Développements d'algèbre et d'analyse

Auguste Hoang Duc

2010

Table des matières

Mises en garde

Ce document regroupe les développements sur lesquels j'ai travaillé lors de ma préparation à l'agrégation de mathématique. Des démonstrations restent encore incomplètes et parfois des arguments ont été implicitement éludés. Les preuves ont été largement modifiées à mon goût et n'ont parfois rien à voir avec les références que je donne.

Enfin, je remercie les personnes suivantes :
– Les anciens agrégés qui ont mis à disposition en ligne leurs développements.
– Le site de la prépa agreg de Rennes.
– Les élèves et les préparateurs de ma prépa agreg.

Première partie

Développements mixtes

Chapitre 1

Développements

1 Sous-groupe compacts de $GL_n(\mathbb{R})$

Leçons concernés

- 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.
- 119 - Exemples d'actions de groupes sur les espaces de matrices.
- 121 - Matrices équivalentes.Matrices semblables. Applications.
- 131 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
- 135 - Isométries d'un espace affine euclidien de dimension finie. Forme réduite. Applications en dimensions 2 et 3.
- 137 - Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.
- 141 - Utilisation des groupes en géométrie.
- 203 - Utilisation de la notion de compacité.
- 206 - Théorèmes de point fixe, exemples et applications.

A Un théorème de point fixe

On considère E un $\mathbb{R}$-espace vectoriel de dimension finie.

Théorème. Soient G un sous-groupe compact de $GL(E)$ et K un convexe compact de $\mathbb{R}^n$ tel que $G.K \subset K$. Alors il existe $x \in K$ tel que

$$\forall g \in G,\ g.x = x.$$

Démonstration. • Soit $g \in L(E)$ tel que $g(K) \subset K$. Montrons que g admet un point fixe dans K. Soit $x_0 \in K$ et la suite des itérés $(u^i(x_0))_{i\in\mathbb{N}}$ (non nécessairement convergente) et on note $x_n = \frac{1}{n}\sum_{i=0}^{n-1} u^i(x_0)$ sa moyenne de Cesaro. On a alors

$$u(x_n) - x_n = \frac{u^n(x_0) - x_0}{n}.$$

Comme la suite $(u^n(x_0))_{n\in\mathbb{N}}$ est dans le compact K, on en déduit que $\lim_{n\to+\infty} u(x_n) - x_n = 0$. Donc toute valeur d'adhérence (et il en existe puisque K est compact) de $(x_n)_{n\in\mathbb{N}}$ est point fixe g.

• On définit la norme N sur E de la façon suivante :

$$\forall x \in E,\ N(x) = \sup_{g\in G} \|g.x\|_2 = \max_{g\in G} \|g.x\|_2.$$

Alors le norme N est clairement invariante par G, c'est-à-dire que :

$$\forall x \in E,\ \forall g \in G,\ N(g.x) = N(g).$$

De plus N et est strictement convexe, c'est-à-dire

$$\forall x, y \in \mathbb{R}^n,\ N(x+y) = N(x) + N(y) \Longrightarrow (x, y) \text{ est positivement lié.}$$

En effet : soient $x, y \in \mathbb{R}^2$ et prenons $g_0 \in G$ tel que $N(x+y) = \|g_0.x + g_0.y\|_2$. Ce qui implique que

$$N(x+y) = \|g_0.x + g_0.y\|_2 \leq \|g_0.x\|_2 + \|g_0.y\|_2 \leq N(x) + N(y),$$

donc si $N(x)+N(y)=N(x+y)$ alors $\|g_0.x+g_0.y\|_2=\|g_0.x\|_2+\|g_0.y\|_2$ et par convexité de la norme $\|.\|_2$, les vecteurs $g_0.x$ et $g_0.y$ sont positivement liés et par injectivité de g_0, la famille (x,y) sont positivement liés.

• Soit $u_1,\dots,u_k$ une famille finie de G. Montrons que cette famille a un point fixe commun dans K. On pose $v=\frac{1}{k}\sum_{i=1}^k u_i$. Par convexité on a $v(K)\subset K$, donc il existe un point $a\in K$ fixe par v. On a alors

$$\begin{array}{rcll} N(a)=N(v.a) & \leq & \frac{1}{k}\sum_{i=1}^k N(u_i.a) & \\ & \leq & \frac{1}{k}\sum_{i=1}^k N(a) & \text{(par invariance)} \\ & \leq & N(a) & . \end{array}$$

Par convexité de la norme N, les $(u_i.a)_{i\in[1,k]}$ sont positivement liés : par exemple $\forall i>1, u_i.a=\lambda_i u_1.a$ avec $\lambda_i\geq 0$, et par invariance de la norme on en déduit que $\forall i>1,\lambda_i=1$ sauf si $a=0$ (ce qui donne déjà un point fixe). Donc on a

$$\forall i\in[1,k],\ a=v.a=u_1.a=u_i.a.$$

• Fin de la preuve : pour $g\in G$ on note

$$F_g=\Big\{x\in K\mid g.x=x\Big\}$$

Alors F_g est un fermé de K et $\bigcap_{g\in G}F_g\neq\emptyset$ car sinon on pourrait extraire une intersection finie vide. □

B Sous-groupe compacts de $GL_n(\mathbb{R})$

On rapelle le lemme de Kakutani.

Lemme (Kakutani)**.** Dans un espace vectoriel de dimension finie, l'enveloppe convexe d'un compact est compact.

Théorème. Si G est un sous-groupe compact de $GL_n(\mathbb{R})$, alors G est conjugué à un groupe de $O_n(\mathbb{R})$.

Démonstration. Celà revient à montrer que G fixe une forme quadratique définie positive. On note Q l'ensemble des formes quadratiques de $\mathbb{R}^n$ et Q^{++} l'ensemble des formes quadratiques définies positives. On rappelle que Q^{++} est un demi-cône convexe ouvert de Q. Soit G' l'image de G par la représentation $G\to GL(Q)$. Soit q_0 un produit scalaire quelconque, on note K l'enveloppe convexe de $G'.q_0$ dans Q (c'est l'orbite de q_0 par G). L'ensemble K est compact par lemme de Kakutani. Comme $G'.q_0$ est stable par G', le compact K l'est aussi. Donc en appliquant le théorème précédent, on en déduit que G' admet un point fixe dans $K\subset Q^{++}$. □

Remarque. On trouvera la preuve dans : [[Ale99]], [FGN, Alg 3, 3.38] ou [Goblot, Thème d'algèbre].

2 Théorème de John

Leçons concernées
- 123 - Déterminant. Exemples et applications.
- 148 - Formes quadratiques réelles. Exemples et applications.
- 219 - Problèmes d'extremums.
- 229 - Fonctions monotones et fonctions convexes.

A Préliminaires

On considère E un espace euclidien (de dimension finie). On note $Q^+(E)$ l'ensemble des formes quadratiques positive sur E et $Q^{++}(E)$ l'ensemble des formes quadratiques définits positives. Soit $q \in Q^{++}(E)$ une forme quadratique définie positive. On définit les éléments suivants associés à q.
- Son ellipsoïde est sa boule unité, c'est-à-dire l'ensemble $\mathcal{E}(q) := q^{-1}([0,1])$.
- Son volume $Vol(q)$ est la mesure de Lebesgue de $\mathcal{E}(q)$.
- Son déterminant est le déterminant de sa matrice dans une base orthonormée. C'est aussi le détermiant de $A_q \in S^{++}(E)$ son endomorphisme autoadjoint associé (définit par : $\forall x \in E, q(x) = \langle x, Ax\rangle$).

Lemme. Pour $q, q' \in Q^{++}(E)$, si $\mathcal{E}(q) = \mathcal{E}(q')$, alors $q = q'$.

Démonstration. En effet si $\mathcal{E}(q) = \mathcal{E}(q')$, alors pour tout $x \in E - \{0\}$, on a $q(\frac{x}{\sqrt{q(x)}}) \leq 1$, donc $q'(\frac{x}{\sqrt{q(x)}}) \leq 1$, soit $q'(x) \leq q(x)$. Par symétrie des rôle, on a égalité. □

Lemme. On a $Vol(q) = Vol(B(0,1))\ \det q^{-1/2}$.

Démonstration du lemme. Si $A_q \in S^{++}(E)$ est l'endomorphisme symétrique associé à q alors

$$\forall x \in E, q(x) \leq 1 \iff \left\|\sqrt{A}x\right\|^2 \leq 1.$$

On en déduit que $\mathcal{E}_q = \sqrt{A}^{-1}(B(0,1))$, puis que $Vol(q) = Vol(B(0,1))\ \det q^{-1/2}$. □

B Théorème de John

Théorème (John)**.** Si K est un compact d'intérieur non vide, alors il existe une unique ellipsoïde de volume minimal contenant K.

Démonstration. D'après les préliminaires, le théorème se reformule de la façon suivante : il existe une unique forme quadratique q définie positive, tel que $K \subset \{q \leq 1\}$ et tel que $\det q$ soit maximal.

Soit $q \in Q^{++}(E)$. Pour $M > 0$, on note

$$X := \Big\{q \in Q^+(E) \mid\ E_q \supset K\Big\} = Q^+ \cap \bigcap_{x \in K} \Big\{q \in Q : q(x) \leq 1\Big\}$$

L'ensemble X est un convexe fermé de $Q(E)$ (car c'est une intersection de convexes fermés) et est non vide car K est inclus dans une boule. De plus X est borné : en effet, si $q \in Q^+$ et si on note K' le plus petit fermé convexe symétrique contenant K, on a alors $E_q \subset K'$ (car E_q est symétrique et convexe). Comme $int(K) \neq \emptyset$, il existe $r > 0$ tel que $B(0,r) \subset K'$ [y réfléchir], ce qui donne

$$\forall q \in X, sup_{\|x\| \leq r} q(x) \leq 1$$

c'est-à-dire que X est borné (on munit, par exemple, l'espace vectoriel $Q(E)$ de la norme infinie sur la sphère unité euclidienne de E).

$$\boxed{\text{Donc } X \text{ est un convexe compact non vide}}.$$

Lemme. L'application déterminant est strictement log-concave sur $Q^{++}(E)$ (on rappelle que $Q^{++}(E)$ est convexe).

Démonstration du lemme. On se donne $(e_i)_{i\in[1,n]}$ une base orthonormée. Pour $p, q \in Q^{++}(E)$ et $t \in]0,1[$, il existe $(f_i)_{i\in[1,n]}$ une base orthonormée pour le produit scalaire p telle que la matrice $Mat_f(q)$ soit diagonale (par théorème de diagonalisation des formes quadratiques en espace euclidien). On note $\lambda_1, \ldots, \lambda_n$ les coefficients diagonaux de $Mat_f(q)$ et $P := Mat_e(f)$ la matrice de passage de $(e_i)_{i\in[1,n]}$ vers $(f_i)_{i\in[1,n]}$. On a alors

$$\begin{aligned} \det\Big((1-t)p + tq\Big) &= \det {}^tP . \prod_{i=1}^n \Big((1-t) + t\lambda_i\Big) . \det P, \\ \text{et} \qquad \det p^{1-t} . \det q^t &= \det {}^tP \prod_{i=1}^n \lambda_i^{\beta} \det P \end{aligned}$$

Or par inégalité arithmético-géométrique, on a $(1-t) + t\lambda \geq 1^{1-t}.\lambda_i^t$ $(i \in [1,n])$. Ce qui donne

$$\det\Big((1-t)p + tq\Big) \geq \det p^{1-t} . \det q^t.$$

De plus il y a égalité si et seulement si il y a égalité dans l'inégalité arithmético-géométrique, c'est-à-dire que $\forall i \in [1,n], \lambda_i = 1$, soit $p = q$. Ce qui prouve la stricte log-concavité. □

Par compacité l'application det atteint son maximum sur X. Comme ce maximum est stricement positif (X contient le produit scalaire $r\|.\|^2$, pour r assez petit), il est atteint sur $X \cap Q^{++}$ (qui est convexe) et d'après ce lemme, ce maximum est unique. Ce qui prouve l'existence et l'unicité de l'ellipse de volume minimal contenant K. □

Remarque. On trouvera la preuve par exemple dans : [[Ale99] [?]], [[FG95] : Alg 3, Ex 3.37].

3 Théorème de Cartan

Leçons concernées
- 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.
- 127 - Exponentielle de matrices. Applications.
- 214 - Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.
- 215 - Applications différentiables définies sur un ouvert de Rn. Exemples et applications.
- 217 - Sous variétés de Rn. Exemples.

A Préliminaires

On considère G un sous groupe fermé de $GL_n(\mathbb{R})$.

Théorème (Algèbre de Lie)**.** On note

$$L_G := \Big\{ X \in \mathcal{M}_n(\mathbb{R}) \mid \forall t \in \mathbb{R}, exp(tX) \in G \Big\}.$$

Alors L_G est une sous-algèbre de Lie de $\mathcal{M}_n(\mathbb{R})$ (on note $[.,.]$ le crochet de Lie).

Démonstration. L'ensemble L_G est clairement stable par multiplication scalaire.

Lemme. Pour $A, B \in M_n(\mathbb{R})$, on a

$$\lim_{k\to+\infty} \Big(exp(A/k)exp(B/k) \Big)^k = exp(A+B).$$

Démonstration du lemme. En faisant un développement limité, on a

$$exp(A/k)exp(B/k) = Id + \frac{A+B}{k} + O(\frac{1}{k^2}).$$

Pour k assez grand, on peut prendre le logarithme et en multipliant par k on a

$$k\ Log\Big(exp(A/k)exp(B/k) \Big) = (A+B) + o(1).$$

D'où

$$exp\Big(k\ Log\Big(exp(A/k)exp(B/k) \Big) \Big) = \Big(exp(A/k)exp(B/k) \Big)^k = exp(A+B) + o(1),$$

ce qui démontre le lemme. □

Soit $A, B \in L_G$ et $t \in \mathbb{R}$. Alors on a

$$exp(tA+tB)) = \lim_{k\to+\infty} \Big(exp(tA/k)exp(tB/k) \Big)^k.$$

Comme $exp(tA/k)$ et $exp(tB/k)$ sont dans G qui est fermé, on en déduit que $A+B \in L_G$. Ce qui montre que L_G est un espace vectoriel.

Lemme. Pour $A, B \in M_n(\mathbb{R})$, on a

$$\lim_{k\to+\infty} \Big(exp(A/k)exp(B/k)exp(-A/k)exp(-B/k) \Big)^{k^2} = exp([A,B]).$$

Démonstration du lemme. En faisant un développement limité, on a

$$exp(A/k)exp(B/k)exp(-A/k)exp(-B/k) = \tfrac{AB-BA}{k^2} + O(\tfrac{1}{k^3}).$$

On conclut alors comme dans le lemme précédent. □

Comme précédamment, ce lemme montre que L_G est stable par crochet de Lie. □

Remarque. Pour le théorème de Cartan, on a seulement besoin de savoir que L_G est un sous-espace vectoriel.

B Théorèmes

Théorème (Cartan)**.** Tout sous-groupe fermé de $GL_n(\mathbb{R})$ est une sous-variété.

Démonstration. Il suffit montrer qu'un voisinage de 0 est une sous-variété [y réfléchir]. On note L_G l'algèbre de Lie de G et E un supplémentaire de L_G dans $\mathcal{M}_n(\mathbb{R})$.

Lemme. Il existe un voisinage V de 0 dans E tel que

$$\forall x \in V,\ exp(x) \in G \Longrightarrow x = 0.$$

Démonstration du lemme. Raisonnons par l'absurde : il existerait alors $(x_n)_{n\in\mathbb{N}}$ une suite de $E\setminus\{0\}$ telle que $exp(x_n) \in G$ pour tout $n \in \mathbb{N}$ et $x_n \xrightarrow{n\to+\infty} 0$. Quitte à extraire on peut supposer que la suite $(x_n/\|x_n\|)_{n\in\mathbb{N}}$ de la sphère unité de E converge de limite noté $v \in E - \{0\}$.

Montrons que $v \in L_G$. Soit $t \in \mathbb{R}$, on note $t\frac{x_n}{\|x_n\|} = (N_n + d_n)x_n$ avec $N_n \in \mathbb{Z}$ et $\alpha_n \in [0, 1[$. On a alors

$$\forall n \in \mathbb{N},\ exp(t\frac{x_n}{\|x_n\|}) = exp(x_n)^{N_n} exp(d_n x_n).$$

Comme $exp(N_n x_n) \in G$ et $exp(d_n.x_n) \xrightarrow{n\to+\infty} 1$, on en déduit que $exp(tv) \in G$. Donc $v \in L_G$, ce qui est absurde car v est dans la sphère unité de E. □

On prend V comme dans le lemme. On définit l'application

$$\begin{array}{rccc} \phi: & L_G \oplus E & \longrightarrow & GL_n(\mathbb{R}) \\ & A + B & \longmapsto & exp(A)exp(B) \end{array}.$$

Alors $D_0\phi = Id$, donc il existe un voisinage $U \times W \subset L_G \times E$ tel que $W \subset V$ et où ϕ réalise un C^∞-difféomorphisme. On a alors

$$\phi(U \times \{0\}) = \phi(U \times W) \cap G.$$

En effet pour $(A, B) \in U \times W$ tel que $\phi(A, B) \in G$, alors $e^B \in e^{-A}G = G$, donc par construction de V, $B = 0$, d'où $\phi(U \times W) \cap G \subset \phi(U \times \{0\})$. L'autre inclusion est claire, ce qui prouve que $\phi(U \times W) \cap G$ est une sous-variété. □

Remarque.
- La preuve se trouve dans [[GT98] Part. I, Chap. 2, Ex. 19].
- Voir aussi [Mneimé et Testard : Théorème ?] pour une autre démonstration.

4 Théorème de stabilité de Liapounov

Leçons concernées

- 124 - Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
- 127 - Exponentielle de matrices. Applications.
- 130 - Matrices symétriques réelles, matrices hermitiennes.
- 131 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
- 148 - Formes quadratiques réelles. Exemples et applications.
- 215 - Applications différentiables définies sur un ouvert de R^n. Exemples et applications.
- 220 - Équations différentielles $X_0 = f(t, X)$. Exemples d'études qualitatives des solutions.
- 221 - Équations différentielles linéaires, exemples et applications.

Théorème. Soit E un $\mathbb{R}$-espace vectoriel normé de dimension finie, $f : E \to E$ un champ de vecteurs tel que $f(0) = 0$ et $Spec(Df(0)) \subset \{\mathrm{Re} < 0\}$. On note ϕ son flot. Alors il existe un voisinage U de 0 et $\lambda > 0$, $C > 0$ deux constantes tels que : pour tout $x \in U$ et $t > 0$, $\phi_t(x)$ existe et

$$\|\phi_t(x)\|^2 \leq Ce^{-t\lambda}.$$

Démonstration. On note $A = Df(0)$. On peut supposer que la norme $\|.\|$ de E est euclidienne (grâce à l'équivelence des normes). Le lemme suivant montre que l'on peut définir la fonction (de Liapounov)

$$q : \begin{array}{ccc} E & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \int_0^{+\infty} \|e^{tA}x\|^2 dt \end{array}.$$

Lemme. Il existe $P(X) \in \mathbb{R}[X]$ un polynôme et $\lambda_0 > 0$ tels que pour tout $t > 0$

$$\|e^{tA}\| \leq |P(|t|)|.e^{-t\lambda_0},$$

où $\|.\|$ est la norme subordonnée sur $L(E)$.

Démonstration du lemme. On prend $\lambda_0 > 0$ tel que $Spec(A) \in \mathbb{R}_{\leq -\lambda_0}$. On note $A = D + N$ la décomposition de Dunford de A, et N_0 la norme infinie dans une base de diagonalisation (complexe) de D. Il suffit de montrer le lemme pour la norme N_0. On a alors $N_0(e^{tD}) \leq e^{-t\lambda_0}$, puis

$$N_0(e^{tA}) \leq N_0(e^{tD})\ N_0(e^{tN}) \leq e^{-t\lambda_0} \sum_{k=0}^{n-1} \frac{|t|^k}{k!} N_0(N)^k.$$

Il suffit de prendre $P(X) = \sum_{k=0}^{n-1} \frac{X^k}{k!} N_0(N)^k$. □

La fonction q définit un produit scalaire [y réfléchir], et par équivalence des normes il suffit de montrer le théorème pour la norme $\sqrt{q}$.

En appliquant le théorème de dérivation sous l'intégrale [y réfléchir], pour $x \in E$, on a

$$\forall h \in E, Dq(x).h = \int_0^{+\infty} 2\langle e^{tA}x, e^{tA}h\rangle dt.$$

En prenant $h = Ax$, on obtient

$$Dq(x).Ax = \int_0^{+\infty} 2\langle e^{tA}x, e^{tA}Ax\rangle dt = \int_0^{+\infty} \frac{d}{dt}\|e^{tA}.x\|^2 dt,$$

ce qui donne

$$Dq(x).Ax = -\|x\|^2.$$

Celà veut dire que q est une fonction de Liapounov forte pour le champs de vecteur défini par A.

On note $\varepsilon(x) = o(\|x\|)$ tel que $f(x) = A.x + \varepsilon(x)$. Pour $X(t)$ solution de $X' = f(X)$, on a

$$\frac{d}{dt}q(X) = Dq(X).(Ax + \varepsilon(X)) = -\|X\|^2 + Dq(X).\varepsilon(X).$$

Lemme. Il existe $\alpha > 0$ et $\beta > 0$ tel que

$$\forall x \in E, q(x) \leq \alpha \Longrightarrow -\|x\|^2 + Dq(x).\varepsilon(x) \leq -\beta q(x).$$

Démonstration du lemme. Comme $\nabla q(x) = 2\left(\int_0^{+\infty} e^{t({}^tA+A)}\right).x = O(\|x\|)$, on a $Dq(x).\varepsilon(x) = o(\|x\|^2)$. Il existe alors $\alpha > 0$ tel que

$$\forall x \in E, q(x) \leq \alpha \Longrightarrow |Dq(x).\varepsilon(x)| \leq \frac{\|x\|^2)}{2}.$$

Donc

$$\|x\| \leq \alpha \Longrightarrow -\|x\|^2 + Dq(x).\varepsilon(x) \leq \frac{-\|x\|^2}{2}.$$

□

Lemme. Soient α comme dans le lemme précédent et $(I, X(t))$ une solution maximale tels que $q(X(0)) < \alpha$, alors $I \supset \mathbb{R}_+$ et

$$\forall t > 0, q(X(t)) \leq \alpha.$$

Démonstration. On note $t_0 = inf\{t \in I \cap \mathbb{R}_+ | q(X(t) \leq \alpha\}$. Si $t_0 < sup(I)$, alors $q(X(t_0)) = \alpha$ et $\frac{d}{dt}q(X(t_0)) \geq 0$, ce qui contredit $\frac{d}{dt}q(X(t_0)) \leq -\beta q(X(t_0)$. Donc $q(X(t)) \leq \alpha$ pour tout $t \in I \cap \mathbb{R}_+$ et on en déduit que $I \supset \mathbb{R}_+$. □

Fin de la preuve du théorème : d'après les deux lemmes précédents, on a pour $X(t)$ solution telle que $q(X(0)) \leq \alpha$

$$\forall t > 0 \frac{d}{dt}q(X(t)) \leq -\beta q(X(t)),$$

et en intégrant (il faut regrouper d'un coté et multiplier par $e^{t\beta}$) on obtient

$$\forall t > 0, q(X(t)) \leq q(X(0))e^{-t\beta}.$$

IL suffit alors de prendre $C = sup_{x \leq \alpha} q(x)$. □

Remarque. La preuve se trouve dans [[Rou], Ex 46].

5 Lemme de Morse

Leçons concernées
- 130 - Matrices symétriques réelles, matrices hermitiennes.
- 131 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
- 148 - Formes quadratiques réelles. Exemples et applications.
- 214 - Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.
- 215 - Applications différentiables définies sur un ouvert de Rn. Exemples et applications.
- 218 - Applications des formules de TAYLOR.

A Notations

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie.
- On note $Q(E) = \{q \in L(E, E^*) : {}^t q = q\}$ l'ensemble des formes quadratiques sur E.
- Pour $q \in Q(E)$ et $x \in E$, on note $q[x] = {}^t x.q.x$.
- Pour $q \in Q(E)$ non dégénérée, on note $S(q) = \{H \in L(E) : {}^t H.q = q.H\}$ l'ensemble des endomorphismes auto-adjointes pour q. Les applications suivantes sont alors des isomorphismes d'espaces vectoriels réciproques l'une de l'autre

$$\begin{array}{rcl} S(q) & \longrightarrow & Q(E) \\ H & \longmapsto & q.H \end{array}.$$

$$\begin{array}{rcl} Q(E) & \longrightarrow & S(q) \\ p & \longmapsto & q^{-1}.p \end{array}.$$

B Théorème

Théorème (Lemme de Morse)**.** Soit E un espace vectoriel de dimension finie et $f : E \to \mathbb{R}$ une fonction C^k. On suppose que
- $k \geq 3$.
- $f(0) = 0$.
- $Df(0) = 0$.
- $D^2 f(0)$ est une forme quadratique non dégénérée.

Alors il existe $\phi : U \to V$, un C^{k-2}-difféomorphisme entre deux voisinages de 0 tel que $D\phi(0) = \mathrm{Id}_E$ et

$$\forall x \in U,\ f(x) = \frac{1}{2} D^2 f(0)[\phi(x)].$$

Démonstration. On commence par le lemme suivant.

Lemme. Soit $q \in Q(E)$ non-dégénérée. Alors l'application

$$\begin{array}{rccl} \Phi : & S(q) & \longrightarrow & Q(E) \\ & A & \longmapsto & {}^t A.q.A = q \circ A \end{array}$$

induit un C^∞-difféomorphisme d'un voisinage de Id_E vers un voisinage de q.

Démonstration du lemme. Il suffit de montrer que $D\Phi(\mathrm{Id}_E)$ est inversible. Pour $A \in S(q)$, la différentielle de Φ en A est

$$D\Phi(A).H = {}^t(dA).q.A + {}^t A.q.dA.$$

En prenant $A = \mathrm{Id}_E$, on obtient $D\Phi(A) = {}^t dA.q + q.dA = 2q.dA$, qui est bijective (on rappelle que pour $H \in S(q)$, on a ${}^t H.q = q.H$). □

Par formule de Taylor à l'ordre 2 appliqué à f en 0, on a

$$\forall x \in E,\ f(x) = \int_0^1 (1-t)\ D^2 f(tx)[x]dt = p_x[x],$$

avec $p_x = \int_0^1 (1-t) D^2 f(tx) dt \in Q(E)$. On a alors $p_0 = \frac{1}{2} D^2 f(0)$. D'après le lemme (appliqué à $q = p_0$), il existe $F : \Omega \subset Q(E) \to \Omega' \subset S(p_0)$, un C^∞-difféomorphisme tel que

$$\forall q \in \Omega,\ q = p_0 \circ F(q).$$

L'application $x \mapsto p_x$ de E dans $Q(E)$ est de classe C^{k-2} (la domination est facile car $[0,1]$ est compact). Il existe alors U un voisinage de 0 tel que $\{p_x : x \in U\} \subset \Omega$. On en déduit que

$$\forall x \in U,\ f(x) = p_0 \circ F(p_x)[x] = p_0[F(p_x).x].$$

On prend alors

$$\begin{array}{rccc} \phi : & U \subset E & \longrightarrow & E \\ & x & \longmapsto & F(p_x).x \end{array}.$$

Il reste à montrer que $D\phi(0) = \mathrm{Id}_E$. On a

$$D\phi(0) = D_{|x=0}\big(F(p_x)\big).0 + F(p_0).dx.$$

Or $D_{|x=0}\big(F(p_x)\big).0 = 0_{L(E)}$ et $F(p_0) = \mathrm{Id}_E$ par définition de F, d'où $D\phi(0) = dx = \mathrm{Id}_E$. □

Remarque.
- On trouvera une preuve plus matricielle dans [[Rou], Ex 114] et [[Gou94b], Anal, Chap V, Pb 4].
- Voir [Doukhan et Sifre] pour une preuve sous les hypothèses : f de classe C^1 et $D^2 f(0)$ existe et est non dégénérée.

6 Méthode du gradient à pas optimal et à pas conjugué

Leçons concernées

- 140 - Systèmes d'équations linéaires. Systèmes échelonnés. Résolution. Exemples et applications.
- 232 - Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.
- 219 - Problèmes d'extremums.

