pour cela d'avoir un polynôme annulateur avec un terme constant non nul).

Pour passer de k à $k+1$, on écrit la formule de taylor pour les polynômes :

$$P(X+Y) = P(X) + YP'(X) + Y^2Q(X,Y)$$

On l'applique en $X = A_k$ et $Y = -P(A_k)P'(A_k)^{-1}$:

$$P(A_{k+1}) = P(A_k) - P(A_k)P'(A_k)^{-1}P'(A_k) + P(A_k)^2P'(A_k)^{-2}Q(A_k,Y) = P(A)^{2^{k+1}}B_{k+1}(A)$$

avec $B_{k+1} \in \mathbb{C}[X]$.

$P'(A_{k+1})$ est encore inversible par le lemme argument que pour $k=0$ puisque $P(A_{k+1})$ est nilpotente. Cela achève la récurrence.

2ème étape :

Si $2^k \geq n$, $P(A_k) = 0$, donc $A_{k+1} = A_k$ et la suite stationne en une matrice notée D. On a $P(D) = 0$, donc D est diagonalisable et c'est un polynôme en A.

$$A - D = A_0 - A_{k+1} = \sum_{i=0}^{k} P(A_i)P'(A_i)^{-1}$$

chaque terme de la somme est nilpotent et les matrices commutent entre elles, donc $A-D$ est nilpotente. □

Remarque : Le polynôme P se calcule sans avoir besoin des valeurs propres car c'est $\frac{\chi}{\chi \wedge \chi'}$. La preuve marche pour un sous-corps de $\mathbb{C}$ en remplaçant diagonalisable par diagonalisable sur $\mathbb{C}$.

Leçons concernées : polynômes d'endo, endo diag, endo trig et nilpotent.

29 Méthode de Newton

Ref : Rouvière p.152 + Dumas

THÉORÈME 29.1 *Soit $f : [c,d] \to \mathbb{R}$ de classe $\mathcal{C}^2$, s'annulant en un unique point a tel que $c < a < d$, avec $f'(a) > 0$. On définit $\varphi : [c,d] \to \mathbb{R}$, de classe $\mathcal{C}^1$, par $\varphi(x) = x - \frac{f(x)}{f'(x)}$.*

1) Il existe $\alpha > 0$, tel que $[a-\alpha, a+\alpha]$ est stable par φ et la suite récurrente définie par :

$$x_0 \in [a-\alpha, a+\alpha] \text{ et } x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

converge vers a au moins à l'ordre 2.

2) Si $f''(a) \neq 0$, la convergence est exactement d'ordre 2.

3) Si $f'(a) = 0$, il y a seulement convergence linéaire a priori.

PREUVE.

Interprétation géométrique : on prend la tangente en x_n et on regarde son intersection avec l'axe des x. On itère ce procédé. L'équation $f(x) = 0$ est équivalent à $f(x) = x$.

1) φ est $\mathcal{C}^1$ de dérivée $\varphi'(x) = 1 - \frac{f'^2 - f''f}{f'^2} = \frac{f''f}{f'^2}$. En particulier, $\varphi'(a) = 0$, donc le point fixe a est superattractif, mais ce n'est pas immédiat que la convergence est d'ordre 2 car φ est seulement $\mathcal{C}^1$.

Comme $|\varphi'(a)| < 1$, il existe $\alpha > 0$ tel que $[a-\alpha, a+\alpha]$ est stable par φ.

Estimons la quantité $\|\varphi(x) - a\|$:

$$\varphi(x) - a = x - a + \frac{f(x) - f(a)}{f'(x)} = \frac{f(a) - f(x) - (a-x)f'(x)}{f''(x)}$$

Par un développement de Taylor-Lagrange à l'ordre 2 pour f, on obtient un $a \in]a, x[$ tel que :

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

En posant $C = \frac{\max|f''|}{2\min f'}$, où les max et min sont pris sur l'intervalle stable $[a-\alpha, a+\alpha]$, on obtient :

$$|\varphi(x) - a| \leq C|x-a|^2$$

Ainsi, $|x_{n+1} - a| \leq C|x_n - a|^2$ et par récurrence $|x_n - a| \leq \frac{1}{C}(C|x_0 - a|)^{2^n}$. D'où la convergence au moins à l'ordre 2.

2) Supposons $f' > 0$ (quitte à prendre $-f$) et $f'' > 0$ sur $[c,d]$ (condition de convexité globale) alors l'intervalle $[a,d]$ est stable et la convergence est d'ordre exactement 2 pour $x_0 \in [a-\alpha, d]$. En effet, si $x_0 \in [a,d]$, comme $\varphi(x) = x - \frac{f(x)}{f'(x)} \leq x$ sur $[a,d]$, x_n est décroissante et ne peut que converger vers a, unique point fixe.

On peut préciser l'ordre de convergence, on va montrer que c'est exactement 2.

Si $a - \alpha \leq x_0 \leq a$, $x_1 \leq a$ puisque $\varphi(x) \leq x$ sur $[a-\alpha, a]$.. Après une itération, on retombe à droite de a, regardons maintenant le cas $x_0 > a$.

Par Taylor-Lagrange à l'ordre 2 pour f :

$$x_{n+1} - a = \frac{f''(z_n)}{2f'(x_n)}(x_n - a)^2$$

avec $a < z_n < x_n$, donc $\frac{f''(z_n)}{2f'(x_n)}$ tend vers $\frac{f''(a)}{2f'(a)}$. D'où l'équivalent :

$$x_{n+1} - a \sim \frac{f''(a)}{2f'(a)}(x_n - a)^2$$

ce qui montre que la convergence n'est pas d'ordre > 2.

3) Si $f'(a) = 0$, on a seulement convergence linéaire. Tout d'abord, φ n'est pas bien définie en a mais le développement limité montre que φ reste $\mathcal{C}^1$.

$$\varphi'(x) = \frac{f(x)f''(x)}{f'(x)^2} = \frac{\frac{1}{2}(x-a)^2 f''(a) + o((x-a)^2)}{((x-a)f''(a) + o(x-a))^2} f''(a) = \frac{1}{2} + o(1)$$

Par le théorème de limite de la dérivée, φ se prolonge en a et est de classe $\mathcal{C}^1$ sur $[c, d]$. De plus, $\varphi'(a) \leq \frac{1}{2}$, donc il y a convergence exactement d'ordre 1 sur un voisinage de a car c'est un point fixe attractif. (S'il y avait convergence d'ordre 2, on aurait $\varphi'(a) = 0$ comme le montre l'inégalité : $|\varphi(x) - a| \leq C|x - a|^2$.) □

Leçons concernées : f(x)=0, développement asymptotique, suites récurrentes, formules de Taylor, (théorèmes de point fixe), fonctions monotones et convexes.

30 Suite récurrente : convergence lente

ref : FGN analyse 1

THÉORÈME 30.1 *Soit f une application définie au voisinage de 0 qui a un développement limité de la forme :*

$$f(x) = x - ax^\alpha + o(x^\alpha)$$

avec $a > 0$ et $\alpha > 1$. Alors la suite récurrente $u_{n+1} = f(u_n)$ admet l'équivalent :

$$u_n \sim \frac{1}{(na(\alpha-1))^{\frac{1}{1-\alpha}}}$$

PREUVE. Le développement montre que f est continue en 0 et dérivable en 0. De plus, le développement montre que $0 < f(x) < x$ sur $]0, \eta]$ pour un $\eta < 0$. L'intervalle $[0, \eta]$ est donc stable par f et la suite u_n est bien définie si $u_0 \in [0, \eta]$ et est décroissante. Elle converge donc vers 0 qui est l'unique point fixe de f sur $[0, \eta]$.

Comme $f'(0) = 1$, 0 n'est pas un point fixe attractif (au sens : $|f'(0)| < 1$), en particulier on n'a pas de convergence géométrique. Si u_n convergeait au moins géométriquement (à l'ordre 1), alors $0 \leq u_n \leq k^n$ avec un $k < 1$ pour n assez grand et donc $\frac{f(u_n)}{u_n} = \frac{u_{n+1}}{u_n} \leq k < 1$ et la dérivée en 0, si elle existe est plus petite que k.

On va utiliser le deuxième terme du développement de Taylor de f pour préciser la vitesse de convergence de (u_n). Pour cela, raisonnons par analogie avec une équation différentielle :

$u_{n+1} - u_n$ s'interprète comme une dérivée discrète $\Delta(u_n)$, on a donc $\Delta(u_n) = -au_n^\alpha + o(u_n^\alpha)$.

Les solutions de $y' = -ay^\alpha$ vérifient $y^{1-\alpha} = -a(1-\alpha)t$, donc on s'attend à un équivalent de la forme $u_n \sim C.n^{\frac{1}{1-\alpha}}$.

$$\begin{aligned} u_{n+1}^{1-\alpha} - u_n^{1-\alpha} &= f(u_n)^{1-\alpha} - u_n^{1-\alpha} \\ &= (u_n - au_n^\alpha + o(u_n^\alpha))^{1-\alpha} - u_n^{1-\alpha} \\ &= u_n^{1-\alpha}(1 - a(1-\alpha)u_n^{\alpha-1} + o(u_n^{\alpha-1})) - u_n^{1-\alpha} \\ &= a(\alpha-1) + o(1) \end{aligned}$$

La série de terme constant $a(\alpha-1)$ diverge grossièrement, donc les sommes partielles sont équivalentes :

$$u_n^{1-\alpha} \sim na(\alpha-1)$$

Puis,

$$u_n \sim (na(\alpha-1))^{\frac{1}{1-\alpha}}$$

□

Application : $f(x) = \ln(1+x) = x - \frac{x^2}{2} + o(x^2)$, on trouve $u_n \sim \frac{2}{n}$.

En écrivant plus de termes dans le développement de Taylor de f, on trouve des termes supplémentaires dans le développement asymptotique de (u_n) :

Ici, on a $\alpha = 2$, donc l'équation importante est :

$$\frac{1}{u_{n+1}} - \frac{1}{u_n} = \frac{1}{\ln(1+u_n)} + \frac{1}{u_n}$$

Développons, le terme de droite à l'ordre 1 :

$$\frac{1}{\ln(1+x)} - \frac{1}{x} = \frac{1}{x - \frac{x^2}{2} + \frac{x^3}{3} + o(x^3)} - \frac{1}{x} = \frac{1}{x}(1 + \frac{x}{2} - \frac{x^2}{3} + \frac{x^2}{4} + o(x^2)) - \frac{1}{x} = \frac{1}{2} - \frac{x}{12} + o(x)$$

Donc,

$$\frac{1}{u_{n+1}} - \frac{1}{u_n} = \frac{1}{2} - \frac{u_n}{12} + o(u_n)$$

Comme $u_n \sim \frac{2}{n}$, la série des u_n diverge et les sommes partielles sont équivalentes :

$$\frac{1}{u_n} = \frac{n}{2} - \frac{\ln n}{12} + o(\ln n) = \frac{n}{2}(1 - \frac{\ln n}{6n} + o(\frac{\ln}{n}))$$

Donc,

$$u_n = \frac{2}{n}\frac{1}{1 - \frac{\ln n}{6n}} = \frac{2}{n}(1 + \frac{\ln n}{6n} + o(\frac{\ln n}{n})) = \frac{2}{n} + \frac{\ln n}{3n^2} + o(\frac{\ln n}{n^2})$$

Leçons concernées : convergence de suite, comportement asymptotique, suite récurrente, $f(x) = 0$.

31 Méthode du gradient conjugué

Ref : Allaire, Dumas, Ciarlet.

THÉORÈME 31.1 *Soit $A \in \mathrm{S}^{++}(n,\mathbb{R})$ et $b \in \mathbb{R}^n$. On prend $x_0 \in \mathbb{R}^n$ quelconque et on définit $r_0 = b - Ax_0$ et ses sous-espaces vectoriels (dits de Krylov) associés :*

$$K_m(r_0) = \mathrm{Vect}\{r_0, \dots, A^m r_0\}$$

Il existe une unique suite (x_m) définie par récurrence par les conditions :

$$x_m \in x_0 + K_{m-1} \quad , \quad r_m = b - Ax_m \perp K_{m-1} \quad et \quad r_m \in K_m$$

et cette suite stationne vers l'unique solution de $Ax = b$ après au plus n itérations.

idée : On introduit la fonctionnelle quadratique $J(x) = \frac{1}{2} < Ax, x > - < b, x >$, comme A est définie positive, les niveaux de J sont l'image par une transformation affine de cercles concentriques. Il existe donc un unique minimum que l'on cherche numériquement par une méthode de descente. Ce minimum est alors un point critique de J, c'est-à-dire une solution de $\nabla J(x) = Ax - b = 0$.

PREUVE. Remarquons tout d'abord que la suite des sous-espaces vectoriels (K_m) est strictement croissante pour l'inclusion puis stationne. En effet, la suite est croissante et doit stationner car $\mathbb{R}^n$ est de dimension finie. De plus, si i désigne le plus petit indice tel que $K_{m_0} = K_{m_0+1}$ alors K_{m_0} est stable par A puisque $A(A^{m_0} r_0) \in K_{m_0}$ et (K_m) stationne alors à partir de m_0.

On cherche x_m sous la forme $x_m = x_0 + y_m$ avec $y_m \in K_{m-1}$. Remarquons que $r_m = Ax_0 + Ay_k - b = r_0 + Ay_m \in K_m$.

La condition d'orthogonalité s'écrit :

$$\begin{aligned} < b - Ax_m, \vec{y} >= 0, \forall y \in K_m &\Leftrightarrow < b - Ax_0 - Ay_m, y >= 0, \forall y \in K_m \\ &\Leftrightarrow < A^{-1} r_0 - y_m, y >_A = 0, \forall y \in K_m \end{aligned}$$

C'est-à-dire, y_m est la projection orthogonale de $A^{-1} r_0$ sur K_m pour le produit scalaire défini par A, qui est bien défini de manière unique. D'où l'existence et l'unicité de x_m.

Au rang critique k_0, on trouve $r_{m_0+1} \in K_{m_0+1} = K_{m_0}$ mais aussi $r_{m_0+1} \perp K_{m_0}$, c'est-à-dire, $r_{m_0+1} = 0$ et x_{m_0+1} est solution du système linéaire et $m_0 + 1 \leq n$, on a fait au plus n itérations. □

Cette preuve est théorique et ne donne pas immédiatement d'algorithme pour mettre la méthode en pratique. Voyons comment le mettre en oeuvre.