A Position du problème

Soient E un espace euclidien de dimension finie, A un endomorphisme symétrique définie positive et B un vecteur de E. On cherche à résoudre le système

$$Ax = B.$$

Considérons la fonctionnelle

$$\begin{array}{rccc} J: & E & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \frac{1}{2}\langle x, Ax\rangle - \langle B, x\rangle \end{array}.$$

Comme A est définie positve, J admet un unique minimum. De plus, on a $\nabla J(x) = Ax - B$, donc l'unique minimum de J est la solution de $Ax = B$. On cherche alors à trouver x tel que

$$J(x) = \min_{y \in E} J(y).$$

B Méthode du gradient à pas optimal

La méthode consiste à définir la suite $(x_n)_{n\in\mathbb{N}}$ par

$$\begin{cases} x_0 \in E. \\ \forall n \in \mathbb{N},\ x_{n+1} = argmin_x\Big\{J(x) \mid x \in x_n + \mathbb{R}\nabla J(x_n)\Big\}. \end{cases}$$

On remarque que si $\nabla J(x_n) = 0$ pour un $n \in \mathbb{N}$, alors la suite stationne. On note t_n tel que $x_{n+1} = x_n + t_n \nabla J(x_n)$. En développant, on obtient

$$J(x_n - t\nabla J(x_n)) = \frac{1}{2}\langle \nabla J(x_n), A\nabla J(x_n)\rangle . t^2 - \Big(\langle \nabla J(x_n), Ax_n\rangle - \langle \nabla J(x_n), B\rangle\Big)t + \frac{1}{2}\langle x_n, Ax_n\rangle - \langle B, x_n\rangle.$$

Comme t_n est le minimum de ce polynôme du second degré, on a

$$t_n = \frac{\langle \nabla J(x_n), \nabla J(x_n)\rangle}{\langle \nabla J(x_n), A\nabla J(x_n)\rangle}.$$

Lemme. La fonctionnelle J est elliptique, c'est-à-dire qu'il existe $\alpha > 0$ tel que

$$\forall x, y \in E,\ \langle \nabla J(x) - \nabla J(y), x - y\rangle \geq \alpha \|x - y\|^2.$$

Ce qui implique qu'elle est coercive, c'est-à-dire que $\lim_{\|x\|\to+\infty} |J(x)| = +\infty$, et on a

$$J(y) - J(x) \geq \langle \nabla J(x), y - x\rangle + \frac{\alpha}{2}\|y - x\|^2.$$

Démonstration du lemme. La fonctionnelle est elliptique car, on a

$$\langle \nabla J(x) - \nabla J(y), x - y\rangle = \langle A(x - y), x - y\rangle.$$

On a

$$\begin{array}{rcl} J(y) - J(x) & = & \displaystyle\int_0^1 \langle \nabla J(x + t(y - x)), y - x\rangle dt \\ & = & \displaystyle\int_0^1 \langle \nabla J(x + t(y - x)) - \nabla J(x), t(y - x)\rangle \frac{dt}{t} + \langle J(x), y - x\rangle \\ & \geq & \displaystyle\frac{\alpha}{2}\|y - x\|^2 + \langle J(x), y - x\rangle. \end{array}$$

□

Théorème. La suite $(x_n)_{n\in\mathbb{N}}$ converge vers la solution de $Ax = B$.

Démonstration. (Rapide) La suite $(J(x_n))_{n\in\mathbb{N}}$ décroît et est minoré, donc converge. Par théorème des extrema liés les vecteurs $\nabla J(x_{n+1})$ et $x_{n+1} - x_n$ sont orthogonaux, donc

$$\frac{\alpha}{2}\|x_{n+1} - x_n\|^2 \leq J_{x_n} - J_{x_{n+1}} \xrightarrow{n\to+\infty} 0.$$

Comme ∇J est une fonction uniformément continue, on en déduit que $(\nabla J(x_n) - \nabla J(x_{n-1}))_{n\in\mathbb{N}}$ tend vers 0.

Comme les vecteurs $\nabla J(x_n)$ et $\nabla J(x_{n+1})$ sont orthogonaux, on en déduit que :

$$\|\nabla J(x_n)\|^2 = \langle \nabla J(x_n), \nabla J(x_n) - \nabla J(x_{n-1})\rangle \leq \|\nabla J(x_n)\|.\|\nabla J(x_n) - \nabla J(x_{n-1})\|.$$

Donc $(\nabla J(x_n))_{n\in\mathbb{N}}$ tend vers 0.

Si on note x^* le point où J est minimale, alors on a

$$\alpha\|x_n - x^*\|^2 \leq \langle \nabla J(x_n) - \nabla J(x^*), x_n - x^*\rangle \leq \|\nabla J(x_n)\|.\|x_n - x^*\|.$$

D'où $\|x_n - x^*\| \leq \|\nabla J(x_n)\| \xrightarrow{n\to+\infty} 0$.

□

C Méthode du gradient à pas congugué

La méthode consiste à définir la suite $(x_n)_{n\in\mathbb{N}}$ par

$$\begin{cases} x_0 \in E. \\ \forall n \in \mathbb{N},\ x_{n+1} = argmin_x\Big\{J(x) : x \in x_n + vect(\nabla J(x_0), \nabla J(x_1), \dots, \nabla J(x_n))\Big\}. \end{cases}$$

Théorème. La suite $(x_n)_{n\in\mathbb{N}}$ converge vers la solution de $Ax = B$ en au plus $\dim E$ itérations. De plus la suite est donnée par les formules explicites :

$$d_{-1} = 0,\ x_0 \in E,$$

pour $n \in \mathbb{N}$, tant que $\nabla J(x_n) \neq 0$.

$$\begin{cases} d_n = \nabla J(x_n) + \frac{\|\nabla J(x_n)\|^2}{\|\nabla J(x_{n-1})\|^2} d_{n-1}, \\ t_n = \frac{\langle \nabla J(x_n), d_n\rangle}{\langle d_n, Ad_n\rangle} \\ x_{n+1} = x_n - t_n d_n. \end{cases}$$

Les d_n donnent alors les directions de descentes.

Démonstration. On démontre d'abord les deux lemmes suivants qui donnent des relations d'orthogonalité.

Lemme. La famille $(\nabla J(x_n))_{n\in\mathbb{N}}$ est orthognonale.

Démonstration du lemme. Le théorème des extréma liés montre que pour tout $n \in \mathbb{N}$, le vecteur $\nabla J(x_{n+1})$ est orthogonal à $vect(\nabla J(x_0), \dots, \nabla J(x_n))$. □

On en déduit que $(\nabla J(x_n))_{n\in\mathbb{N}}$ s'annule pour un rang $N \leq \dim E$ et à partir de ce rang la suite stationne vers la solution de $Ax = B$. On note N ce rang. On note $(\Delta x_n)_{n\in[0,N-1]}$ la suite des différences :

$$\forall n \in [0, N-1], \Delta x_n = x_{n+1} - x_n \in vect(\nabla J(x_0), \dots, \nabla J(x_n)).$$

Lemme. La famille $(\Delta x_n)_{n\in[0,N-1]}$ est A-orthogonale et pour tout $n \in [0, N-1]$, on a

$$vect(\Delta x_0, \dots, \Delta x_n) = vect(\nabla J(x_0), \dots, \nabla J(x_n))$$

Démonstration du lemme. On remarque que pour $x, y \in E$, on a $A(x - y) = \nabla J(x) - \nabla J(y)$. Donc d'après le lemme précédent, on a

$$\forall n \in [0, N-1],\ A\Delta x_n = \nabla J(x_{n+1}) - \nabla J(x_n) \in vect(\nabla J(x_0), \dots, \nabla J(x_{n-1}))^\perp,$$

avec la convention $vect(\nabla J(x_0), \dots, \nabla J(x_{n-1})) = \{0\}$ si $n = 0$. Ce qui veut dire que Δx_n est A-orthogonal à $vect(\nabla J(x_0), \dots, \nabla J(x_n))$ qui contient $\Delta x_{n-1}, \dots, \Delta x_0$.

On montre le deuxième point par récurrence sur n. Pour $n = 0$ c'est clair. Soit $n \in [1, N-1]$ et supposons le résultat vrai au rang $n-1$. On a $\Delta x_n \in vect(\nabla J(x_0), \dots, \nabla J(x_n))$ par définition de x_{n+1}. Comme $\nabla J(x_n) \neq 0$, on a $\Delta x_n \notin vect(\nabla J(x_0), \dots, \nabla J(x_n))$, ce qui prouve le résultat. □

Ce lemme montre que la famille $(\Delta x_n)_{n\in[0,N-1]}$ est à constante près le A-orthogonalisé de Gram-Schmidt de $(\nabla J(x_n))_{n\in[0,N-1]}$. On note $(d_n)_{n\in[0,N-1]}$ l'orthogonalisé de Gram-Schmidt de $(\nabla J(x_n))_{n\in[0,N-1]}$ pour le produit scalaire défini par A et $t_n \in \mathbb{R}$ tel que $\Delta x_n = -t_n d_n$. Ce qui donne $x_{n+1} - x_n = -t_n d_n$. Soit $n \in [0, N-1]$. Le vecteur d_n est donné par les formules de Gram-Schmidt

$$\begin{aligned} d_n &= \nabla J(x_n) - \textstyle\sum_{k=0}^{n-1} \frac{\langle \nabla J(x_n), Ad_k\rangle}{\langle d_k, Ad_k\rangle} d_k \\ &= \nabla J(x_n) - \textstyle\sum_{k=0}^{n-1} \frac{\langle \nabla J(x_n), A\Delta x_k\rangle}{\langle d_k, A\Delta x_k\rangle} d_k. \end{aligned}$$

Comme on a $A\Delta x_k = \nabla J(x_{k+1}) - \nabla J(x_k)$, le premier lemme montre que seul le terme en $k = n-1$ est non nul, ce qui donne

$$d_n = \nabla J(x_n) + \frac{\|J(x_n)\|^2}{\|\nabla J(x_{n-1})\|^2} d_{n-1}.$$

Comme, pour $t \in \mathbb{R}$, on a

$$J(x_n + td_n) = \langle d_n, Ad_n\rangle t^2 + 2\langle \nabla J(x_n), d_n\rangle t + \langle \nabla J(x_n), x_n\rangle.$$

on en déduit l'expression de t_n. □

Remarque. Voir [Ciarlet, Analyse numérique et optimisation] et [Serre, Matrix].

7 Sous-espaces de dimension finie de $C(\mathbb{R},\mathbb{R})$ stables par translation

Leçons concernées

- 118 - Exemples d'utilisation de la notion de dimension en algèbre et en géométrie.
- 120 - Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
- 123 - Déterminant. Exemples et applications.
- 220 - Équations différentielles $X' = f(t, X)$. Exemples d'études qualitatives des solutions.
- 221 - Équations différentielles linéaires, exemples et applications.

A Théorème

Théorème. Soit E un sous-espace de $C^0(\mathbb{R},\mathbb{R})$ stable par translation de dimension finie n. Alors E est l'espace des solutions d'une équation linéaire à coefficients constants d'ordre n.

B Première preuve

Soit $(f_1,\dots,f_n)$ une base de E. Soit $a \in \mathbb{R}$. Comme E est stable par translation la famille $(f_1(.+a),\dots,f_n(.+a))$ est une famille de E, donc il existe $M(a) \in \mathcal{M}_n(\mathbb{R})$ tel que

$$\begin{pmatrix} f_1(.+a) \\ \vdots \\ f_n(.+a) \end{pmatrix} = M(a) \begin{pmatrix} f_1(.) \\ \vdots \\ f_n(.) \end{pmatrix}.$$

(Les matrices colonnes sont dans $\mathcal{M}_{n,1}(E)$). On va montrer que la fonction $a \mapsto M(a)$ est de classe C^1. On note $g_i(x) = \int_0^x f_i(t)dt$. La famille $(g_i)_{i\in[1,n]}$ est alors libre car la famille des dérivées est libre. En intégrant l'expression ci dessus de 0 à x on en déduit que

$$\begin{pmatrix} g_1(.+a)-g_1(a) \\ \vdots \\ g_n(.+a)-g_n(a) \end{pmatrix} = M(a) \begin{pmatrix} g_1(.) \\ \vdots \\ g_1(.) \end{pmatrix}.$$

Lemme. Il existe $x_1,\dots,x_n \in \mathbb{R}$ telle que la matrice $[g_i(x_j)]$ soit inversible

Démonstration du lemme. On note $F = vect(g_1,\dots,g_n)$. On considère la famille $\{ev_x : x \in \mathbb{R}\} \subset F^*$ où ev_x est l'évaluation en x. Comme l'orthogonal de cette famille est nulle, c'est une famille génératrice, donc on peut extraire une base $(ev_{x_1},\dots,ev_{x_n})$ de E^*. La matrice $[ev_{x_i}(g_j)]_{i,j} = [g_j(x_i)]_{i,j}$ est alors inversible. □

On a alors pour tout $a \in \mathbb{R}$

$$\begin{pmatrix} g_1(x_1+a)-g_1(a) & \cdots & g_1(x_n+a)-g_1(a) \\ \vdots & & \vdots \\ g_n(x_1+a)-g_n(a) & \cdots & g_n(x_n+a)-g_1(a) \end{pmatrix} = M(a) \begin{pmatrix} g_1(x_1) & \cdots & g_1(x_n) \\ \vdots & & \vdots \\ g_n(x_1) & \cdots & g_1(x_n) \end{pmatrix}.$$

et en inversant la matrice $[g_i(x_j)]_{i,j}$, on en déduit que $a \mapsto M(a)$ est C^1.

En évaluant en $x = 0$ dans l'équation au dessus [?], on en déduit que pour tout $a \in \mathbb{R}$

$$\begin{pmatrix} f_1(a) \\ \vdots \\ f_n(a) \end{pmatrix} = M(a) \begin{pmatrix} f_1(0) \\ \vdots \\ f_n(0) \end{pmatrix}.$$

Donc les $f_i$sont de classe C^1. En dérivant par rapport à a et en prenant $a = 0$, on a

$$\begin{pmatrix} f_1' \\ \vdots \\ f_n' \end{pmatrix} = M'(0) \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}.$$

Donc l'espace E est stable par dérivation. On note $P(X) \in \mathbb{R}[X]$ le polynôme minimal de la dérivation sur E. On a alors $\deg P \leq n$ et E est inclus dans l'espace des solutions de $P(d/dx) = 0$ qui est de dimension $\deg P$. Donc on a égalité entre ces deux ensemble.

C Deuxième preuve preuve

On prend une famille $(x_1, \dots, x_n)$ de $\mathbb{R}$ tel que la famille $(ev_{x_1}, \dots, ev_{x_n})$ soit base de $L(E, \mathbb{R})$ et on prend $(f_1 \dots, f_n)$ une base de E. On munit l'espace $L(E)$ de la norme

$$\forall A \in L(E),\ \|A\|_{L(E)} := \max_{i,j} |ev_{x_i}.A.f_j| = \max_{i,j} |A.f_j(x_i)|.$$

On définit l'action linéaire de $\mathbb{R}$ sur E par translation :

$$\begin{array}{rccc} \Phi : & \mathbb{R} & \longrightarrow & GL(E) \\ & a & \longmapsto & (f \mapsto f(.+a)) \end{array}.$$

Lemme. L'application Φ est continue. C'est-à-dire que Φ est un sous-groupe à un paramètre de $GL(E)$.

Démonstration. Soit $x \in \mathbb{R}$, on a

$$\forall y \in \mathbb{R},\ \|\Phi(x+y) - \Phi(x)\|_{L(E)} = \max_{i,j} |f_j(x_i + x + y) - f_j(x_i + x)|.$$

Comme les f_j sont continues aux points $x_i + t$ $(i, j \in [1, n])$, on en déduit que $\lim_{y \to 0} \|\Phi(x+y) - \Phi(x)\|_{L(E)} = 0$. □

On va montrer que les sous-groupes à un paramètres sont su type $x \mapsto exp(xA)$, avec $A \in L(E)$, mais on a seulement besoin de savoir que Φ est dérivable en 0.

Lemme. L'application ϕ est de classe C^1.

Démonstration. Par propriété de groupe on a

$$\forall x, y \in \mathbb{R},\ \Phi(x+y) = \Phi(x).\Phi(y).$$

Soit $\varepsilon > 0$. En intégrant pour $y \in [0, \varepsilon]$, on a

$$\forall x \in \mathbb{R},\ \int_x^{x+\varepsilon} \Phi(z)dz = \Phi(x). \int_0^{\varepsilon} \Phi(z)dz.$$

L'application $x \mapsto \int_x^{x+\varepsilon} \Phi(z)dz$ est C^1 car Φ est continue. Montrons que pour un certain $\varepsilon > 0$ l'endomorphisme $\int_0^{\varepsilon} \Phi(z)dz \in L(E)$ est inversible. On a

$$\|\mathrm{Id}_E - \frac{1}{\varepsilon} \int_0^{\varepsilon} \Phi(z)dz\| = \frac{1}{\varepsilon} \int_0^{\varepsilon} \|\mathrm{Id}_E - \phi(z)\|dz \leq \|\mathrm{Id}_E - \phi(z)\|_{L^\infty([0,\varepsilon])}.$$

Par continuité de cette quantité est inférieur à $1/2$ pour $\varepsilon > 0$ assez petit et $\int_0^{\varepsilon} \Phi(z)dz$ sera alors inversible.

En inversant dans l'expression [?], on en déduit que Φ est C^1. □

On note $A = \Phi'(0) \in L(E)$.

Lemme. On a

$$\forall \in x \in \mathbb{R}, \Phi(x) = exp(xA).$$

Démonstration. En dérivant $\Phi(x+y) = \Phi(x).\Phi(y)$ par rapport à x et en évaluant en $x = 0$, on obtient.

$$\Phi'(y) = A.\Phi(y).$$

Donc $\Phi(y) = \Phi(0)exp(tA) = exp(tA)$. □

On a pour tout $x \in \mathbb{R}$ et $f \in E$:

$$\begin{array}{rcl} \forall y \in \mathbb{R}^*,\ \dfrac{f(x+y) - f(x)}{y} & = & ev_x.\left(\dfrac{1}{y}(\Phi(y) - \Phi(0))\right).f \\ & \xrightarrow{y \to 0} & ev_x.A.f = (A.f)(x). \end{array}$$

Donc f est dérivable et $f' = A.f$ pour tout $f \in E$.

On conclut comme dans la preuve précédente.

Remarque.
- La deuxième preuve est dûe à Sébastien Alvarez.
- On trouvera la première preuve aux endroits suivants : [FGN, Algèbre 1, Ex 6.28], [Leichtnam, Analyse, 4.10 p92], [BMP, Chap 3, Ex 3.9]

8 Sur l'exponentielle matricielle

Leçons concernées
- 114 - Anneau des séries formelles. Applications.
- 124 - Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
- 127 - Exponentielle de matrices. Applications.
- 215 - Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.
- 241 - Suites et séries de fonctions. Exemples et contre-exemples.
- 243 - Convergence des séries entières, propriétés de la somme. Exemples et applications.

A Préléminaires

Définition. Pour $A, B \in \mathcal{M}_n(\mathbb{C})$, on définit l'application $A \otimes B \in L(\mathcal{M}_n(\mathbb{C}))$ par

$$A \otimes B : \begin{array}{ccc} \mathcal{M}_n(\mathbb{C}) & \longrightarrow & \mathcal{M}_n(\mathbb{C}) \\ M & \longmapsto & AMB \end{array}.$$

On a alors les formules élémentaires suivantes :
- L'application $(A, B) \mapsto A \otimes B$ est bilinéaire.
- $(A \otimes I_n)^n = A^n \otimes I_n$.
- $exp(A \otimes I_n) = e^A \otimes I_n$.
- $(A \otimes I_n).(I_n \otimes B) = (I_n \otimes B).(A \otimes I_n) = A \otimes B$.

Lemme. Pour $A, B \in \mathcal{M}_n(\mathbb{C})$, on a

$$Spec(A \otimes I_n - I_n \otimes B) = \{\lambda - \mu \mid \lambda \in Spec(A), \mu \in Spec(B)\}.$$

Démonstration. Trigonaliser A et B. □

B Points critiques de l'exponentielle

On note $F(T) = \sum_{n=0}^{+\infty} \frac{(-T)^n}{n+1!} = \left(\frac{1-e^{-T}}{T}\right) \in \mathbb{Q}[[T]]$.

Théorème (Points critiques de l'exponentielle)**.** Soit $X \in \mathcal{M}_n(\mathbb{C})$. Alors

$$Dexp(X) = exp(X \otimes I_n) F(X \otimes I_n - I_n \otimes X)$$

De plus, X est point critique de l'exponentiel si et seulement si

$$\exists \lambda, \mu \in Spec(X),\ \lambda - \mu \in 2i\pi\mathbb{Z}^*.$$

Démonstration. En dérivant la série exponentielle (appliquer le théorème de domination), on obitent

$$Dexp(X) = \sum_{n=1}^{+\infty} \frac{1}{n!} \sum_{p+q=n-1} X^p \otimes X^q = \sum_{p,q=0}^{\infty} \frac{X^p \otimes X^q}{p+q+1!}.$$

Lemme. Pour $X, Y \in \mathcal{M}_n(\mathbb{C})$, On a

$$\sum_{p,q=0}^{\infty} \frac{X^p \otimes Y^q}{p+q+1!} = exp(X \otimes Id) F(X \otimes Id - Id \otimes Y).$$

Démonstration du lemme. On calcule la quantité suivante

$$\begin{aligned}(X \otimes Id - Id \otimes Y) \sum_{p,q=0}^{+\infty} \frac{X^p \otimes Y^q}{p+q+1!} &= exp(X \otimes Id) - exp(Id \otimes Y) \\ &= exp(X \otimes Id)(1 - exp(-X \otimes Y + Id \otimes Y))\end{aligned}$$

Si $X \otimes Id - Id \otimes Y$ est inversible on obtient le résultat en simplifiant. Sinon en prend une suite (X_n, Y_n) tendant vers (X, Y) telle que $0 \notin Spec(X_n \otimes Id - Id \otimes Y_n)$. □

La formule pour $Dexp(X)$ s'obtient en prenant $Y = X$. Pour les points critiques on a

$$\begin{aligned} D_X exp \text{ inversible} &\iff F(X \otimes Id - Id \otimes X) \text{ inversible} \\ &\iff 0 \notin SpecF(X \otimes Id - Id \otimes X) \\ &\iff 0 \notin \Big\{F(\lambda - \mu) \mid \lambda, \mu \in Spec(X)\Big\}. \end{aligned}$$

□

Remarque. – Cette preuve a été élaboré par moi-même à partir de la remarque de [[GT98] Part. 1, Chap. 2, Ex. 22] dans lequel on trouvera une variante.
– Voir [Mneimée] ou [[Rou] Ex 109 ?] pour une preuve qui utilise les équations différentielles.

C Image de l'exponentiel

Proposition. L'exponentiel est une bijection des matrices nilpotentes vers les matrices unipotentes (vrai en corps quelconque).

Démonstration. Utiliser la série logarithme. □

Théorème. $exp(\mathcal{M}_n(\mathbb{C})) = GL_n(\mathbb{C})$.

Démonstration. Soit $M = DU$ avec D diagonalisable et U unipotent tels que D et U commutent. Alors on pose

$$N = \log(I_n + (U - I_n)) \text{ et } \delta = \sum_{i=1}^{k} \log \lambda_i \ P_i,$$

avec $(\lambda_i)_{i\in[1,k]}$ les valeurs propres de M, $\log \lambda_i$ un antécédent de λ_i par exp et $(P_i)_{i\in[1,k]}$ les projecteurs sur les sous-espaces propres. Les matrices N et δ sont respectivement polynômiales en U et D donc commuttent. Ce qui donne $exp(\delta + N) = DU$. □

Théorème. $exp(\mathcal{M}_n(\mathbb{R})) = GL_n(\mathbb{R})^2$.

Démonstration.

Lemme. Pour $A \in \mathcal{M}_n(\mathbb{C})$ il existe $P(X) \in \mathbb{C}[X]$ tel que $A = exp(P(A))$.

Démonstration du lemme. Si on note $A = DU$, il existe $Q(X) \in \mathbb{C}[X]$ tel que $D = exp(Q(D))$ (cf. preuve précédente) et on a $U = exp(\log(U))$. Comme $Q(D)$ et $\log(U)$ commutent, on a $A = exp(Q(D) + \log(U))$. On conclut en utilisant le fait que D et U sont polynômiales en A. □

Pour $A \in \mathcal{M}_n(\mathbb{R})$, il existe $P \in \mathbb{C}[X]$ tel que $A = exp(P(A))$. On en déduit que $A^2 = exp(P(A) + \overline{P}(A))$ avec $P(A) + \overline{P}(A) \in \mathcal{M}_n(\mathbb{R})$. Donc tout carré de $GL_n(\mathbb{R})$ est une exponentiel. Réciproquement si $A = exp(B)$ alors $A = exp(B/2)^2$. □

9 Équation des planètes

Leçons concernées
- 136 - Coniques. Applications.
- 216 - Étude métrique des courbes. Exemples.
- 220 - Équations différentielles $X' = f(t, X)$. Exemples d'études qualitatives des solutions..

A Position du problème

On considère l'équation dans $\mathbb{R}^3 \setminus \{O\}$ avec conditions initiales :

$$\begin{cases} \dot{M} = -\frac{1}{OM^2}\frac{\overrightarrow{OM}}{OM} \\ M(0) = M_0 \in \mathbb{R}^3 \setminus \{O\} \\ \dot{M}(0) = v_0 \in \mathbb{R}^3. \end{cases} .$$

Cette équation vérifie les hypothèses de Cauchy-Lipschitz.

B Cas des trajectoires rectilignes

Théorème. Si v_0 est colinéaire à $\overrightarrow{OM_0}$, alors la trajectoire est sur la demi droite $]OM_0)$.

Démonstration. Celà vient du fait que le champ vecteurs est tangente à la sous-variété $]OM_0)$. □

Le cas $v_0 \in (OM_0)$ se ramène donc à résoudre en domension 1 l'équation :

$$\dot{r} = -\frac{1}{r^2},$$

où $r = \|OM\|$. On ne traitera pas ce cas là (qui peut peut faire le sujet d'un autre développement).

C Cas des trajectoires coniques

Théorème. On suppose que $v_0 \notin (OM_0)$ et on note $M(t)$ la solution maximale et I son intervalle de définition. Alors la trajectoire est une conique et $I = \mathbb{R}$.

Démonstration. On remarque d'abord la chose suivante.

Lemme. Pour tout $t \in I$, les vecteurs $\dot{M}(t)$ et $\overrightarrow{OM(t)}$ sont libres.

Démonstration. Si ce n'était pas le cas, alors on est dans le cas précédent et donc les vecteurs $\left(\frac{dM(t)}{dt}, \overrightarrow{OM}(t)\right)$ sont liés pour tout $t \in I$. □

Ensuite on introduit une intégrale première.

Lemme (Moment cinétique et constante des aires)**.** La quantité $\overrightarrow{C} = \overrightarrow{OM} \wedge \frac{dM}{dt}$ est constante (non nulle par hypothèse et on l'appelle la constante des aires).

Démonstration. Il suffit de dériver. □

On en déduit que la trajectoire se fait dans le plan $H = O + \overrightarrow{C}^{\perp}$. On identifie alors ce plan à $\mathbb{C}$ et on note $c = \det(\overrightarrow{OM_0}, v_0)$.

Comme la courbe $M(t)$ ne passe pas par zéro, on peut la paramétrer de la façon suivante :

$$M(t) = r(t)e^{i\theta(t)}.$$

On a alors $\dot{M}(t) = \dot{r}(t)e^{i\theta(t)} + r(t)\dot{\theta}(t)ie^{i\theta(t)}$, soit $C = r(t)^2\dot{\theta}(t)$. Donc $\boxed{\theta \text{ est un paramétrage admissible}}$, et on a $\frac{d}{dt} = \frac{d}{d\theta}\frac{d\theta}{dt} = Cu^2\frac{d}{d\theta}$, avec $u = r^{-1}$. On en déduit que

$$\frac{dM}{dt} = Cu^2\frac{d}{d\theta}(re^{i\theta}) = -C\frac{du}{d\theta}e^{i\theta} + Cuie^{i\theta}.$$

$$\frac{d^2M}{dt^2} = Cu^2\frac{d}{d\theta}(\frac{dM}{dt}) = -C^2u^2(\frac{d^2u}{d\theta^2} + u)e^{i\theta}.$$

Ce qui donne finalement

$$\frac{d^2u}{d\theta^2} + u = \frac{1}{C^2}.$$

On en déduit que la solution u en fonction du paramètre θ est de la forme

$$u(\theta) = \frac{1}{C^2}(1 + e\cos(\theta + \phi)),$$

avec e et ϕ des constantes dépendantes des conditions initiales, soit

$$M(\theta(t)) = \frac{C^2}{1 + e\cos(\theta(t) + \phi)}.$$

Pour simplifier on suppose que $M(t = 0)$ est sur $\mathbb{R}_{>0}$ et que $\dot{M}(t = 0)$ est colinéaire à $i\mathbb{R}$. On écrit alors $M(0) = r_0$ et $\dot{M}(0) = i|v_0|$. Donc $\theta(t = 0) = 0$, ce qui donne

$$\begin{cases} C = r_0|v_0|, \\ u(\theta = 0) = r_0^{-1}, \\ \frac{du}{d\theta}_{|\theta=0} = \frac{dr^{-1}}{dt}_{|t=0}\frac{dt}{d\theta} = -v_0. \end{cases}$$

On en déduit que $\forall t \in I$, $\frac{1}{OM(t)} \leq \frac{1}{C^2}(1 + |e|)$, et donc la solution est Lipchitzienne et ne peut pas exploser en temps fini. Donc $I = \mathbb{R}$. □

Remarque.
- Pour avoir θ en fonction de t, il reste à résoudre l'équation différentielle

$$\frac{d\theta}{dt} = Cu^2(\theta) = \frac{1}{C^3}(1 + e\cos(\theta + \phi))^2,$$

  qui est complet puisque globalement lipschitzienne (on sépare les variables et utilise les techniques d'intégrations usuelles, mais on se retrouve avec une fraction compliquée...).
- La solution n'est pas définie sur $\mathbb{R}$, si v_0 est colinéaire à $\overrightarrow{OM}$.

10 Théorème de Gershörin

Leçons concernées
- 245 - Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$.

Préliminaires

Définition. Soit $M = [a_{ij}]_{i,j} \in M_n(\mathbb{C})$. Les *disques de Gershgörin* sont les disque fermées $\bar{D}_i := \bar{D}(a_{ii}, \sum_{j\neq i} |a_{ij}|)$. Le *domaine de Gershgörin* D est l'union des disques de Gershgörin.

Proposition. Le spectre de M est inclus dans le domaine de Gershgörin.

Théorème de Gershgörin

Théorème. Soit G une composante connexe du domaine de Gershgörin et p de nombre de disques qu'il contient. Alors il y a exactement p valeurs propres dans G avec multiplicité algébrique.

Démonstration. On prend γ une courbe (non nécessairement connexe) orienté telle que

$$\forall z \in D, \begin{cases} Ind_\gamma(z) = 1, & \text{si } z \in G \\ Ind_\gamma(z) = 0, \text{si } a \notin G \end{cases}.$$

(On admet l'existence d'une telle courbe ?). Alors le nombre de valeurs propres de M dans G est

$$\frac{1}{2i\pi} \int_\gamma \frac{\chi'_M(z)}{\chi_M(z)} dz.$$

On note pour tout $t \in [0,1]$ la matrice

$$M_t = \Big[a_{ij}(t)\Big]_{i,j\in[1,n]} \text{ avec } a_{ii}(t) = a_{ii} \text{ et } a_{ij}(t) = t.a_{ij}.$$

Alors l'application suivante est continue :

$$\begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{R} \\ t & \longmapsto & \frac{1}{2i\pi} \int_\gamma \frac{\chi'_{M(t)}(z)}{\chi_{M(t)}(z)} dz \end{array}.$$

En effet, on remarque d'abord que pour tout $t \in [0,1]$, la fonction $z \mapsto \chi_{M(t)}(z)$ ne s'annule par sur γ, car le domaine de Gershgörin de $M(t)$ est inclus dans celui de M. Ensuite, la continuité s'en déduit par convergence dominée sur le domaine d'intégration γ qui est compact. Comme c'est une fonction à valeur entière, elle est constante. En $t = 0$ elle vaut p, donc en $t = 1$ elle vaut p. □

Remarque. La preuve se trouve dans [Serre, Matrix].

Deuxième partie

Développements d'algèbre et de géométrie

Chapitre 2

Groupes et géométrie

1 Théorème de Banach-Tarski faible

Leçons concernées
- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.
- 108 - Exemples de parties génératrices d'un groupe. Applications.
- 133 - Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).
- 135 - Isométries d'un espace affine euclidien de dimension finie. Forme réduite. Applications en dimensions 2 et 3.
- 141 - Utilisation des groupes en géométrie.

A Énoncé du théorème

Théorème. On note B_3 la boule unité de $\mathbb{R}^3$. Alors, il existe :
- X un sous-ensemble de B_3 de mesure pleine.
- Une partition de X en 4 parties : $X = A_1 \sqcup A_2 \sqcup A_3 \sqcup A_4$.
- Deux rotations $f, g \in SO_3(\mathbb{R})$.

Tels que

$$X = A_1 \sqcup f(A_2) = A_3 \sqcup g(A_4).$$

B Preuve du théorème

On note F_2 libre non abélien de générateur a et b. On rappelle qu'une action G sur X est libre si pour tout $g \in G - \{1\}$, l'ensemble $Fix(g) := \{x \in X | g.x = x\}$ est vide.

On commence par la proposition suivante.

Proposition. Si F_2 agit sur un ensemble X de façon libre, alors il existe une partition $X = A_1 \sqcup A_2 \sqcup A_3 \sqcup A_4$ tel que

$$X = A_1 \sqcup a.A_2 = A_3 \sqcup b.A_4.$$

Démonstration. Le lemme suivant montre la proposition pour $X = F_2$ munie de l'action par translation à gauche.

Lemme. Il existe une partition de F_2 en $F_2 = H_1 \sqcup H_2 \sqcup H_3 \sqcup H_4$, tel que

$$G = H_1 \sqcup a.H_2 = H_3 \sqcup b.H_4.$$

Démonstration. On prend

$$\begin{aligned}
H_1 &= \Big\{u \in G : u \text{ commence par } a \text{ ou est du type } a^{-n} \text{ avec } n \geq 0\Big\},\\
H_2 &= \Big\{u \in G : u \text{ commence par } a^{-1} \text{ et n'est pas du type } a^{-n} \text{ avec } n \geq 1\Big\},\\
H_3 &= \Big\{u \in G : u \text{ commence par } b\Big\},\\
H_4 &= \Big\{u \in G : u \text{ commence par } b^{-1}\Big\}.
\end{aligned}$$

On a alors

$$a.H_2 = \Big\{v \in G : v \text{ ne commence pas par } a \text{ et n'est pas du type } a^{1-n} \text{ avec } n \geq 1\Big\} = G - H_1,$$

$$b.H_4 = \Big\{v \in G : v \text{ ne commence pas par } b\Big\} = G - H_3.$$

□

On revient au cas général. Pour tout $x \in X$, on a une bijection $Orb(x) := F_2.x \simeq F_2$, donc

$$\begin{array}{rcl} Orb(x) & = & H_1.x \sqcup H_2.x \sqcup H_3.x \sqcup H_4.x \\ & = & H_1.x \sqcup a.(H_2.x) = H_3.x \sqcup b.(H_4.x). \end{array}$$

On choisit alors E un ensemble de représentants des orbites de F_2 sur X et on prend

$$\forall i \in [1,4], A_i = \bigsqcup_{x \in E} H_i.x.$$

□

Pour démontrer le théorème il suffit alors de trouver une action libre par rotations sur une une partie de B_3 de mesure pleine. On prend f la rotation d'axe (Oz) d'angle $\cos^{-1}\frac{3}{5}$ et g la rotation d'axe (Ox) d'angle $\cos^{-1}\frac{3}{5}$:

$$f = \begin{bmatrix} 3/5 & -4/5 & 0 \\ 4/5 & 3/5 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \frac{1}{5}\begin{bmatrix} 3 & -4 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$g = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3/5 & -4/5 \\ 0 & 4/5 & 3/5 \end{bmatrix} = \frac{1}{5}\begin{bmatrix} 5 & 0 & 0 \\ 0 & 3 & -4 \\ 0 & 4 & 3 \end{bmatrix}.$$

On note $\langle f, g\rangle$ le groupe engendré par f et g.

Lemme. Le groupe $\langle f, g\rangle$ est libre de base (f, g), c'est-à-dire que le morphisme suivant est bijectif :

$$\begin{array}{rccc} R : & F_2 & \longrightarrow & G \\ & u = a^{\alpha_1}b^{\alpha_1}\dots & \longmapsto & f^{\alpha_1}g^{\alpha_2}\dots \end{array}.$$

Démonstration du lemme. Pour u un mot, on note $|u|$ sa taille et

$$\begin{pmatrix} p(u) \\ q(u) \\ r(u) \end{pmatrix} := 5^{|u|}R(u).e_1$$

la première colonne de $5^{|u|}R(u)$ qui est à coefficients dans $\mathbb{Z}$.

Montrons par récurrence sur $|u|$ que : pour tout mot u non vide se terminant par $a^{\pm 1}$, on a $5 \nmid q(u)$.
- Si $|u| = 1$, alors $u = a^{\pm 1}$ et $q(u) = \pm 4$.
- Si $|u| \geq 2$, alors u est de l'un des quatre types suivants :
$$v = a^{\pm 2}v,\ a^{\pm 1}b^{\pm 1}v,\ b^{\pm 1}a^{\pm 1}v \text{ ou } b^{\pm 2}v,$$
avec v un mot de longueur $|u| - 2$.
• Si $u = abv$, alors le mot bv est non vide et se termine par $a^{\pm 1}$. On a
$$5^{|u|}R(u) = 5f.5^{|bv|}R(bv),$$
ce qui donne
$$q(u) = 4p(bv) + 3q(bv).$$
De même on a $p(bv) = 5p(v)$. Par hypothèse de récurrence $q(bv) \neq 0 \mod 5$. D'où $q(u) \neq 0 \mod 5$.
• Si $u = bav$ (v se termine par a ou est vide). On a
$$5^{|u|}R(u) = 5g.5^{|av|}R(av),$$

ce qui donne

$$q(u) = 3q(av) - 4r(av).$$

On a $r(av) = 5r(v)$. Par hypothèse de récurrence $q(av) \neq 0 \mod 5$. D'où $q(u) \neq 0 \mod 5$.
• Si $u = aav$ (v se termine par a ou est vide). On a

$$q(u) = 4p(av) + 3q(av).$$

$$p(av) = 3p(v) - 4q(v) \text{ et } p(av) = 4p(v) + 3q(v),$$

ce qui donne

$$q(u) = -25q(v) + 6q(av).$$

Comme av n'est pas le mot vide et se termine par $a^{\pm 1}$, par hypothèse de réccurrence $q(av) \neq 0 \mod 5$, d'où $q(u) = 0 \mod 5$.
• les autres cas se traitent de la même façon.

Donc si u se termine par $a^{\pm 1}$, alors $R(u) \neq I_3$. En raisonnant sur la dernière colonne, on en déduit que si u se termine par $b^{\pm 1}$, alors $R(u) \neq I_3$, ce qui montre l'injectivité de R. □

On fait agir F_2 sur B_3 via f et g. Si on pose

$$X := B_3 - \left(\bigcup_{g \in F_2 - \{1\}} Fix(g) \right),$$

alors X est de mesure pleine (car F_2 est dénombrable et $Fix(g)$ est une droite d'après le lemme) et F_2 agit sur X de façon libre par construction.

Remarque. La preuve se trouve sur le polycopié de Logique de P. Dehornoy [Lemmes 2.22, 2.23 et 2.24].

2 Groupes des isométries des polyèdres

Leçons concernées

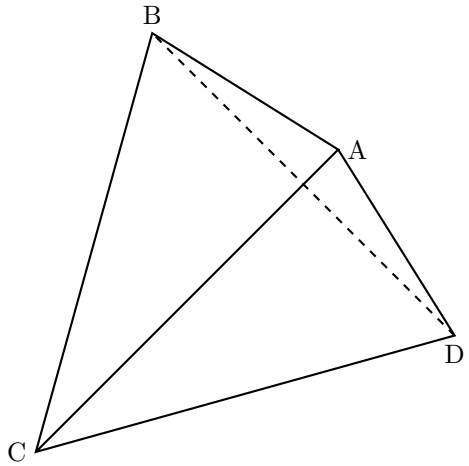
- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 104 - Groupes finis. Exemples et applications.
- 105 - Groupe des permutations d'un ensemble fini. Applications.
- 107 - Sous-groupes finis de $O_2(\mathbb{R})$ et de $SO_3(\mathbb{R})$. Applications.
- 133 - Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).
- 135 - Isométries d'un espace affine euclidien de dimension finie. Forme réduite. Applications en dimensions 2 et 3.
- 141 - Utilisation des groupes en géométrie.
- 149 - Groupes finis de petit cardinal.

On regardera [Tauvel] ou [Berger] pour la définition, l'existence et l'unicité des polyèdres réguliers.

Isométries du tétraèdre

Soit $T = ABCD$ un tétraèdre régulié centré en 0. On note

- $Isom(T)$ (resp. $Isom^+(T)$) le sous-groupe de $O_3(\mathbb{R})$ (resp. $SO_3(\mathbb{R})$) stabilisant T.
- $\mathfrak{S}(T)$ de groupe des permutations de sommets de T.



L'action de $Isom(T)$ sur T est fidèle car les sommets du tétraèdre sont libres. Donc on a une injection naturelle $Isom(T) \to \mathfrak{S}(T)$.

Théorème (Groupe des isométries du tétraèdre)**.** L'application naturelle $Isom(T) \to \mathfrak{S}(T)$ est un isomorphisme de groupe.

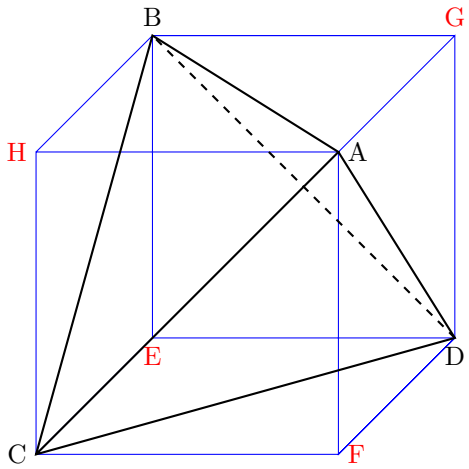
Démonstration. Exercice (on vérifie que toutes les transpositions de T sont obtenues grâce à des réflexions). □

Théorème (Groupe des isométries directes du tétraèdre)**.** Sur $Isom(T) = \mathfrak{S}(T)$ le déterminant et la signature coïncident. Donc l'application naturelle $Isom^+(T) \to \mathfrak{A}(T)$ est un isomorphisme.

Démonstration. La composée $\mathfrak{S}(T) \xrightarrow{\sim} Isom(T) \xrightarrow{\det} \{-1, 1\}$ est un morphisme surjectif, donc c'est la signature. □

Isométries du cube (et de l'octaèdre)

On note Γ un cube centré en 0 (par exemple les 8 points $(\pm 1, \pm 1, \pm 1)$) et $T = ABCD$ l'un des deux tétraèdres inscrit dans le cube. On note aussi $E = -A$, $F = -B$, $G = -C$, $H = -D$ (ce sont les sommets de l'autre tétraèdre inscrit dans Γ).



On remarque que $Isom(T) \subset Isom(C)$, car si $f \in SO_3(\mathbb{R})$ préserve T, alors f préserve aussi $-T$, donc préserve Γ.

Théorème (Groupe des isométries du cube)**.** Le groupe $Isom(\Gamma)$ est égal au produit direct $Isom(T) \times \{Id, -Id\}$. Plus précisément l'application suivante est un isomorphisme de groupe

$$\begin{array}{ccc} Isom(T) \times \{Id, -Id\} & \longrightarrow & Isom(\Gamma) \\ (\sigma, \tau) & \longmapsto & \sigma\tau \end{array}.$$

Démonstration. Un élément de $Isom(C)$ soit préserve T et $-T$ soit échange T et $-T$ (car la diagonale d'une face est envoyée sur la diagonale d'une autre face). Donc l'application

$$\begin{array}{ccc} Isom(T) \times \{Id, -Id\} & \longrightarrow & Isom(\Gamma) \\ (\sigma, \tau) & \longmapsto & \sigma.\tau \end{array}$$

est surjectif. Elle est injective car $Isom(T) \cap \{Id, -Id\} = \{Id\}$. Comme tous les éléments de $Isom(T)$ commutent avec tous les éléments de $\{Id, -Id\}$, on en déduit que c'est un morphisme de groupe. □

En particulier $Isom(\Gamma) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ et $\boxed{Isom(\Gamma) \text{ est d'ordre } 48}$.

Théorème (Groupe des isométries directes du cube)**.** Les applications suivantes sont des isomorphismes de groupes réciproques l'une de l'autre

$$F_1 : \begin{array}{ccc} Isom(T) & \longrightarrow & Isom^+(\Gamma) \\ \sigma & \longmapsto & \det(\sigma).\sigma \end{array}.$$

$$F_2 : \begin{array}{ccc} Isom^+(\Gamma) \subset Isom(T) \times \{Id, -Id\} & \longrightarrow & Isom(T) \\ \sigma.\tau & \longmapsto & \sigma \end{array}$$

Démonstration. La fonction F_1 est clairement un morphisme de groupe et la fonction F_2 est simplement la projection $Isom(T) \times \{Id, -Id\} Isom(T) \to Isom(T)$ restreinte à $Isom^+(\Gamma)$.

Si $\sigma \in Isom(T)$, alors $F_2 \circ F_1(\sigma) = F_1(\sigma.\det\sigma)$, et comme cette écriture est la décomposition sur $Isom(T) \times \{Id, -Id\}$, on en déduit que $F_2 \circ F_1(\sigma) = \sigma$. Si $\sigma.\tau \in Isom^+(\Gamma)$, alors comme $\det(\sigma.\tau) = 1$ on en déduit que $\tau = \det(\sigma)Id$. Il en découle que $F_2 \circ F_1(\sigma.\tau) = \sigma.\tau$. Donc F_1 et F_2 sont des bijections réciproques l'une de l'autre. □

En particulier $\boxed{Isom^+(\Gamma) \simeq \mathfrak{S}_4}$.

Remarque.
- Le groupe $Isom(\Gamma)$ est à la fois le produit direct $Isom(T) \times \{Id, -Id\}$ et le produit direct $Isom^+(\Gamma) \times \{Id, -Id\}$ (mais en tant de que sous-groupe de $SO_3(\mathbb{R})$, les groupes $Isom(T)$ et $Isom^+(\Gamma)$ sont différents).
- En tant qu'élément de $\mathfrak{S}(\Gamma)$ tout isométrie préservant le cube est de signature $+1$ [y réfléchir]. Donc $Isom(\Gamma)$ s'injecte dans $\mathfrak{A}(\Gamma)$ qui est de cardinal $8!/2 = 20160$.

La proposition suivante donne un isomorphisme canonique entre $Isom^+(\Gamma)$ et le groupe des permutations d'un ensebmle à 4 éléments.

Proposition. Si on note X l'ensemble des 4 diagonales du cube, alors l'application naturelle $Isom^+(\Gamma) \to \mathfrak{S}(X)$ est un isomorphisme de groupe.

Démonstration. Si $f \in Isom^+(\Gamma)$ agit par l'identité sur X, alors f a 4 vecteurs propres linéairements indépendant et non orthognaux. Donc $f = Id$. Donc l'application $Isom^+(\Gamma) \to \mathfrak{S}(X)$ est injective et par cardinalité elle est bijective. □

Isométries du dodécaèdre (et de l'icosaèdre)

Soit D un dodécaèdre.

Lemme.
- Il y a 5 cubes $\Gamma_1, \ldots, \Gamma_5$ inscrits dans le dodécaèdre.
- Le groupe $Isom^+(D)$ agit fidèlement sur l'ensemble $\{\Gamma_1, \ldots, \Gamma_5\}$.

Démonstration. .[A completer] [Faire un dessin]. □

Donc $Isom^+(D)$ s'injecte dans $\mathfrak{S}_5$.

Théorème (Groupe des isométries directes du dodécaèdre)**.** On a $Isom^+(D) \cong \mathfrak{A}(\{\Gamma_1, \ldots, \Gamma_5\}) \simeq \mathfrak{A}_5$.

Démonstration. On note $H = Isom(D) \cap Isom(\Gamma_1)$ le sous-groupe de $Isom(D)$ conservant Γ_1. On note aussi r une rotation d'ordre 5 d'axe le centre l'une des faces de D. Alors le groupe $\langle r \rangle = \{Id, r, r^2, r^3, r^4\}$ agit transitivement sur les cinq cubes.

Lemme. L'application suivante est une bijection :

$$\begin{array}{ccc} H \times \langle r \rangle & \longrightarrow & Isom(D) \\ (h, r^k) & \longmapsto & hr^k \end{array}$$

Démonstration du lemme. Cette application est injective car $H \cap \langle r \rangle = \{Id\}$, et elle est surjective car le groupe $\langle r \rangle$ agit transitivement sur les 5 cubes. □

Remarque. Ce **n'est ni** un produit semi-direct ni un produit direct.

Lemme. On a $Card(H) = 12$.

Démonstration du lemme. Le groupe H est un sous-groupe de $Isom^+(\Gamma_1) \simeq \mathfrak{S}_4$. Il contient les éléments d'ordre 3 (ce sont les rotations d'ordre 3 passant par un sommet de Γ_1), donc contient $\mathfrak{A}_4$. Comme il ne contient pas d'élements d'ordre 4 (faire un dessin), on a donc $H \simeq \mathfrak{A}_4$. □

Donc $Isom^+(D)$ est d'ordre $12 \times 5 = 60$ et s'injecte dans $\mathfrak{S}_5$, on en déduit que $Isom^+(D) \simeq \mathfrak{A}_5$. □

Remarque. Voir [Arn69].

3 $\mathfrak{S}_p$ est un groupe de Galois sur $\mathbb{Q}$

Leçons concernées
- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 104 - Groupes finis. Exemples et applications.
- 105 - Groupe des permutations d'un ensemble fini. Applications.
- 108 - Exemples de parties génératrices d'un groupe. Applications.
- 110 - Nombres premiers. Applications.
- 116 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Préliminaires

Sur le groupe $\mathfrak{S}_p$

Lemme. Soit p un nombre premier. Si H est un sous-groupe de $\mathfrak{S}_p$ qui contient une transposition et agit transitivement sur $[1,p]$, alors $H = \mathfrak{S}_p$

Démonstration du lemme. Comme H agit transitivement, alors $H/Stab_H(1)$ est de cardinal p. Donc $p|H$ et il existe un élément $\gamma \in H$ d'ordre p. Comme p est premier γ est un p-cycle. Comme de plus H contient une transposition, on en déduit que $H = \mathfrak{S}_p$ (on utiise encore le fait que p est premier). □

Groupe de Galois Soit $P(X) \in \mathbb{Q}[X]$ un polynôme irréductible, $X = \{x_1, \dots, x_n\}$ l'ensemble de ses racines et K son corps de décomposition. On note $Gal(K/Q)$ l'ensemble des automorphismes de K. Alors le groupe $Gal(K/Q)$ agit fidèlement sur X et donc s'injecte dans $\mathfrak{S}_n$.

Proposition. Le groupe $Gal(K/Q)$ agit transitivement sur X.

Démonstration. Soient $x, y \in X$. On peut définir l'application

$$\begin{array}{rccc} f: & \mathbb{Q}[x] & \longrightarrow & K \\ & P(x) & \longmapsto & P(y) \end{array}.$$

On a d'une part l'injection naturelle $i : \mathbb{Q}[x] \to K$ et d'autre part l'injection $f : \mathbb{Q}[x] \to K$. Donc par unicité du corps de décomposition il existe $\Phi \in Aut(K/\mathbb{Q}[x]) \subset Gal(K/\mathbb{Q})$ tel que $f = \Phi \circ i$, ce qui donne $\Phi(x) = y$. □

Théorème de Rouché

Théorème (Rouché)**.** ...

Théorème

Théorème. Pour p premier, il existe un polynôme de $\mathbb{Q}[X]$ dont le groupe de Galois est $\mathfrak{S}_p$.

Démonstration. Si on exhibe un polynôme $P(X) \in \mathbb{Q}[X]$ irréductible de degré p, tel que $P(X)$ a $p-2$ racines réelles distinctes et 2 racines complexes conjuguées, alors son groupe de Galois est $\mathfrak{S}_p$.

On note $Q(X) = (X^2+1)\prod_{i=1}^{p-2} X - i \in \mathbb{Z}[X]$ (qui a $p-2$ racines réels et 2 racines complexes conjuguées). Pour tout $k \in \mathbb{N}$, on pose $Q_k(X) = kp^2Q(X) + X^p + p$. Alors $\deg Q_k = p$, et $Q_k(X) = X^p \mod p$ et $p^2 \mod Q(0)$, donc par critère d'Eisenstein $Q_k(X)$ est irréductible sur $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$. On note $P_k(X) = \frac{Q_k(X)}{kp^2} = Q(X) + \frac{X^p+p}{kp^2}$.

Montrons que pour k convenable le polynôme $P_k(X)$ vérifie ce que l'on demande. La suite $(P_k(X))_{k\in\mathbb{N}}$ converge uniformément sur tout compact vers $Q(X)$. Comme $Q(X)$ est non constant, par théorème de Rouché il existe $r \in]0, 1/4[$ et $k \in \mathbb{N}$ tels que : pour toute racine w de $Q(X)$, le polynôme $P_k(X)$ a exactement une racine dans $D(w,r)$. Pour $w = 1, 2, \dots, p-2$, la racine de $P_k(X)$ dans $D(w,r)$ est réelle car son conjugué est aussi racine de $P_k(X)$. De même les deux racines dans $D(i,r)$ et $D(-i,r)$ sont conjugués l'une de l'autre. Donc le polynôme $P_k(X)$ répond à la question. □

Remarque. La preuve a été prise sur la liste de développements de Igor Kortchemski.

4 Liste de quelques sous-groupes finis

Leçons concernées
- 104 - Groupes finis. Exemples et applications.
- 110 - Nombres premiers. Applications.
- 149 - Groupes finis de petit cardinal.

A Préliminaires

Si G est un groupe et $n \in \mathbb{N}$, on note $G[n] = \{x \in G : x^n = 1\}$ ses points de n torsions.

Proposition. Si G est un groupe, alors on a une bijection naturelle

$$Hom(\mathbb{Z}/n\mathbb{Z}, G) \cong Hom(\mathbb{Z}/n\mathbb{Z}, G[n]) \cong G[n],$$

où $G[n]$ est l'ensemble des points de n torsions de G et $Hom(\mathbb{Z}/n\mathbb{Z}, G[n])$ est l'ensemble des morphismes de groupe $\mathbb{Z}/n\mathbb{Z} \to G[n]$ à valeur dans $G[n]$ (l'ensemble $G[n]$ n'est pas nécéssairement un groupe).

Proposition. Soient $n, m \in \mathbb{N}^*$.
- On a un isomorphisme canonique de groupe : $Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
- Le groupe $(\mathbb{Z}/n\mathbb{Z})[m]$ est cyclique d'ordre $pgcd(n, m)$, c'est-à-dire : $(\mathbb{Z}/n\mathbb{Z})[m] \simeq \mathbb{Z}/pgcd(n, m)\mathbb{Z}$.

Proposition. Soient Get H deux groupes. Soient $\phi, \psi \in Hom(G, Aut(H))$ et $\alpha \in Aut(G)$ tels que $\phi = \psi \circ \alpha$. Alors l'application suivante est un isomorphisme de groupe

$$\begin{array}{ccc} H \rtimes_\psi G & \longrightarrow & H \rtimes_\phi G \\ (x, y) & \longmapsto & (x, \alpha(y)) \end{array}.$$

B Groupes d'ordre pq

Soient p, q deux nombres premiers et G un groupe d'ordre pq.

• Si $p = q$, alors comme $Z(G)$ est non trivial et que $G/Z(G)$ est cyclique, on en déduit que G est abélien. Donc

$$G \cong \mathbb{Z}/p^2\mathbb{Z} \text{ ou } G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

• Si $p < q$, alors le nombre de q-Sylow divise p et est congru à $1 \mod q$. Donc il n'y qu'un seul q-Sylow noté Q et il est distingué. Si P est un p-Sylow, alors $Q \cap P = \{1\}$ (car $Q \simeq \mathbb{Z}/q\mathbb{Z}$ et $P \simeq \mathbb{Z}/p\mathbb{Z}$). Donc :

$$G = Q \rtimes P \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}.$$

On cherche alors l'ensemble des morphismes $Hom(\mathbb{Z}/p\mathbb{Z}, Aut(\mathbb{Z}/q\mathbb{Z})) = Hom(\mathbb{Z}/p\mathbb{Z}, Aut(\mathbb{Z}/q\mathbb{Z})[p]) \simeq \mathbb{Z}/pgcd(p, q-1)\mathbb{Z}$.

1. Si p ne divise pas $q-1$, alors il n'y a que le morphisme constant. Donc $\boxed{G \cong \mathbb{Z}/pq\mathbb{Z}}$.
2. Si p divise pas $q-1$. Alors $Aut(\mathbb{Z}/q\mathbb{Z})[p] \simeq \mathbb{Z}/p\mathbb{Z}$. Comme un morphisme de groupe non constant de $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ est bijective, on en déduit que si $\phi, \psi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z})[p]$ sont deux morphismes non constants, alors il existe $f \in Aut(\mathbb{Z}/p\mathbb{Z})$ tel que tel que $\phi \circ f = \psi$ (à savoir $f = \phi^{-1} \circ \psi$), donc les produits semi-directs $\mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$ sont isomorphes. Donc $\boxed{\text{il n'y qu'un seul produit semi-direct}}$ non direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Remarque. Si $p = 2$, alors $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est le groupe dihédrale d'ordre $2q$.

Groupes d'ordre 8

Théorème. Un groupe d'ordre 8 non-abélien est isomorphe soit à D_8 soit à $\mathbb{H}_8$.

Démonstration. .[A completer] □

Groupes d'ordre 12

Théorème. Il y a cinq groupes d'ordre 12, dont 2 sont abéliens, qui sont les suivants :

$$\begin{array}{lllll} \text{Les abéliens :} & \mathbb{Z}/12\mathbb{Z}, & \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}. & & \\ \text{Les non-abéliens :} & \mathbb{Z}/3\mathbb{Z}\rtimes\mathbb{Z}/4Z, & \mathbb{Z}/3\mathbb{Z}\rtimes V_4, & V_4\rtimes\mathbb{Z}/3\mathbb{Z}, & \end{array}$$

où $V_4 := \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Démonstration. On se donne G un groupe d'ordre 12. Par théorème de Sylow, le nombre de 3-sylow est 1 ou 4 (et le nombre de 2-sylow n_2 vaut 1 ou 3, mais on ne s'en servira pas).

• **Cas 1 :** si $n_3 = 1$. Alors l'unique 3-sylow, noté $S_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est distingué et si S_2 est un 2-sylow, alors $S_3 \cap S_2 = \{1\}$ (regarder la torsion), donc $G = S_3 \rtimes S_2$.

Cas 1.1 : si $S_2 \simeq \mathbb{Z}/4\mathbb{Z}$, alors $Hom(\mathbb{Z}/4\mathbb{Z}, Aut(\mathbb{Z}/3\mathbb{Z})) \simeq \mathbb{Z}/2\mathbb{Z}$, donc soit $\boxed{G \simeq \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}}$ soit G est isomorphe à $\boxed{\text{l'unique produit semi-direct } \mathbb{Z}/3\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z}}$.

Cas 1.2 : si $S_2 \simeq V_4$. Les lemmes suivants permettent de déterminer $Hom(V_4, Aut(\mathbb{Z}/3\mathbb{Z})) \simeq Hom(V_4, \mathbb{Z}/2\mathbb{Z})$.

Lemme. On a : $Aut(V_4) = Bij(V_4 \setminus \{0\}) \simeq \mathfrak{S}_3$.