Au cours de la preuve, on a vu que (r_m) est une famille orthogonale pour le produit scalaire usuel et que $K_m = \mathrm{Vect}(r_0, \dots, r_m)$. Introduisons les directions de descentes $d_m = x_{m+1} - x_m \in K_m$. La famille d_k est A-orthogonale : en effet un récurrence immédiate donne : pour $m \geq l$,

$$< Ad_{m+1}, d_l >=< Ax_{m+2} - Ax_{m+1}, d_l >=< r_{m+2} - r_{m+1}, d_l >= 0$$

La famille (d_m) apparait alors comme une orthogonalisée de Gram-Schmidt des (r_m) pour le produit scalaire défini par A.

Expliquer sur un dessin, la différence entre la direction du gradient et la direction conjuguée : en dimension 2, on termine en 2 coups. Voici donc l'algorithme :

Soit $p_0 = r_0$ et pour $m \geq 0$,

$$p_m = r_m - \sum_{j=0}^{m-1} \frac{< r_m, p_j >_A}{< p_j, p_j >_A} p_j = r_m - \sum_{j=0}^{n-1} \beta_j p_j$$

où

$$\beta_j = \frac{< r_m, p_j >_A}{< p_j, p_j >_A}$$

C'est une famille orthogonalisée de Gram-Schmidt de (r_m), elle diffère de d_m par des constantes positives : $\exists \alpha_m > 0$ tel que :

$$d_m = x_{m+1} - x_m = \alpha_m p_m$$

On cherche alors une méthode itérative pour calculer les β_j et les α_m.

On a :

$$r_{m+1} - r_m = A(x_m - x_{m+1}) = -\alpha_m A p_m$$

Donc :

$$< r_m, p_j >_A = < r_m, \frac{r_j - r_{j+1}}{\alpha_j} >$$

Puis,

$$\beta_j = 0 \text{ si } j \leq m-2, \quad = -\frac{< r_m, r_m >}{\alpha_{m-1} < p_{m-1}, p_{m-1} >_A} \text{ si } j = m-1$$

Enfin, α_m s'obtient par orthogonalité des r_i :

$$< r_{m+1} - r_m >= 0 = < r_m - \alpha_m A p_m, r_m >= \|r_m\|^2 - \alpha_m < A p_m, p_m + \beta_{m-1} p_{m-1} >= \|r_m\|^2 - \alpha_m \|p_m\|_A^2$$

Donc

$$\alpha_m = \frac{\|r_m\|^2}{\|p_m\|_A^2}$$

On en déduit un algorithme itératif : On choisit x_0 quelconque, on pose $p_0 = b - Ax_0$, puis :

$$r_{m+1} = r_m - \frac{\|r_m\|^2}{\|p_m\|_A^2} A p_m$$
$$p_{m+1} = r_{m+1} + \frac{\|r_{m+1}\|^2}{\|r_m\|_A^2} p_m$$
$$x_{m+1} = x_m + \frac{\|r_{m+1}\|^2}{\|p_{m+1}\|_A^2} p_m$$

Remarque : L'indice m est plus pertinent que k pour éviter de prononcer "caca" qui peut déstabiliser le jury et soi-même.

Leçons concernées : Problème d'extremum, f(x)=0, systèmes linéaires.

32 $\mathcal{D}(\Omega)$ est dense dans $L^p(\Omega)$

Ref : Brézis en anglais p.109.

THÉORÈME 32.1 *Soit Ω un ouvert de $\mathbb{R}^N$, l'espace $\mathcal{D}(\Omega)$ des fonctions $\mathcal{C}^\infty$ à support compact inclus dans Ω.*

PREUVE. idée : On va procéder par convolution par une approximation de l'unité sur $\mathbb{R}^n$, puis traiter le cas d'un ouvert quelconque Ω par troncature. On admet le fait que $\mathcal{C}_c^0$ est dense dans L^p (provient de la régularité de la mesure de Lebesgue). On se donne une approximation de l'unité ρ_n, vérifiant :

$$\rho_n \in \mathcal{C}_c^\infty(\mathbb{R}^N), \quad \text{supp}(\rho_n) \subset \overline{B}(0, \frac{1}{n}), \quad \int \rho_n = 1, \quad \rho_n \geq 0$$

LEMME 32.2 *Soit $f \in \mathcal{C}^0(\mathbb{R}^N)$, alors $\rho_n * f \xrightarrow[n\to\infty]{} f$ uniformément sur tout compact.*

PREUVE. Soit K un compact et $\epsilon > 0$. Par le théorème de Heine, f étant continue sur le ϵ-voisinage compact de K, il existe $\delta > 0$ tel que

$$|f(x-y) - f(x)| < \epsilon, \quad \forall x \in K, \forall y \in B(0, \delta)$$

Ecrivons alors, pour $x \in \mathbb{R}^N$,

$$(\rho_n * f)(x) - f(x) = \int (f(x-y) - f(x))\rho_n(y)\mathrm{d}y = \int_{B(0,\frac{1}{n})} (f(x-y) - f(x))\rho_n(y)\mathrm{d}y$$

Pour $n > \frac{1}{\delta}$ et $x \in K$, on trouve :

$$|(\rho_n * f)(x) - f(x)| \leq \epsilon \int \rho_n = \epsilon$$

□

Traitons le cas $\Omega = \mathbb{R}^N$:
Soit $\epsilon > 0$, on utilise la densité de $\mathcal{C}_c^0$ dans L^p : soit $f_1 \in C_c^0(\mathbb{R}^N)$ tel que $\|f - f_1\|_1 < \epsilon$.
D'après le lemme, $\rho_n * f_1 \xrightarrow[n\to+\infty]{} f_1$ uniformément sur les compacts. Comme ρ_n et f_1 sont à supports compacts, cette convergence est globale :

$$\text{supp}(\rho_n * f_1) \subset \overline{B}(0, \frac{1}{n}) + \text{supp}(f_1) \subset \overline{B}(0,1) + \text{supp}\, f_1$$

Cette dernière partie est compacte, donc on a convergence uniforme sur ce compacte, donc convergence L^p :

$$\|\rho_n * f_1 - f_1\|_p \xrightarrow[n\to\infty]{} 0$$

Reste à faire un coup d'inégalité triangulaire :

$$\|\rho_n * f - f\|_p \leq \|\rho_n * (f - f_1)\|_p + \|\rho_n * f_1 - f_1\| + \|f_1 - f\|$$

Par l'inégalité de young, $\|\rho_n * (f - f_1)\|_p \leq \|f - f_1\|_p$.
En passant à la limité supérieure, on trouve :

$$\limsup_{n\to\infty} \|\rho_n * f - f\|_p \leq 2\epsilon, \quad \forall \epsilon > 0$$

D'où :

$$\rho_n * f \xrightarrow[n\to\infty]{} f \text{ dans } L^p$$

Cas d'un ouvert Ω quelconque :

La difficulté supplémentaire est que $\rho_n * f$ n'est pas à support dans Ω mais dans $\Omega + \overline{B}(0, \frac{1}{n})$. On va d'abord réduire un peu le support de f puis convoler par ρ_n de telle sorte qu'on reste à support dans Ω.

Prenons $f \in L^p(\Omega)$ qu'on étend sur $\mathbb{R}^N$ en posant $f = 0$ hors de Ω. Prenons un exhaustion de Ω par des compacts :

$$K_n = \{x \in \mathbb{R}^N | d(x, \mathbb{R}^N \setminus \Omega) \geq \frac{2}{n}\}$$

Comme Ω est ouvert, pour tout $x \in \Omega$, $d(x, \mathbb{R}^N \setminus \Omega) < 0$.

On pose alors $f_n = \mathbb{1}_{K_n} f$ si bien que :

$$\text{supp}(\rho_n * f_n) \subset \overline{B}(0, \frac{1}{n}) + K_n \subset \Omega$$

Donc $\rho_n * f_n \in \mathcal{D}(\Omega)$ et on a :

$$\begin{aligned} \|\rho_n * f_n - f\|_{L^p(\Omega)} &= \|\rho_n * f_n - f\|_{L^p(\mathbb{R}^N)} \\ &\leq \|\rho_n * f_n - f_n\|_{L^p(\mathbb{R}^N)} + \|f_n - f\|_{L^p(\mathbb{R}^N)} \end{aligned}$$

Par convergence dominée, $f_n \xrightarrow[n\to+\infty]{} f$ dans $L^p(\mathbb{R}^N)$, et par le lemme, $\rho_n * f \xrightarrow[n\to+\infty]{} f$ dans $L^p(\mathbb{R}^N)$. D'où $f_n \xrightarrow[n\to+\infty]{} f$ dans $L^p(\Omega)$. □

33 Topologie des classes de similitude

Ref : FGN, algèbre 1.

THÉORÈME 33.1 *Soit $A \in \mathcal{M}(n, \mathbb{C})$.*
- *A est nilpotente si et seulement si la classe de similitude de A adhère à 0.*
- *A est diagonalisable si et seulement si la classe de similitude est fermée.*

PREUVE.
Tout repose sur le lemme suivant :

LEMME 33.2 *Dans la classe de similitude de A, on peut trouver des matrices triangulaires supérieures dont les coefficients strictement au-dessus de la diagonale sont arbitrairement petits.*

PREUVE. Comme $\mathbb{C}$ est algébriquement clos, on peut commencer par trigonaliser : $T = P^{-1}AP$. Soit f l'endomorphisme canoniquement associé à T et $\mathcal{B}$ la base canonique de $\mathbb{C}^n$. Modifions la base $\mathcal{B}$ par le procédé suivant : $\mathcal{B}' = (e'_1 = \epsilon e_1, e'_2\epsilon^2 e_2, \ldots, e'_n\epsilon^n e_n)$. Dans cette base, on a :

$$f(e'_j) = f(\epsilon^j e_j) = \epsilon^j f(e_j) = \epsilon^j \sum_i t_{i,j} e_i = \sum_i t_{i,j}\epsilon^{j-i} e'_i$$

Pour $j > i$, les coefficients surdiagonaux $t_{i,j}\epsilon^{j-i}$ sont arbitrairement petit quand ϵ est petit. □

Cas nilpotent
Si A est nilpotente, le lemme nous fournit des matrices semblables à A avec des coefficients surdiagonaux petits et les termes diagonaux sont les valeurs propres, c'est-à-dire 0 puisque A est nilpotente. On trouver donc dans la classe de similitude de A des matrices aussi proche de 0 que l'on veut.

Réciproquement, par continuité du polynôme caractéristique par rapport à la matrice : si A_p tend vers B avec A_p semblable à A.

$$\chi_A = X^n = \chi_B$$

Donc B est nilpotente par Cayley-Hamilton.
Cas diagonalisable
Si A est diagonalisable, son polynôme minimal π_A est scindé à racines simples. Si A_p tend vers B avec A_p semblable à A, on a $\pi_A(A_p) = 0$ pour tout p, et en passant à la limite : $\pi_A(B) = 0$, donc B est diagonalisable. De plus, A et B ont même polynôme caractéristique par continuité du polynôme caractéristique :

$$\chi_A = \chi_{A_p} \xrightarrow[p\to\infty]{} \chi_B$$

Donc A et B sont diagonalisables et ont même polynôme caractéristique donc sont semblables.
Réciproquement, si la classe de similitude est fermée, on trouve des matrices diagonales dans la classe de similitude par le lemme. □

Leçons concernées : endo diag, endo nilpotents, polynômes d'endomorphismes.

34 Table des caractères de $\mathfrak{S}_4$

Ref : Maison + Fulton-Harris.

THÉORÈME 34.1 *On va faire la table des caractères de $\mathfrak{S}_4$ et on en déduira que $\mathfrak{S}_4/V_4 \simeq \mathfrak{S}_3$.*

PREUVE.

	1 id	6 (12)	8 (123)	3 (12)(34)	6 (1234)
1	1	1	1	1	1
ϵ	1	-1	1	1	-1
T	3	1	0	-1	-1
ϵ T	3	-1	0	-1	1
W	2	0	-1	2	0

On commence par remplir le caractère trivial et le signature. Ensuite, on va trouver une représentation de dimension 3 de manière géométrique à partir du tétraèdre.

PROPOSITION 34.2 *Soit T un tétraèdre régulier de l'espace affine euclidien. On a l'isomorphisme de groupe :*

$$\mathrm{Isom}(T) \simeq \mathfrak{S}_4$$

PREUVE.

Une isométrie (même une transformation affine) du tétraèdre permute les sommets car ce sont les seuls points extrémaux du tétraèdre et que la notion d'extrémalité est affine. D'où le morphisme de groupes :

$$\mathrm{Isom}(T) \to \mathfrak{S}_4$$

Ce morphisme est injectif car une transformation affine, et a fortiori une isométrie, est déterminée par l'image d'une base affine et les sommets en forment une. Il est surjectif car l'image contient les transpositions que l'on réalise par les réflexions par rapport aux plans médiateurs aux arêtes. C'est donc un isomorphisme. □

Cela fournit une représentation de dimension 3 :

$$\mathfrak{S}_4 \to \mathrm{O}(3,\mathbb{R}) \to \mathrm{GL}(3,\mathbb{C})$$

On va calculer son caractère, montrer qu'il est de longueur 1 et en déduire qu'il est irréductible.
On calcule la trace de chaque isométrie :

- Transpositions : ce sont des réflexions par rapport aux plans médiateurs (déjà vu), donc c'est de trace 1.
- 3-cycles : ce sont des rotations d'angle $\frac{2\pi}{3}$, donc de trace $1 + 2\cos(\frac{2\pi}{3}) = 0$.
- bitranspositions : ce sont des symétries par rapport à des droites, donc de trace -1.
- 4-cycles : on calcule sa matrice dans la base (e_1, e_2, e_3), des vecteurs joignant le centre à 3 sommets. On trouve $\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$ qui est de trace -1.

On calcule :

$$< \chi_T, \chi_T >= \frac{1}{24}(3^2 + 6 \times 1 + 8 \times 0 + 3 \times (-1)^2 + 6 \times (-1)^2) = 1$$

Donc c'est bien une représentation irréductible (il est légitime de l'écrire dans la table).