Démonstration du lemme. Soit $\sigma \in Bij(V_4 \setminus \{0\})$. On remarque que si (a, b, c) désignent les trois éléments de $V_4 \setminus \{0\}$, alors $a + b = c$. Donc pour $x, y \in V_4$, si $x = y$, alors $\sigma(x) + \sigma(y) = 0 = \sigma(x + y)$, et sinon $(\sigma(x), \sigma(y), \sigma(x + y))$ sont distincts et d'après la remarque on a $\sigma(x) + \sigma(y) = \sigma(x + y)$. Donc σ est un morphisme de groupe. □

Lemme. Soient $f, g \in Hom(V_4, \mathbb{Z}/2\mathbb{Z})$ non constants. Alors il existe $\alpha \in Aut(V_4)$ tel que $f = g \circ \alpha$.

Démonstration du lemme. Comme f est non constant il existe $a \in V_4 \setminus \{0\}$ tel que $f(a) = 1$. Si on note b, c les deux autres éléments non nuls, alors $f(b) + f(c) = f(a) = 1$. Quitte à inverser b et c, on peut supposer que $f(b) = 1$ et $f(c) = 0$.

De même avec g que l'on peut écrire $g(a') = g(b') = 1$ et $g(c') = 0$. On en déduit alors un morphisme α qui convient. □

On en déduit qu'à isomorphisme $\boxed{\text{il n'y a qu'un seul produit semi-direct non direct } \mathbb{Z}/3\mathbb{Z}\rtimes V_4}$ et il y a le produit direct $\boxed{\mathbb{Z}/3\mathbb{Z}\times V_4 \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}}$.

• **Cas 2 :** si $n_3 = 4$. Comme les éléments non nul de $\mathbb{Z}/3\mathbb{Z}$ engendre $\mathbb{Z}/3\mathbb{Z}$, on en déduit que l'intersection de deux 3-sylow distincts est trivial. L'union des 3-sylow contient alors $1 + 2 \times 4 = 9$ éléments. On en déduit qu'il n'y a qu'un seul 2-sylow (qui est de cardinal 4), et par même argument que ci-dessus, on a $G = S_2 \rtimes S_3$.

Cas 2.1 : si $S_2 \simeq \mathbb{Z}/4\mathbb{Z}$, alors $Hom(\mathbb{Z}/3\mathbb{Z}, Aut(\mathbb{Z}/4\mathbb{Z})) \simeq \{1\}$, donc le produit est direct.

Cas 2.2 : si $S_2 \simeq V_4$, alors $Hom(\mathbb{Z}/3\mathbb{Z}, Aut(V_4)) \simeq \mathfrak{S}_3[3] \simeq \mathbb{Z}/3\mathbb{Z}$.

Lemme. Soient $f, g \in Hom(\mathbb{Z}/3\mathbb{Z}, Aut(V_4)[3])$ non constants. Alors il existe $\alpha \in Aut(\mathbb{Z}/3\mathbb{Z})$ tel que $f = g \circ \alpha$.

Démonstration du lemme. On raisonne comme dans le lemme précédent en remarquant que f et g sont bijectives. □

Donc $\boxed{\text{il n'y a qu'un seul produit semi-direct non direct } V_4 \rtimes \mathbb{Z}/3\mathbb{Z}}$ (et il y a le produit directe déjà compté). □

Remarque. On a
- $V_4 \rtimes \mathbb{Z}/3\mathbb{Z} = \mathfrak{A}_4$.
- $\mathbb{Z}/3\mathbb{Z} \rtimes V_4 = D_{12}$.
- $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z} =$?????.

Remarque.
- On a ainsi la liste de tous les groupes d'ordre ≤ 15.
- Pour les groupe d'ordres 16, voir :
  http ://math.sun.ac.za/ mwild/Marcel Wild - Home Page_files/Groups16AMM.pdf
- Voir aussi :
  http ://en.wikipedia.org/wiki/List_of_small_groups

Remarque. Voir [[Com98] : Chapitre I, Section 5.2 et 5.3], [[Gou94b] : Chapitre 1, Probleme 9], [[Per96] : Th ?].

5 Loi de réciprocité quadratique

Leçons concernées
- 105 - Groupe des permutations d'un ensemble fini. Applications.
- 109 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 110 - Nombres premiers. Applications.
- 112 - Corps finis. Applications.
- 146 - Résultant de deux polynômes, applications à l'intersection de courbes ou de surfaces algébriques.

Préliminaire

Lemme (Frobénius-Zolotarev en dimension 1)**.** Pour $x \in \mathbb{Z}/p\mathbb{Z}^\times$, si on note $m_x : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la multiplication par a, alors

$$\varepsilon(m_x) = \left(\frac{x}{p}\right).$$

Démonstration du lemme. L'application $\mathbb{Z}/p\mathbb{Z}^\times \to \mathbb{Z}/2\mathbb{Z}, x \mapsto \varepsilon(m_x)$ est un morphisme de groupe. Si x_0 est un générateur de $\mathbb{Z}/p\mathbb{Z}^\times$, alors m_x est un cycle de longueur $p-1$, donc est de signature -1. Donc $\mathbb{Z}/p\mathbb{Z}^\times \to \{-1,1\}$ est un morphisme surjectif, et on en déduit que c'est le symbole de Legendre. □

Théorème

Théorème (Loi de réciprocité quadratique)**.** Soient p, q deux nombres premiers ≥ 3. Alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Démonstration. On considère l'application

$$\begin{array}{rccc} \lambda : & [0, pq-1] & \longrightarrow & [0, pq-1] \\ & n = aq + b & \longmapsto & bp + a \end{array}.$$

où $a \in [0, p-1]$ et $b \in [0, q-1]$. Alors λ est bijective (sa bijection réciproque est évidente).

Lemme. La signature de λ est $(-1)^{(p-1)(q-1)/4}$.

Démonstation du lemme. Pour $n = aq + b$ et $n' = a'q + b'$, on remarque que

$$n < n' \iff (a < a') \text{ ou } (a = a' \text{ et } b < b') \text{ (c'est ordre lexicographique)},$$

en effet : $n - n' = (a - a')q + (b - b')$, avec $b - b' \in [-(q-1), q+1]$, donc $n - n'$ est du signe de $(a - a')$ si $a \neq a'$.

Supposons que $n < n'$. Si $a = a'$, alors $b < b'$ et $\lambda(n) = bp + a < b'p + a' = \lambda(n')$. Si $a < a'$, alors

$$\lambda(n') < \lambda(n) \iff (b' < b) \text{ ou } (b' = beta < a') \iff (b' < b).$$

Donc un couple (n, n') avec $n < n'$ est inversé si et seulement si ($a < a'$ et $b > b'$), et il en y en a $\binom{p}{2}\binom{q}{2} = \frac{p(p-1)}{2}.\frac{q(q-1)}{2}$. D'où la formule (utiliser le fait que p, q sont impaires). □

Par lemme chinois l'application suivante est une bijection

$$\begin{array}{rccc} & [0, pq-1] & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ & n & \longmapsto & (n \mod p, n \mod q) \end{array}.$$

On note $\lambda_* : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ le pushforward de l'application λ. L'application λ^* est de signature $(-1)^{(p-1)(q-1)/4}$

$$\begin{array}{ccc} \frac{[0,pq-1]}{aq+b} & \xrightarrow{\lambda} & \frac{[0,pq-1]}{bp+a} \\ \simeq\downarrow & & \simeq\downarrow \\ \frac{\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}}{(aq+b,b)} & \xrightarrow[\lambda_*]{} & \frac{\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}}{(a,bp+a)} \end{array}.$$

On note, avec les convention $a \in [0, p-1]$ et $b \in [0, q-1]$

$$\begin{array}{rccc} f: & \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z} \\ & (a,b) & \longmapsto & (aq+b,b) \end{array},$$

$$\begin{array}{rccc} g: & \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z} \\ & (a,b) & \longmapsto & (a,bp+a) \end{array}.$$

Comme le diagramme suivant commute

$$\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z} & \xrightarrow{\quad\lambda_*\quad} & \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}\ . \\ & {\scriptstyle f}\nwarrow \quad \nearrow{\scriptstyle g} & \\ & \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z} & \end{array}$$

Lemme. On a $\varepsilon(f)=\left(\frac{q}{p}\right)$ et $\varepsilon(g)=\left(\frac{p}{q}\right)$.

Démonstration. Soit $b_0\in[0,q-1]$. L'application $m_q:\mathbb{Z}/p\mathbb{Z}\times\{b_0\}\to\mathbb{Z}/p\mathbb{Z}\times\{b_0\}$ est de signature $\left(\frac{q}{p}\right)$ d'après le théorème de Frobénius-Zolotarev. La translation par 1 de $\mathbb{Z}/p\mathbb{Z}\times\{b_0\}\to\mathbb{Z}/p\mathbb{Z}\times\{b_0\}$ est un cycle de longueur p donc est de signature $+1$. Donc la translation par b est de signature $+1$, on en déduit que $f_{|\mathbb{Z}/p\mathbb{Z}\times\{b_0\}}$ est de signature $\left(\frac{q}{p}\right)$, puis que f est de signature $\left(\frac{q}{p}\right)^q=\left(\frac{q}{p}\right)$. De même g est de signature $\left(\frac{p}{q}\right)$. □

On conclut avec le fait que $\varepsilon(f)\varepsilon(g)=\varepsilon(\lambda_*)$.

□

Loi de réciprocité pour 2

Théorème. On a pour p premier impair

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}.$$

Démonstration. On note $a\in\overline{\mathbb{F}}_p$ une racine 8^{em} de 1, et $t=a+a^{-1}$.

On a $t^2=2$, car $t^2=a^2+a^{-2}+2=2$ (car $a^4=-1$). Ce qui donne $t^{p-1}=\left(\frac{2}{p}\right)$. Puis

$$\left(\frac{2}{p}\right)t=t^p.$$

Si $p=\pm1 \mod 8$, alors $t^p=a^p+a^{-p}=t$, et si $p=\pm3 \mod 8$, alors $t^p=a^p+a^{-p}=a^4t=-t$. On en déduit que

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}=\begin{cases}1 & ,\text{si } p=\pm1 \mod 8\\ -1 & ,\text{si } p=\pm3 \mod 8\end{cases}.$$

□

Applications

Tests de primalités des nombres de Fermat

Proposition. Si $F_k=2^{2^k}+1$ (avec $k\geq1$), alors F_k est premier si et seulement si

$$3^{(F_k-1)/2}=-1 \mod F_k.$$

(Cette condition implique que F_k est pseudo-premier en base 3).

Démonstration. Si F_k est premier, alors par loi de réciprocité, on a

$$\left(\frac{3}{F_k}\right)\left(\frac{F_k}{3}\right)=(-1)^{(3-1)(F_k-1)/4}=+1.$$

Comme $\left(\frac{F_k}{3}\right)=F_k \mod 3=-1$, on en déduit que $3^{(F_k-1)/2}=-1 \mod F_k$.

Réciproquement si $3^{(F_k-1)/2}=-1 \mod F_k$. Soit q un diviseur premier de F_k, alors $3^{(F_k-1)/2}=-1 \mod q$. Si d est l'ordre de 3 dans $\mathbb{Z}/q\mathbb{Z}^\times$, alors $d|F_k-1$, mais comme F_k-1 est une puissance de 2, on en déduit que $d=F_k-1$. Donc $\mathbb{Z}/q\mathbb{Z}^\times$ est d'ordre au moins F_k-1 et on en déduit que $q=F_k$. □

Cas particuliers du théorème de Dirichlet

Proposition. Il existe une infinité de nombres premiers congrues à $1 \mod 4$.

Démonstration. Par loi de réciprocité quadratique pour p impaire, $p = 1 \mod 4$ si et seulement si $-1 \mod p$ est un carré.

Supposons qu'il n'y a qu'un nombre fini de nombres premiers $p_1, \dots, p_n$ congrue à $1 \mod 4$. On note $N = (2.p_1 \dots p_n)^2 + 1$. Soit q un diviseur impaire de N. Alors $(p_1 \dots p_n)^2 = -1 \mod q$. On en déduit que $-1 \mod q$ est un carré ce qui est absurde car q n'est pas l'un des p_i. □

Proposition. Il existe une infinité de nombres premiers congrues à $1 \mod 6$.

Démonstration. On remarque que pour p impaire, $p = 1 \mod 6$ si et seulement si $-3 \mod p$ est un carré. En effet $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)(-1)^{(3-1)(p-1)/4}\left(\frac{p}{3}\right) = p \mod 3$. Donc

$$-3 \mod p \text{ est un carré} \iff p = 1 \mod 3 \iff p = 1 \mod 6.$$

La dernière équivalence vient du fait que p est impaire.

Supposons qu'il n'y a qu'un nombre fini de nombres premiers $p_1, \dots, p_n$ congrue à $1 \mod 6$. On note $N = 3.(2.p_1 \dots p_n)^2 + 1$. Soit q un diviseur impaire de N. Alors $3.(2.p_1 \dots p_n)^2 = -1 \mod q$. En multipliant par 3 cette dernière égalité, on en déduit que $-3 \mod q$ est un carré, ce qui est absurde. □

Proposition. Il existe une infinité de nombres premiers congrues à $-1 \mod 10$.

Démonstration. On remarque que pour p impaire, $p = \pm 1 \mod 10$ si et seulement si $5 \mod p$ est un carré. En effet $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = p^2 \mod 5$. Donc

$$5 \mod p \text{ est un carré} \iff p = \pm 1 \mod 5 \iff p = \pm 1 \mod 10.$$

La dernière équivalence vient du fait que p est impaire.

Supposons qu'il n'y a qu'un nombre fini de nombres premiers $p_1, \dots, p_n$ congrue à $-1 \mod 10$. On note $N = 5.(2.p_1 \dots p_n)^2 + 1$. Soit q un diviseur impaire de N. Alors $5.(2.p_1 \dots p_n)^2 = 1 \mod q$. On en déduit que $5 \mod q$ est un carré, donc $q = \mp 1 \mod 10$. Ceci entraine que tout diviseur de N (forcément impaire) est congrue à $+1 \mod 10$, ce qui donne $N = +1 \mod 10$. C'est absurde car la forme de N donne $N = -1 \mod 10$. □

Deuxième preuve du théorème

Préliminaires

Le localisé de $\mathbb{Z}[X]$ par rapport à X est l'anneau

$$\mathbb{Z}[X, X^{-1}] = \left\{ \tfrac{F(X)}{X^k} : F(X) \in \mathbb{Z}[X], k \in \mathbb{N} \right\}.$$

Cet anneau vérifie la propriété fonctorielle suivante

Proposition. Si $\mathbb{A}$ est une $\mathbb{Z}$-algèbre (i.e. un anneau) et si $f : \mathbb{Z}[X] \to \mathbb{A}$ est un morphisme de $\mathbb{Z}$-algèbre tel que $f(X) \in \mathbb{A}^\times$, alors f se prolonge de façon unique en un morphisme de $\mathbb{Z}$-algèbre $\mathbb{Z}[X, X^{-1}] \to \mathbb{A}$.

Démonstration. Explicitement c'est l'application qui à $F(X) = P(X)/X^k \in \mathbb{Z}[X, X^{-1}]$ associe $f(P(X))/f(X)^k$, et on vérfie qu'elle est l'unique solution du problème. □

Dans la preuve on aura seulement besoin de savoir que l'on peut définir les morphismes suivants

$$. \mod p : \begin{array}{ccc} \mathbb{Z}[X, X^{-1}] & \longrightarrow & \mathbb{F}_p(X) \\ F(X) & \longmapsto & F(X) \mod p \end{array},$$

$$ev_a : \begin{array}{ccc} \mathbb{Z}[X, X^{-1}] & \longrightarrow & \mathbb{Q} \\ F(X) & \longmapsto & F(a) \end{array}, \text{ pour } a \in \mathbb{Z}^*,$$

$$ev_{X^{-1}} : \begin{array}{ccc} \mathbb{Z}[X, X^{-1}] & \longrightarrow & \mathbb{Z}[X, X^{-1}] \\ F(X) & \longmapsto & F(X^{-1}) \end{array},$$

$$ev_{X+X^{-1}} : \begin{array}{ccc} \mathbb{Z}[X, X^{-1}] & \longrightarrow & \mathbb{Z}[X, X^{-1}] \\ F(X) & \longmapsto & F(X + X^{-1}) \end{array},$$

Proposition. Pour $\mathbb{A}$ un anneau l'application suivante est une bijection

$$\begin{array}{rccc} ev_{X+X^{-1}}: & \mathbb{A}[X] & \longrightarrow & \{Q(X)\in\mathbb{A}[X,X^{-1}] : Q(X)=Q(X^{-1})\} \\ & P(X) & \longmapsto & P(X+X^{-1}) \end{array},$$

Démonstration. Cf polynômes réciproques. □

Preuve théorème

On note $P(X)=\prod_{k=1}^{(p-1)/2}(X-\cos(2\pi d/n))$.

Lemme. On a $P(X+X^{-1})=\frac{\Phi_p(X)}{X^{(p-1)/2}}$.

Démonstration. On a successivement

$$\begin{array}{rcl} P(X+X^{-1}) & = & \prod_{d=1}^{(p-1)/2} X+X^{-1}-\cos(2i\pi d/n) \\ & = & \frac{1}{X^{(p-1)/2}}\prod_{d=1}^{(p-1)/2}\Big(X^2-\cos(2\pi d/n)X+1\Big) \\ & = & \frac{1}{X^{(p-1)/2}}\prod_{d=1}^{(p-1)/2}(X-e^{2i\pi k/p}).(X-e^{-2i\pi k/p}) \\ & = & \frac{\Phi_p(X)}{X^{(p-1)/2}}. \end{array}$$

□

La proposition [?] montre que $P(X)\in\mathbb{Z}[X]$.

Lemme. On a $P(X) \mod p = (X-2)^{(p-1)/2} \mod p$.

Démonstration. On a

$$\begin{array}{rcl} \frac{\Phi_p(X)}{X^{(p-1)/2}} \mod p & = & (X-1)^{p-1}\frac{1}{X^{(p-1)/2}} \mod p = \Big(\frac{(X-1)^2}{X}\Big)^{(p-1)/2} \mod p \\ & = & (X+X^{-1}-2)^{(p-1)/2} \mod p. \end{array}$$

Donc $P(X+X^{-1}) \mod p = (X+X^{-1}-2)^{(p-1)/2} \mod p$, et on en déduit que $P(X) \mod p = (X-2)^{(p-1)/2} \mod p$ (Cf lemme) (remarquer qu'on utilise le fait que $\Big(ev_{X+X^{-1}}(P(X)\Big) \mod p = ev_{X+X^{-1}}\Big(P(X) \mod p\Big)$). □

On note $Q(X)=\prod_{l=1}^{(q-1)/2} X-\cos(2\pi l/q)$. On a alors

$$\begin{array}{rcl} Res(P(X),Q(X)) \mod q & = & Res(P(X) \mod q, Q(X) \mod q) \\ & = & Res(P(X) \mod q, (X-2)^{(q-1)/2} \mod q)\ . \\ & = & P(2)^{(q-1)/2} \mod q \end{array}$$

Or, on a

$$\begin{array}{rcl} P(2) & = & ev_1(P(X+X^{-1}).X^{(p-1)/2}) = ev_1(\Phi_p(X)) \\ & = & p. \end{array}$$

D'où

$$\boxed{Res(P(X),Q(X)) \mod q = p^{(q-1)/2} \mod q = \Big(\frac{p}{q}\Big)}.$$

De même on a

$$\boxed{Res(Q(X),P(X)) \mod p = q^{(p-1)/2} \mod p = \Big(\frac{q}{p}\Big)}.$$

Le lemme suivant montre qu'on a en fait $Res(P(X),Q(X))=\Big(\frac{p}{q}\Big)$ et $Res(Q(X),P(X))=\Big(\frac{q}{p}\Big)$ (Il n'y a plus $\mod p$ et $\mod q$).

Lemme. On a $Res(P(X),Q(X)), Res(Q(X),P(X))\in\{-1,1\}$.

Démonstration. On a

$$Res(P,Q)=\prod_{l=1}^{(q-1)/2} P(\cos(2\pi l/q))=\prod_{l=1}^{(q-1)/2} P(e^{2i\pi l/q}+e^{-2i\pi l/q}).$$

puis

$$Res(P,Q)^2 = \prod_{l=1}^{q-1} P(e^{2i\pi l/q} + e^{-2i\pi l/q}) = \prod_{\zeta \in U_q \setminus \{1\}} \frac{\Phi_p(\zeta)}{\zeta^{(p-1)/2}}.$$

Or on a

$$\prod_{\zeta \in U_q \setminus \{1\}} \zeta = 1.$$

et

$$\prod_{\zeta \in U_q \setminus \{1\}} \Phi_p(\zeta) = \prod_{\zeta \in U_q \setminus \{1\}} \frac{\zeta^p - 1}{\zeta - 1} = 1,$$

car l'application suivante est bijective (car $p \neq q$)

$$\begin{array}{ccc} U_p \setminus \{1\} & \longrightarrow & U_q \setminus \{1\} \\ \zeta & \longmapsto & \zeta^p \end{array}.$$

Donc $Res(P,Q)^2 = 1$, et de même $Res(Q,P)^2 = 1$. □

On en déduit que $Res(P(X), Q(X)) \mod p = \left(\frac{q}{p}\right)$ et $Res(Q(X), P(X)) = \left(\frac{p}{q}\right)$. Le théorème s'en déduit de la formule d'échange dans le résultant (on rappelle que $\deg P = \frac{p-1}{2}$ et $\deg Q = \frac{q-1}{2}$).

Remarque.
- Cette preuve a été proposé par Samuel Le Fourn et Thibaud Regnier.
- Voir [[RBB06], Chap 6.6.3], [[Gou94a], Chapitre 1, Sujet d'etude 2 ?], [[AJ06], Th ?].

6 Quelques théorèmes sur les coniques

Leçons concernées

- 118 - Exemples d'utilisation de la notion de dimension en algèbre et en géométrie.
- 123 - Déterminant. Exemples et applications.
- 136 - Coniques. Applications.
- 137 - Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.
- 146 ? ? ?.
- 148 - Formes quadratiques réelles. Exemples et applications.

Théorème de Pascal

Théorème (Pascal)**.** Soient A, B, C, A', B', C', 6 points du plan projectif tels que 3 quelconques d'entre eux ne sont jamais alignés. On note $P = (BC') \cap (B'C)$, $Q = (CA') \cap (C'A)$, $R = (AB') \cap (A'B)$. Alors les 6 points (A, B, C, A', B', C') sont sur une conique si et seulement si les 3 points (P, Q, R) sont alignés.

Démonstration. • On se place dans l'espace projectif $P^(\mathbb{R})$ et quitte à appliquer une homographie, on peut supposer que $A = [1 : 0 : 0]$, $B = [0 : 1 : 0]$ et $C = [0 : 0 : 1]$ (on rappelle que ces trois points ne sont pas alignés). On note les coordonnées des points : $A = [a : a' : a'']$, $B = [b : b' : b'']$ $C = [c : c' : c'']$.

• On calcule le point P de la façon suivante : la droite (BC') a pour équation barycentrique (ou projective)

$$\det \begin{pmatrix} x & b & 0 \\ y & b' & 0 \\ z & b'' & 1 \end{pmatrix} = b'x - by = 0.$$

De même la droite $(B'C)$ a pour équation

$$\det \begin{pmatrix} x & 0 & c \\ y & 1 & c' \\ z & 0 & c'' \end{pmatrix} = c''x - cz = 0.$$

Leur point d'intersection a alors pour coordonnées :

$$(b', -b, 0) \wedge (c'', 0, -c) = (bc, b'c, bc'').$$

On fait de même pour Q et R, et on trouve :

$$P = (bc, b'c, bc''),\ Q = (c'a, c'a', c''a'),\ R = (ab'', a''b, a''b'').$$

• Les points (P, Q, R) son alignés si et seulement si

$$d := \det \begin{pmatrix} bc & b'c & bc'' \\ c'a & c'a' & c''a' \\ ab'' & a''b & a''b'' \end{pmatrix} = 0.$$

• Une conique qui passe par A', B', C' a pour équation barycentrique : $Q : \alpha yz + \beta zx + \gamma xy = 0$ [y réfléchir]. La conique Q passe par les points (A, B, C) si et seulement si

$$d' = \det \begin{array}{rcl} \alpha a'a'' + \beta a''a + \gamma aa' & = & 0 \\ \alpha b'b'' + \beta b''b + \gamma bb' & = & 0 \\ \alpha b'b'' + \beta b''b + \gamma bb' & = & 0 \end{array} = 0.$$

Donc les points A, B, C, A', B', C' sont sur une même conique si et seulement si

$$\det \begin{pmatrix} a'a'' & a''a & aa' \\ b'b'' & b''b & bb' \\ c'c'' & c''c & cc' \end{pmatrix} = 0.$$

Comme les six points ne sont pas alignés trois à trois, les coefficients de A, B et de C sont tous non nuls. En factorisant la première ligne de d par bc, la deuxème ligne par $c'a'$ et la troisième ligne par $a''b''$, on en déduit que

$$d = s \det \begin{pmatrix} 1 & b'/b & c''/c \\ a/a' & 1 & c''/c' \\ a/a'' & a''/b'' & 1 \end{pmatrix} = 0.$$

avec $s = bcc'a'a''b''$. En distributant sur chaque colonne on retrouve d. Donc $d = 0$ si et seulement si $d' = 0$.

La conique est unique car d' est de rang au moins 2 : en effet comme A, B, C' ne sont pas aligné on a

$$\det \begin{pmatrix} a' & a \\ b' & b \end{pmatrix} = \begin{pmatrix} a' & a & 0 \\ b' & b & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq 0.$$

Elle est non dégénérée car sinon ce serait l'union de deux droites ce qui implique qu'au moins trois points seraient alignés [y réfléchir]. □

Remarque. Son théorème dual est le suivant.

Théorème (Brianchon)**.** Soient a, b, c, a', b', c', 6 droites du plan (affine ou projectif) tels que 3 quelconques d'entre eux ne sont jamais concourantes (ou parallèles). On note $d_a = (b \cap c, b' \cap c')$, $d_b = (c \cap a, c' \cap a')$, $d_c = (a \cap b, a' \cap b')$. Alors ces 6 droites (a, b, c, a', b', c') sont tangentes à une conique si et seulement si les 3 droites (d_a, d_B, d_c) sont alignés.

Remarque. Voir [Tisseron, Th ?], [Ladegaillerie Th ?].

Théorème de Poncelet

Théorème (Poncelet)**.** On considère C une conique à centre de foyers F_1 et F_2. Soit M un point et T, T' les points de contact des tangentes issus de M. Alors

- $\widehat{TMT'}$ et $\widehat{TMT'}$ ont même bissectrice.
- F_1M est la bissectrice de $\widehat{TF_1T'}$ (de même pour F_2M).

[Dessin]

Démonstration. .[A completer] □

7 Action du groupe modulaire

Leçons concernées

- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 108 - Exemples de parties génératrices d'un groupe. Applications.
- 138 - Homographies de la droite projective complexe. Applications.
- 139 - Applications des nombres complexes à la géométrie.
- 141 - Utilistion des groupes en géométrie.

Préliminaires

Le demi-plan de Poincaré est

$$\mathcal{H} = \Big\{ z \in \mathbb{C} \mid \operatorname{Im} z > 0 \Big\}$$

. Le *groupe modulaire* $SL_2(\mathbb{Z})$ agit sur $\mathcal{H}$ par homographie : pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ et $z \in \mathcal{H}$, l'action de γ sur z est

$$\gamma.z = \tfrac{az+b}{cz+d}.$$

Un calcul montre que

$$\operatorname{Im} \gamma.z = \tfrac{\operatorname{Im} z}{|cz+d|^2}.$$

On note $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Les actions de ces matrices sur z sont alors

$$S.z = \tfrac{-1}{z} \text{ et } T.z = z + 1.$$

Générateurs du groupe modulaire

Proposition. Le groupe modulaire est engendré par S, T.

Démonstration. Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. On montre par récurrence sur $|c|$ que γ est dans le sous-groupe engendré par S et T. Si $c = 0$ alors soit $a = d = 1$ auquel cas

$$\gamma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = T^b,$$

soit $a = d = -1$, auquel cas

$$\gamma = \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} = S^2 T^{-b}.$$

Si $|c| \geq 1$, alors comme :

$$\gamma T^n = \begin{pmatrix} * & * \\ c & nc + d \end{pmatrix},$$

avec n tel que $|nc + d| \leq |c|/2$, on a :

$$\gamma T^n S = \begin{pmatrix} * & * \\ nc + d & -c \end{pmatrix},$$

avec $|nc + d| < |c|$, ce qui permet de conclure par hypothèse de récurrence. □

Domaine fondamental

Proposition. Un domaine fondamental est donné par

$$D = \{z \in \mathcal{H} \mid Re(z) \in [-1/2, 1/2], |z| \geq 1\}.$$

Démonstration. Soit $z \in \mathcal{H}$. On rapelle que $\operatorname{Im} \gamma.z = \frac{\operatorname{Im} z}{|cz+d|^2}$. On en déduit que l'ensemble suivant est fini

$$\Big\{ \operatorname{Im} \gamma.z \mid \gamma \in SL_2(\mathbb{Z}), \operatorname{Im} \gamma.z \geq \operatorname{Im} z \Big\}.$$

On prend alors $\gamma \in SL_2(\mathbb{Z})$ tel que $\operatorname{Im} \gamma.z$ est maximale. On choisit $n \in \mathbb{Z}$ tel que $\operatorname{Re}(T^n.\gamma.z) \in [-1/2, 1/2]$ et on pose $z_1 = T^n.\gamma.z$. Comme $\operatorname{Im} S.z_1 = \frac{\operatorname{Im} z_1}{|z|^2} \leq \operatorname{Im} z_1$, on a $|z_1| \geq 1$. Ce qui montre que $z_1 \in D$ et que toute orbite rencontre D.