On en trouve une autre en tordant T par le caractère signature qui est bien irréductible car on a $< \chi_{\epsilon T}, \chi_{\epsilon T} >=< \chi_T, \chi_T >$.

D'après la théorie des caractères, il y a autant de caractères irréductibles que de classes de conjugaison et on trouve sa dimension par la formule :

$$\sum_{W \text{ irr}} (\dim W)^2 = |G|$$

On calcule :

$$1^2 + 1^2 + 3^2 + 3^2 + x^2 = 24$$

C'est donc une représentation de dimension 2 que l'on note W. On trouve son caractère en utilisant l'orthogonalité des colonnes. On a terminé la table des caractères.

Petite application : On remarque que dans cette représentation le sous-groupe distingué V_4 des bitranspositions agit trivialement. En effet, ce sont des endomorphismes d'ordre 2, donc de valeur propre ± 1, et leur trace valant 2, c'est id. (Plus généralement, $\ker \rho = \{g \in G | \chi(g) = \chi(1)\}$ par le même raisonnement sur les valeurs propres).

On en déduit donc une représentation du quotient par passage au quotient :

$$\mathfrak{S}_4/V_4 \to \mathrm{GL}(W)$$

Cette représentation est encore irréductible car si V est une sous-représentation, c'est aussi une sous-représentation de $\mathfrak{S}_4$ puisque V_4 agit trivialement, donc c'est W ou $\{0\}$.

Le groupe quotient $\mathfrak{S}_4/V_4$ admet donc une représentation irréductible de dimension 2, donc ce n'est pas un groupe abélien, c'est donc isomorphe à $\mathfrak{S}_3$.

On comprend alors que la représentation W est la représentation du quotient $\mathfrak{S}_3$ qui agit par isométrie du triangle équilatéral.

□

Remarque : L'isomorphisme $\mathfrak{S}_4/V_4 \simeq \mathfrak{S}_3$ se montre aussi par l'argument de Gromov : $2+2 = 4$ de trois façons différentes. Ce développement est un va et vient constant entre algèbre et géométrie, c'est la motivation principale.

Leçons concernées : Représentations, Représentations petit cardinal, Groupe symétrique, Groupe fini, Groupes en géométrie, Isométrie d'un espace affine, Groupe opérant sur un ensemble, (Groupe distingué et quotient).

35 Diagonalisabilité et semi-simplicité

Ref : Mneimné, Tauvel.

THÉORÈME 35.1 *Soit E un k-espace vectoriel de dimension finie et $u \in \mathrm{End}(E)$.*
- *u est diagonalisable si et seulement si tout sous-espace admet un supplémentaire stable.*
- *u est diagonalisable si et seulement si χ_u est scindé et tout sous-espace* stable *admet un supplémentaire stable.*

PREUVE.
Si u est diagonalisable
Son polynôme caractéristique est scindé ce que l'on voit en mettant u sous forme diagonale, et par invariance de χ par changement de base.

Soit F un sous-espace de E. Soit $(e_1, \dots, e_n)$ une base de vecteurs propres de u et $(f_1, \dots, f_p)$ une base de F. Par le théorème de la base incomplète, on peut compléter la famille libre $(f_1, \dots, f_p)$ en une base de E en rajoutant $n-p$ vecteurs parmi la base $(e_1, \dots, e_n)$, quitte à réindexer, on peut supposer que c'est $(e_{p+1}, \dots, e_n)$, ces vecteurs engendrent alors un sous-espace stable supplémentaire de F.

Si tout sous-espace admet un supplémentaire stable.

On construit une base de vecteurs propres de la manière suivante : Prenons un hyperplan H quelconque, il existe une droite stable supplémentaire, donc dirigée par un vecteur propre e_1. Si on a construit une famille libre de vecteurs propres $(e_1, \dots, e_k)$, on prend un hyperplan contenant $\mathrm{Vect}(e_1, \dots, e_k)$, et on trouve une droite stable $\mathrm{Vect}(e_{k+1})$ supplémentaire à H. On conclut par récurrence.

Si χ_u est scindé et tout sous-espace stable admet un supplémentaire stable

On raisonne par récurrence sur la dimension. En dimension 1, c'est clair puisque tout endomorphisme est diagonal. Si c'est vrai en dimension $n-1$, montrons le en dimension n. Comme χ_u est scindé, u admet un vecteur propre, qui dirige donc une droite stable. Par hypothèse, on peut trouver un hyperplan stable H supplémentaire à cette droite. L'endomorphisme induit u_H est encore scindé car χ_{u_H} divise χ_u. Il est également semi-simple : si F est un sous-espace de H stable par u_H. Vu comme sous-espace de E, F est stable par u, donc admet un supplémentaire G dans E, stable par u. On a donc la décomposition $E = F \oplus G$ respectée par u. On intersecte avec H, et on obtient, comme $F \subset H$, $H = F \oplus (G \cap H)$ et $G \cap H$ est un supplémentaire de F dans H stable par u_H.

On conclut par récurrence. □

On peut utiliser ce critère (qui est élémentaire) pour faire une preuve géométrique (sans polynôme annulateur) du fait suivant :

COROLLAIRE 35.2 *Soit u un endomorphisme diagonalisable de E et F un sous-espace stable par u, alors l'endomorphisme induit u_F est diagonalisable.*

PREUVE. Soit F stable par u, et soit G un sous-espace de F stable par u_F. Le premier critère dit que G admet un supplémentaire H dans E stable par u, on intersecte avec F, comme $G \subset F$:

$$F = G \oplus (H \cap F)$$

$H \cap F$ est donc un supplémentaire de G dans F, stable par u_F. Donc u_F est diagonalisable d'après le premier critère du théorème. □

36 $\exp : \mathrm{S}(n,R) \to \mathrm{S}^{++}(n,\mathbb{R})$

THÉORÈME 36.1 $\exp : \mathrm{S}(n,R) \to \mathrm{S}^{++}(n,\mathbb{R})$ *est un homéomorphisme.*

PREUVE. *Espace d'arrivée :*

Si $A \in \mathrm{S}(n,\mathbb{R})$, d'une part $\exp(A)$ est symétrique, d'autre part, par le théorème spectral, A est diagonalisable : $\exists P \in \mathrm{GL}(n,\mathbb{R})$, (en fait $\mathbb{O}(n,\mathbb{R})$)

$$P^{-1}AP = \mathrm{diag}(\lambda_i)$$

Alors $P^{-1}\exp(A)P = \mathrm{diag}(\exp\lambda_i)$, donc ses valeurs propres sont strictement positives, donc $\exp(A) \in \mathrm{S}^{++}(n,\mathbb{R})$.

Bijectivité :

Soit $B \in \mathrm{S}^{++}(n,\mathbb{R})$ défini positive, si $B = \exp(A)$, avec $A \in \mathrm{S}(n,\mathbb{R})$. On va voir que A est déterminée par B. Si $\lambda \in \mathrm{Sp}(A)$, alors $E_\lambda(A) \subset E_{e^\lambda}(B)$. Comme A est symétrique, elle est diagonalisable en base orthonormée, donc :

$$\mathbb{R}^n = \bigoplus E_\lambda(A) \subset \bigoplus E_{e^\lambda}(B)$$

Donc pour tout λ, il y a égalité $E_\lambda(A) = E_{e^\lambda(B)}$. Donc A et B ont les mêmes sous-espaces propres, et sur chacun le rapport d'homothétie de A est le logarithme de celui de B, uniquement déterminé car $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est bijective. Réciproquement l'endomorphisme construit ainsi est bien un logarithme symétrique de B ; Cela donne l'injectivité et la bijectivité de l'application.

Homéomorphisme :

L'exponentielle est continue car la série la définissant est normalement convergente. Il reste à montrer que la réciproque est continue. On va utiliser le critère séquentielle et on rau besoin de contrôler des matrices par leur spectre ce qui est légitimé par le lemme suivant :

LEMME 36.2 *Soit A une matrice symétrique, alors $\rho(A) = \|A\|_2$.*

PREUVE. Tout d'abord, $\|\|_2$ est invariant par conjugaison par $\mathrm{O}(n)$. En effet, $\|O^{-1}AO(x)\|_2 = \|Ax\|_2$. Comme les matrices symétriques sont diagonalisables en base orthonormée, il suffit de calculer la norme 2 d'une matrice diagonale. Si $A = \mathrm{diag}(\lambda_1,\dots,\lambda_n)$ avec $\lambda_1 \le \cdots \le \lambda_n$, on a :

$$\|Ax\|_2^2 = \sum_i \lambda_i^2 x_i^2 \le \rho(A)^2\|x\|_2^2$$

Donc $\|A\|_2 \le \rho(A)$.

$$\|Ae_n\|_2^2 = \rho(A)^2 x_n^2 = \rho(A)^2\|x_2\|^2$$

Donc $\|A\|_2 = \rho(A)$. □

Si $A_p = \exp(B_p)$ et $A = \exp(B)$ avec $A_p \xrightarrow[p\to\infty]{} A$, montrons que $B_p \xrightarrow[n\to\infty]{} B$. On a $A_p \to A$ et $A_p^{-1} \to A$ par continuité de l'application inverse sur $\mathrm{GL}(n,\mathbb{R})$. Par le lemme, cela implique que $\rho(A_p) \xrightarrow[p\to\infty]{} \rho(A)$ et $\rho(A_p^{-1}) \xrightarrow[p\to\infty]{} \rho(A^{-1})$. En particulier, les spectres des matrices (A_p) sont dans un compact commun de $\mathbb{R}_+^*$. Par passage au logarithme, les valeurs propres de B_p restent dans un compact commun de $\mathbb{R}$ et par le sens difficile du lemme, la suite B_p est bornée. Ainsi B_p admet une sous-suite convergente par Bolzano-Weierstrass, vers une matrice $\tilde{B}$ qui est encore symétrique car $\mathrm{S}(n,\mathbb{R})$ est fermé et on a $\exp(\tilde{B}) = \exp(B)$ par continuité de l'exponentielle. On trouve donc $\tilde{B} = B$ par injectivité de exp, puis B_p n'ayant qu'une seule valeur d'adhérence, converge en fait vers B. □

37 Théorème de Pascal

ref : Eiden

THÉORÈME 37.1 *Soit $\mathcal{C}$ une conique non dégénérée du plan projectif et six points distincts A, B, C, A', B' et C' sur $\mathcal{C}$. On construit $R = (AB') \cap (A'B)$, $Q = (CA') \cap (C'A)$ et $P = (B'C) \cap (BC')$. Alors les points P, Q et R sont alignés.*

PREUVE. Les coniques projectives non dégénérées sont équivalentes, en effet, elles sont données par les zéros d'une forme quadratique non dégénérée à 3 variables, dont le seul invariant affine est la signature. La seule signature intéressante est $(2,1)$ car la signature $(3,0)$ donne une conique vide et les autres signatures s'obtiennent à partir de celles-ci en multipliant la forme quadratique par -1, ce qui ne change pas la conique. On peut donc trouver une homographie (du plan projectif réel, donc un élément de $\mathrm{PGL}(3,\mathbb{R})$) qui envoie la conique $\mathcal{C}$ sur un cercle que l'on peut supposer être le cercle unité $\mathbb{U}$ de $\mathbb{C}$. Les homographies préservent les notions d'incidence, donc il suffit de démontrer le théorème de Pascal sur le cercle unité $\mathbb{U}$.

On va maintenant utiliser les nombres complexes via la structure de droite projective complexe et le groupe $\mathrm{PGL}(2,\mathbb{C})$.

Un certain type d'homographie se prête bien au problème, ce sont les involutions de Frégier :

PROPOSITION 37.2 *On définit une involution de Frégier de centre $a \in P^2(\mathbb{R}) \setminus \mathbb{U}$ comme l'application de $\mathbb{U}$ dans $\mathbb{U}$ qui envoie un point m sur l'autre intersection m' de la droite (am) avec $\mathbb{U}$. Si cette droite est tangente, on pose $m' = m$. Alors ces transformations sont la restriction à $\mathbb{U}$ d'éléments d'ordre 2 de $\mathrm{PGL}(2,\mathbb{C})$.*

PREUVE. Si $a \in \mathbb{C}$ (pas à l'infini), on cherche le point m' sous la forme $m' = a + \lambda(m-a)$ (c'est-à-dire sur la droite (am)), solution de de $z\overline{z} = 1$ (c'est-à-dire sur $\mathbb{U}$). On trouve l'équation vérifiée par λ :

$$\lambda((m-a)\overline{a} + (\overline{m} - \overline{a})a) + \lambda^2 |m-a|^2 = 1 - |a|^2$$

On sait que $\lambda = 1$ est solution car $m \in \mathbb{U}$, il est donc facile de trouver la deuxième racine :

$$\lambda = \frac{|a|^2 - 1}{|m-a|^2}, \quad \text{puis,} \quad m' = \frac{a-m}{1-\overline{a}m}$$

C'est bien la forme d'une homographie de $\mathbb{P}^1(\mathbb{C})$. On obtient le cas où a est à l'infini, en passant à la limite : si $a = Re^{i\theta}$ avec $R \to \infty$, on trouve $m' = -\frac{e^{2i\theta}}{m}$ à la limite, qui est encore bien une homographie. On remarque que des valeurs de θ qui diffèrent d'un multiple de π donnent la même transformation après envoi du point à l'infini ce qui est cohérent.

Voici les expressions matricielles (relevées à $\mathrm{GL}(2,\mathbb{C})$) de ces homographies :

$$\begin{pmatrix} -1 & a \\ -\overline{a} & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & -e^{2i\theta} \\ 1 & 0 \end{pmatrix}$$

Un calcul montre que leurs carrés sont des homothéties, donc ces homographies sont d'ordre 2. Remarque : Quitte à multiplier par un scalaire non nul, on peut trouver un représentant dan $\mathrm{GL}(2,\mathbb{C})$ qui soit d'ordre 2, on a que deux choix : il faut choisir une racine carrée de $1 - \overline{a}a$. □

Voici pourquoi les involutions de Frégier se prêtent bien au problème. Tout d'abord, elles sont liés à l'alignement via le fait évident : pour Y, Z sur le cercle, $I_X(Y) = Z \Leftrightarrow X, Y, Z$ alignés.

Notons $P_0 \in P^2(\mathbb{R})$ l'intersection de (QR) et $(B'C)$, il suffit de montrer que $P_0 \in (BC')$, c'est-à-dire $P_0 = P$.