Soient $z, z' \in D$ ayant même orbite et $\gamma \in SL_2(\mathbb{Z})$ tel que $z' = \gamma.z$. On peut supposer pqr exemple que $\operatorname{Im} z \leq \operatorname{Im} z'$. On a alors $|cz + d|^2 \leq 1$. Or

$$|cz + d|^2 = c^2|z|^2 + 2\operatorname{Re}(z)cd + d^2.$$

En minorant $2\operatorname{Re}(z).cd \geq -|c|\ |d|$ et $c^2|z|^2 \geq c^2$, on en déduit que

$$|cz + d|^2 \geq c^2 - |c|\ |d| + d^2 = (|c| - |d|)^2 + |c|\ |d|.$$

Donc :

$$(|c| - |d|)^2 + |c|\ |d| \leq 1.$$

Comme $(|c| - |d|)^2 + |c|\ |d|$ un entier non nul, on en déduit les égalités suivantes

$$\begin{cases} (|c| - |d|)^2 + |c|\ |d| = 1 \\ 2\operatorname{Re}(z).cd = -|c|\ |d| \\ c^2|z|^2 = c^2 \end{cases}.$$

- Si $|z| > 1$, alors $c = 0$, donc $\gamma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, puis $z' = z$ ou $\pm z$ si $|\operatorname{Re} z| = 1/2$.
- Si $|z| = 1$ et $|\operatorname{Re}(z)| < 1/2$. Alors $c = 0$ ou $d = 0$ et on en déduit que $z' = z$ ou $-1/z$ [y réfléchir].
- Si $|z| = 1$ et $|\operatorname{Re}(z)| = 1/2$, alors $z = j$ ou $-j^2$ et comme $\operatorname{Im} z' = \operatorname{Im} z$ on a donc $z' = j$ ou $-j^2$.

□

Réseaux de $\mathbb{C}$

Définition. Un *réseau* de $\mathbb{C}$ ou *tore complexe* est un sous-groupe du type $\Lambda = \mathbb{Z}u \oplus \mathbb{Z}v$, avec u, v deux vecteurs libres sur $\mathbb{R}$. Deux réseaux Λ_1, Λ_2 sont dit isomorphes s'il existe $a \in \mathbb{C}$ tel que $a\Lambda_1 = \Lambda_2$.

Proposition. On note R l'ensemble des réseaux modulo isomorphismes. Alors l'application suivante est une bijection

$$\begin{array}{rcl} \mathcal{H}/SL_2(\mathbb{Z}) & \longrightarrow & R \\ \tau \mod SL_2(\mathbb{Z}) & \longmapsto & \mathbb{Z} \oplus \mathbb{Z}\tau \end{array}.$$

Démonstration. Pour $\tau, \tau' \in \mathcal{H}$, on a

$$\begin{aligned} \mathbb{Z}\tau \oplus \mathbb{Z} \sim \mathbb{Z}\tau' \oplus \mathbb{Z} &\iff \exists \lambda \in \mathbb{C}^*, \mathbb{Z}\lambda\tau \oplus \mathbb{Z}\lambda = \mathbb{Z}\tau' \oplus \mathbb{Z} \\ &\iff \exists \lambda \in \mathbb{C}^*, \exists \gamma \in SL_2(\mathbb{Z}), \begin{cases} \lambda\tau = a\tau' + b \\ \lambda = c\tau' + d \end{cases} \\ &\iff \exists \gamma \in SL_2(\mathbb{Z}), \tau = \gamma.\tau'\ . \end{aligned}$$

Ce quiveut dire que l'application $\mathcal{H} \to R$ passe au quotient et devient injective. Elle est surjective car tout réseau $\mathbb{Z}u \oplus \mathbb{Z}v$ est isomorphe à $\mathbb{Z} \oplus \pm\frac{u}{v}\mathbb{Z}$. □

Remarque. Voir [Mic], [FGN, Alg 1, Ex 2.17]..

Géométrie hyperbolique

Définition. La *métrique* hyperbolique sur $\mathcal{H}$ est $\frac{|dz|}{y^2}$.

Proposition. Cette métrique est invariante par le groupe modulaire.

Démonstration. .[A completer] □

Proposition. Les géodésiques sont les droites et cercles orthogonaux à $\mathbb{R}$.

Démonstration. .[A completer] □

Remarque. Ce développement a été proposé par Sébastien Alvarez.

8 $PSU_2(\mathbb{C}) \simeq SO_3(\mathbb{R})$

Leçons concernées

- 133 - Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).
- 135 - Isométries d'un espace affine euclidien de dimension finie. Forme réduite. Applications en dimensions 2 et 3.
- 138 - Homographies de la droite projective complexe. Applications.
- 139 - Applications des nombres complexes à la géométrie.
- 141 - Utilisation des groupes en géométrie.

Preuve $PSU_2(\mathbb{C}) \simeq SO_3(\mathbb{R})$ via les homographies et la projection stéréographique

Préliminaires

On note $\pi : \mathbb{S}^2 \to \hat{\mathbb{C}}$ la projection stéréographique

$$\begin{array}{rccc} \pi : & \mathbb{S}^2 \subset \mathbb{C}\times\mathbb{R} & \longrightarrow & \hat{\mathbb{C}} \\ & (z,t) & \longmapsto & \frac{z}{1-t} \end{array}.$$

(on fera attention quand $t = 1$ et $z = 0$)

$$\begin{array}{rccc} \pi^{-1} : & \hat{\mathbb{C}} & \longrightarrow & \mathbb{S}^2 \\ & z & \longmapsto & (\frac{2z}{|z|^2+1}, \frac{|z|^2-1}{|z|^2+1}) \end{array}.$$

On note G le groupe circulaire (groupe engendré par les homographie et la conjugaison). On rappelle les résultats suivants

Proposition. $PGL_2(\mathbb{C})$ est distingué dans G.

Théorème (fondamental de la géométrie affine)**.** Une application de $\mathbb{R}^n \to \mathbb{R}^n$ qui envoie 3 points alignés sur 3 points alignés est une application affine.

Théorème. Une application de $\hat{\mathbb{C}} \to \hat{\mathbb{C}}$ qui envoie cercles-droites sur cercles-droites est dans le groupe ciculaire.

Démonstration. Soit f une telle application. Quitte à composer f par une homographie, o peut supposer que $f(0) = 0$ $f(1) = 1$ et $f(\infty) = \infty$. L'applicaiton f envoie alors les droites (cercles passant par ∞) sur les droites donc f est affine. Comme $f(0) = 0$, c'est une aplication linéaire. On note C le cerlce unité. Comme $f(C)$ est un cercle-droite ne passant pas ∞, c'est un cercle et elle passe par 1. Comme f commute avec $-id_{\mathbb{C}}$, on en déduit que $-f(C) = f(-C) - f(-C)$, ce qui donne $f(C) = C$. Donc $f \in O_2(\mathbb{R})$, et comme $f(1) = 1$, c'est donc l'identité ou la conjugaison. □

Théorème

Si R est une application de $\mathbb{S}^2$, on note $\tilde{R}$ son application sur $\hat{C}$

Théorème. Via la projection stéréographique, on a $SO_3(\mathbb{R}) = PSU_2(\mathbb{C})$. C'est-à-dire que l'application suivante est un isomorphisme de groupe

$$\begin{array}{rccc} SO_3(\mathbb{R}) & \longrightarrow & PSU_2(\mathbb{C}) \\ R & \longmapsto & \tilde{R} \end{array}.$$

Démonstration. On voit facilement que : si R est la rotation $R = \begin{pmatrix} \cos\theta & -\sin\theta & \\ \sin\theta & \cos\theta & \\ & & 1 \end{pmatrix}$, alors $\tilde{R}.z = e^{i\theta}z = \begin{pmatrix} e^{i\theta/2} & \\ & e^{-i\theta/2} \end{pmatrix}$.

Lemme. Si $R \in SO_3(\mathbb{R})$, alors $\tilde{R}$ est dans le groupe circulaire.

Démonstration. Comme la projection stéréographique envoie cercle sur cercle droite, l'application $\tilde{R}$ enchange les cercles-droites donc est dans le groupe circulaire. □

Lemme. Si $R \in SO_3(\mathbb{R})$, alors $\tilde{R}$ est dans $PGL_2(\mathbb{C})$.

Démonstration. La rotation R est conjugué à une rotation R' d'axe (Oz). Donc $\tilde{R}$ est conjugué à $\tilde{R}' \in PGL_2(\mathbb{R})$ dans G. Comme $PGL_2(\mathbb{C})$ est distingué, on a donc $R \in PGL_2(\mathbb{C})$. □

Lemme. Si $R \in SO_3(\mathbb{R})$, alors $\tilde{R}$ est dans $PSU_2(\mathbb{C})$.

Démonstration. Si $A = -id_3$, alors $\tilde{A}(z) = -\frac{1}{\bar{z}}$. Comme A_0 commute avec R, l'homographie $\tilde{R}$ commute avec $\tilde{A}$. Si on note $\tilde{R} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod \mathbb{C}^*$ avec $ad - bc = 1$, celà donne $\tilde{R}(-\frac{1}{\bar{z}}) = (-\frac{1}{(\tilde{R})})$, soit

$$\tfrac{-a+b\bar{z}}{-c+d\bar{z}} = -\tfrac{\bar{c}z+\bar{d}}{\bar{a}z+\bar{b}}.$$

Donc il existe $\lambda \in \mathbb{C}^*$ tel que

$$\begin{pmatrix} b & -a \\ d & -c \end{pmatrix} = -\lambda \begin{pmatrix} \bar{c} & \bar{d} \\ \bar{a} & \bar{b} \end{pmatrix}.$$

En prenant le déterminant on obtient $\lambda^2 = 1$, donc $\lambda = 1$ ou -1. Ce qui donne $\bar{a} = \lambda d$ et $\bar{b} = -\lambda c$, mais comme $ad - bc = 1$ on a $\lambda = 1$, puis $\tilde{R} = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in PSU_2(\mathbb{R})$. □

Lemme. Tout élément de $PSU_2(\mathbb{C})$ est du type $\tilde{R}$.

Démonstration. Soit $T = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mod C^* \in PSU_2(\mathbb{C})$. Si $T(0) = 0$, c'est-à-dire $b = 0$, alors $T(z) = \frac{a}{\bar{a}}z$ est du type $e^{i\theta}z = \tilde{\mathbb{R}_\theta}z$. Comme $SO_3(\mathbb{R})$ agit transitivement sur $\mathbb{S}^2$, il existe $R \in SO_3(\mathbb{R})$ tel que $\tilde{R}(T(0)) = 0$. Donc $\tilde{R} \circ T$ est du type $e^{i\theta}z$. □

Ce qui achève la preuve du théorème. □

Remarque. Cette preuve a été mise au point par Julien Sabin et Samuel Le Fourn.

Preuve $PSU_2(\mathbb{C}) \simeq SO_3(\mathbb{R})$ via les quaternions

Première démonstration démonstration

Définition.
- Les *quaternions* est l'ensemble des matrices $\begin{pmatrix} z & -\bar{w} \\ w & \bar{z} \end{pmatrix}$ avec $z.w \in \mathbb{C}$. On note $\mathbb{H}$ cet ensemble. C'est alors un corps et on le munie de la norme euclidienne usuelle qui est aussi donné par le déterminant.
- On note E l'orthogonal de $\mathbb{R}$ dans $\mathbb{H}$. C'est alrs un espace euclidien de dimension 3.
- On vérifie que la sphère unité de $\mathbb{H}$ est $SU_2(\mathbb{C})$.

Proposition. Les groupes $SU_2(\mathbb{C})$ et $SO(E)$ sont des sous-variétés de dimension 3 connexes.

Démonstration. Pour $SU_2(\mathbb{C})$ c ;est clair, car c'est la sphère unité de $\mathbb{H}$ qui est de dimension 4. Pour $SO(E)$ c'est classique. □

Théorème. L'application suivante est un isomorphisme de groupe C^∞

$$\begin{array}{ccc} PSU_2(\mathbb{C}) & \longrightarrow & SO(E) \\ q & \longmapsto & q \otimes q^{-1} \end{array}$$

Démonstration. .[A completer] □

Deuxième démonstration

Définition. Soit E un espace euclidien orienté de dimension 3. On note $\mathbb{H} = \mathbb{R} \oplus E$ munie du produit

$$(x + \overrightarrow{u}).(y + \overrightarrow{v}) = (xy - \overrightarrow{u}.\overrightarrow{v}) + (x\overrightarrow{v} + y\overrightarrow{u} + \overrightarrow{u} \wedge \overrightarrow{v})$$

L'espace $\mathbb{H}$ est alors un corps dont le centre est $\mathbb{R}$.

Lemme. La multiplication par q à gauche ou à droite sur $\mathbb{H}$ est de déterminant $N(q)^2 = ||q||^4$.

Théorème. Soit $q \in \mathbb{H}$.
- L'application

$$\begin{array}{rccc} int_q : & \mathbb{H} & \longrightarrow & \mathbb{H} \\ & x & \longmapsto & qxq^{-1} \end{array}.$$

est dans $SO(\mathbb{H})$ et stabilise E.
- $int_q = int_{q/||q||}$.
- Si $q = \cos\theta + \sin\theta\overrightarrow{N} \in S$, l'action de int_q sur E est la rotation d'axe dirigé par $\overrightarrow{N}$ d'angle 2θ.
- Le morphisme de groupe
$$\begin{array}{ccc} S & \longrightarrow & SO(\mathbb{H}) \\ q & \longmapsto & x \mapsto qxq^{-1} \end{array}$$
induit un isomorphisme $S/\{1,-1\} \to SO(E)$.

Démonstration. Comme la norme est multiplicative int_q est orthogonal, et par le lemme précédent son déterminant est 1. Comme int_q stabilise $\mathbb{R}$, il stabilise son orthognale E.

Si $q = \cos\theta + \sin\theta\overrightarrow{N}$, alors en calculant on trouve que
$$\begin{array}{rcl} q.\overrightarrow{v}.q^{-1} & = & \cos^2\theta\overrightarrow{v} + 2\sin^2\theta\langle\overrightarrow{v}.\overrightarrow{N}\rangle\overrightarrow{N} - \sin^2\theta + 2\sin\theta\cos\theta\overrightarrow{N}\wedge\overrightarrow{u}\,m \\ & = & \langle\overrightarrow{v}.\overrightarrow{N}\rangle\overrightarrow{N} + \cos 2\theta\left(\overrightarrow{v} - \langle\overrightarrow{v}.\overrightarrow{N}\rangle\overrightarrow{N}\right) + \sin 2\theta\overrightarrow{N}\wedge\overrightarrow{u}. \end{array}$$

Ce qui est bien la rotation d'angle 2θ d'axe $\overrightarrow{N}$.

Deux quaternions unitaires $q = \cos\theta + \sin\theta\overrightarrow{N}$ et $q' = \cos\theta' + \sin\theta'\overrightarrow{N'}$ définissent la même rotations si et seulement si
$$\begin{cases} \overrightarrow{N} = \overrightarrow{N'} & \text{et } 2\theta = 2\theta' \mod 2\pi \\ \overrightarrow{N} = -\overrightarrow{N'} & \text{et } 2\theta = -2\theta' \mod 2\pi \end{cases}$$

C'est-à-dire
$$\begin{cases} \overrightarrow{N} = \overrightarrow{N'} & \text{et } \theta = \theta' \mod 2\pi \\ \overrightarrow{N} = \overrightarrow{N'} & \text{et } \theta = \theta' + \pi \mod 2\pi \\ \overrightarrow{N} = -\overrightarrow{N'} & \text{et } \theta = -\theta' \mod 2\pi \\ \overrightarrow{N} = -\overrightarrow{N'} & \text{et } \theta = -\theta' + \pi \mod 2\pi \end{cases}$$

Ce qui implique que $q = q'$ ou $q = -q'$. □

Preuve de $PSL_2(\mathbb{R}) \simeq O_0(2,1)$

Théorème. Le groupe $PSL_2(\mathbb{R})$ est isomorphe (non canoniquement) à $O_0(2,1)$.

Démonstration. .[A completer] □

Remarque. Ce développement a été proposé par Blanche Buet.

9 $PSL_2(\mathbb{R}) \simeq O_0(2,1)$

Leçons concernées
- 119 -
- ? ? ?

Théorème. Le groupe $PSL_2(\mathbb{R})$ est isomorphe (non canoniquement) à $O_0(2,1)$ (la composante connexe de I_3 dans $O(2,1)$).

Démonstration. On définit l'espace vectoriel suivant

$$E = \ker Tr = \Big\{ M \in \mathcal{M}_2(\mathbb{R}) : Tr(M) = 0 \Big\}.$$

Le déterminant est alors une forme quadratique sur E et est de signature $(2,1)$ [y réfléchir]. Le groupe $SL_2(\mathbb{R})$ agit par conjugaison sur E et préserve det. On a alors une application

$$\begin{array}{rccc} \Phi : & SL_2(\mathbb{R}) & \longrightarrow & O(E) \\ & A & \longmapsto & M \mapsto AMA^{-1} \end{array},$$

où $O(E)$ est l'ensemble des $f \in L(E)$ telles que $\det \circ f = \det$.

Lemme. Les groupes $SL_2(\mathbb{R})$ et $O(E)$ sont des sous-variétés de dimension 3

Démonstration du lemme. On le fait pour $O(E)$. On note $Q(E)$ l'ensemble des forme quadratique sur E. On note q la forme quadratique déterminant sur E et on note $S(q) = \{f \in L(E) : {}^t f.q = f.q\}$ l'ensemble des $f \in L(E)$ qui sont auto-adjointes pour q. Comme q est non dégénérée, on a l'isomorphisme d'espace vectoriel suivant

$$\begin{array}{rccc} S(E) & \longrightarrow & Q(E) \\ f & \longmapsto & x \mapsto {}^t x.q.f.x \end{array}.$$

On a $u^{-1}(q)$ avec

$$\begin{array}{rccc} u : & L(E) & \longrightarrow & Q(E) \\ & f & \longmapsto & {}^t f.q.f \end{array},$$

et la différentielle de u en Id_E est

$$\begin{array}{rccc} Du(Id_E) : & L(E) & \longrightarrow & Q(E) \\ & h & \longmapsto & {}^t h.q + q.h \end{array}$$

Donc u est une submersion en Id_E (car $Du(Id_E) : S(E) \to Q(E)$ est bijective). L'ensemble $O(E)$ est alors une sous-variété de dimension $\dim L(E) - \dim Q(E) = 3$ au voisinage de Id_E. Par propriété de groupe, c'est une sous-variété. □

Lemme. L'application Φ est C^1, et sa différentielle en I_2 est

$$\begin{array}{rccc} D\Phi(I_2) : & T_{I_2} SL(\mathbb{R}) & \longrightarrow & T_{Id} O(E) \\ & H & \longmapsto & M \mapsto HM - MH \end{array}$$

Démonstration du lemme. L'application

$$\begin{array}{rccc} \Psi : & GL_2(\mathbb{R}) & \longrightarrow & GL(\mathcal{M}_2(\mathbb{R})) \\ & A & \longmapsto & M \mapsto AMA^{-1} \end{array},$$

est C^∞, donc sa restrition $SL_2(\mathbb{R}) \to O(E)$ est aussi C^1 [y réfléchir]. En déduit la différentielle par restriction. □

Comme $D\Phi(I_2)$ est bijective [y réfléchir], on en déduit que $\Phi(SL_2(\mathbb{R}))$ est un sous-groupe ouvert de $O(E)$ et comme $SL_2(\mathbb{R})$ est connexe, c'est la composante connexe de $O(E)$. Donc Φ est surjective, et on montre que $\ker \Phi = \{-I_2, I_2\}$ [y réfléchir]. □

Remarque. Ce développement a été proposé par Blanche Buet.

10 Théorème de Wantzel et de Gauss

Leçons concernées
- 116 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- 118 - Exemples d'utilisation de la notion de dimension en algèbre et en géométrie.
- 120 - Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
- 144 - Problèmes d'angles et de distances en dimension 2 ou 3.

Théorème de Wantzel

Théorème (Wantzel, 1837)**.** Soit $\Sigma \subset \mathbb{R}$ contenant $\{0,1\}$ et E le sous-corps de $\mathbb{R}$ qu'il engendre. Un réel x est constructible à partir de Σ si et seulement s'il existe une suite de sous-corps de $\mathbb{R}$

$$E = E_0 \subset E_1 \subset \cdots \subset E_n$$

telle que
- $x \in E_n$.
- $\forall i \in [i,n], [E_i : E_{i-1}] = 2$.

Démonstration. Pour l'implication directe on utilise le lemme suivant

Lemme. Soient $x, y, x', y', z \in \mathbb{C}$ et K le corps engendré par les coordonées de x, y, x', y'.
- Si z est l'intersection des droites (x,y) et (x',y'), alors les coordonnées de z sont dans K.
- Si z est l'intersection du cercle $C(x, |y-x|)$ et de la droite $C(x', |y'-x'|)$, alors il existe une extension de degré au plus 2 de K incluse dans $\mathbb{R}$ et contenant les coordonnées de z.
- De même si z est l'intersection du cercle $C(x, |y-x|)$ et de la droite (x',y').

Démonstration du lemme. Si z est l'intersection du cercle $C(x, |x-y|)$ et de la droite (x',y'), avec $x = a+ib$, $y = c+id$, $x' = a'+ib'$, $y' = c'+id'$, alors l'abcisse de z est racine de $Res_X((X-a)^2 + (Y-b)^2 - (a-c)^2 - (b-d)^2, (c'-a')(Y-b') - (d'-b')(X-a'))$ qui est de degré 2 (regarder la matrice de Sylvester).

Si z est l'intersection de deux cercles, il suffit de faire la différence des deux équations pour se ramené à l'équation d'une droite (qui est l'axe radical des deux cercles) et d'un cercle. □

Soit $x \in \mathbb{R}$ constructible et soit $P_1, \ldots, P_n$, comme dans la définition. Pour $i \in [1,n]$, si on note E_i le sous-corps de $\mathbb{R}$ engendré par Σ et les coordonnées de $P_1, \ldots, P_i$, alors d'après le lemme c'est une suite d'extensions de E tel que $[E_{i+1} : E_i] = 1$ ou 2.

Pour la réciproque, on utilise le lemme suivant.

Lemme. Si F est un sous-corps de $\mathbb{R}$ et K une extension de F de degré 2, alors tout élément de K est constructible à partir de F.

Démonstration. Comme K est de degré 2 sur F, il existe $\alpha \in K$ tel que $\alpha^2 \in F$ et $K = F[\alpha]$. Comme on peut construire une racine carré, en déduit que α est construtible, puis que tout élément de K est constructible. □

La réciproque découle du lemme. □

Remarque. On trouvera la preuve dans par exemple [CL05] ou [Esc00].

Théorème de Gauss

Théorème (Gauss)**.** Un polygône à n cotés est constructible si et seulement si n est du type

$$n = 2^p F_{k_1} \ldots F_{k_r},$$

avec $p \in \mathbb{N}$ et F_{k_i} des nombres premiers de Fermat distincts.

Démonstration. .[A completer] □

11 $\mathfrak{A}_5$ est le seul groupe simple d'ordre 60

Leçons concernées
- 103 - Exemples et applications des notions de sous-groupe distingué et de groupe quotient.
- 104 - Groupes finis. Exemples et applications.
- 105 - Groupe des permutations d'un ensemble fini. Applications.
- 149 - Groupes finis de petit cardinal.

Préliminaire

Proposition. Si H est un sous-groupe de $\mathfrak{S}_n$ d'indice 2, alors $H = \mathfrak{A}_n$.

Démonstration. Si H est d'indice 2 alors H est distingué, et le morphisme $G \mapsto G/H \simeq \mathbb{Z}/2\mathbb{Z}$ est surjectif, donc c'est la signature. □

Proposition. Le groupe $\mathfrak{A}_5$ est simple.

Démonstration. Cf ? □

Théorème

Théorème. Tout groupe simple d'ordre 60 est isomorphe à $\mathfrak{A}_5$.

Démonstration. Soit G un tel groupe.

Lemme. Si H est un sous-groupe de G, alors $[G : H] \geq 5$.

Démonstration. Car sinon le noyau de l'action de G sur G/H fournit un sous-groupe distingué non trivial, puis que $\operatorname{Card} \mathfrak{S}(G/H) \leq 4! = 24$. □

Lemme. Il existe un sous-groupe H d'indice 5.

Démonstration. Supposons le contraire. D'après le théorème de Sylow, le nombre de 2-sylow est $1, 3, 5$ ou 15 (un 2-sylow est de cardinal 4). Celà ne peut être que 15, car sinon l'action de G sur ses deux sylow a un noyau non trivial.

Montrons que l'intersection de deux 2-sylows est trivial. Soient S et S' deux 2-sylow et $t \in S \cap S'$. On note $C(t)$ son centralisateur. Alors $C(t)$ contient S et S' (car S et S' sont abélien), donc son cardinal est un multiple de 4 et est supérieur à 5. Comme son cardinal divise 60, on en déduit qu'il vaut 12 ou 60. Comme $C(t)$ n'est pas d'indice 5, on a $\operatorname{Card} C(t) = 60$. Par hypothèse on en déduit que $C(t) = G$ et donc $t \in Z(G) = \{1\}$ ce qui est absurde.

Donc l'union des 2-sylow est de cardinal $1 + 3 * 15 = 46$. D'autre part par théorème de Sylow le nombre de 5-sylow est 1 ou 6, et vaut 6 car G est simples. Comme les 5-sylow sont monogènes d'ordre premier, l'intersection de deux 5-sylow est trivial. L'ensemble des 5-sylow fournissent donc $4 * 6 = 24$ éléments d'ordre 5, ce qui donne un contradiction car $46 + 24 > 60$. □

Il existe alors un sous-groupe d'ordre 5. La représentation de G sur G/H fournit une injection (car G est simple) de G dans $\mathfrak{S}_5$. Comme le seul sous-groupe d'indice 2 de $\mathfrak{S}_5$ est $\mathfrak{A}_5$, on en déduit que $G \simeq \mathfrak{A}_5$. □

Remarque. Voir [?]

12 Simplicité de $\mathfrak{A}_n$

Leçons concernées
- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 104 - Groupes finis. Exemples et applications.
- 105 - Groupe des permutations d'un ensemble fini. Applications.
- 145 - Méthodes combinatoires, problèmes de dénombrement.
- 149 - Groupes finis de petit cardinal.

Théorème. Pour $n \geq 5$, $\mathfrak{A}_n$ est simple.

Remarque.
- Pour $n \leq 3$, $\mathfrak{A}_n$ est simple.
- $\mathfrak{A}_4$ n'est pas simple (regarder son groupe de Klein).

Démonstration. • On commence par $n = 5$. Soit H un sous-groupe distingué de $\mathfrak{A}_5$. Le groupe $\mathfrak{A}_5$ a 60 éléments :
- 1 d'ordre 1.
- 15 d'ordre 2 (produits de deux transpositions).
- 20 d'ordre 3 (3-cycles).
- 24 d'ordre 5 (5-cycles).

$*$ Les 3-cycles sont conjugués dans $\mathfrak{A}_5$: en effet, les deux 3-cycles $(a,b,c)(d)(e)$ et $(a',b',c')(d')(e')$ sont conjugués par les deux permutations

$$\begin{bmatrix} a & b & c & d & e \\ a' & b' & c' & d' & e' \end{bmatrix} \text{ et } \begin{bmatrix} a & b & c & d & e \\ a' & b' & c' & e' & d' \end{bmatrix},$$

et l'un des deux est pair.

$*$ Les double-transpositions sont conjugués dans $\mathfrak{A}_5$: en effet, les permutations $(a,b)(c,d)(e)$ et $(a',b')(c',d')(e')$ sont conjugués par

$$\begin{bmatrix} a & b & c & d & e \\ a' & b' & c' & d' & e' \end{bmatrix} \text{ et } \begin{bmatrix} a & b & c & d & e \\ a' & b' & d' & c' & e' \end{bmatrix},$$

et l'un des deux est pair.

$*$ Les 5-sylows de $\mathfrak{A}_5$ sont de cardinal 5. Si H contient un élément d'ordre de 5 alors il contient un 5-Sylow donc tous les 5-Sylow (car les sylows sont conjugués), i.e. tous les éléments d'ordre 5.

On en déduit que si H contient un élément d'ordre 2 alors il les contient tous, et de même pour les éléments d'ordre 3 et 5. Si H contient l'élément neutre et que les doubles transpositions alors $\sharp H = 1 + 15 = 16$ qui ne divise pas 60, donc c'est absurde. De même si H contient que les 3-cycles ou que les 5-cycles. Si H ne contient que le neutre, les double-tranpositions et les 3 cycles alors $\sharp H = 1 + 15 + 20 = 36$ donc c'est absurde. De même si H ne contient que le neutre, les double-tranpositions et les 5-cycles, ou les 3-cycles et 5-cycles. Donc $\boxed{H = \mathfrak{A}_5}$.

• Cas général : soit H sous-groupe distingué de $\mathfrak{A}_n$ et $\sigma \in H \setminus \{id\}$. Il existe $a \in \left\{1, \ldots, n\right\}$ non fixe par σ et $c \notin \{a, \sigma(a), \sigma^2(a)\}$. On note

$$b = \sigma(a) \text{ et } \tau = (a, c, \sigma(a)) \text{ et } \rho = \tau\sigma\tau^{-1}\sigma^{-1}.$$

Comme $\sigma\tau^{-1}\sigma^{-1} = (\sigma.a, \sigma.d, \sigma.d)$, on en déduit que $\rho = (a,c,b)(\sigma.a, \sigma.b, \sigma.c)$. On note $F = \{a, b, c, \sigma.a, \sigma.b, \sigma.c\}$. L'ensemble F a au plus 5 éléments et quitte à rajouté un élément ; on peut supposer que F est une partie à 5 éléments stable par ρ. On note $H_0 = H \cap \mathfrak{A}(F)$. Le sous-groupe H_0 est alors distingué dans $\mathfrak{A}(F)$ contenant $\rho \neq id$ car $\rho(b) = \tau\sigma(b) \neq b$. Donc $H_0 = \mathfrak{A}(F) \subset H$ et H contient un trois cycle. □

Remarque. Voir [Per96],.