La transformation $J = I_{P_0} \circ I_Q \circ I_R$ vérifie, par construction, $J(B) = B'$. Si on arrive à montrer qu'elle est involutive, on aura aussi $J(B') = B$, mais $J(B') = I_{P_0}(C')$. Donc B, C' et P_0 sont alignés.

Il reste à montrer que J est involutive, pour cela on va utiliser un peu de connaissance du groupe $\mathrm{PGL}(2,\mathbb{C})$.

LEMME 37.3 – *Un élément de* $\mathrm{PGL}(2,\mathbb{C})$ *est d'ordre* 2 *si et seulement si il est de trace nulle.*
– *Si* X, Y, Z *sont alignés dans* $P^2(\mathbb{R})$, *l'homographie* $J = I_X \circ I_Y \circ I_Z$ *est d'ordre 2.*

PREUVE. Le premier point est un calcul. Attention, la trace n'est définie qu'à un facteur multiplicatif non nul près, mais "trace nulle" a un sens.

Pour le deuxième point, calculons la trace du produit. Il y a trois cas à distinguer selon que les points sont à l'infini ou non.

Si tous les points sont alignés sur la droite à l'infini, les matrices des homographies sont de la forme :

$$\begin{pmatrix} 0 & -e^{2i\theta_j} \\ 1 & 0 \end{pmatrix}$$

Elles permutent donc les droites $< e_1 >$ et $< e_2 >$ en somme directe dans $\mathbb{C}^2$. Si on en compose trois comme ça, on trouve donc une matrice de trace nulle car permute encore les deux droites. (ou sinon on peut faire le calcul).

Si les trois points sont dans le plan affine, les matrices des involutions sont :

$$U = \begin{pmatrix} -1 & a \\ -\overline{a} & 1 \end{pmatrix}.V = \begin{pmatrix} -1 & b \\ -\overline{b} & 1 \end{pmatrix}.W = \begin{pmatrix} -1 & \mu a + (1-\mu)b \\ -\mu\overline{a} - (1-\mu)\overline{b} & 1 \end{pmatrix}$$

pour un $\mu \in \mathbb{R}$. On écrit alors

$$\mathrm{tr}(WVU) = (1-\mu)\,\mathrm{tr}(V^2U) + \mu\,\mathrm{tr}(UVU) = (1-\mu)(1-\overline{b}b)\,\mathrm{tr}(U) + \mu(1-\overline{a}a)\,\mathrm{tr}(V) = 0 + 0 = 0$$

car $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. La même formule permet de se restreindre à cet ordre du produit WVU.

Il reste le cas où un des point est à l'infini (si deux y sont le troisième aussi), il s'obtient par passage à la limite du cas précédent. □ □

Leçons concernées : nbre complexe en géométrie, groupes en géométrie, coniques.

38 Irréductibilité de Φ_n

ref : Perrin

THÉORÈME 38.1 *Le polynôme Φ_n est irréductible sur $\mathbb{Q}$.*

PREUVE. L'idée est de montrer que Φ_n est le polynôme minimal de ζ pour $\zeta \in \mu_n^*$ quelconque. Un polynôme minimal est toujours irréductible presque par définition et on a ce polynôme miminal divise Φ_n. Pour montrer l'autre divisibilité, la proposition clé est la suivante :

PROPOSITION 38.2 *Soit $\zeta \in \mu_n^*$ et p premier ne divisant pas n. On note f et g les polynômes minimaux de ζ et ζ^p sur $\mathbb{Q}$. Alors f et g sont dans $\mathbb{Z}[X]$ et $f = g$.*

PREUVE. On a $\zeta^n = (\zeta^p)^n = 1$ donc f et g divisent $X^n - 1$. Mais comme $\mathbb{Z}[X]$ est factoriel (Gauss), on peut décomposer ce dernier en produit de polynômes irréductibles sur $\mathbb{Z}[X]$ et unitaire :

$$X^n - 1 = P_1 \times \cdots \times P_r$$

Chaque P_i est unitaire et irréductible sur $\mathbb{Z}$ donc par Gauss, P_i est irréductible sur $\mathbb{Q}$, et par unicité, la décomposition ci-dessus est la décomposition en produits d'irréductibles dans $\mathbb{Q}[X]$. Ainsi, f et g figurent parmi les P_i et sont donc dans $\mathbb{Z}[X]$.

Si f et g étaient distincts, on aurait fg divise $X^n - 1$ puisque f et g sont premiers entre eux (irréductibles distincts). Soit $h = g(X^p)$, on a $h(\zeta) = 0$ donc f divise h dans $\mathbb{Q}[X]$, mais aussi dans $\mathbb{Z}[X]$ car f est unitaire. En réduisant modulo p, on trouve $\overline{h} = (\overline{g}(X))^p$ d'après le morphisme de Frobenius. Donc tout facteur irréductible φ de $\overline{f}$ dans $\mathbb{F}_p[X]$ (attention $\overline{f}$ n'est pas irréductible dans $\mathbb{F}_p[X]$ a priori), apparait dans $\overline{h}$ donc dans $\overline{g}$, donc φ^2 divise $X^n - \overline{1}$. Mais $X^n - \overline{1}$ est premier avec sa dérivée $\overline{n}X^{n-1} - \overline{1}$ puisque $\overline{n} \neq 0$ dans $\mathbb{F}_p$, donc n'admet pas de facteur carré. C'est contradictoire, donc $f = g$. □

A partir de la proposition, on remarque que si f est le polynôme minimal de ζ, ζ^p est aussi racine de f, et par récurrence immédiate, $\zeta^{p_1^{\alpha_1} \cdots p_m^{\alpha_m}}$ avec $p_i \not| n$ est racine de f. Autrement dit, f contient toutes les racines primitives n-ièmes de l'unité (qui sont les ζ^m avec $m \wedge n = 1$), donc $\deg f \geq \deg \Phi_n$, puis $f = \Phi_n$. □

Remarque : comme Φ_n est à coefficients entiers et unitaire, il est aussi irréductible sur $\mathbb{Z}$.

Rappel : Si $n \geq 1$ et k est un corps de caractéristique ne divisant pas n, le polynôme $P_n(X) = X^n - 1$ est séparable : ses racines dans un corps de décomposition K_n de k sont simples. En effet, $P_n' = nX^{n-1}$ donc $P_n \wedge P_n' = 1$. L'ensemble $\mu_n(K_n)$ des racines de P_n est un sous-groupe de K_n^* donc est cyclique. Il est d'ordre n car les racines de $X^n - 1$ sont simples. Ses générateurs forment une partie à $\varphi(n)$ éléments appelés racines *primitives* n-ièmes de l'unité. On définit alors

$$\Phi_{n,k} = \prod_{\zeta \in \mu_n(K_n)^*} (X - \zeta)$$

Dans le cas où $k = \mathbb{Q}$, on trouve le polynôme de $\mathbb{C}[X]$:

$$\Phi_n = \prod_{m \wedge n = 1} (X - e^{\frac{2i\pi m}{n}})$$

En partitionant $\mu_n(K_n)$ selon l'ordre de ses éléments, on trouve la formule :

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Cette formule permet de montrer par récurrence sur n que :

- Φ_n est à coefficients entiers
- Φ_n est universel au sens où on obtient les autres (sur un corps k) comme image de Φ_n par le morphisme $\mathbb{Z}[X] \to k[X]$

Leçons concernées : groupes des nombres complexes de module 1, polynôme irréductible, anneaux Z/nZ.

39 Théorème de Dirichlet version faible

ref : ?

THÉORÈME 39.1 *Soit $n \geq 2$, il existe une infinité de nombres premiers de la forme $1 + an$ avec $a \in \mathbb{N}$ (c'est-à-dire dans la classe de 1 modulo n).*

PREUVE. Commençons par un lemme qui nous fournit un critère pour trouver des nombres premiers congrus à 1 modulo n parmi les facteurs premiers de $\Phi_n(a)$.

LEMME 39.2 *Soit $a \in \mathbb{N}$ et p premier tel que : p divise $\Phi_n(a)$ et p ne divise pas $\Phi_d(a)$ pour d divisant n et $d \neq n$. Alors :*

$$p = 1 \pmod{n}$$

PREUVE. On écrit la relation liant les polynômes cyclotomiques :

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

On a p divise $\Phi_n(a)$, donc p divise $a^n - 1$, autrement dit $a^n = 1$ dans $\mathbb{Z}/p\mathbb{Z}$. L'ordre ω de a dans $\mathbb{Z}/p\mathbb{Z}^\times$ est alors un diviseur de n. On réexploite une deuxième fois la relation entre polynômes cyclotomiques :

$$a^\omega - 1 = \prod_{d|\omega} \Phi_d(a)$$

Le premier membre vaut 0 modulo p alors que le deuxième est non nul sauf si $\omega = n$ par hypothèse. Ensuite, le théorème de Lagrange dans $\mathbb{Z}/p\mathbb{Z}^*$ donne n divise $p-1$, c'est-à-dire $p = 1 \pmod{n}$. □

La stratégie est de trouver des nombres premiers congrus à 1 modulo n arbitrairement grand, fixons donc $N \geq 1$ et cherchons $p > N$. On pose $a = 3 \times N!$, ce nombre a l'avantage d'être grand et de contenir tous les facteurs premiers jusque N, c'est tout ce qu'on lui demande.

$$|\Phi_n(a)| = \prod |a - e^{\frac{2ik\pi}{n}}| \geq \prod (a-1) \geq 2$$

$\Phi_n(a)$ contient donc un facteur premier $p \geq 2$, on va montrer qu'il est plus grand que N et qu'il est congru à 1 modulo n.

Pour le premier point, on remarque que si $p \leq N$, p divise a, donc p divise $\Phi_n(a) - \Phi_n(0)$ qui est un polynôme en a sans facteur constant. Comme p divise $\Phi_n(a)$, il divise aussi $\Phi_n(0) = \pm 1$. C'est absurde, donc $p > N$.

Pour le deuxième point, on utilise le lemme : le polynôme $X^n - 1$ est à racines simples dans $\mathbb{Z}/p\mathbb{Z}$ car il est premier avec son polynôme dérivé nX^{n-1} ($n \neq 0 \pmod{p}$ car $p > N \geq n$ ne peut diviser n). Or p ne peut pas diviser un autre $\Phi_d(a)$ pour $d|n$, $d \neq n$, sans que a soit racine double de $X^n - 1$, donc d'après le lemme $p = 1 \pmod{n}$. □

Remarque : 1) La version forte établit la même chose dans la classe de m modulo n dès que $m \wedge n = 1$.

2) On utilise un peu de connaissance des polynômes cyclotomiques, à mettre dans le plan ou à démontrer si le temps le permet.

Leçons concernées : anneaux $\mathbb{Z}/n\mathbb{Z}$, nombres premiers, nombres complexes de module 1.

40 Table des caractères de D_4 et H_8

ref : Maison

THÉORÈME 40.1 *Les groupes D_4 et H_8 ont même table des caractères mais ne sont pas isomorphes*

PREUVE. Commençons par D_4. Il s'agit du groupe d'isométrie du carré, il est engendré par un rotation r et une réflexion s. Conjuguer une rotation par une symétrie donne la rotation d'angle opposé : $srs^{-1} = r^{-1}$. Alors que conjuguer une rotation par une symétrie donne une symétrie d'axe bougé par la rotation : $rsr^{-1} = s_{r(axe)}$. Ces relations permettent de donner les classes de conjugaison :

$$\{\mathrm{id}\}, \{-\mathrm{id}\}, \{r, r^{-1}\}, \{s, rsr^{-1}\}, \{sr, rs\}$$

Le carré donne une représentation de dimension 2 (via complexification : $\mathrm{O}(2,\mathbb{R}) \to \mathrm{GL}(2,\mathbb{R}) \to \mathrm{GL}(2,\mathbb{C})$). Elle est irréductible car sinon, il y aurait un vecteur propre commun à toutes les transformations de D_4, mais deux symétries d'axe non orthogonaux n'ont aucun vecteur propre commun, donc ce n'est pas possible. On peut commencer la table des caractères avec la triviale et celle de dimension 2 du carré.

	1 id	1 $-\mathrm{id}$	2 r	2 s	2 rs
trivial	1	1	1	1	1
	1	1	1	-1	-1
	1	1	-1	1	-1
	1	1	-1	-1	1
Carré	2	-2	0	0	0

On sait que la somme des carrés des dimensions des représentations irréductibles vaut 8, cela force les trois dernières représentations à être de dimension 1. On cherche alors des morphismes de D_4 dans $\mathbb{C}^*$. Les symétries étant d'ordre 2 sont envoyées dans $\{\pm 1\}$ et la rotation est le produit de deux symétries donc envoyées aussi dans $\{\pm 1\}$. On cherche donc des morphismes $D_4 \to \{\pm 1\}$. Ils sont déterminés par l'image des générateurs r et s, il n'y a aucune contrainte car la seule relation à vérifier est $srs^{-1} = r^{-1}$ qui est clairement vérifié dans $\{\pm 1\}$. On complète donc en mettant ± 1 pour r et s et les autres sont déterminés (noter que $-\mathrm{id} = r^2$).

Passons à H_8. C'est l'ensemble $\{\pm 1, \pm i, \pm j, \pm k\}$ avec les relations $ij = k$, $jk = ki$, $ki = j$ et $i^2 = j^2 = k^2 = \pm 1$. Le centre est $\{\pm 1\}$ et on a par exemple $jij^{-1} = -i$, les classes de conjugaison sont donc :

$$\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}$$

On quotiente par le centre $\{\pm 1\}$, on trouve un groupe d'ordre 4 dont tous les éléments sauf le neutre sont d'ordre 2, c'est donc $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ses représentations sont de dimension 1 car c'est un groupe abélien, elles sont "produits" de représentations de $\mathbb{Z}/2\mathbb{Z}$, on remplit la table avec celles-là qui sont triviales sur -1. On trouve la dernière (de dimension 2) par orthogonalité des colonnes.

	1 1	1 -1	2 i	2 j	2 k
trivial	1	1	1	1	1
	1	1	1	-1	-1
	1	1	-1	1	-1
	1	1	-1	-1	1
	2	-2	0	0	0

On remarque que les tables des caractères sont les mêmes. Pourtant les groupes ne sont pas isomorphes : il y a 2 éléments d'ordre 4 dans D_4 (r et r^{-1}) alors qu'il y en a 6 dans H_8.

□

41 Enveloppe convexe du groupe orthogonal

ref : Giorgi ?

THÉORÈME 41.1 *L'enveloppe convexe de* $\mathrm{O}(n,\mathbb{R})$ *est la boule unité de* $\mathcal{M}(n,\mathbb{R})$ *pour la norme* 2.

PREUVE. Commençons par une proposition :

PROPOSITION 41.2 *Le dual de* $\mathcal{M}(n,\mathbb{K})$ *est l'ensemble des applications de la forme* $M \to \mathrm{tr}(AM)$ *pour* $A \in \mathcal{M}(n,K)$.

PREUVE. On définit l'application linéaire $\mathcal{M}(n,\mathbb{K}) \to \mathcal{M}(n,\mathbb{K})^*$ qui à A associé $\mathrm{tr}(A.)$. Son noyau est l'ensemble des matrices A telles que $\mathrm{tr}(AM) = 0$ pour tout $M \in \mathcal{M}(n,\mathbb{K})$. On applique cela pour chaque matrice élémentaire $M = E_{i,j}$. Cela donne : $0 = \mathrm{tr}(AE_{i,j}) = a_{j,i}$, puis $A = 0$. □

Comme $\mathrm{O}(n)$ est compact, son enveloppe convexe est aussi compacte d'après Carathéodory ($[0,1]^{n+1} \times K \to \mathrm{conv}(K)$ est continue surjective). Une matrice orthogonale est de norme 2 égale à 1, et la boule unité est convexe par inégalité triangulaire. D'où $\mathrm{conv}(\mathrm{O}(n)) \subset K$. Pour l'autre sens, on va utiliser le théorème de Hahn Banach. Si $M \in K \setminus \mathrm{conv}(\mathrm{O}(n))$, on peut séparer strictement le convexe compact $\{M\}$ du convexe fermé $\mathrm{conv}(\mathrm{O}(n))$ par un hyperplan : il existe φ forme linéaire sur $\mathbb{M}(n,\mathbb{R})$ telle que $\sup_{O\in\mathrm{O}(n)} \varphi(O) < \varphi(M)$. Par contraposée, il suffit donc de montrer que pour toute forme linéaire φ, on a :

$$\varphi(M) \leq \sup_{O\in\mathrm{O}(n)} \varphi(O)$$

D'après la proposition, cela revient à montrer cela pour $\varphi = \mathrm{tr}(A.)$.

On utilise la décomposition polaire : $A = \Omega S$ avec $\Omega \in \mathrm{O}(n)$ et $S \in \mathrm{S}^+(n,\mathbb{R})$. Soit (e_i) est une base orthonormée de vecteurs propres pour S.

Majorons donc $\mathrm{tr}(AM)$, écrivons :

$$\mathrm{tr}(AM) = \mathrm{tr}(MA) = \sum_i < MAe_i, e_i >= \sum_i < Ae_i, M^*e_i > \leq \sum_i \|Ae_i\|\|M^*\|_2 \leq \sum_i \|Ae_i\|$$

car $\|M^*\|_2 = \|M\|_2 \leq 1$.

On a alors d'une part

$$\sum_i \|Ae_i\| = \sum_i \|Se_i\|$$

et d'autre part

$$\sup_{O\in\mathrm{O}(n,\mathbb{R})} \mathrm{tr}(AO) \geq \mathrm{tr}(A\Omega^{-1}) = \mathrm{tr}(\Omega^{-1}\Omega S) = \mathrm{tr}(S) = \sum_i < Se_i, e_i >= \sum_i \|Se_i\|$$

car e_i propre pour S à valeur propre positive.

On a donc ben $\mathrm{tr}(AM) \leq \sup_{O\in\mathrm{O}(n)} \mathrm{tr}(AO)$ pour tout $A \in \mathbb{M}(n,\mathbb{R})$. Donc la boule unité pour la norme 2 de $\mathcal{M}(n,\mathbb{R})$ est bien l'enveloppe convexe de $\mathrm{O}(n,\mathbb{R})$. □

Leçons concernées : formes linéaires et hyperplans, endo remarquable d'un ev euclidien, matrices symétriques et réelles, convexité barycentres.

42 Théorème des lacunes d'Hadamard

ref : ZQ

Définition: Soit $f(z) = \sum a_n z^n$ une série entière de rayon de convergence 1. Un point du cercle $\mathbb{U}$ est dit *régulier* si f admet un prolongement analytique sur un voisinage de ce point, il est dit *singulier* sinon.

La première remarque est que tous les points du bord ne peuvent être réguliers, sinon f aurait un prolongement analytique sur un disque de rayon $1+\epsilon$ (par compacité du cercle) et d'après la formule de Cauchy, f étant holomorphe admet un développement en série entière $\sum b_n z^n$ de rayon $1+\epsilon$. (on utilise ici holomorphe implique analytique avec DSE sur le plus grand disque possible). Par unicité du développement, $a_n = b_n$ est la série $\sum a_n z^n$ est de rayon > 1, contradiction.

On donne maintenant une condition suffisante pour que tous les points du bord soient singuliers.

THÉORÈME 42.1 (LACUNES D'HADAMARD) *Soit $(\lambda_n)_{n\geq 1}$ une suite d'entiers > 0 tels que $\frac{\lambda_{n+1}}{\lambda_n} \geq \alpha > 1$. Soit une série entière $\sum a_n z^{\lambda_n}$ de rayon de convergence 1. Alors tous les points du bord sont singuliers.*

PREUVE. idée : la série entière est de rayon 1 bien qu'elle soit lacunaire, c'est donc que ses coefficients non nuls sont trop gros pour que la fonction s'étende analytiquement. On va donc supposer par l'absurde qu'un point est régulier (1) et on va montrer qu'alors le rayon doit être strictement plus grand que 1, contradiction.

Si on montre que 1 est singulier, alors pour tout $e^{i\theta} \in \mathbb{U}$, la série $\sum a_n e^{i\theta\lambda_n} z^{\lambda_n}$ est toujours de rayon 1 car la taille des coefficients n'a pas changé et toujours lacunaire, donc 1 est singulier pour cette série, c'est-à-dire $e^{i\theta}$ est singulier pour la série initiale $\sum a_n z^{\lambda_n}$.

Supposons donc que f admet un prolongement analytique sur l'ouvert $\Omega = D \cup D(1,\eta)$.

Comme $\frac{\lambda_{n+1}}{\lambda_n} \geq \alpha > 1$, on peut trouver $p \in \mathbb{N}$ tel que $\frac{p+1}{p} \leq \alpha$ et donc $p\lambda_{n+1} \geq (p+1)\lambda_n$.

On introduit alors la fonction

$$\varphi(z) = \frac{z^{p+1} + z^p}{2}$$

qui a deux vertus : elle envoie un disque $D(0,1+\epsilon)$ dans Ω, et $\varphi(z)^{\lambda_n}$ et $\varphi(z)^{\lambda_{n+1}}$ sont des polynômes de degrés disjoints.

En effet, si $z \in \overline{D}\{1\}$, $\frac{|z^p(z+1)|}{2} < 1$ et $\varphi(1) = 1$. Donc $\varphi(\overline{D}) \subset \Omega$ mais comme $\overline{D}$ est compact, Ω ouvert et φ continue, on peut trouver $\epsilon > 0$ tel que $\varphi(\overline{D}(0,1+\epsilon)) \subset \Omega$.

La fonction $g \circ \varphi$ est donc holomorphe sur $D(0,1+\epsilon)$ comme composée de deux fonctions holomorphes. Par la formule de Cauchy, $g \circ \varphi$ admet un développement en série entière centré en 0 de rayon $\geq 1+\epsilon$:

$$g \circ \varphi(z) = \sum b_n z^n$$

Par unicité du développement en série entière et comme il n'y a pas de mélange entre les $(\frac{z^p+z^{p+1}}{2})^{\lambda_n}$ pour différentes valeurs de n, on peut écrire pour $N \in \mathbb{N}$ et $z \in \mathbb{C}$,

$$\sum_{n=0}^{N} a_n (\frac{z^p + z^{p+1}}{2})^{\lambda_n} = \sum_{n=0}^{(p+1)\lambda_N} b_n z^n$$

En prenant $z \in]1, 1+\epsilon[$, et en faisaint tendre N vers l'infini, on aboutit à une contradiction :

– Le premier membre diverge grossièrement car $|\frac{z^p+z^{p+1}}{2}| > 1$ et la série $\sum a_n z^{\lambda_n}$ est de rayon 1.

– Le second membre converge car $|\frac{z^p+z^{p+1}}{2}| < (1+\epsilon)$ et la série $\sum b_n z^n$ est de rayon $\geq 1+\epsilon$.
Leçons concernées : prolongement de fonction, séries entières, fonctions holomorphes. □

43 Algorithme de Berlekamp

ref : Beck On cherche à trouver tous les facteurs irréductibles de P, on peut le faire algorithmiquement grâce au théorème suivant.

THÉORÈME 43.1 *Soit $P \in \mathbb{F}_q[X]$ un polynôme sans facteur carré. On peut calculer le nombre de facteurs irréductibles et si il y en a plusieurs on peut trouver effectivement (algorithmiquement) un polynôme $V \in \mathbb{F}_q[X]$ tel que V soit non constant modulo P et :*

$$P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, V - \alpha)$$

PREUVE. Remarquons que si V est non constant modulo P, $\operatorname{pgcd}(P, V - \alpha)$ est un diviseur strict de P pour tout α, donc on a décomposé P en produit de facteurs de degré strictement plus petits, on peut alors itérer le procéder, jusqu'à tomber sur les facteurs irréductibles.

$\mathbb{F}_q[X]$ est une $\mathbb{F}_q$-algèbre et (P) est un idéal de cette algèbre, donc on peut quotienter : $R = \mathbb{F}_q[X]/(P)$ est encore une $\mathbb{F}_q$-algèbre. L'élévation à la puissance q dans cette algèbre est $\mathbb{F}_q$ linéaire d'après le morphisme de Frobenius : $(x+y)^q = x^q + y^q$ et $x^q = 1$ pour $x \in \mathbb{F}_q$. C'est donc un endomorphisme de $\mathbb{F}_q$-algèbres. L'ensemble de ses points fixes $\ker(\varphi - \mathrm{id})$ forme alors une sous-algèbre de R.

Grâce au lemme chinois, on peut décomposer l'algèbre R : si $P = P_1 \times \cdots \times P_r$ est la décomposition de P en facteurs irréductibles, comme P est dans facteur carré les P_i sont premiers entre eux deux à deux. On a donc l'isomorphisme ψ de $\mathbb{F}_q$-algèbres suivant :

$$R \to \mathbb{F}_q[X]/P_1 \times \cdots \times \mathbb{F}_q[X]/P_r$$

Chaque facteur est un corps car les P_i sont irréductibles.

On peut alors transporter l'endomorphisme de Frobenius par cet isomorphisme :

$$\tilde{\varphi} = \psi \circ \varphi \circ \psi^{-1}$$

L'endomorphisme $\tilde{\varphi}$ de $\mathbb{F}_q$-algèbre correspond à l'élévation à la puissance q sur chaque facteur, en effet :

$$\psi \circ \varphi \circ \psi^{-1}(x) = \psi(\psi^{-1}(x))^q = (\psi(\psi^{-1}(x)))^q = x^q$$

Comme chaque facteur est une extension de $\mathbb{F}_q$, on a $x^q = x \Leftrightarrow x \in \mathbb{F}_q$, en effet, les éléments de $\mathbb{F}_q$ vérifient l'équation (par Lagrange) et il n'y a que q solutions a une équation de degré q dans un corps. Donc $\ker(\tilde{\varphi} - \mathrm{id}) = \mathbb{F}_q^r$ et $r = \dim \ker(\tilde{\varphi} - \mathrm{id}) = \dim \ker(\varphi - \mathrm{id})$. Ce nombre se calcule donc par un programme d'algèbre linéaire (on écrit cet endomorphisme dans la base $(1, x, \ldots, x^{\deg P - 1})$ de $\mathbb{F}_q[X]/(P)$ et on réduit la matrice sous forme échelonnée par pivot).

Maintenant, si $r \geq 2$, comme la droite $\mathbb{F}_q.1$, on peut trouver $V \in \ker(S - \mathrm{id})$ non constant, c'est-à-dire $V^q - V \pmod P$ non constant.

On a alors $V \pmod{P_i} = \alpha_i \in \mathbb{F}_q$. Donc P_i divise $V - \alpha_i$, et donc $P = P_1 \ldots P_r$ divise $\prod \operatorname{pgcd}(P, (V - \alpha))$ comme les P_i sont premiers entre eux. Dans l'autre sens, les $\operatorname{pgcd}(P, (V - \alpha))$ sont premiers entre eux deux à deux et divisent tous P, donc le produit divise P. D'où l'égalité voulue :

$$P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, V - \alpha)$$

Chaque facteur de ce produit est de degré strictement plus petit par ce qu'on a déjà remarqué, donc l'algorithme termine.

□

Remarque : Si P a des facteurs multiples, on prend :

$$\frac{P}{\text{pgcd}(P, P')}$$

qui est alors sans facteur carré.

Leçons concernées : corps finis, polynômes irréductibles.

44 Théorème fondamental des courbes dans l'espace

ref : Ramis-Deschamps-Odoux 5

THÉORÈME 44.1 *On se place dans un espace affine euclidien orienté E de direction $\vec{E}$ de dimension 3. Soit φ et ψ des applications d'un intervalle I à valeurs réelles. On suppose φ de classe $\mathcal{C}^1$ et strictement positive et ψ continue. Alors il existe un arc géométrique $\mathcal{C}^3$ orienté et birégulier admettant un paramétrage par longueur d'arc défini sur J dont les courbures et torsions sont respectivement φ et ψ. Deux tels arcs solutions diffèrent d'un déplacement de l'espace.*

PREUVE. idée : une courbe est définie par son vecteur tangent en intégrant. Si on adjoint au vecteur tangent, les vecteurs normaux et binormaux, le trièdre qu'ils forment est solution d'une équation différentielle linéaire, on peut alors utiliser Cauchy-Lipschitz.