13 Simplicité de $SO_3(\mathbb{R})$

Leçons concernées
– ? ? ?.

On rapelle les résultats suivants.

Proposition. Les groupe $SO_3(\mathbb{R})$ est connexe.

Démonstration. Utiliser la forme normale des rotations. □

Proposition. Le centre $SO_3(\mathbb{R})$ est $\{I_3\}$.

Démonstration. Utiliser le fait que toute droite est sous-espace propre d'une rotation. □

Proposition. Le groupe $SO_3(\mathbb{R})$ est engendré par les retournements.

Démonstration du lemme. Le groupe $O_3(\mathbb{R})$ est engendré par les réflexions, donc $SO_3(\mathbb{R})$ est engendré par les doubles réflexions. En remarquant que si τ est une réflexion alors $-\tau$ est un demi-tour, on en déduit que $SO_3(\mathbb{R})$ est engendré par les demi-tours. □

Théorème. $SO_3(\mathbb{R})$ est simple.

Démonstration. Soit H sous-groupe distingué de $SO_3(3)$. Si H est connexe alors $\{\cos^{-1}(Tr(M)-1)/2 | M \in H\}$ est connexe et non réduit à un point donc H contient un élément M tel que $\cos^{-1}(Tr(M)-1)/2 = \pi/N$ pour un certain N. Il s'en suit que H contient le demi-tour M^N et comme les demi-tours sont conjugués, on en déduit que $H = SO_3(\mathbb{R})$. Si H est non connexe, on note H^0 la composante connexe de I_3 dans H. Alors H^0 est un groupe car l'application $H^0 \times H^0 \to H, (x,y) \mapsto xy^{-1}$ a pour image un connexe contenant I_3, donc est incluse dans H^0. Et de même en considérant l'application $G \times H^0 \to H, (g,h) \mapsto ghg^{-1}$, on montre que H^0 est distingué dans $SO_3(\mathbb{R})$. Donc soit $H^0 = \{I_3\}$, soit $H^0 = SO_3(\mathbb{R})$. Si $H^0 = \{I_3\}$, alors pour $h \in H$ et $SO_3(\mathbb{R}) \to H, g \mapsto [g,h]$ est à valeur dans $H^0 = \{I_3\}$, donc $H \subset Z(SO_3(\mathbb{R})) = \{I_3\}$. □

14 Théorème de Sylow

Leçons concernées
- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 103 - Exemples et applications des notions de sous-groupe distingué et de groupe quotient.
- 104 - Groupes finis. Exemples et applications.

Théorème. Soit G un groupe fini, $\operatorname{Card} G = p^\alpha m$ avec $p \nmid m$. On note N le nombre de p-Sylow. Alors
- Tout sous-p-groupe est inclu dans un p-Sylow.
- Les p-sylow sont tous conjugués (donc $N | \operatorname{Card} G$).
- $N = 1 \mod p$ et $N|m$.

Démonstration. On commence par lemme suivant.

Lemme. Soit K un groupe, $G \subset K$ et S un p-Sylow de K. Alors il existe $a \in K$ tel que $G \cap aHa^{-1}$ soit un p-Sylow de G.

Démonstration du lemme. On fait agir G sur K/S. On a $\operatorname{Stab} aH = aSa^{-1} \cap G$ et par formule des classes

$$\operatorname{Card} K/S = \sum_a \operatorname{Card} Orb(aS) = \sum_a \frac{\operatorname{Card} G}{\operatorname{Card} \operatorname{Stab}(aSa^{-1} \cap G)},$$

où a parcours un ensemble de représentants des orbites.
Comme $p \nmid \operatorname{Card} K/H$, il existe a tel que $p \nmid \operatorname{Card} \operatorname{Orb} aS$ et donc $aSa^{-1} \cap G$ est un p-Sylow de G. □

Comme $G \subset SL_n(\mathbb{F}_p)$ avec $n = \operatorname{Card} G$ et que $SL_n(\mathbb{F}_p)$ admet un p-Sylow (le groupe des triangulaires supérieurs unipotent), $\boxed{\text{le groupe } G \text{ admet aussi un } p\text{-Sylow}}$.

Soit S un p-Sylow de G et H est un sous-p-groupe de G, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H, c'est-à-dire $aSa^{-1} \cap H = H$ puis $H \subset aSa^{-1}$. Donc tout sous-p-groupe est inclus dans un p-Sylow et $\boxed{\text{tous les } p\text{-Sylow sont conjugués}}$.

Soit S un p-Sylow de G. On note X l'ensemble des p-Sylow et on fait agir S sur X par conjugaison. Comme S est un p-groupe, on a $\operatorname{Card} X = \operatorname{Card} X^S \mod p$. Soit $T \in X^S$. Comme $T \lhd S$, l'ensemble ST est un sous-groupe de G. Comme $\operatorname{Card}(ST) = \frac{\operatorname{Card}(S)\operatorname{Card}(T)}{\operatorname{Card}(S \cap T)}$ est une puissance de p, et comme ST contient les p-Sylow S et T on en déduit que $ST = S = T$. Donc $X^S = \{S\}$ et $\boxed{N = 1 \mod p}$. Comme X est une orbite on a $N | \operatorname{Card} G$, et comme $pgcd(N, p) = 1$, on en déduit que $\boxed{n|m}$. □

Remarque ([Per96])**.** , [[Gou94a] : Chap. 1, Prob. 7].

15 Théorème de Burnside

Leçons concernées
- 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.
- 128 - Endomorphismes trigonalisables. Endomorphismes nilpotents.
- 129 - Algèbre des polynômes d'un endomorphisme en dimension finie. Applications.

Préliminaire

Proposition. Soit $A \in \mathcal{M}_n(K)$. Si pour tout $k \in [0, n-1]$, on a $Tr(A^k) = 0$, alors A est nilpotente..

Démonstration. .[A completer] □

Théorème

Théorème (Burnside)**.** Si G est un sous groupe de $GL_n(\mathbb{C})$ d'exposant fini, alors G est de cardinal fini.

Démonstration. On note p l'exposant de G. Tout élément de G est alors diagonalisable dans $GL_($. On note E le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ engendré par G et on prend $(A_1, \dots, A_r)$ une famille de G qui engendre E. Comme G est un groupe, l'espace E est une algèbre. On définit l'application

$$\begin{array}{rccc} \Phi : & G & \longrightarrow & \mathbb{C}^r \\ & M & \longmapsto & (Tr(MA_i))_{i\in[1,r]} \end{array}.$$

Lemme. Pour $M, N \in E$, si $\Phi(M) = \Phi(N)$, alors

$$\forall k \in \mathbb{N}, Tr((MN^{-1})^k) = n.$$

Démonstration. On remarque que par linéarité on a

$$\forall A \in E, Tr(MA) = Tr(NA).$$

Pour $k \in \mathbb{N}$, on a $Tr((MN^{-1})^{k+1}) = Tr(M.N^{-1}(MN^{-1})^k)$. Comme $N^{-1}(MN^{-1})^k \in E$, on en déduit que $Tr(N.N^{-1}(MN^{-1})^k) = Tr((MN^{-1})^k)$. On conclut par récurrence que $Tr((MN^{-1})^k) = Tr(Id) = n$. □

Lemme. L'application Φ est injective sur G.

Démonstration. Si $M, N \in G$ sont tels que $\Phi(M) = \Phi(N)$, alors $Spec(MN^{-1}) = \{1\}$. Comme $MN^{-1} \in G$ est diagonalisable, on en déduit que $MN^{-1} = Id$. □

Comme les éléments $Tr(MA_i)$ $(A \in G, i \in [1, r])$ sont des sommes de racines p^{em} de l'unité, on en déduit que $\Phi(G)$ est fini. Donc G est fini. □

Remarque. Voir [FGN, Alg 2, Ex 3.6]

16 Sous-groupes finis de $SO_3(\mathbb{R})$

Leçons concernées
- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 104 - Groupes finis. Exemples et applications.
- 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications.
- 107 - Sous-groupes finis de $O_2(\mathbb{R})$ et de $SO_3(\mathbb{R})$. Applications.
- 135 - Isométries d'un espace affine euclidien de dimension finie. Forme réduite. Applications en dimensions 2 et 3.
- 141 - Utilistion des groupes en géométrie.
- 145 - Méthodes combinatoires, problèmes de dénombrement.

Théorème. Les sous-groupes finis de $SO_3(\mathbb{R})$ sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$, D_{2n}, $\mathfrak{S}_4$, $\mathfrak{A}_4$ ou $\mathfrak{A}_5$.

Démonstration. Soit G un goupe fini de cardinal $n \leq 2$. On note $X = \{P \in \mathbb{S}^2 \mid \exists g \in G \setminus \{Id\} g.P = P\}$. On note $N = card(X)$ et on a $2 \leq N \leq 2n$. Alors G agit sur X car si $g, h \in G$ et P fixe par h, alors $g.P$ est fixe par ghg^{-1}. On note k le nombre d'orbite. Alors par Burnside

$$nk = \sum_{g \in G} Fix(g) = N + 2(n-1).$$

ce qui donne $N = (k-2)n + 2$ et $2 \leq k \leq 4(1 - 1/n)$, puis $k = 2, 3$.

• **Cas 1 :** si $k = 2$. Alors $N = 2$ et $X = \{P, -P\}$. Donc tous les élement de G laisse fixe $vect(P)$, puis G s'injecte dans $SO(P^\perp)$. Donc G est cyclique d'ordre n.

• **Cas 2 :** si $k = 3$. Alors $N = n+2$. On note X_1, X_2 et X_3 les 3 orbites, avec $card(X_1) \leq card(X_2) \leq card(X_3)$. On a $card(X_1) + card(X_2) + card(X_3) = n + 2$, donc $CardX_1 \leq (n+2)/3 \leq CardX_3$. Comme $CardX_3 | n$, et que pour $P \in X_3$, $Stab(x) \geq 2$, on a $CardX_3 = n/2$ et $Stab(x) = 2$. Ce qui donne $card(X_1) + card(X_2) = n/2 + 2$, donc $(n+4)/4 \leq Card(X_2)$, puis $Card(X_2) = n/2$ ou $n/3$.

•• **Cas 2.1 :** si $k = 2$ et $Card(X_2) = n/2$. Alors $CardX_1 = 2$. Soit $P \in X_1$, on a $Stab(P) \subset SO(P^\perp)$ et $card(Stab(P)) = n/2$, donc $Stab(P)$ est un groupe cyclique d'ordre $n/2$. Pour $g_0 \notin Stab(P)$, on a $g_0.P = -P$, donc -1 est valeur propre de g_0 et g_0 est retournement d'axe perpendiculaire à P. On a $g_0 Stab(P) g_0^{-1} = Stab(g_0.P) = Stab(P)$ et $Stab(P) \cap \{Id, g_0\}$. Donc $G = Stab(P) \rtimes \{Id, g_0\}$. Donc $\boxed{G \simeq D_n}$, car G est non abélien sauf pour $n/2 = 2$.

•• **Cas 2.1 :** si $k = 2$ et $Card(X_2) = n/2$. Alors $CardX_1 = 2$. Soit $P \in X_1$, on a $Stab(P) \subset SO(P^\perp)$ et $card(Stab(P)) = n/2$, donc $Stab(P)$ est un groupe cyclique d'ordre $n/2$. Pour $g_0 \notin Stab(P)$, on a $g_0.P = -P$, donc -1 est valeur propre de g_0 et g_0 est retournement d'axe perpendiculaire à P. On a $g_0 Stab(P) g_0^{-1} = Stab(g_0.P) = Stab(P)$ et $Stab(P) \cap \{Id, g_0\}$. Donc $G = Stab(P) \rtimes \{Id, g_0\}$. Donc $\boxed{G \simeq D_n}$, car G est non abélien sauf pour $n/2 = 2$.

♣ **Cas 2.1 :** si $card(X_2) = n/2$. Alors $cardX_1 = 2$. Soit $P \in X_1$, on a $Stab(P) \subset SO(P^\perp)$ et $card(Stab(P)) = n/2$, donc $Stab(P)$ est un groupe cyclique d'ordre $n/2$. Pour $g_0 \notin Stab(P)$, on a $g_0.P = -P$, donc -1 est valeur propre de g_0 et g_0 est retournement d'axe perpendiculaire à P. On a $g_0 Stab(P) g_0^{-1} = Stab(g_0.P) = Stab(P)$ et $Stab(P) \cap \{Id, g_0\}$. Donc $G = Stab(P) \rtimes \{Id, g_0\}$. Donc $\boxed{G \simeq D_n}$, car G est non abélien sauf pour $n/2 = 2$.

♣ **Cas 2.2 :** si $card(X_2) = n/3$. Alors $card(X_1) = n/6 + 2$, donc $card(X_1) = n/5, n/4, n/3$.

⋆ **Cas 2.2.1 :** si $card(X_1) = n/3$. Alors $n + 2 = n/3 + n/3 + n/2$, donc $\boxed{\text{n=12}}$, puis $card(X_1) = 4$, $card(X_2) = 4$, $card(X_3) = 6$. Le groupe G agit sur X_1 et l'action est fidèle car les 4 points ne sont pas alignés. Donc $\boxed{G = Isom^+(X_1) \simeq \mathfrak{A}_4}$. Donc l'action est 2-transitive sur X_1 et on en déduit que X_1 est un tétraèdre.

⋆ **Cas 2.2.2 :** si $card(X_1) = n/4$. Alors $n + 2 = n/4 + n/3 + n/2$, donc $\boxed{\text{n=24}}$, puis $card(X_1) = 6$, $card(X_2) = 8$, $card(X_3) = 12$. Pour $i \in [1, 3]$ et $P \in X_i$. Comme $Stab(-P) = Stab(P)$, on a $card(Orb(-P)) = card(P)$, donc $Orb(-P) = Orb(P)$. Donc les X_i sont stables par $-Id$.

On se fixe $P \in X_1$ et $Q \in X_1 \setminus \{P, -P\}$. Alors $Stab(P)$ est cyclique d'ordre 4 engendré une rotation r. Comme Q n'est sur l'axe on en déduit que Q, rQ, r^2Q, r^3Q sont distincts, puis $X_1 = \{P.-P, Q, rQ, r^2Q, r^3Q\}$. Comme $-Q \in \{Q, rQ, r^2Q, r^3Q\}$ et que seul r^2 a -1 comme valeur propre on en déduit que $Q = r^2Q$, puis que Q est orthognal à P. On en déduit que P, Q, rQ est une base orthonormé puis que X_1 est un octaèdre. Donc $\boxed{G = Isom^+(X_1)}$.

⋆ **Cas 2.2.3 :** si $card(X_1) = n/5$. Alors $n + 2 = n/6 + n/3 + n/2$, donc $\boxed{\text{n=60}}$, puis $card(X_1) = 12$, $card(X_2) = 20$, $card(X_3) = 30$. [A completer].

□

Remarque. Voir [Com98], [Ber77]. [Goblot Theme de geometrie] [FGN, Alg 3 Ex 2.15].

17 Groupes de pavages

Leçons concernées
- 141 - Utilistion des groupes en géométrie.
- 139 - Applications des nombres complexes à la géométrie.

Définition. Un pavage du plan euclidien E est un couple (P, G) où P est un compact d'intérieur non vide de E et G un sous-groupe de $Isom^+(E)$ vérifiant :
- $E = \bigcup_{g\in G} g(P)$.
- Pour tout $g, h \in G$, si $int(g(P)) \cap int(h(P)) \neq \emptyset$, alors $g(P) = h(P)$.

Théorème. Il existe cinq types de pavages à "conjugaison près".

Démonstration. Soit G un groupe de pavage.

Lemme (Discrétisation)**.** Le groupe G est discret.

Démonstration du lemme. Il suffit de montrer que toute suite convergente est stationnaire. Soit $(g_n)_{n\in\mathbb{N}}$ une suite de G convergeant vers g. Soit $x \in g(ing(K)) = int(g.K)$. Comme $\lim_{n\to+\infty} g_n.x = g.x$, il existe $N > 0$ tel que

$$\forall n \geq N, g_n.x \in int(g.K).$$

Or $g_n.x \in int(g_n.K)$, donc $g_n = g$ pour $n \geq N$. □

Lemme (Groupe des translations)**.** On note T l'ensemble des translation de G. Alors il existe u, v deux vecteurs indépendants tels que $T = \mathbb{Z}\tau_u \oplus \mathbb{Z}\tau_v$.

Démonstration du lemme. Si T ne contient aucune translation non nulle, alors toute les rotations commutteraient et donc aurait le même centre. Ce qui impliquerait que $G(P)$ est borné. Donc T contient une translation.

Supposons que toutes les translations ont même direction. Pour $r \in G - T$ et $\tau_u \in T$, on a $r\tau_u r^{-1} = \tau_{\vec{r}.u}$, donc $\vec{r} = Id$ ou $-Id$. Donc toute rotation différente de Id est une symétrie centrale. L'hypothèse sur T permet de dire que tous les centres sont alignés. Ce qui implique que $G(P)$ est inclus dans une bande.

Donc T contient au moins deux translations indépendantes et comme T est discret, on en déduit que T est du type $T = \mathbb{Z}\tau_u \oplus \mathbb{Z}\tau_v$. □

Lemme (Groupe des rotations)**.** Le groupe $\vec{G} \subset SO_2(\mathbb{R})$ est cyclique d'ordre $1, 2, 3, 4, 6$.

Démonstration du lemme. Soit $r \in G$. Alors $\vec{r}$ stabilise $T \subset \mathbb{R}^2$, car $r \in G$, on a $r\tau_{\vec{u}}r^{-1} = \tau_{\vec{r}.\vec{u}}$. Donc $Trace(\vec{r}) \in \mathbb{Z}$, donc son angle est dans $\{0, \pm\pi/3, \pm\pi/2, \pm 2\pi/3\}$. Donc $\vec{G} \subset \mathbb{Z}/12\mathbb{Z}$, ce qui permet de conclure. □

Lemme (Structure de G)**.** Soit $r \in G$ tel que $\vec{r}$ engendre $\vec{G}$. On note R le sous-groupe engendré par r. Alors $G = T \rtimes R$.

Démonstration du lemme. Soit $g \in G$. Il existe $k \in \mathbb{N}$ tel que $\vec{g} = \vec{r}^k =$. On a alors $g \circ r^{-k} \in T$. □

Donc G est du type $\mathbb{Z}^2 \rtimes \mathbb{Z}/n\mathbb{Z}$ avec $n \in \{1, 2, 3, 4, 6\}$.
- Si $G = \mathbb{Z}\vec{u} \oplus \mathbb{Z}\vec{v}$ et $G' = \mathbb{Z}\vec{u'} \oplus \mathbb{Z}\vec{v'}$ sont deux sous-groupes isomorphes à $\mathbb{Z}^2$, alors ils sont conjugués par $f \in Aff(\mathbb{R}^2)$ telle que $\vec{f}(\vec{u}) = \vec{u'}$ et $\vec{f}(\vec{v}) = \vec{v'}$.
- Si G et G' sont isomorphes à $\mathbb{Z}^2 \rtimes \mathbb{Z}/2\mathbb{Z}$, alors ils sont aussi conjugués sous $Aff(\mathbb{R}^2)$.
- Si G est isomorphe à $\mathbb{Z}^2 \rtimes \mathbb{Z}/3\mathbb{Z}$, alors comme T est stable par $\vec{G} = \mathbb{Z}/3\mathbb{Z}$, il est du type $T = \mathbb{Z}\vec{u} \oplus \mathbb{Z}j\vec{u}$. Si $G = (\mathbb{Z}\vec{u} \oplus \mathbb{Z}j\vec{u}) \rtimes \langle r\rangle$ et $G' = (\mathbb{Z}\vec{u'} \oplus \mathbb{Z}j\vec{u'}) \rtimes \langle r'\rangle$, alors G et G' sont conjugués par $f \in Isom^+(\mathbb{R}^2)$ telle que $\vec{f}(\vec{u}) = \vec{u'}$ et f envoie le centre de r sur le centre de r'.
- Les autre cas se traitent comme le cas précédent.

□

Remarque. Voir [[Ber77] Tome ? Chap ?]

18 Théorème fondamental de la géométrie affine

Leçons concernées

? ? ? .

Théorème. Soit E un espace affine sur k et $f : E \to E$. On suppose que $\dim E \geq 2$, f est bijectif et conserve l'alignement. Alors f est semi-linéaire.

Démonstration. .

• Fait 1 : les images de k points indépendants sont encore indépendants. Soient $A_1, \dots, A_k$ indépendants, on complète en une base affine $A_1, ..., A_{n+1}$. L'hypothèse que f conserve l'alignement implique que

$$f(< A_1, ..., A_{n+1} >) \subset < f(A_1), ..., f(A_{n+1}) >$$

En effet : si $X \in E$, X est aligné avec A_{n+1} et un certain $X_n \in < A_1, \dots, A_n >$, ensuite X_n est aligné avec A_n et un certain $X_{n-1} \in < A_1, \dots, A_{n-1} >$, etc... Donc $f(X_2) \in < f(A_1), f(A_2) >$, $F(X_3) \in < f(X_1), f(A_3) > \subset < f(A_1), f(A_2), f(A_3) >$, etc... $f(X) \in < f(A_1), \dots, f(A_{n+1}) >$.

Comme f est surjective et que les points $f(A_1), \dots, f(A_{n+1})$ sont indépendants, on en déduit que les points $f(A_1), \dots, f(A_k)$ sont indépendants.

• Fait 2 : l'application f envoie des droites sur des droites et deux droites parallèles sur deux droites parallèles. Soit $D = (AB)$ une droite. Comme f conserve l'alignement $f(D) \subset (f(A), f(B))$. Soit $X \notin D$, alors A, B, X sont indépendants et $f(A), f(B), f(X)$ sont indépendants, donc $f(D^c) \subset f(D)^c$, d'où $f(D) = (f(A), f(B))$. Soient D, D' deux droites parrallèles et $P =< A, B, C >$ un plan contenant D, D'. Alors $f(D) \subset f(P) \subset Q :=< f(A), f(B), f(C) >$ et de même $f(D') \subset Q$. Comme f est injective on a $f(D) \cap f(D') = \emptyset$ donc $f(D)$ et $f(D')$ sont parallèles (car elles sont contenues dans un même plan).

• Fait 3 : soient $O, A, B, C \in E$ tels que $\overrightarrow{OC} = \overrightarrow{OA} + \overrightarrow{OB}$, O, A, B non alignés, O', A', B', C' leurs image par f, alors $\overrightarrow{O'C'} = \overrightarrow{O'A'} + \overrightarrow{O'B'}$, i.e en vectorialisant en O et O', f est additive sur les points non alignés. On a $(OA)//(BC)$ $(OB)//(AC)$ donc $(O'A')//(B'C')$ et $(O'B')//(A'C')$, donc par règle du paralélllogramme $\overrightarrow{O'C'} = \overrightarrow{O'A'} + \overrightarrow{O'B'}$ (le parallélogramme est non plat puisque O, A, B ne sont pas alignés)

• Maintenant on construit un morphisme de corps $\sigma : k \to k$. Soient $O, X \in E$, pour $\lambda \in k$ on pose $\sigma(\lambda)$ tel que $\overrightarrow{O'A'} = \sigma(\lambda)\overrightarrow{O'X'}$ avec $\overrightarrow{OA} = \lambda\overrightarrow{OX}$. L'application σ est une bijection car $f : (OX) \to (O'X')$ l'est. Montrons que c'est un morphisme de corps : pour $\lambda, \mu \in k$, comme $\dim E \geq 2$, on peut construire et points $O + (\lambda + \mu)\overrightarrow{OX}$, $O + (\lambda\mu)\overrightarrow{OX}$ grâce à des parallèles.

• Enfin, l'application f est σ-affine : en effet, par théorème Thalès l'application σ est indépendant de X. □

Remarque. Dans le cas $k = R$, le seul automorphisme est Id.

Remarque. Voir [Aud06], [Ber77].

19 Théorème de Minkovski

Leçons concernées
– ? ? ?

Théorème de Minkovski

Théorème (Minkovski)**.** Soient Λ un réseau de $\mathbb{R}^n$ et C un convexe compact symétrique par rapport à 0. On suppose que $Vol(C) \geq 2^n Vol(\Lambda)$. Alors $C \cap \Lambda \setminus \{0\}$ est non vide.

Démonstration. .[A completer] □

Théorème des deux carrés et des quatre carrés

Théorème (des deux carrés faible)**.** Si p est un nombre premier congrue à $1 \mod p$, alors p est somme de deux carrés.

Démonstration. Comme $p = 1 \mod 4$, on peut prendre $u \in \mathbb{N}$ tel que $u^2 = 1 \mod p$. On considère l'application

$$\begin{array}{rccc} \Phi : & \mathbb{Z}^2 & \longrightarrow & \mathbb{F}_p \\ & (a,b) & \longmapsto & a - ub \mod p \end{array}.$$

Alors Φ est surjective et $\ker \Phi = \{(a,b) \in \mathbb{Z}^2 : a = ub \mod p\}$. On a $Vol(\ker \Phi) = \operatorname{Card} \operatorname{Im} \Phi = p$ (utiliser les diviseurs élémentaires). On prend pour convexe $B(0,R)$ tel que $R^2\pi = 4p$. On a alors pour $(a,b) \in \ker \Phi \cap B(0,R) \setminus \{0\}$, $a^2 + b^2 = 0 \mod p$ et $0 < a^2 + b^2 \leq \frac{4}{\pi} p < 2p$, d'où $a^2 + b^2 = p$. □

Théorème (des quatre carrés)**.** Soit p un nombre premier impaire. Alors p est somme de quatre carrées.

Démonstration. On prend $u, v \in \mathbb{N}$ tel que $u^2 + v^2 + 1 = 0 \mod p$. On considère l'application

$$\begin{array}{rccc} \Phi : & \mathbb{Z}^4 & \longrightarrow & \mathbb{F}_p^2 \\ & (a,b,c,d) & \longmapsto & (ua + vb - c \mod p, va - ub - d \mod p) \end{array}.$$

Alors Φ est surjective (faire varier c et d) et $\ker \Phi = \{(a,b) \in \mathbb{Z}^2 : ua + vb = c \mod p, va - ub = d \mod p\}$. On a $Vol(\ker \Phi) = p^2$. On prend pour convexe $B(0,R)$ tel que $R^4?? = 2^4 p^2$. On a alors pour $(a,b,c,d) \in \ker \Phi \cap B(0,R) \setminus \{0\}$, $a^2 + b^2 + c^2 + d^2 \leq R = ?? < 2p$ et $(ua + vb)^2 = c^2 \mod p$, $(va - ub)^2 = d^2 \mod p$, ce qui donne en sommant $a^2 + b^2 + c^2 + d^2 = 0 \mod p$. □

Remarque. Voir [Tauvel, cour de maths ?].

20 Automorphismes de $\mathfrak{S}_n$

Leçons concernées
- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 103 - Exemples et applications des notions de sous-groupe distingué et de groupe quotient.
- 105 - Groupe des permutations d'un ensemble fini. Applications.

Théorème. Pour $n \neq 6$, tous les automorphisme de $\mathfrak{S}_n$ sont intérieurs.

Démonstration. .[A completer] □

Remarque. Voir par exemple [Perrin].

Chapitre 3

Algèbre linéaire

1 Théorème de Lie-Kolchin

Leçons concernées

- 103 - Exemples et applications des notions de sous-groupe distingué et de groupe quotient.
- 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.
- 121 - Matrices équivalentes.Matrices semblables. Applications.
- 124 - Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
- 125 - Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.

Préliminaires

Lemme. Un sous-groupe abélien de $GL_n(\mathbb{C})$ est cotrigonalisable.

Lemme. L'image d'un groupe connexe résoluble par un morphisme de groupe continue est encore un groupe connexe résoluble.

Démonstration. La connexité vient de la continuité et la résolubilité vient du fait que l'image du groupe dérivée est le groupe dérivée de l'image. □

Lemme. Le sous-groupe dérivé d'un groupe connexe est connexe.

Démonstration. .A completer □

Théorème

Théorème. Si G est un sous-groupe connexe et résoluble de $GL_n(\mathbb{C})$, alors G est conjugué à sous-groupe des matrices triangulaires supérieures inversibles.

Démonstration. On raisonne par récurrence sur la dimension. C'est clair si $n = 1$.

Supposons que G admet un sous-espace stable F strict. On pose $G_1 = \left\{ g_{|F} \mid g \in G \right\} \subset GL(F)$ et $G_1 = \left\{ g \mod F \mid g \in G \right\} \subset GL(E/F)$, qui sont connexes résolubles par le lemme [?]. En appliquant l'hypothèse de récurrence, les G_1 groupes et G_2 sont trigonalisables et on en déduit que G est trigonalisable.

Supposons que G n'a pas de sous-espace stable (i.e. irréductible). On note m le plus petit entier telle que $D^m(G) = \{I_n\}$. Si $m = 0$ ou 1, alors G est abélien et donc trigonalisable.