Rappel :

Etant donné un arc paramétré par longueur d'arc $\alpha : I \to E$ de classe $\mathcal{C}^3$ et birégulier ($T' \neq 0$), on rappelle les formules de Serret-Frénet qui donnent l'équation différentielle vérifié par la base de Frénet :$(T(s), N(s), B(s))$,

$$T'(s) = \kappa(s)N(s), \quad N'(s) = -\kappa(s)N(s) - \gamma(s)B(s), \quad B'(s) = \gamma(s)N(s)$$

Existence :

Fixons une base orthonormée directe (u_0, v_0, w_0) de $\vec{E}$. Le système différentiel linéaire de $\vec{E}^3$ donné par :

$$U'(s) = \varphi(s)V(s), \quad V'(s) = -\varphi(s)V(s) - \psi(s)W(s), \quad W'(s) = \psi(s)V(s)$$

admet d'après le théorème de Cauchy-Lipschitz linéaire, une unique solution (U, V, W) définie sur I telle que $(U(0), V(0), W(0)) = (u_0, v_0, w_0)$.

Montrons qu'alors $(U(s), V(s), W(s))$ est une base orthonormée directe pour tout $s \in \mathbb{R}$. On pose $P(s)$ la matrice 3×3 dont les colonnes sont $(U(s), V(s), W(s))$ dans la base (u_0, v_0, w_0). On a alors :

$$P'(s) = P(s)A(s) \text{ avec } A(s) = \begin{pmatrix} 0 & -\varphi(s) & 0 \\ \varphi(s) & 0 & \psi(s) \\ 0 & -\psi(s) & 0 \end{pmatrix}$$

Donc en dérivant P^tP, on trouve :

$$(P^tP)' = P'({}^tP) + P({}^tP)' = PA^tP - PA^tP = 0$$

Comme $P^tP = I_n$ en $s = s_0$, $P(s)$ est orthogonale pour tout s et comme $\det(P) > 0$ en $s = s_0$ $P(s)$ reste dans $\mathrm{SO}(n)$ par connexité.

On définit alors l'arc α qui passe par α_0 à l'instant s_0 :

$$\alpha(s) = \alpha_0 + \int_{s_0}^{s} U(\sigma)\mathrm{d}\sigma$$

D'après le système différentiel, on voit que U est $\mathcal{C}^2$ car φ et V sont $\mathcal{C}^1$. Donc l'arc α est $\mathcal{C}^3$. On a $\alpha'(s) = U(s)$, donc U est le vecteur tangent T. Ensuite, $\alpha''(s) = U'(s) = \varphi(s)V(s)$, et comme $V(s)$ est unitaire et $\varphi(s)$ est strictement positive, $V(s)$ est le vecteur normal $N(s)$ et φ est la courbure κ. Enfin, $W(s)$ est le vecteur binormal B car (U, V, W) est une base orthonormée directe, puis, $V'(s) = -\varphi(s)V(s) - \psi(s)W(s)$, donc la torsion γ de cette courbe est ψ.

Unicité à déplacement près :

Si $\beta : I \to \mathbb{R}$ est un autre arc solution, par unicité dans Cauchy-Lipschitz, sa base de Frénet (T, N, B) satisfait la même équation différentielle, et la condition initiale s'ajuste par l'unique rotation g de l'espace $\vec{E}$ qui envoie $(T(s_0), N(s_0), B(s_0))$ sur (u_0, v_0, w_0) et le point de départ $\beta(s_0)$ s'ajuste par une translation de vecteur $a = \beta(s_0)\vec{\alpha_0}$: l'arc $a + g(\beta(s_0)\vec{\beta}(s))$. On utilise ici le fait que les déplacements agissent transitivement sur les repères orthonormés directs, on peut écrire le déplacement explicitement comme : $f(M) = \alpha_0 + g(\beta(s_0)\vec{M})$. □

Leçons concernées : étude métrique des courbes, équa diff linéaire.

45 Equation de la chaleur sur le cercle

ref : Candelpergher + Maison

THÉORÈME 45.1 *Soit $u_0 \in L^2(\mathbb{R}/2\pi\mathbb{Z};\mathbb{R})$. L'équation de la chaleur $\partial_t u = \partial_{xx} u$ admet une unique solution u :$]0,+\infty[\times\mathbb{R}/2\pi\mathbb{Z} \to \mathbb{R}$ de classe $\mathcal{C}^2$ telle que $u(t,.) \to u_0$ dans $L^2(\mathbb{R}/2\pi\mathbb{Z})$.*

PREUVE. On raisonne par analyse synthèse :
Analyse :
Prenons u solution du problème.
Pour chaque instant t, $x \mapsto u(t,x)$ est de classe $\mathcal{C}^1$, donc sa série de Fourier est normalement convergente et est égale à la fonction :

$$\forall t > 0, \forall x \in \mathbb{R}/2\pi\mathbb{Z}, \quad u(t,x) = \sum_{n\in\mathbb{Z}} c_n(t) e^{inx}$$

où $c_n(t) = \frac{1}{2\pi}\int_0^{2\pi} u(t,x)e^{-inx}\mathrm{d}x$.
Comme u est $\mathcal{C}^1$ des deux variables et $[0,2\pi]$ est un segment, la fonction c_n est $\mathcal{C}^1$ sur $]0,+\infty[$ par dérivation sous le signe intégral et $c_n'(t) = \frac{1}{2\pi}\int_0^{2\pi} \partial_t u(t,x)e^{-inx}\mathrm{d}x$.
On utilise maintenant l'équation, puis des intégrations par parties où on utilise la périodicite :

$$\begin{aligned} c_n'(t) = \frac{1}{2\pi}\int_0^{2\pi} \partial_x x u(t,x)e^{-inx}\mathrm{d}x &= \frac{1}{2\pi}[\partial_x u(t,x)e^{-inx}]_0^{2\pi} + \frac{in}{2\pi}\int_0^{2\pi} \partial_x u(t,x)e^{-inx}\mathrm{d}x \\ &= 0 + \frac{in}{2\pi}[u(t,x)e^{-inx}]_0^{2\pi} - \frac{n^2}{2\pi}\int_0^{2\pi} u(t,x)e^{-inx}\mathrm{d}x \\ &= 0 + 0 - n^2 c_n(t) \end{aligned}$$

Donc en résolvant l'équation différentielle, on trouve pour $t > 0$,

$$c_n(t) = c_n^0 e^{-n^2 t}$$

On voudrait montrer que les c_n^0 sont les coefficients de u_0 en passant à la limite quand t tend vers 0. C'est possible par le théorème de Parseval : puisque $u(t,.) \to u_0$ dans L^2, par l'isométrie $L^2 \to l^2$, $(c_n(t)) \to c_n(u_0)$ dans l^2, donc pour tout n, $c_n^0 = c_n(u_0)$. On peut alors écrire la solution u en fonction de la donnée initiale u_0 : $\forall t > 0, \forall x \in \mathbb{R}/2\pi\mathbb{Z}$,

$$u(t,x) = \sum_{n\in\mathbb{Z}} c_n(u_0)e^{-n^2 t}e^{inx} = \sum_{n\in\mathbb{Z}}(\frac{1}{2\pi}\int_0^{2\pi} u_0(y)e^{-iny}\mathrm{d}y)e^{-n^2 t}e^{inx}$$

Comme pour $t > 0$ et $x \in \mathbb{R}$,

$$\sum_n \int_0^{2\pi} |u_0(y)|e^{-n^2 t}\mathrm{d}y < +\infty$$

Par le théorème de convergence dominée, on peut intervertir les sommations :

$$u(t,x) = \frac{1}{2\pi}\int_0^{2\pi}(\sum_{n\in\mathbb{Z}} e^{-n^2 t}e^{in(x-y)})u_0(y)\mathrm{d}y$$

On reconnait alors un produit de convolution par le noyau de la chaleur défini par : $\forall t > 0$, $\forall x \in \mathbb{R}/2\pi\mathbb{Z}$,

$$K(t,x) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} e^{-n^2 t}e^{inx}$$

Synthèse :

Il reste à vérifier que $u(t,x) = K(t,x) * u_0(x)$ est bien solution du problème. Il faut d'abord vérifier la régularité, on va voir l'effet régularisant de l'équation de la chaleur : montrons que u est $\mathcal{C}^\infty$ sur $]0,+\infty[\times\mathbb{R}/2\pi\mathbb{Z}$. On pose $K_n(t,x) = \frac{1}{2\pi}e^{-n^2t}e^{inx}$ si bien que $K = \sum K_n$. Pour $k,l \in \mathbb{N}$, $x \in \mathbb{R}/2\pi\mathbb{Z}$ et $t > a > 0$,

$$|\frac{\partial^{k+l}}{\partial t^k \partial x^l}K(t,x)| \leq \frac{1}{2\pi}n^{2k+l}e^{-n^2a}$$

Le second membre est un terme général de série convergente, donc par le théorème de dérivation sous le signe somme, K est $\mathcal{C}^\infty$ sur $]a,+\infty[\times\mathbb{R}/2\pi\mathbb{Z}$, et ceci pour tout $a > 0$, donc K est $\mathcal{C}^\infty$ sur $]0,+\infty[\times\mathbb{R}/2\pi\mathbb{Z}$. Et on remarque que $\partial_t K = \partial_{xx}K$.

Ensuite u s'exprime comme une intégrale à paramètre :

$$u(t,x) = \int_0^{2\pi} K(t,x-y)u_0(y)\mathrm{d}y$$

L'intégrande est $\mathcal{C}^\infty$ des deux variables (t,x) et pour tout $k,l \in \mathbb{N}$ et $t > a > 0$, on a la majoration indépendante de x et t :

$$|\frac{\partial^{k+l}}{\partial t^k \partial x^l}K(t,x-y)u_0(y)| \leq C|u_0(y)|$$

avec $C > 0$ constante qui majore la fonction continue $\frac{\partial^{k+l}}{\partial t^k \partial x^l}K(t,x)$ comme précédemment, et u_0 est intégrable sur $[0,2\pi]$. Par le théorème de dérivation sous le signe intégral, on en déduit que u est $\mathcal{C}^\infty$ (en particulier $\mathcal{C}^2$ comme souhaité) sur $]0,+\infty[\times\mathbb{R}/2\pi\mathbb{Z}$. Et en dérivant sous l'intégrale on trouve $\partial_t u = \partial_{xx}u$ puisque $\partial_t K = \partial_{xx}K$.

Il reste à vérifier que $u(t,.) \to u_0$ dans $L^2(\mathbb{R}/2\pi\mathbb{Z})$, par Parseval, il suffit de montrer que $c_n(u(t,.)) \to c_n(u_0)$ dans $l^2(\mathbb{Z})$.

L'interversion somme intégral

$$\|c_n(u(t,.)) - c_n(u_0)\|_{l^2}^2 \leq \sum_{n\in\mathbb{Z}} |1-e^{-n^2t}|^2|c_n(u_0)|^2$$

Le terme de droite est une série qui converge normalement sur $]0,+\infty[$ car :

$$|1-e^{-n^2t}|^2|c_n(u_0)|^2 \leq 4|c_n(u_0)|^2$$

et $(c_n(u_0)) \in l^2$ car $u_0 \in L^2$ par Parseval.

Pour tout $n \in \mathbb{Z}$, $|1-e^{-n^2t}|^2|c_n(u_0)|^2 \xrightarrow[t\to 0]{} 0$, donc par le théorème de la double limite, $\|c_n(u(t,.)) - c_n(u_0)\|_{l^2}^2 \xrightarrow[t\to 0]{} 0$ ce qui achève la démonstration. □

Leçons concernées : séries de Fourier, problème d'interversion de limites, suites et séries de fonctions, suites et séries de fonctions intégrables, intégrales à paramètre.

46 Théorème de Molien

ref : Leichtnam, Peyré.

THÉORÈME 46.1 *Soit G un sous-groupe fini de $GL(n,\mathbb{C})$. Cette représentation (fidèle) induit une représentation de G sur l'espace $A=\mathbb{C}[X_1,\dots,X_n]$ qui préserve la décomposition en composantes homogènes $A=\oplus_k A_k$. Si $a_k(G)$ désigne la dimension du sous-espace A_k^G des vecteurs invariants sous G, la série génératrice des $a_k(\rho)$ s'exprime par la formule :*

$$\sum_{k=0}^{+\infty} a_k(G)X^k = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(\mathrm{id}-Xg)}$$

PREUVE. On définit la représentation $\rho : G \to GL(A)$ par $g.P=\rho(g)(P)=P\circ g^{-1}$, cela correspond à un changement de variable linéaire dans le polynôme. C'est bien à valeurs dans $\mathrm{GL}(A)$ car c'est linéaire dans en P et l'inverse est évident. C'est bien un morphisme de groupes car $(gh).P=P\circ(gh)^{-1}=(P\circ h^{-1})\circ g^{-1}=g.(h.P)$.

Cela préserve les composantes homogènes, ce que l'on peut voir sur les monômes, si $g=(a_{i,j})$ et $P=X_1^{a_1}\dots X_n^{a_n}$ avec $a_1+\dots+a_n=k$,

$$g.P=(a_{1,1}X_1+\dots+a_{1,n}X_n)^{a_1}\times\dots\times(a_{n,1}X_1+\dots+a_{n,n}X_n)^{a_n}$$

On voit en développant que $g.P$ est encore un polynôme homogène de degré k.

On note ρ_k la représentation de G induite sur A_k. On cherche $a_k(G)=\dim A_k(G)$, on va utiliser la formule général donnée par le lemme suivant :

LEMME 46.2 *Soit V une représentation d'un groupe G. Si $V^G=\{v\in V|\forall g\in G, g.v=v\}$, alors*

$$\dim V^G=\frac{1}{|G|}\sum_{g\in G}\chi(g)$$

PREUVE. On introduit l'endomorphisme :

$$p=\frac{1}{|G|}\sum_{g\in G} g$$

C'est un projecteur par le calcul :

$$p\circ p=\frac{1}{|G|^2}\sum_g\sum_h gh=\frac{1}{|G|^2}\sum_g |G|p=p$$

Son image est V^G : si $v\in V^G$, on a clairement $pv=v$, donc $v\in\mathrm{im}\,p$ et si $v=\frac{1}{|G|}\sum_{g\in G}gw$, clairement, $h.v=\frac{1}{|G|}\sum_{g\in G}hgw=v$. On conclut par le fait que la trace d'un projecteur est la dimension de son espace image. □

Il suffit donc de calculer les traces des éléments $\rho_k(g)$. Pour $g\in G$, $\mathrm{tr}(\rho_k(g))$ ne dépend que de la classe de conjugaison de $\rho_k(g)$ dans $\mathrm{GL}(A_k)$. Comme G est fini, tous les éléments de g, sont d'ordre fini, donc diagonalisable car annule un polynôme de type X^d-1 qui est scindé à racines simples. Soit donc $u\in\mathrm{GL}(n,\mathbb{C})$ telle que $ugu^{-1}=\mathrm{diag}(\lambda_1,\dots,\lambda_n)$ où les λ_i sont les valeurs propres de g. Pour $k\in\mathbb{N}$, les monômes $(X_1^{k_1}\dots X_n^{k_n})$ avec $k_1+\dots+k_n=k$, forment une base de A_k. Il suffit de voir l'action de g sur ces éléments :

$$(ugu^{-1}.X^{k_1}\dots X^{k_n}=\lambda_1^{k_1}\dots\lambda_n^{k_n}X_1^{k_1}\dots X_n^{k_n}$$

Donc comme la trace est invariante par conjugaison :

$$\mathrm{tr}(\rho_k(g)) = \mathrm{tr}(\rho_k(u)\rho_k(g)\rho_k(u^{-1})) = \mathrm{tr}(\rho_k(ugu^{-1}) = \sum_{k_1+\cdots+k_n=k} \lambda_1^{k_1}\dots\lambda_n^{k_n}$$

On en déduit :

$$\begin{aligned}
\sum_{k\geq 0} a_k(G)X^k &= \sum_{k\geq 0}\frac{1}{|G|}\sum_{g\in G}(\sum_{k_1+\cdots+k_n=k}\lambda_1^{k_1}\dots\lambda_n^{k_n})X^k \\
&= \frac{1}{G}\sum_{g\in G}\sum_{k\geq 0}(\sum_{k_1+\cdots+k_n=k}\lambda_1^{k_1}X^{k_1}\dots\lambda_n^{k_n}X^{k_n}) \\
&= \frac{1}{G}\sum_{g\in G}\prod_{i=1}^{n}(\sum_{k_i\geq 0}\lambda_i^{k_i}X^{k_i}) \quad \text{(Produit de Cauchy)} \\
&= \frac{1}{G}\sum_{g\in G}\prod_{i=1}^{n}\frac{1}{1-\lambda_i X_i} \quad \text{(Développement en série formelle de } \frac{1}{1-\lambda X}) \\
&= \frac{1}{G}\sum_{g\in G}\frac{1}{\det(\mathrm{id}-Xg)}
\end{aligned}$$

□

Leçons concernées : séries formelles, polynômes à n indéterminées, représentations,

47 Probabilités que deux entiers soient premiers entre eux

ref : FGN algèbre 1, p.156.

THÉORÈME 47.1 *Pour $n \geq 1$, on note r_n la probabilité que deux entiers de $[1,n]$ soient premiers entre eux. On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \mathbb{Z}$ par $\mu(p_1 \dots p_r) = (-1)^r$ et $\mu(d) = 0$ si d a un facteur carré. Alors :*

- $r_n = \frac{1}{n^2} \sum_{d=1}^{n} \mu(d) E(\frac{n}{d})^2$
- $r_n \xrightarrow[n\to+\infty]{} \frac{6}{\pi^2}$

PREUVE. On note A_n l'ensemble des couples $(a,b) \in [1,n]^2$ tels que $a \wedge b = 1$. On a alors $r_n = \frac{|A_n|}{n^2}$. On note $p_1, \dots, p_k$ l'ensemble des nombres premiers plus petits que n et U_i l'ensemble des couples (a,b) tels que p_i divise a et b. Alors A_n est le complémentaire de l'union des U_i. Pour calculer le cardinal de l'union des U_i, on utilise la formule du crible :

$$\operatorname{card}(\bigcup_{i=1}^{k} U_i) = \sum_{I\neq, I\subset[1,k]} (-1)^{1+\operatorname{card}(I)} \operatorname{card}(\bigcap_{i\in I} U_i)$$

Pour $I \subset [1,k]$, l'intersection $\cap_{i\in I} U_i$ est l'ensemble des couples (a,b) tels a et b sont divisibles par $\prod_{i\in I} p_i$. Il y a exactement $E(\frac{n}{\prod p_i})$ nombre de $[1,n]$ divisible par $\prod p_i$, car il faut simplement choisir le quotient de n par $\prod p_i$. Pour avoir le nombre de couples de nombres divisibles par $\prod p_i$ on élève au carré : on trouve $E(\frac{n}{\prod p_i})^2$.

La formule du crible donne alors :

$$\begin{aligned}\operatorname{card}(A_n) = n^2 - \operatorname{card}(\bigcup_{i=1}^{k} U_i) &= n^2 - \sum_{I\neq, I\subset[1,k]} (-1)^{\operatorname{card}(I)+1} E(\frac{n}{\prod_{i\in I} p_i})^2 \\ &= \sum_{d=1}^{n} \mu(d) E(\frac{n}{d})^2\end{aligned}$$

puisque tout entier entre 1 et n est un produit des p_i, et seuls apparaissent les nombres sans facteur carré dans la somme grâce à la multiplication par μ.

Donc

$$r_n = \frac{1}{n^2} \sum_{d=1}^{n} \mu(d) E(\frac{n}{d})^2$$

Comme $\frac{1}{n^2} E(\frac{n}{d})^2 \sim d^2$, on est amené à comparer r_n à $\sum_d \frac{\mu(d)}{d^2}$.

On a $\frac{n}{d} - 1 < E(\frac{n}{d}) \leq \frac{n}{d}$ que l'on élève au carré, puisque tout est positif, on obtient :

$$\frac{1}{n^2} - \frac{2}{dn} < \frac{1}{n^2} E(\frac{n}{d})^2 - \frac{1}{d^2} \leq 0$$

Cela permet de majorer :

$$|r_n - \sum_{d=1}^{n} \frac{\mu(d)}{d^2}| \leq \sum_{d=1}^{n} \frac{2}{dn} + \frac{1}{n^2} = O(\frac{\ln n}{n})$$

puisque $\sum_{k=1}^{n} \frac{1}{k} \sim \ln n$.

Calculons le produit $\sum \frac{1}{n^2} \times \sum \frac{\mu(d)}{d^2}$. Comme chacune de ces séries est sommable, la suite double $\sum_{n,d} \frac{\mu(d)}{d^2 n^2}$ est aussi sommable. On écrit la partition :

$$(\mathbb{N}^*)^2 = \bigsqcup_{i\in\mathbb{N}^*} \{(d,n)|dn=i\} = \bigsqcup_{i\in\mathbb{N}^*} \bigsqcup_{l|i} \{(n,d)|nd=i, d=l\}$$

Donc :

$$\sum_{d,n} \frac{\mu(d)}{d^2n^2} = \sum_{i\in\mathbb{N}^*} \sum_{l|i} \frac{\mu(l)}{i^2} = \sum_{i\in\mathbb{N}^*} \frac{1}{i^2} \sum_{l|i} \mu(l)$$

Il nous reste à calculer $\sum_{d|n} \mu(d)$. On pose $S(n) = \sum_{d|n} \mu(d)$. On a $S(1) = 1$, montrons que $S(n) = 0$ pour $n \geq 2$. Décomposons n en facteurs premiers : $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, les diviseurs de n sont des produits de p_i et leur μ est nul dès qu'un facteur carré apparait. On regroupe les diviseurs d de n selon le nombre de facteurs premiers qu'ils contiennent :

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{k} C_k^i (-1)^i = (1-1)^k = 0$$

Donc $\sum_{d,n} \frac{\mu(d)}{n^2d^2} = 1$ et comme $\sum \frac{1}{n^2} = \frac{\pi^2}{6}$, on trouve $r_n \xrightarrow[n\to\infty]{} \frac{6}{\pi^2}$.

□

Leçons concernées : convergence suite, séries, combinatoire.

48 Point de Fermat-Torricelli

ref : FGN algèbre 3 p.258, Eiden.

THÉORÈME 48.1 (PTOLÉMÉE) *Soit $ABCD$ un quadrilatère convexe d'un plan euclidien. Alors $AC.BD \leq AB.CD + AD.BC$ avec égalité si et seulement si A, B, C et D sont cocycliques ou alignés.*

PREUVE. On assimile le plan euclidien à $\mathbb{C}$, on note a, b, c et d les affixes des points A, B, C et D. On écrit alors $|AC.BD| = |(a-c)(b-d)|$ etc, et on remarque que :

$$(c-a)(d-b) = (b-a)(d-c) + (d-a)(c-b)$$

On en déduit l'inégalité par l'inégalité triangulaire, et il y a égalité si et seulement si les vecteurs sont positivement liés, c'est-à-dire si

$$\arg(b-a)(d-c) = \arg(d-a)(c-b) \pmod{2\pi}$$

c'est-à-dire :

$$\arg\frac{b-a}{d-a} = \arg\frac{c-b}{d-c} = \arg\frac{b-c}{d-c} + \pi \pmod{2\pi}$$

En terme d'angles orientés de vecteurs (ou demi-droites), cela signifie :

$$(\vec{AB}, \vec{AD}) = (\vec{CB}, \vec{CD}) + \pi \pmod{2\pi}$$

Par le théorème de l'angle inscrit, cela signifie que A, B, C, et D sont cocycliques.

□

THÉORÈME 48.2 (POINT DE FERMAT) *Soit ABC un triangle non aplati du plan affine euclidien identifié à $\mathbb{C}$ via un repère orthonormé. On note a, b et c les affixes des points A, B et C. On construit les points A', B' et C' tels que ACB', $CB'A$ et $A'CB$ soient des triangles équilatéraux directs. On a :*

1. *Les droites (AA'), (BB') et (CC') concourent en un point M*
2. *Si les angles du triangle ABC sont tous $\leq \frac{2\pi}{3}$ alors M est un minimum de la fonction de Fermat $f(M) = MA + MB + MC$.*

PREUVE. On utilise la caractérisation du triangle équilatéral :

$$pqr \text{ est équilatéral } \Leftrightarrow p + jq + j^2 r = 0$$

Calculons les affixes des points :

$$a' = -jc - j^2 b, \quad b' = -ja - j^2 c, \quad c' = -jb - j^2 a$$

Puis,

$$a'' = \frac{-jc - j^2 b + c + b}{3}, \quad b'' = \frac{-ja - j^2 c + a + c}{3}, \quad c'' = \frac{-jb - j^2 a + a + b}{3}$$

Enfin,

$$a'' + jb'' + j^2 c'' = \frac{1}{3}(-jc - j^2 b + c + b + j(-ja - j^2 c + a + c) + j^2(-jb - j^2 a + a + b)) = 0$$

Cela montre le premier point, passons au deuxième.

La rotation de centre A et d'angle $\frac{\pi}{3}$ envoie C' sur B et C sur B'. En particulier, les droites (BB') et (CC') forment un angle de mesure $\frac{\pi}{3}$. Elles s'intersectent donc un point noté M et l'angle $C\hat{M}B$ vaut $\frac{2\pi}{3}$. De plus, le point A, centre de la rotation est sur une bissectrice des droites (BB') et (CC'). Les droites (AM) et (BB') forment donc un angle de mesure $\frac{\pi}{3}$, tout comme les droites (AA') et (BB') par un raisonnement symétrique au précédent. Ainsi, M est sur la droite (AA') et il y a bien concours.

Comme on a $AMC = AMB = BMC = \frac{2\pi}{3}$, d'après le théorème de l'angle au centre, M est sur chacun des cercles circonscrits aux triangles extérieurs ACB', $AC'B$ et $BA'C$.

On applique enfin le théorème de Ptolémée dans le quadrilatère inscriptible $MBA'C$:

$$MB \times A'C + MC \times A'B = MA' \times BC$$

Comme $BA'C$ est équilatéral, cela donne :

$$MB + MC = MA'$$

Puis,

$$f(M) = MA + MA' = AA'$$

Ici, on a besoin que M soit situé entre A et A' ce qui est équivalent à $B\hat{A}C \leq \frac{2\pi}{3}$.

On sait aussi que $AA' = BB' = CC'$, en regardant les rotations d'angle $\frac{\pi}{3}$ de centre A, B et C.

Montrons que AA' est la valeur minimale de la fonction f. Si N désigne un point du plan et N' l'image de N par la rotation de centre B et d'angle $\frac{\pi}{3}$. On a $NB = NN'$ car le triangle NBN' est équilatéral. On a aussi $N'A' = NC$ car la rotation précédente conserve les distances et envoie A' sur C. On trouve donc par inégalité triangulaire :

$$f(N) = NA + NB + NC = AN + NN' + N'A' \geq AA'$$

□

Leçons concernées : nombres complexes en géométrie, problèmes d'angle et de distance.

49 Equation de la chaleur et distributions

ref : Zuily.

On cherche à résoudre le problème d'évolution suivant : équation de la chaleur avec condition initiale :

$$\partial_t u - \Delta u = 0$$
$$u(0,.) = u_0$$

avec $u \in \mathcal{C}^2(]0,+\infty[\times\mathbb{R})$ et $u_0 \in \mathcal{C}^0_c(\mathbb{R})$. Si u est régulière jusqu'en $t = 0$, c'est-à-dire $u \in \mathcal{C}^0([0,+\infty[\times\mathbb{R})$, la condition initiale a un sens. (En fait, c'est toujours le cas si $u_0 \in \mathcal{C}^0_c(\mathbb{R})$).

Si u_0 est moins régulière, par exemple $L^p(\mathbb{R})$, on peut encore donner un sens à la condition initiale en imposant : $u(t,.) \underset{t\to 0}{\longrightarrow} u_0$ dans $L^p(\mathbb{R})$.

Si u_0 est encore moins régulière : $u_0 \in \mathcal{E}'(\mathbb{R})$, cela n'a plus de sens et on va donc traduire ce problème et montrer l'existence d'une distribution solution du problème.