On va montrer que si $m \geq 2$, alors on arrive à une contradiction. On note $H = D^{m-1}(G)$. Alors H est abélien et inclus dans $SL_n(\mathbb{C}) = D(GL_n(\mathbb{C}))$ (car $m - 1 \geq 1$). On définit

$$F = \{x \in E : \forall h \in H, \exists \lambda_h \in \mathbb{C}, h.x = \lambda_h x\}.$$

Alors F est un sous-espace vectoriel non nul car H est abélien. Montrons que F est stable par G, on aura alors $F = E$, puis $H \subset \mathbb{C} \cap SL_n(\mathbb{C}) = \mathbb{U}_n$. Soient $g \in G$ et $x \in F$, alors pour tout $h \in H$, on a $h.(gx) = g(g^{-1}hg).x$. Or H est distingué donc $g^{-1}hg \in H$, puis $h.(gx) = \lambda_{g^{-1}hg}x$. Donc $G(F) \subset F$.

On en déduit que H est inclus dans $\mathbb{U}_n$, donc est fini. Comme H est connexe, il s'en suit que $H = \{I_n\}$, ce qui contredit la minimalité de m. □

Remarque. Voir [CL05].

2 Décomposition de Dunford effective

Leçons concernées

- 124 - Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
- 126 - Endomorphismes diagonalisables en dimension finie.
- 128 - Endomorphismes trigonalisables. Endomorphismes nilpotents.
- 129 - Algèbre des polynômes d'un endomorphisme en dimension finie. Applications.
- 224 - Comportement asymptotique de suites numériques. Rapidité de convergence. Exemples.
- 226 - Comportement d'une suite réelle ou vectorielle définie par une itération $u_{n+1} = f(u_n)$. Exemples.
- 232 - Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.

Soit $A \in \mathcal{M}_N(\mathbb{C})$. Le but est de trouver sa décomposition de Dunford : $A = D + N$. Si on note

$$Q(X) = \prod_{\lambda \in Spec(A)} X - \lambda,$$

on remarque que D est un zéro du polynôme $Q(X)$ dans $\mathbb{C}[A]$. L'idée est alors de trouver D par la méthode de Newton.

Remarque. Le polynôme $Q(X)$ est calculable car

$$Q(X) = \frac{\chi_A(X)}{pgcd(\chi_A(X), \chi_A'(X))}.$$

Théorème. On définit la suite

$$A_0 = A \text{ et } \forall n \in \mathbb{N}, A_{n+1} = A_n - \frac{Q(A_n)}{Q'(A_n)}.$$

Alors la suite $(A_n)_{n\in\mathbb{N}}$ est bien définie et stationne à D.

Démonstration. Montrons par récurrence sur $n \in \mathbb{N}$ que $Q(A_n)$ est inversible et que $Q(A_n) \in Q(A)^{2^n}.\mathbb{C}[A]$. On remarque d'abord que $Q(A)$ est nilpotent car $\chi_A(X)|Q(X)^r$ pour r assez grand ($r = N$ par exemple).

Pour $n = 1$, la propriété est claire.

Supposons le résultat vrai au rang n. Alors le terme A_{N+1} est bien défini et on a

$$A_{n+1} - A_n \in Q(A_N).\mathbb{C}[A].$$

Donc $A_{n+1} - A_n$ est nilpotent. D'autre part, comme $Q'(A_{n+1}) - Q'(A_n) \in (A_{n+1} - A_n).\mathbb{C}[A]$ on en déduit que $Q'(A_{n+1}) - Q'(A_n)$ est nilpotent. Par hypothèse récurrence $Q'(A_n)$ est inversible, ce qui implique que $Q'(A_{n+1})$ est inversible (la somme d'un nilpotent et d'un inversible est inversible). Par formule de Taylor, il existe $R(X, H) \in \mathbb{C}[X, H]$ tel que

$$Q(X + H) = Q(X) + Q'(X)H + H^2R(X, H).$$

On en déduit que

$$Q(A_{n+1}) = Q\left(A_n - \frac{Q(A_n)}{Q'(A_n)}\right) \in Q(A_n)^2.\mathbb{C}[X],$$

puis que $Q(A_{n+1}) \in Q(A)^{2^{n+1}}.\mathbb{C}[A]$. Ce qui prouve la propriété au rang $n + 1$.

On en déduit que $Q(A_n) = 0$ pour n tel que $2^n \geq N$, et que $(A_n)_{n\in\mathbb{N}}$ stationne. On note $D = A_{n_0}$ sa limite. Comme $Q(X)$ est simplement scindé, la matrice D est diagonalisable. On pose $N = A - D$. Comme

$$N = A_0 - A_{n_0} = \sum_{n=1}^{n_0} A_{n-1} - A_n = \sum_{n=1}^{n_0} \frac{Q(A_{n-1})}{Q'(A_{n-1})} \in Q(A).\mathbb{C}[A],$$

on en déduit que N est nilpotent. □

Remarque. Voir [[RBB06], Chap. 3, Pb 3.1]

3 Théorème de l'amitié

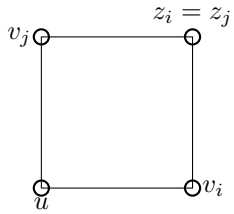
Leçons concernées

- 124 - Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
- 126 - Endomorphismes diagonalisables en dimension finie.
- 130 - Matrices symétriques réelles, matrices hermitiennes.
- 145 - Méthodes combinatoires, problèmes de dénombrement.

Théorème. Soit G un graphe à n sommets tel que toute paire de sommets admet exactement un sommet adjacent commun. Alors il existe un sommet adjacent à tous les autres.

Démonstration. On raisonne par l'absurde. Supposons qu'aucun sommet ne soit adjacent à tous les autres.

Montrons que tous les sommets ont le même degré (c'est-à-dire même nombre de voisins). Soit $u \in G$, k son degré et $(v_1, \dots, v_k)$ ses voisins. Soit $w \in G - \{u\}$ qui n'est adjacent à u. Pour $i \in [1, k]$, on note z_i le voisin commun de w et v_i. Alors on a $z_i \neq z_j$ si $i \neq j$, car sinon $z_i = z_j$ et u auraient v_i et v_j pour voisin commun.



Donc w a au moins k voisins, et par symétrie des rôles, $\deg w = \deg u$. On a donc montrer que deux sommets non-adjacents ont même degré. On note x le sommet commun à u et v. Pour $y \in G - \{u, v, x\}$, soit u soit v n'est pas voisin de y, donc $\deg y = k$. Donc $\deg y = k$ pour tout $z \in G - \{x\}$, et comme x n'est pas voisin de tous les sommets on a aussi $\deg x = k$.

On note $A = [a_{i,j}]$ la matrice d'incidence de G :

$$\forall i, j \in [1, n], a_{i,j} = \begin{cases} 1 & \text{si i et j sont voisins} \\ 0 & \text{sinon} \end{cases}.$$

On note $(b_{i,j})_{i,j}$ les coefficients de A^2. On a alors

$$\forall i \in [1, n], b_{i,i} = \sum_{k=1}^{n} a_{i,k}^2 = k,$$

$$\forall i, j \in [1, n], b_{i,j} = \sum_{k=1}^{n} \underbrace{b_{i,k} b_{k,j}}_{=0 \text{ si j non voisin}} = 1.$$

Donc si on note $U = [1] \in \mathcal{M}_n(\mathbb{R})$ la matrice avec que des 1, on a

$$A^2 + (1 - k) I_n = U.$$

On note $u = {}^t[1, \dots, 1] \in \mathbb{R}^n$. Comme $Au = ku$ et $Uu = nu$, on en déduit que $k^2 - k + 1 = n$. La matrice U a pour valeur propre n avec multiplicité 1 et 0 avec multiplicité $n - 1$, donc la valeur propre k est de multiplicité 1 (pour A) et les autres valeurs propres λ de A vérifient $\lambda^2 - k + 1 = 0$. On note s la multiplicité de $\sqrt{k-1}$ et t la multiplicité de $-\sqrt{k-1}$. Comme $Tr(A) = 0$, on en déduit que $(s - t)\sqrt{k-1} + k = 0$. En élevant au carré on en déduit que $k - 1$ divise $k^2 = (k-1)^2 + 2(k-1) + 1$, donc $k - 1 = 1$, ce qui donne $k = 2$ puis $n = 3$. On vérifie qu'il n'y a qu'un seul graphe à 3 sommets vérifiant les hypothèses. □

Remarque. Voir [AZ03].

4 Critère de nilpotence

Références [BMP, Chap 4, Ex 4.17]

Leçons concernées
– ? ? ?

Préliminaires

Théorème

Théorème. Soient k un corps clos de caractéristique nulle et E un k-espace vectoriel de dimension finie et $G \subset F$ deux sous-espaces vectoriels de $L(E)$. On note T le sous-ensemble de $GL(E)$ défini par

$$T = \Big\{ M \in L(E) : \forall f \in F, [M, f] \subset G \Big\}.$$

Soit $M \in T$ tel que $\forall N \in T, Tr(MN) = 0$. Alors M est nilpotent.

Démonstration. Comme k est clos, il existe $(e_i)_{i\in[1,n]}$ une base de jordanisation de M. On a alors pour tout $i \in [1, n]$, on a $Me_i = \lambda_i e_i$, avec $(\lambda_i)_{i\in[1,n]}$ les valeurs propres de M. Il faut montrer que les valeurs propres de u sont nulles.

On note H le sous-$\mathbb{Q}$-espace vectoriel $H = vect_{\mathbb{Q}}(\lambda_1, \dots, \lambda_n)$ de k. Montrons que $L_{\mathbb{Q}}(H, \mathbb{Q}) = 0$, ce qui montrera que $H = 0$ puis que M est nilpotent. Soit $\phi \in L_{\mathbb{Q}}(H, \mathbb{Q})$. On pose

$$N = \sum_{i=1}^{n} \phi(\lambda_i) e_i.e_i^* \in L(E).$$

Montrons que $N \in T$. Il faut montrer que $[N, F] = ad_N(F)$ est inclus dans G. Par hypothèse $ad_M(F) \subset G$, et comme $G \subset F$, on en déduit par récurrence que

$$\forall k \geq 1, ad_M^k(F) \subset G.$$

On aura $ad_N(F) \subset G$, en montrant que $ad_N = P(ad_M)$, avec $val(P) \geq 1$. [A completer].

Donc $N \in T$ et par hypothèse sur M, on a

$$0 = Tr(MN) = \sum_{i=1}^{n} \phi(\lambda_i) Tr(Me_i.e_i^*) = \sum_{i=1}^{n} \phi(\lambda_i)\lambda_i.$$

En appliuqnt ϕ, on en déduit que $\sum_{i=1}^{n} \phi(\lambda_i)^2 = 0$. Comme les $(\phi(\lambda_i))_{i\in[1,n]}$ sont dans $\mathbb{Q}$, on en déduit qu'ils sont tous nulles puis que ϕ est nulle. Ce qui achève la preuve. □

5 Déterminant de Cauchy et théorème de Müntz

Leçons concernées

- 115 - Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.
- 123 - Déterminant. Exemples et applications.
- 148 - Formes quadratiques réelles. Exemples et applications.

Préliminaires

Proposition (Déterminant de Gram)**.** ...

Proposition (Déterminant de Cauchy)**.** ...

Proposition (Produit infini)**.** Soient $(u_n)_{n\in\mathbb{N}}$ une suite de réells dans $]0,1[$. Alors

$$\sum_{n=1}^{+\infty} u_n < +\infty \iff \lim_{N\to+\infty} \prod_{n=1}^{N} 1 - un \text{ converge dans } \mathbb{R}_{>}0,$$

$$\sum_{n=1}^{+\infty} u_n + +\infty \iff \lim_{N\to+\infty} \prod_{n=1}^{N} 1 - un = 0.$$

Théorème de Müntz

Théorème. On considère l'espace $L^2([0,1])$. Soit $(\alpha_i)_{i\in\mathbb{N}}$ une suite de $\mathbb{R}_+$ tendant vers $+\infty$. Alors la famille $(X^{\alpha_i})_{i\in\mathbb{N}}$ est dense dans $L^2([0,1])$ si et seulement si $\sum_{i=0}^{+\infty} \frac{1}{\alpha_i} = +\infty$.

Démonstration. .[A completer] □

Remarque. Voir [Gou94b].

6 Enveloppe convexe du groupe orthogonal

Leçons concernées

- 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.
- 132 - Formes linéaires et hyperplans en dimension finie. Exemples et applications.
- 137 - Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.

Préliminaire

Théorème (Hahn-Banach)**.** Soit F un convexe fermé et C un convexe compact de $\mathbb{R}^n$. Alors il existe une forme linéaire ϕ et une constante c telle que

$$\sup_{x\in F} < \phi(c) < inf_{y\in C}\phi(y).$$

Proposition. Soient A une partie de $\mathbb{R}^n$ et $x \in \mathbb{R}^n$. Alors on a

$$x \in \overline{Conv(A)} \iff \forall \phi \in L(\mathbb{R}^n, \mathbb{R}), \phi(x) \leq sup_{y\in A}\phi(y).$$

Démonstration. Supposons que $x \in \overline{Conv(A)}$. Soit $\phi \in L(\mathbb{R}^n, \mathbb{R})$. On prend une suite $(x_n)_{n\in\mathbb{N}}$ de $Conv(A)$ convergeant vers x. On a alors

$$\forall n \in \mathbb{N}, \phi(x_n) \leq sup_{y\in Conv(A)}\phi(y).$$

Or on a $sup_{y\in Conv(A)}\phi(y) = sup_{y\in A}\phi(y)$ [exercice], et en passant à la limite, on en déduit le résultat.

Réciproquement, si $x \notin \overline{Conv(A)}$, alors par théorème de Hahn-Banach, il existe ϕ et c tel que $sup_{y\in Conv(A)} < c < \phi(x)$. □

Proposition. Toute forme linéaire de $\mathcal{M}_n(\mathbb{R})$ est du type $Tr(A.)$.

Théorème

Théorème. Soit $n \in \mathbb{N}^*$. On munit $\mathcal{M}_n(\mathbb{R})$ de la norme subordonnée à la norme 2. Alors l'enveloppe convexe de la boule unité est $O_n(\mathbb{R})$. De plus l'ensemble des points extrémaux de $O_n(\mathbb{R})$ est exactement $O_n(\mathbb{R})$.

Démonstration. On a clairement $Conv(O_n(\mathbb{R})) \subset \bar{B}_{\mathcal{M}_n(\mathbb{R})}(0,1)$. Réciproquement, soit $X \in \bar{B}_{\mathcal{M}_n(\mathbb{R})}(0,1)$ et $A \in \mathcal{M}_n(\mathbb{R})$. Il s'agit de montrer que

$$Tr(AX) \leq sup_{Y\in O_n(\mathbb{R})}Tr(AY).$$

On considère $A = SO$ la décomposition polaire de A. On a alors

$$sup_{Y\in O_n(\mathbb{R})}Tr(AY) = sup_{Y\in O_n(\mathbb{R})}Tr(SY) \geq Tr(S).$$

On prend $(e_i)_{i\in[1,n]}$ une base orthonormée de diagonalisation de S. On a alors

$$Tr(AX) = Tr(SOX) = \sum_{i=1}^n \langle e_i, SOX.e_i\rangle = \sum_{i=1}^n \langle S.e_i, OX.e_i\rangle.$$

Par Cauchy-Schwarz et le fait $\|M\|_2 \leq 1$, on a

$$\langle S.e_i, OX.e_i\rangle \leq \|S.e_i\|.\|OM.e_i\| \leq \|S.e_i\|.$$

Or comme S est positif et que $(e_i)_{n\in[1,n]}$ est une base orthonormée adapté, on a

$$Tr(AX) \leq \sum_{i=1}^n \|S.e_i\| = Tr(S).$$

Pour les points extrémaux : soient $X \in O_n(\mathbb{R})$ et $2X = A + B$ avec $A, B \in B_{\mathcal{M}_n(\mathbb{R})}(0,1)$. On a alors pour tout $x \in \mathbb{R}^n$:

$$2\|x\|_2 = \|2X.x\|_2 = \|Ax + Bx\|_2 \leq \|Ax\| + \|Bx\| \leq 2\|x\|.$$

Donc on a égalité les deux inégalités : la première égalité implique que (Ax, Bx) est positivement liée et la deuxième implique $\|Ax\| = \|x\|$ et $\|Bx\| = \|x\|$, ce qui donne $Ax = Bx$, puis $Xx = Ax = Bx$ pour tout $x \in \mathbb{R}^n$, soit $X = A = B$.

Réciproquement soit $X = OS \in B_{\mathcal{M}_n(\mathbb{R})}(0,1)$ tel que $S \neq Id$. Il faut montrer que X n'est pas extrémal. On rappelle que $\|X_2\| = \sqrt{\rho({}^tXX)} = \rho(S)$. Supposons le contraire. Quitte à changer la base on peut supposer que $S = diag(d_1, \ldots, d_n)$, avec $d_1 \neq 1$. On prend $r > 0$ tel que $d_1 - r > 0$ et $d_1 + r < 1$. On a alors $S2^{-1}(S_1 + S_2)$, avec $S_1 = diag(d_1 + r, d_2 \ldots, d_n)$ et $S_2 = diag(d_1 - r, d_2 \ldots, d_n)$, ce qui donne $2X = (S_1O + S_2O)$, avec $S_1O, S_2O \in B_{\mathcal{M}_n(\mathbb{R})}(0, 1.$ □

7 Endomorphismes semi-simples

Leçons concernées
- 111 - Anneaux principaux. Applications.
- 124 - Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
- 125 - Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.
- 126 - Endomorphismes diagonalisables en dimension finie.
- 129 - Algèbre des polynômes d'un endomorphisme en dimension finie. Applications.

Définition. Un endomorphisme est dit *semi-simple* si tout sous-espace stable admet un supplémentaire stable.

Théorème. Un endomorphisme est semi-simple si et seulement si son polynôme minimal est sans facteur carré.

Démonstration. Soit f un endomorphisme et $\mu_f(X)$ son polynôme minimal.

Supposons que f est semi simple. Soit $P(X)$ un diviseur irréductible de μ_f et $Q = P(X)^{-1}\mu_f(X)$. Comme $\ker P(f)$ est stable par f, il admet un supplémentaire que l'on note F.

On a $Q = \mu_{f_{|F}}$: en effet, comme $Q(f).P(f) = 0$, on a $Q(f)(F) \subset \ker P(f)$, et comme $Q(f)(F) \subset F$, on a donc $Q(f)(F) = 0$ puis $\mu_{f_{|F}}|Q$. Réciproquement le polynôme $\mu_{f_{|F}}P$ annule f donc $\mu_f = PQ|\mu_{f_{|F}}P$, $\mu_f|Q$.

On a $\mu_f = pgcd(\mu_{f_{|\ker P}}, \mu_{f_{|\ker P}}) = pgcd(P, Q)$ et $\mu_f = PQ$, d'où $pgcd(P, Q) = 1$.

Réciproqueemnt, si μ_f est sans facteurs carrés. On note $(P_i(X))_{i\in[1,p]}$ les facteurs irréductibles de $\mu_f(X)$. On a $E = \bigoplus_{i=1}^{p} \ker P_i(f)$ et $\mu_{f_{|\ker P_i(f)}} = P_i$.

Lemme. Si F est un sous-espace stable par f et si $(E_i)_{i\in[1,r]}$ sont les sous-espaces caractéristiques de f, alors

$$F = \bigoplus_{i=1}^{r} F \cap E_i.$$

.

Démonstration du lemme. La somme est clairement directe et on a $\bigoplus_{i=1}^{r} F \cap E_i \subset F$. Pour l'inclusion récirpoque : soit $x \in F$ décomposer en $x = x_1 + \cdots + x_r \in \bigoplus_{i=1}^{r} E_i$. Il sagit de montrer que $x_i \in F$ pour tout $i \in [1, r]$. Pour $i \in [1, r]$, on a $x_i = \pi_i(x)$, avec π_i le projecteur sur E_i. Comme p_i est polynomiale en f et que F est stable, on en déduit que $x_i \in F$. □

Il suffit alors de montrer de le lemme suivant.

Lemme. Si μ_f est irréductible, alors f est semi-simple.

Démonstration du lemme. Soit F sous-espace stable par F différent de E et $\{0\}$. Soit $x \in E \setminus F$, alors son polynôme minimal est $\mu_f(X)$. On note E_x le sous-espace cyclique engendré par x. Montrons que E_x est en somme direct avec F. Soit $P.x \in F$. Si μ_f ne divise pas P, alors il existe $Q(X)$ tel que $Q(X)P(X) = 1 \mod \mu_f(X)$, donc $x = QP.x \in F$ ce qui contredit $x \notin F$. Donc $E_x \cap F = 0$. Par récurrence on construit $x_1, \ldots, x_k$ tels que $E = F \oplus E_{x_1} \cdots \oplus E_{x_k}$. □

Ce qui achève la preuve du théorème. □

Corollaire. Si k est parfait, alors f est semi-simple si et seulement si f est diagonalisable dans $\overline{k}$.

Remarque. Voir [FGN, Algèbre, Tome 2, p. 122, ? ? ?], [[Gou94a], Chapitre 4, Probleme 18 (19 dans la seconde edition)], [[BMP04], Chap 4, Ex 4.23 et Chap 6, Ex 6.8]

8 Décomposition d'Iwasawa

Leçons concernées
- 131 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
- 133 - Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).
- 135 - Isométries d'un espace affine euclidien de dimension finie. Forme réduite. Applications en dimensions 2 et 3.
- 148 - Formes quadratiques réelles. Exemples et applications.

Théorème. Soit $n \in \mathbb{N}^*$. On note
- $\mathcal{K}$ l'ensembles des matrices orthogonales de $M_n(\mathbb{R})$.
- $\mathcal{A}$ l'ensembles des matrices diagonales à coefficients strictement positives.
- $\mathcal{N}$ L'ensembles des matrices triangulaires supérieures unitpotents.

Alors l'application suivante est un C^∞-difféomorphisme

$$\begin{array}{rccc} \Phi : & K \times A \times N & \longrightarrow & GL_n(\mathbb{R}) \\ & (k,a,n) & \longmapsto & kan \end{array}.$$

Démonstration. • Définition de la bijection réciproque. Soit $(b_{i\in[1,n]})$ la base canonique de $\mathbb{R}^n$. On définit l'application $\Phi : GL_n(\mathbb{R}) \to \mathcal{K} \times \mathcal{A} \times \mathcal{N}$ de la façon suivante : soit $M \in GL_n(\mathbb{R})$. On note
- $(e_i)_{i\in[1,n]}$ la famille de vecteurs telle que $Mat_b(e_1, \dots, e_n) = M$.
- (f_i) l'orthogonalisé de Gramm-Schmidt de $(e_i)_{i\in[1,n]}$.
- $(a_i)_{i\in[1,n]}$ la famille de réels $a_i = \|f_i\|$.
- (u_i) l'orthonormalisé de Gramm-Schmidt de $(e_i)_{i\in[1,n]}$, c'est-à-dire que $u_i = a_i^{-1} f_i$.

On pose alors $\Phi(M) = (K_M, A_M, N_M)$, avec

$$K_M = Mat_b(u_1, \dots, u_n),\ A_M = diag(a_1, \dots, q_n) \text{ et } N_M = Mat_f e_1, \dots, e_n.$$

On a évidamment $K_M \in \mathcal{K}$, $A_M \in \mathcal{A}$ et défintion de l'orthogonalisé de Gramm-Schmidt on a $N_M \in \mathcal{N}$.

• Montrons que $\Psi = \Phi^{-1}$. Soit $M \in GL_n(\mathbb{R})$. On reprend les notations ci-dessus. On a

$$K_M A_M = Mat_b(u_1, \dots, u_n) diag(a_1, \dots a_n) = Mat_b(a_1 u_1, \dots, a_n u_n) = Mat_b(f_1, \dots, f_n),$$

d'où

$$K_M A_M N_M = Mat_b(f_1, \dots, f_n) Mat_f(e_1, \dots, e_n) = Mat_b(e_1, \dots, e_n).$$

Donc $\Phi \circ \Psi(M) = M$.

Réciproqument soit $(K, A, N) \in K_M, A_M, N_M$. On note
- $M = \Phi(K, A, N) = K, A, N$.
- $(u_i)_{i\in[1,n]}$ la famille de vecteurs telle que $Mat_b(u_1, \dots, u_n) = K$.
- $(a_i)_{i\in[1,n]}$ les coefficients diagonaux de A.
- $(f_i)_{i\in[1,n]}$ la famille de vecteurs telle que $f_i = a_i u_i$.
- $(e_i)_{i\in[1,n]}$ la famille de vecteurs telle que $Mat_f(e_1, \dots, e_n) = N$.

De la même façon que ci-dessu on a

$$M = Mat_b(u_1, \dots, u_n) diag(a_1, \dots a_n) at_f(e_1, \dots, e_n) = Mat_b(e_1, \dots, e_n).$$

Comme K est orthogonale, la famille $(u_i)_{i\in[1,n]}$ est est famille orthonormée, la famille $(f_i)_{i\in[1,n]}$ est une famille orthogonale et on a $a_i = \|f_i\|$. Comme $Mat_f(e_1, \dots, e_n) = N$ est triangulaire supérieur à diagonale égale à 1, on en déduit que $(f_i)_{i\in[1,n]}$ est l'orthogonalisé de Gramm-Schmidt de $(e_i)_{i\in[1,n]}$. D'après la définition de (K_M, A_M, N_M), on a $(K_M, A_M, N_M) = (K, A, N)$.

Ce qui prouve que $\Psi = \Phi^{-1}$.

• Il reste à montrer que Φ et Ψ sont C^∞. La fonction Φ est C^∞ car multilinéaire. Avec les notations ci-dessus, pour $M \in GL_n(\mathbb{R})$, on a

$$\begin{array}{rcl} f_1 & = & e_1 \\ f_2 & = & e_2 - \frac{\langle f_1, e_2\rangle}{\|f_1\|^2} f_1 \\ & \dots & \\ f_n & = & e_n - \frac{\langle f_1, e_n\rangle}{\|f_1\|^2} f_1 - \dots - \frac{\langle f_{n-1}, e_n\rangle}{\|f_{n-1}\|^2} f_{n-1}. \end{array}$$

Ce qui permet de montrer par récurrence sur $k \in [1, n]$ que $GL_n(\mathbb{R}) \to \mathbb{R}^n, M \mapsto f_k$ est C^∞. Donc l'application

$$\begin{array}{ccc} GL_n(\mathbb{R}) & \longrightarrow & GL_n(\mathbb{R}^n) \\ M & \longmapsto & Mat_b(f_1, \ldots, f_n) \end{array} ,$$

et comme on a $N_M = Mat_b(f_1, \ldots, f_n)^{-1} Mat_b(e_1, \ldots, e_n)$, on en déduit que l'application

$$\begin{array}{ccc} GL_n(\mathbb{R}) & \longrightarrow & \mathcal{N} \\ M & \longmapsto & N_M \end{array} ,$$

est C^∞. On montre de même que $M \mapsto A_M$ et $M \mapsto K_M$ sont C^∞. □

Remarque. Voir [MT86].

9 Le théorème de Frobenius-Zolotarev

Leçons concernées

- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 103 - Exemples de sous-groupes distingués et de groupes quotients. Applications.
- 104 - Groupes finis. Exemples et applications.
- 105 - Groupe des permutations d'un ensemble fini. Applications.
- 106 - Groupe linéaire d'un espace vectoriel de dimension finie et sous-groupes. Applications.
- 108 - Exemples de parties génératrices d'un groupe.
- 110 - Nombres premiers. Applications.
- 112 - Corps finis. Applications.
- 123 - Déterminant. Exemples et applications.

Théorème. Soit p un nombre premier impair et V un espace vectoriel de dimension n sur $\mathbb{F}_p$. Soit $u \in GL(V)$. Si $\varepsilon(u)$ désigne la signature de u en tant qu'élément de $\mathfrak{S}(V)$, alors

$$\varepsilon(u) = \left(\frac{\det u}{p}\right) = \det u^{(p-1)/2}.$$

Démonstration. On note $D(GL(V))$ le groupe dérivée de $GL(V)$. Alors comme $\{-1, 1\}$ est abélien, l'application signature se factorise dans $GL(V)/D(GL(V))$:

$$\varepsilon : GL(V)/D(GL(V)) \to \{-1, 1\}.$$

Lemme. $D(GL(V) = SL(V)$

Démonstration du lemme. On a clairement $D(GL(V) \subset SL(V)$. Pour l'autre inclusion il suffit de montrer qu'une transvection quelconque est un commutateur. Ce qui est le cas puisque

$$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & \\ & 2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1// & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ & 2 \end{pmatrix}.$$

(Celà vient du fait que toute les transvections sont conjugués et qu'en caractéristique différente de 2 le carré d'une transvection est une transvection). □

On en déduit que $GL(V)/D(GL(V)) \simeq \mathbb{F}_q^*$ via la bijection

$$\begin{array}{ccc} GL(V)/D(GL(V)) & \longrightarrow & \mathbb{F}_q^* \\ M \mod SL(V) & \longmapsto & \begin{pmatrix} \det M & & \\ & 1 & \\ & & \ddots \end{pmatrix} \end{array},$$

et que ε induit un morphisme $\varepsilon' : \mathbb{F}_p^* \to \{-1, 1\}$ tel que

$$\forall M \in GL(V), \varepsilon(M) = \varepsilon'(\det M).$$

Pour déontrer le théorème, il suffit de montrer que ε' est non trivial (puisque comme $\mathbb{F}_p^*$ est cyclique il y a q'un seul morphisme non triviale de $\mathbb{F}_p^*$ vers $\{-1, 1\}$). On prend une bijection entre V et $\mathbb{F}_q = \mathbb{F}_{p^n}$, et ω un générateur de $\mathbb{F}_q^*$. Alors la multiplication par ω est un cycle de taille $q-1$, donc est de signature -1. On en déduit que ε' est non trivial. □

Remarque. Voir [FGN, Algebre 1, 3.20], [BMP04].