On cherche des distributions $u \in \mathcal{S}'(\mathbb{R}^2)$ à support dans $[0,+\infty[\times\mathbb{R}$, vérifiant :

$$\partial_t u - \Delta u = \delta_{t=0} \otimes u_0$$

La raison heuristique est que si on a une solution u définie sur $[0,+\infty[\times\mathbb{R}$ aussi régulière et intégrable que l'on veut, on peut l'étendre en une fonction $\tilde{u}$ en posant 0 sur $]-\infty,0[\times\mathbb{R}$. Elle est régulière hors de la droite $\{t=0\}$ et la formule des sauts nous dit que :

$$\partial_t \tilde{u}(t,x) = \partial_t u(t,x) + \delta_{t=0} u_0(x)$$

Le laplacien concerne les dérivées en espace qui n'ont toujours pas de saut après prolongement à $\mathbb{R}\times\mathbb{R}$, donc on a

$$\partial_t \tilde{u}(t,x) + \Delta\tilde{u}(t,x) = \partial_t u(t,x) + \Delta u(t,x) + \delta_{t=0}u_0(x) = \delta_{t=0}u_0(x)$$

THÉORÈME 49.1 *Si $u_0 \in \mathcal{E}'(\mathbb{R})$, il existe une solution u à ce problème. De plus, si u_0 est dans $\mathcal{C}^0_c(\mathbb{R})$ alors, la solution obtenue est $\mathcal{C}^0$ sur $[0,+\infty[\times\mathbb{R}$ et $\mathcal{C}^\infty$ sur $]0,+\infty[\times\mathbb{R}$ et vérifie la condition initiale au sens classique : $u(0,.) = u_0$.*

PREUVE. L'idée est de transformer l'équation en appliquant la transformée de Fourier partielle en espace. Pour $\varphi \in \mathcal{C}^\infty_c(\mathbb{R}\times\mathbb{R})$, notre convention pour la transformée de Fourier est $\hat{\varphi}(t,\xi) = \int_{\mathbb{R}} \varphi(t,x)e^{-ix\xi}\mathrm{d}x$. Par application de la transformée de Fourier, l'équation devient :

$$\partial_t \hat{u} + \xi^2 \hat{u} = \delta_{t=0} \otimes \hat{u_0}$$

On voit alors que la fonction $v(t,\xi) = e^{-t\xi^2}H(t)\hat{u_0}(\xi)$ où $H(t) = 1_{t\geq 0}$ fonction de Heaviside, v est bien une fonction de $L^\infty(\mathbb{R}^2) \subset \mathcal{S}'(\mathbb{R}^2)$ car $\hat{u_0}$ est L^∞ (même analytique et à croissance lente) car c'est la transformée de Fourier d'une distribution à support compact. Vérifions que c'est solution de l'équation : pour tout $\varphi \in \mathcal{S}(\mathbb{R}^2)$,

$$\begin{aligned}
< \partial_t v, \varphi > = - < v, \partial_t \varphi > &= -\int_{\mathbb{R}^2} e^{-t\xi^2}H(t)\hat{u_0}(\xi)\partial_t\varphi(t,\xi)\mathrm{d}t\mathrm{d}\xi \\
&= -\int_{\mathbb{R}} \hat{u_0}(\xi)\Big(\int_0^{+\infty} e^{-t\xi^2}\partial_t\varphi(t,\xi)\mathrm{d}t\Big)\mathrm{d}\xi \quad \text{(Fubini)} \\
&= -\int_{\mathbb{R}} \hat{u_0}(\xi)\Big(-\varphi(0,\xi) + \xi^2\int_0^{+\infty} e^{-t\xi^2}\varphi(t,\xi)\mathrm{d}t\Big)\mathrm{d}\xi \quad \text{(IPP)} \\
&= < \delta_{t=0}\otimes\hat{u_0}, \varphi > + < \xi^2 v, \varphi >
\end{aligned}$$

Donc v vérifie l'EDP passée en Fourier. La transformée de Fourier est un isomorphisme de $\mathcal{S}'$ dans $\mathcal{S}'$ et elle échange dérivation en multiplication par ξ. Donc si on pose $u(t,x) = \mathcal{F}^{-1}v(t,\xi)$, on voit que E est un solution du problème initial. Comme Fourier échange produit et convolution, on trouve que

$$u = E(t,x) * u_0$$

où

$$E = \int_{\mathbb{R}} e^{-t\xi^2} H(t) e^{ix\xi} \mathrm{d}\xi$$

On a le droit de convoler car $u_0 \in \mathcal{E}'(\mathbb{R}^2)$.

Il reste à montrer la régularité de u dans le cas $u_0 \in \mathcal{C}_c^0$ et le fait que u vérifie les conditions initiales au sens classique. Tout d'abord le noyau E est $\mathbb{C}^\infty$ sur $]0,+\infty[\times\mathbb{R}$ par dérivation sous le signe intégral (le terme $e^{-t\xi^2}$ contrôle tout).

Comme u_0 est une fonction, on a une expression intégrale du produit de convolution :

$$u(t,x) = \int_{\mathbb{R}} E(t,x-y)u_0(y)\mathrm{d}y$$

Encore par dérivation sous le signe intégral, on voit que u est $\mathcal{C}^\infty$ sur $]0,+\infty[\times\mathbb{R}$. Montrons la continuité jusqu'en $t=0$, soit donc $x_0 \in \mathbb{R}$ et $\epsilon > 0$.

$$\begin{aligned} |u(t,x) - u_0(x_0)| &= |\int_{\mathbb{R}} E(t,y)(u_0(x-y) - u_0(x_0))\mathrm{d}y| \\ &= \int_{|y|\leq\eta} |E(t,y)||u_0(x-y) - u_0(x_0)| + 2\|u_0\|_\infty \int_{|y|>\eta} |E(t,y)|\mathrm{d}y \end{aligned}$$

Par continuité de u_0 en x_0 et parce que $E(t,y)$ est un bon noyau pour $t \to 0$, on trouve $|u(t,x) - u_0(x_0)| < \epsilon$ pour (t,x) assez proche de $(0,x_0)$. □

50 Transformée de Fourier-Plancherel

THÉORÈME 50.1 (PLANCHEREL) *Soit $f \in L^2 \cap L^2$. Alors $\|\hat{f}\|_2 = \|f\|_2$. En particulier, $\mathcal{F}(L^1 \cap L^2) \subset L^2$ et, de plus, cette partie est dense.*

PREUVE. Soit $f \in L^1 \cap L^2$. On pose $\tilde{f}(x) = \overline{f(-x)}$ et $g = f * \tilde{f}$, c'est possible car f et $\tilde{f}$ sont L^1, et on a alors $g \in L^1$. On a :

$$g(x) = \int_{\mathbb{R}} f(x-y)\overline{f(-y)}\mathrm{d}y = \int_{\mathbb{R}} f(x+y)\overline{f(y)}\mathrm{d}y = < f, f_{-x} >_{L^2}$$

Par continuité de la translation $x \to f_{-x}$ de $\mathbb{R}$ dans L^2 et par continuité du produit scalaire, on trouve que g est continue. De plus g est bornée par $\|f\|_2^2$ d'après l'inégalité de Cauchy-Schwarz. Par propriété de la transformée de Fourier et du produit de convolution, on a $\hat{g}(x) = |\hat{f}(x)^2|$

On introduit alors la suite $h_\lambda(x) = \sqrt{\frac{2}{\pi}}\frac{\lambda}{\lambda^2+x^2}$. C'est un bon noyau au sens où h_λ est positive, d'intégrale 1, et $\int_{|x|\geq\eta} h_\lambda \xrightarrow[\lambda\to+\infty]{} 0$. C'est la transformée de Fourier inverse de $H(\lambda t) = e^{-\lambda|t|}$ par un calcul simple.

On regarde alors $g * h_\lambda(0)$ où on passera à la limite quand λ tend vers 0. Comme g est L^1 d'après le théorème de Fubini, on a :

$$\begin{aligned} g * h_\lambda(0) = \int g(-t)h_\lambda(t)\mathrm{d}t &= \int g(-t)\int H(\lambda t)e^{ixt}\mathrm{d}x\mathrm{d}t \\ &= \int (\int g(-t)e^{ixt}\mathrm{d}t)H(\lambda x)\mathrm{d}x \\ &= \int \hat{g}(x)H(\lambda x)\mathrm{d}x \end{aligned}$$

Comme h_λ est un bon noyau et g est bornée et continue en 0, on a d'une part :

$$g * h_\lambda(0) \xrightarrow[\lambda\to 0]{} g(0) = \|f\|_2^2$$

D'autre part, comme $\hat{g}(x)$ est positive et $H(\lambda t)$ converge simplement vers 1 en croissant quand λ tend vers 0, on a par le théorème de convergence monotone :

$$g * h_\lambda(0) \xrightarrow[\lambda\to 0]{} \int \hat{g} = \|\hat{f}\|_2^2$$

D'où, $f\|^2 = \|f\|^2$ et $\hat{f}$ est dans L^2.

Pour montrer que l'image Y est dense, on regarde les transformées de Fourier des fonctions $e^{i\alpha x}H(\lambda_x) \in L^1 \cap L^2$ qui sont les $h_\lambda(\alpha - t)$. Si $f \in L^2 \cap Y^\perp$, alors pour tout α,

$$\int \overline{f(t)}h_\lambda(\alpha - t) = 0 = \overline{f} * h_\lambda(\alpha)$$

Comme h_λ est un bon noyau et $\overline{f} \in L^2$, on trouve $\overline{f} = \lim_{\alpha\to 0} \overline{f} * h_\lambda(\alpha) = 0$ dans L^2. On a donc montré que $Y^\perp = \{0\}$, c'est-à-dire Y est dense. □

COROLLAIRE 50.2 *Il existe un unique opérateur de L^2 dans L^2 qui coïncide avec $\mathcal{F}$ sur $L^1 \cap L^2$.*

PREUVE. $L^1 \cap L^2$ est une partie dense de L^2 ce que l'on voit en tronquant la fonction : si $f \in L^2$, alors $f_n = f1_{[-n,n]}$ est dans L^1 car est L^2 et son support est de mesure finie. De plus, $\|f - f_n\|^2 = \int_{|x|>n} |f|^2 \xrightarrow[n\to+\infty]{} 0$ car f est dans L^2. L'opérateur $\mathcal{F} : L^1 \cap L^2 \to L^2$ est continu

pour la norme 2 d'après le théorème de Plancherel (c'est même une isométrie), et l'espace L^2 est complet, donc par le théorème de prolongement des applications uniformément continues (une application linéaire est continue ssi elle est uniformément continue), il existe un unique prolongement de $\mathcal{F}$ à L^2. Le prolongement est encore une isométrie de la norme 2 par passage à la limite dans l'égalité du théorème de Plancherel. Si on sait de plus que l'image est dense, alors l'opérateur est surjectif (prendre une suite de Cauchy..) et par l'inverse est continue car Fourier est une isométrie. □

Leçons : prolongement de fonctions.

51 Méthode de Gauss et polynômes orthogonaux

ref : Demailly On cherche une méthode d'intégration avec un poids fixé w continu positif intégrable sur $]a,b[$ contre tout polynôme, c'est-à-dire on cherche des points (x_j) et des coefficients λ_j telle que l'approximation :

$$\int_\alpha^\beta f(x)w(x)\mathrm{d}x \simeq \sum_{j=0}^{l} \lambda_j f(x_j)$$

A nombre l de points fixé, le théorème suivant nous dit comment choisir les points et les coefficients.

THÉORÈME 51.1 *Il existe un unique choix des (x_j) et (λ_j) tels que la méthode soit d'ordre $N = 2l+1$. Les points (x_j) sont dans $]\alpha,\beta[$ et sont les racines du l-ième polynôme orthogonal pour le poids w.*

PREUVE. *Analyse :*
Soit une méthode d'ordre $\geq 2l+1$. On introduit le polynôme :

$$\pi_{l+1} = \prod_{j=0}^{l}(x - x_j)$$

Pour tout p de degré $\geq l$, $\deg(p\pi_{l+1}) \leq 2l+1$. Donc :

$$\int_0^{2\pi} p\pi_{l+1}w = \sum_{j=0}^{l} \lambda_j p(x_j)\pi_{l+1}(x_j) = 0$$

Donc π_{l+1} est orthogonale à $\mathbb{R}_l[X]$ et comme il est unitaire, c'est le l-ième polynôme orthogonal. Les points (x_j) sont alors les racines de ce polynôme. dont on sait qu'elles sont distinctes et dans $]a,b[$. (En effet, si m_j sont les multiplicités des racines, on prend $\epsilon_j = 1$ si m_j impair, 0 sinon, alors $\prod(X-x_j)^{\epsilon_j}p$ est de signe constant, donc $\int p_n q w > 0$, donc q est de degré n et les multiplicités valent 1.)
Soit L_i les polynômes interpolateurs de Lagrange , c'est-à-dire $L_i(x_j) = \delta_{i,j}$.
On a alors :

$$\lambda_i = \sum_{j=0}^{l} \lambda_j L_i(x_j) = \int L_i(x)w(x)\mathrm{d}x$$

Les coefficients sont donc également déterminés.
Synthèse :
Vérifions que cette méthode donnée par les polynômes orthogonaux est bien d'ordre $2l+1$. Prenons donc les racines x_j et les coefficients $\lambda_j = \int L_j w$.
Si f est de degré l, f est égal aux polynômes interpolateurs de la famille $(x_j, f(x_j))$ par unicité, donc $f = \sum_j f(x_j)L_j$, donc

$$\int fw = \sum_j f(x_j)\int L_j w = \sum_j f(x_j)\lambda_j$$

Si f est de degré $\leq 2l+1$, on fait la division euclidienne de f par $\pi_{l+1} = \prod_j(x-x_j)$:

$$f = q\pi_{n+1} + r$$

avec r et q de degré $\leq l$. En intégrant et en utilisant le fait que π_{n+1} est orthogonal à $\mathbb{R}_l[X]$ et que la méthode est d'ordre au moins l, on trouve :

$$\int fw = \int q\pi_{n+1}w + \int rw = \int rw = \sum_j \lambda_j r(x_j)$$

Cela achève l'existence et l'unicité de la méthode. Il reste à montrer qu'elle n'est pas d'ordre plus grand. Pour cela montrons que la méthode n'est pas exacte sur le polynôme x^{2l+2}. On peut l'écrire $x^{2l+2} = \pi_{l+1}^2 + r(x)$ avec r de degré $\leq 2l+1$. Donc l'erreur vaut :

$$E(x^{2l+2}) = \int x^{2l+2}w - \sum_j \lambda_j x_j^{2l+2} = \int \pi_{l+1}^2 w > 0$$

□