10 Décomposition polaire

Leçons concernées
- 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.
- 127 - Exponentielle de matrices. Applications.
- 130 - Matrices symétriques réelles, matrices hermitiennes.

Théorème

Théorème (Racine carré)**.** L'application suivante est un C^∞-difféomorphisme

$$\begin{array}{rccc} \Phi : & H_n^{++}(\mathbb{C}) & \longrightarrow & H_n^{++}(\mathbb{C}) \\ & M & \longmapsto & M^2 \end{array}.$$

Sa bijection récirpoque est noté $M \mapsto \sqrt{M}$.

Démonstration. On définit l'application $\Psi : H_n^{++}(\mathbb{C}) \to H_n^{++}(\mathbb{C})$ de la façon suivante : pour $M \in H_n^{++}(\mathbb{C})$, on le décompose en

$$M = \sum_{\lambda \in Spec(M)} \lambda P_\lambda,$$

avec P_λ le projecteur sur le sous espace propre $\ker(M - \lambda)$. On pose alors

$$\Psi(M) = \sum_{\lambda \in Spec(M)} \sqrt{\lambda} P_\lambda.$$

On vérifie aisément que $\Psi \circ \Phi = \Phi \circ \Psi = Id$. Donc $\boxed{\Phi \text{ est bijective}}$.

Il reste à montrer que Φ est un difféomorphisme. Soit $M \in H_n^{++}(\mathbb{C})$. Alors on a

$$\forall H \in H_n(\mathbb{C}), D\Phi(M).H = MH + HM.$$

On en déduit que si $(e_j)_{j\in[1,n]}$ est base propre de M pour les valeurs propres $(\lambda_j)_{j\in[1,n]}$, alors la famille $(e_j e_k^*)_{j,k\in[1,n]}$ est base propre de $D\Phi(M)$ pour les valeurs propres $(\lambda_j + \lambda_k)_{j,k\in[1,n]}$. En particulier comme $\lambda_i > 0$ $(i \in [1, n])$, la valeur 0 n'est pas valeur propre de $D\Phi(M)$. Donc $D\Phi(M)$ est inversible. □

Théorème (Décomposition polaire)**.** L'application suivante est un C^∞-difféomorphisme

$$\begin{array}{rccc} f : & H_n^{++} \times U_n(\mathbb{C}) & \longrightarrow & GL_n(\mathbb{C}) \\ & (H, U) & \longmapsto & HU \end{array}.$$

Démonstration. On définit

$$\begin{array}{rccc} g : & GL_n(\mathbb{C}) & \longrightarrow & H_n^{++} \times U_n(\mathbb{C}) \\ & M & \longmapsto & (\sqrt{MM^*}, \sqrt{MM^*}^{-1} M) \end{array}.$$

Comme $MM^* \in H_n^{++}(\mathbb{C})$, $\sqrt{MM^*}^{-1}$ existe et $\sqrt{MM^*}^{-1} M \in U_n(\mathbb{C})$. Donc la fonction g est bien définie et est C^∞. On voit facilement que $g = f^{-1}$. □

Chapitre 4

Anneaux et corps

1 Algorithme de Berlekamp

Leçons concernées
- 112 - Corps finis. Applications.
- 116 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- ? ? ?

Soit $P \in \mathbb{F}_q[X]$. Le but de l'algorithme est de dire que P est irréductible ou de renvoyer un facteur Q non trivial de P. On réapplique alors l'algorithme sur Q et P/Q pour aois la décomposition en facteur irréductible de P.
(Étape 1) On calcule $pgcd(P, P')$.

Lemme. Si $P = \prod_{i=1}^{k} P_i^{\alpha_i}$ est la décomposition en facteur irréductible de P, alors

$$pgcd(P, P') = \prod_{p|\alpha_i} P_i^{\alpha_i} P_i^{\alpha_i} \cdot \prod_{p\nmid\alpha_i} P_i^{\alpha_i - 1} \ .$$

Démonstration. Soit $i \in [1, k]$. On note $P = P_i^{\alpha_i}.R$ avec R premier avec P_i. On alors

$$P' = \alpha_i P_i^{\alpha-1} P_i' R + P_i^{\alpha} R'.$$

Comme $\mathbb{F}_p$ est un corps parfait et que P_i est irréductible, on a $pgcd(P_i, P_i') = 1$. Donc

$$Q^{\alpha_i} || P' \text{ si } \alpha_i = 0 \mod p \text{ et } Q^{\alpha_i} || P' \text{ si } \alpha_i \neq 0 \mod p.$$

D'où le résultat. □

On en déduit que :
- Si $pgcd(P, P') = P$, alors il existe R (que l'on peut calculer en inversant le frobenius dans $\mathbb{F}_q$) tel que $R^p = P$. Et donc R est un facteur non trivial de P.
- Si $pgcd(P, P') \neq 1, P$, alors c'est un facteru non trivial de P.
- Si $pgcd(P, P') = 1$, alors P est sans facteur carré et on applique l'algorithme de Berlekamp suivant.

(Étape 2 [Algorithme de Berlekamp]) On calcule l'espace $E = \ker(f - Id)$ où

$$\begin{array}{rccc} f : & \mathbb{F}_p[X]/P & \longrightarrow & \mathbb{F}_p[X]/P \\ & Q \mod P & \longmapsto & (Q \mod P)^q \end{array} .$$

Lemme. $\dim_{\mathbb{F}_q} E =$ nombre de facteurs irréductibles de P.

Démonstration. il suffit d'appliquer le lemme chinois. □

On déduit que
- Si $\dim E = 1$, alors R est irréductible.
- Si $\dim E \geq 2$, alors on prend $Q \in E \setminus \mathbb{F}_q$. On cherche ensuite $\alpha \in \mathbb{F}_p$ tel que $pgcd(P, Q - \alpha) \neq 1, P$. Celà existe d'après le lemme suivant.

Lemme. On note $P = P_1 \dots P_r$ la décomposition en facteurs irréductibles de P et $\alpha_i = Q \mod P_i \in \mathbb{F}_q$. Alors

$$pgcd(P, Q - \alpha) = \prod_{i/\alpha_i = \alpha} P_i.$$

Démonstration. Clair. □

Un α qui convient est l'un des α_i et le fait que $Q \notin \mathbb{F}_q$ garantit que les $(\alpha_i)_{i \in [1,r]}$ ne sont pas tous égaux.

Remarque. Voir [Dem97] [[BMP04], Chap 6, Ex 5.36].

2 Dénombrement des solutions de $a_1n_1 + \cdots + a_mp_m = n$

Leçons concernées
- 114 - Anneau des séries formelles. Applications.
- 115 - Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.
- 145 - Méthodes combinatoires, problèmes de dénombrement.

Préliminaires

Lemme. Soit $m, n \in \mathbb{N}^*$. Alors $\mathbb{U}_m \cap U_n = \mathbb{U}_{pgcd(m,n)}$.

Démonstration. Si on note $d = pgcd(m, n)$, alors $\mathbb{U}_d \subset \mathbb{U}_m \cap U_n$. Comme $\mathbb{U}_m \cap U_n$ est un sous-groupe fini de $\mathbb{U}$ il existe $f \in \mathbb{N}^*$ tel que $\mathbb{U}_m \cap U_n = \mathbb{U}_f$. En remarquant que

$$e^{2i\pi/f} \in \mathbb{U}_n \iff f|n,$$

on en déduit que $e|d$ puis que $\mathbb{U}_e \subset \mathbb{U}_d$. □

Théorème

Théorème. Soient $\alpha_1, \ldots, \alpha_m$ des entiers stritement positifs premiers entre eux dans leur ensemble. Pour $n \in \mathbb{N}$, on note

$$p_n = Card\Big\{(x_1, \ldots, x_m) \in \mathbb{N}^m \mid \sum_{i=1}^m \alpha_i x_i = n\Big\}.$$

Alors

$$p_n \sim \frac{n^{m-1}}{\alpha_1 \cdots \alpha_m (m-1)}.$$

Démonstration. On note $F(T) = \sum_{n\in\mathbb{N}} p_n T^n$ la série génératrice de $(p_n)_{n\in\mathbb{N}}$. On remarque que l'on a

$$\begin{array}{rcl} p_n & = & \sum_{n_1+\cdots+n_m=n} 1(n_1 \in \alpha_1\mathbb{N}) \ldots 1(n_m \in \alpha_m\mathbb{N}) \\ & = & \big[1(n_1 \in \alpha_1\mathbb{N}) * \cdots * 1(n_m \in \alpha_m\mathbb{N})\big](n) \end{array}.$$

Donc $F(T) = \prod_{i=1}^m \sum_{n_i=0}^{+\infty} 1(n_i \in \alpha_i\mathbb{N}) T^{n_i}$, et comme $\sum_{n_i=0}^{+\infty} 1(n_i \in \alpha_i\mathbb{N}) T^{n_i} = \frac{1}{1-T^{\alpha_i}}$, on en déduit que

$$F(T) = \prod_{i=1}^m \frac{1}{1-T^{\alpha_i}}.$$

La décomposition en éléments simples de $F(T)$ est alors du type

$$F(T) = \sum_{(\zeta,k)\in S} \frac{A_\zeta^k}{(\zeta - T)^k},$$

avec $S = \bigcup_{i=1}^m \mathbb{U}_{\alpha_i} \times [1, m]$ et $A_\zeta^k \in \mathbb{C}$. La décomposition de $(\zeta - T)^{-k}$ en série formelle est

$$\frac{1}{(\zeta-T)^k} = \frac{1}{(k-1)!} \frac{d^{k-1}}{dT^k} \frac{1}{\zeta - T} = \frac{1}{(k-1)!} \frac{1}{\zeta^k} \sum_{n=0}^{+\infty} (n+1) \ldots (n+k-1)(T/\zeta)^n.$$

On en déduit que pour tout $n \in \mathbb{N}$

$$\begin{array}{rcl} p_n & = & \sum_{(\zeta,k)\in S} \frac{A_\zeta^k}{(k-1)!\zeta^{n+k}} (n+1) \ldots (n+k-1) \\ & = & \sum_{(\zeta,k)\in S} \frac{A_\zeta^k}{(k-1)!\zeta^{n+k}} n^{k-1} + o(n^{k-1}). \end{array}$$

Comme $\bigcap_{i=1}^m \mathbb{U}_{\alpha_i} = \mathbb{U}_{pgcd(\alpha_1,\ldots,\alpha_m)} = \{1\}$, on en déduit que 1 est le seul pôle d'ordre m et que les autres pôles sont d'ordre inférieur à $m - 1$, donc

$$p_n \sim \frac{A_1^m}{(k-1)!} n^{k-1}.$$

Comme A_1^m est la fraction $F(T).(1 - T)^m = \prod_{i=1}^m \frac{1}{1+T+\cdots+T^{\alpha_i-1}}$ évalué 1, on en déduit que $A_1^m = \frac{1}{\alpha_1\cdots\alpha_m}$. D'où

$$p_n \sim \frac{n^{-1}}{\alpha_1 \cdots \alpha_m (m-1)}.$$

□

Remarque.
- Voir [[CLF], Analyse 1, Ex 6.9], [[Gob96], Ex 9.2]
- Voir [FGN, Alg 1, Ex 1.4] pour le nombre de dérangement de $[1, n]$.

3 Factorialité de $\mathbb{A}[[X]]$

Leçons concernées
- 111 - Anneaux principaux. Applications.
- 114 - Anneau des séries formelles. Applications.

Préliminaires

Proposition (Critère de factorialité)**.** Si B est un anneau intègre noethérien tel que l'intersection de deux idéaux principaux est encore principal, alors B est factoriel.

Démonstration. L'existence d'une décomposition en irréductible vient du fait que B est noethérien (on utilise l'axiome du chois dépendant). Pour l'unicité il suffit de montrer que tout irréductible est premier.

Soient $a \in B$ irréductible et $b, c \in B$ tel que $a|bc$. Montrons que $a|b$ ou $a|c$. Par hypothèse il existe $p \in B$ tel que $(a) \cap (b) = (p)$. On peut alors écrire $p = \alpha b$ et $ab = up$, avec $\alpha, u \in B$. On en déduit que $a = \alpha u$. Comme a est irréductible, α ou u est inversible. Si α est inversible on en déduit que $p \sim a$ et que $a|b$. Si u est inversible, alors $(a) \cap (b) = (ab)$ et comme $bc \in (a) \cap (b)$, on en déduit que $a|c$. Donc a est premier. □

Proposition. Si $\mathbb{A}$ est noethérien alors, $\mathbb{A}[[X]]$ est noethérien.

Démonstration. .[A completer] □

Proposition (Lemme de Nakayama)**.** Soit $\mathbb{A}$ un anneau, I un idéal de A et M un A-module de type fini. On suppose que $M = I.M$. Alors il existe $\alpha \in A$ tel que $\alpha = 1 \mod I$ et $\alpha.M = 0$.

Démonstration. .[A completer] □

Théorème

Théorème. Si $\mathbb{A}$ est principal, alors $\mathbb{A}[[X]]$ est factoriel.

Démonstration. Soient $a, b \in \mathbb{A}[[X]]$ et $I = (a) \cap (b)$. Le but est de montrer que I est principal.

- 1er cas : $val(a) = val(b) = 0$. On considère l'application

$$\begin{array}{rccc} \Phi : & I & \longrightarrow & \mathbb{A} \\ & F(X) & \longmapsto & F(0) \end{array}$$

Son image est un idéal de l'anneau principal $\mathbb{A}$, donc il existe $c \in I$ tel que $\operatorname{Im}\Phi = c(0).\mathbb{A}$. On va montrer que $I = (c)$.

Lemme. On a $\ker\Phi = X.I$.

Démonstration du lemme. On évidemment $X.I \subset \ker\Phi$. Soit $F \in \ker\Phi$. On peut alors écrire $F = \alpha.a = \beta.b$, avec $val(\alpha), val(\beta) \geq 1$, car $val(a) = val(b) = 0$. On en déduit que $F \in (Xa) \cap (Xb) = X.I$. □

Lemme. On a $\frac{I}{(c)} = X.\frac{I}{(c)}$.

Démonstration du lemme. Soit $F \mod c \in I/c$. Il existe alors $u \in \mathbb{A}$ et $XH \in \ker\Phi = X.I$ tel que $F = uc + XH$, ce qui donne $F \mod c = X(H \mod c)$. □

Par le lemme de Nakayama il existe $\alpha(X) \in \mathbb{A}[[X]]$ tel que $\alpha.\frac{I}{(c)} = 0$ et $\alpha = 1 \mod X$. Comme $\alpha(X)$ est inversible, on en déduit que $\frac{I}{(c)} = 0$, soit $I = \mathbb{A}[[X]].c$.

- Cas général : si a et b sont de valuation quelconque, alors on écrit

$$a = X^m.a' \text{ et } b = X^n.b',$$

avec $val(a') = 0$ et $val(b') = 0$. D'après le premier cas il existe $c \in \mathbb{A}[[X]]$ tel que $(a') \cap (b') = (c)$.

Montrons que $(a) \cap (b) = (X^{\max(n,m)}.c)$: soit $F \in (a) \cap (b)$. Alors F s'écrit $F = G.X^n.a' = H.X^m.b'$. On suppose par exemple que $n \geq m$. Alors on a $val(F(X)) \geq n$ et puisque $val(b'(X)) = 0$, on a aussi $val(H(X).X^m) = val(F(X)) \geq n$. Donc

$$X^{-n}F(X) = G(X).a'(X) = X^{-n}.(H(X).X^m).b'(X) \in (a') \cap (b') = (c).$$

On en déduit que $F(X) \in (X^n.c)$. □

Remarque. – Voir [Sam61].
– Voir [[Cal06], Th 7.34], pour une autre preuve.

4 Théorème de Chevalley-Warning

Leçons concernées
- 112 - Corps finis. Applications.
- 118 - Exemples d'utilisation de la notion de dimension en algèbre et en géométrie.

Théorème. Soient $q = p^s$, $n \in \mathbb{N}$ et $(f_i)_{i\in[1,r]}$ une famille de polynôme non nuls de $\mathbb{F}_[X_1, \dots, X_n]$ telle que $\sum_{i=1}^r \deg f_i \leq n-1$ (c'est le degré total). On note $V = V(f_1, \dots, f_r) \subset \mathbb{F}_q^n$ la variété définie par la famille $(f_i)_{i\in[1,r]}$. Alors on a

$$\operatorname{Card} V = 0 \mod p.$$

Démonstration. On définit $P \in \mathbb{F}_q[X_1, \dots, X_n]$ par

$$P(X_1, \dots, X_n) = \prod_{i=1}^r (1 - f_i^{q-1}(X_1, \dots, X_n)).$$

Comme $f_i^{q-1}(x) = 0$ si $f_i(x) = 0$ et $f_i^{q-1}(x) = 1$ sinon, on en déduit que P est à valeur dans $\{0, 1\}$ et que $P(x) = 0$ si seulement si $x \in V$. D'où

$$\sum_{x\in\mathbb{F}_q^n} P(x) = \operatorname{Card} V \mod p.$$

D'après l'hypothèse $\sum_{i=1}^r \deg f_i \leq n-1$, on a $\deg P \leq (q-1)(n-1)$. On décompose P en monôme

$$P = \sum_\alpha a_\alpha X^\alpha,$$

avec $|\alpha| \leq (q-1)(n-1)$. On a alors

$$\sum_{x\in\mathbb{F}_q^n} P(x) = \sum_{x_1,\dots,x_n\in\mathbb{F}_q} \sum_{\alpha_1,\dots,\alpha_n} a_\alpha x_1^{\alpha_1} \dots x_n^{\alpha_n} = \sum_{\alpha_1,\dots,\alpha_n} a_\alpha \prod_{i=1}^n \sum_{x_i\in\mathbb{F}_q} x_i^{\alpha_i}.$$

Lemme. Soit $m \in \mathbb{N}$. On a

$$\sum_{x\in\mathbb{F}_q} x^m = \begin{cases} -1, & (si) m \geq 0 \text{ et } q-1|m, \\ 0, & \text{sinon.} \end{cases}.$$

En particulier si $m \in [0, q-2]$ alors $\sum_{x\in\mathbb{F}_q} x^m = 0$.

Démonstration du lemme. Si $m = 0$ c'est évident. Si $q-1|m$, alors par Fermat $x^m = 1$ si $x \neq 0$ et $x^m = 0$ si $x = 0$, doù $\sum_{x\in\mathbb{F}_q} x^m = q - 1 = -1$. Et si $q-1 \nmid m$, alors on prend y générateur de $\mathbb{F}_q^*$. Comme $y \mapsto yx$ est une bijection sur $\mathbb{F}_q^*$, on a :

$$\sum_{x\in\mathbb{F}_q} x^m = y^m \sum_{x\in\mathbb{F}_q} x^m.$$

Comme y est d'ordre $q-1$ et que $q-1 \nmid m$, on a donc $y^m \neq 0$, d'où $\sum_{x\in\mathbb{F}_q} x^m = 0$. □

Pour α tel que $\alpha_1 + \dots + \alpha_n \leq (q-1)(n-1)$, il existe $i \in [1, n]$ tel que $\alpha_i \leq q-2$, et donc $\prod_{i=1}^n \sum_{x_i\in\mathbb{F}_q} x_i^{\alpha_i}$. D'où $\sum_{x\in\mathbb{F}_q^n} P(x) = 0$. □

Remarque. Voir [[Ser70], p13].

5 Théorème de d'Alembert-Gauss

Leçons concernées
- 116 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- 118 - Exemples d'utilisation de la notion de dimension en algèbre et en géométrie.
- 203 - Utilisation de la notion de compacité.

Remarque. Voir [[Gou94a], Chapitre II problème 4] [[CL05], Alg. Corp., Th 2.3.4].

Théorème. Le corps $\mathbb{C}$ est algébriquement clos.

Preuve algébrique

On admettra seulement que les fonctions polynômiales de $\mathbb{R}$ vérifient le TVI. On a alors les daux faits suivants

Proposition.
- Tout polynôme réel de degré impaire admet une racine dans $\mathbb{R}$.
- Tout nombre positif admet une racine carré.

Démonstration du théorème. On commence par montrer que tout polynôme réel a une racine dans $\mathbb{C}$. Soit $P \in \mathbb{R}[X]$ de degré $d = 2^n m$ avec m impair. Montrons par récurrence sur n que P admet une racine complexe.

Si $n = 0$, alors d est impaire donc admet une racine réelle.

Soit $n \in \mathbb{N}^*$ et supposons que le résultat est vrai au rang $n-1$. On se fixe $\overline{\mathbb{R}}$ une clôture algébrique de $\mathbb{R}$ et une injection $\mathbb{C} \to \overline{\mathbb{R}}$ (si on ne veut pas utiliser l'axiome du choix on peut choisir une extension où P est scindé). On note $x_1, ..., x_d$ les racines de P dans $\overline{\mathbb{R}}$. Pour tout $t \in \mathbb{R}$, $i, j \in [1, d]$, on note

$$y_{i,j}(t) = x_i + x_j + c x_i x_j.$$

Lemme. Pour tout $t \in \mathbb{R}$, il existe $i_t, j_t \in [1, d]$ tels que $i_t < j_t$ $y_{i_t, j_t}(t) \in \mathbb{C}$.

Démonstration. On note

$$Q_t = \prod_{i<j} (X - y_{i,j(t)}).$$

Les coefficients de Q_t sont polynômials en les $(x_k)_{x \leq k}$ à coefficients dans $\mathbb{R}$ et sont invariants par permutations des (x_i). Donc les coefficients Q_t sont polynômials en les coefficients de P et donc Q est réel. Son degré est

$$\tfrac{d(d-1)}{2} = 2^{d-1} m(d-1).$$

Donc par hypothèse récurrence Q a une racine dans $\mathbb{C}$, c'est-à-dire que l'une des $y_{i,j(t)}$ est dans $\mathbb{C}$. □

Comme $\mathbb{R}$ est infini, il existe alors $s, t \in \mathbb{R}$ différents tel que $(i_s, j_s) = (i_t, j_t) = (i, j)$. Comme $x_i + x_j + s x_i . x_j$ et $x_i + x_j + t x_i . x_j$ sont dans $\mathbb{C}$, on en déduit que $x_i + x_j$ $x_i x_j$ sont dans $\mathbb{C}$.

Lemme. Tout nombre complexe est un carré.

Démonstration du lemme. Soit $z = x + iy \in \mathbb{C}$. On cherche $a + ib \in \mathbb{C}$ tel que $z = (a+ib)^2$, c'est-à-dire

$$\begin{cases} x = & a^2 - b^2 \\ y = & 2ab \end{cases}.$$

Celà implique

$$\begin{cases} x = & a^2 + (-b^2) \\ -\frac{y^2}{4} = & a^2(-b^2) \end{cases},$$

Le sytème suivant

$$\begin{cases} x = & \alpha + \beta \\ -\frac{y^2}{4} = & \alpha\beta \end{cases},$$

admet une solution car le discriminant $\Delta = x^2 + y^2$ est positif, et comme $\alpha\beta < 0$, quitte à échanger, on peut supposer $\alpha \geq 0$ et $\beta \leq 0$. Il existe alors $a, b \in \mathbb{R}$ tel que $x = a^2 - b^2$ et $y^2 = 4a^2b^2$, et quitte à changer le signe de b, on peut choisir (a, b) tel que $y = 2ab$. □

En conséquence tout polynôme du second degré de $\mathbb{C}$ admet une racine et on en déduit que x_i et x_j sont dans $\mathbb{C}$. Ce qui prouve que tout polynôme réel admet un carré.

Pour $P \in \mathbb{C}[X]$, $P\overline{P}$ est réel, donc admet une racine x dans $\mathbb{C}$. On a soit $P(x) = 0$, soit $\overline{P}(x) = 0$ auquel cas $P(\overline{x}) = 0$. Donc dans les deux cas $P(X)$ admet une racine dans $\mathbb{C}$. □

Preuve analytique

Soit $\in \mathbb{C}[X]$. Comme la fonction $z \mapsto |P(z)|$. est coersive, elle atteint son minimum en un point noté z_0.
Supposons que $|P(z_0)| > 0$. On écrit le développement limité

$$P(z_0 + h) = P(z_0)\left(1 + \alpha h + O(h^2)\right).$$

On note $\alpha = \rho e^{i\theta}$. Alors pour $r > 0$ on a

$$\begin{array}{rcl} |P(z_0 + re^{i(\pi-\theta)}| & = & |P(z_0)|\left(1 - \rho r + O(r^2)\right) \\ & \leq & |P(z_0)|\left(|1 - \rho r| + |O(r^2)|\right) \end{array}.$$

Il existe $r_0 \in [0, 1]$ tel que $|O(r_0^2)| < r_0/2$. ce qui donne

$$\begin{array}{rcl} |P(z_0 + re^{i(\pi-\theta)}| & = & |P(z_0)|\left(1 - \rho r + O(r^2)\right) \\ & = & |P(z_0)|\left(1 - \rho r_0/2\right) \\ & < & |P(z_0)| \end{array}.$$

ce qui contredit la minimalité de $|P(z_0)|$.

6 Entiers de Gauss et théorème des deux carrés

Leçons concernées
- 109 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 110 - Nombres premiers. Applications.
- 111 - Anneaux principaux. Applications.

Entiers de Gauss

Théorème. $\mathbb{Z}[i]$ est euclidien pour le stathme carré de la norme.

Démonstration. Soient $z, w \in \mathbb{Z}[i]$. Il existe $q \in \mathbb{Z}[i]$ tel que $r' = z/w - q$ soit de norme inférieure à $1/\sqrt{2}$. On a alors

$$z = qw + wr',$$

avec $N(wr') < N(w)$. □

Proposition. Les inversibles de $\mathbb{Z}[i]$ sont $+1, +i, -1, -i$.

Démonstration. Un élément est inversible si et seulement s'il est de norme 1. □

Proposition. Les irréductibles de $\mathbb{Z}[i]$ sont
- Les εp, avec $\varepsilon \in \mathbb{Z}[i]^\times$ et $p \in \mathbb{N}$ premier tel que $p = 2$ ou $p = -1 \mod 4$.
- Les entiers de Gauss de norme un nombre premier.

Démonstration. Si pour p premier, p est irréductible si et seulement si $\mathbb{Z}[i]/(p) = \mathbb{F}_p[X]/(X^2+1)$ est un corps c'est-à-dire que $p = 2$ ou $(-1)^{(p-1)/2} = -1$.

Si $N(z)$ est premier, alors z n'est pas décomposable (et z n'est pas dasn $\mathbb{Z}$).

Si z est irréductible. Alors $z\overline{z}$ est la décomposition en irréductible de $N(z)$ sur $\mathbb{Z}[i]$. Si $\prod_{i=1}^d p_i$ est la décomposition en nombre premiers de $N(\mathbb{Z})$ dans $\mathbb{Z}$, alors il y a au plus deux facteurs. S'il y a deux facteurs (p, q) alors z est égale à l'un (à multiplication par un inversible près) et $\overline{z}$ est égale à l'autre. Donc z est de type εp. □

Théorème des deux carrés

Théorème (Théorème des deux carrés)**.** Soit $n \in \mathbb{N}$. Alors n est somme de deux carrés si et seulement si :

Les puisances des nombres premiers congrues à 3[4] sont paires dans la décomposition de n.

Démonstration.

Lemme. Un nombre premier $p \geq 3$ est somme de deux carrés si et seulement si p est non-irréductible dans $\mathbb{Z}[i]$, c'est-à-dire congrue à $1 \mod 4$.

Démonstration. Un nombre premier p est somme de deux carré si et seulement si

$$\exists z \in \mathbb{Z}[i], z\overline{z} = p,$$

Si $p = z\overline{z}$, alors p n'est pas irréductible. Réciproquement, si p n'est pas irréductible, alors on écrit $p = zw$ avec z, w non inversible. Ce qui donne $p^2 = N(z)N(w)$ puis $p = N(z) = z\overline{z}$. □

Sit $n \in \mathbb{N}$. On décompose n en facteurs premiers dans $\mathbb{Z}$

$$n = p_1^{a_1} \dots p_s^{a_r} . q_1^{b_1} \dots q_s^{b_s},$$

avec $(p_i)_{i\in[1,r]}$ les nombres premiers qui sont somme de deux carrés et $(q_j)_{j\in[1,s]}$ ceux qui ne le sont pas. Pour $i \in [1, r]$ il existe $z \in \mathbb{Z}[i]$ irréductible tel que $p_i = z_i\overline{z_i}$. La décomposition de n en irréductible sur $\mathbb{Z}[i]$ est alors

$$n = z_1^{a_1} \dots z_r^{a_r} . \overline{z_1^{a_1} \dots z_r^{a_r}} . q_1^{b_1} \dots q_s^{b_s},$$

On voit alors que n s'écrit $z\overline{z}$ si et seulement si tous les $(b_j)_{j\in[1,s]}$ sont pairs. □

Remarque ([Com98] : Chapitre 11.6)**.** ,.

Théorème des deux carrés sans les entiers de Gauss

Voir [[Gou94a] : Chapitre 1, Sujet d'etude 3]

Théorème des quatre carrés

Voir [[Gou94a] : Chapitre 1, Sujet d'etude 4] ou [[CL05], Ex ?]

7 Théorème de Bezout faible projectif

Leçons concernées
- 117 - Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.
- 146 - Résultant de deux polynômes, applications à l'intersection de courbes ou de surfaces algébriques.

Préliminaires

Lemme. Soient $P(X), Q(X) \in k[x]$ de degré p et q.
- $Res_X(\lambda P(X), \mu Q(X)) = \lambda^q \mu^q Res(P, Q)$.
- $Res_X(P(\lambda X), Q(\lambda X)) = \lambda^{pq} Res_X(P(X), Q(X))$.

Démonstration. .[A completer] □

Lemme.
- Si $[a : b] \neq [a' : b']$, alors $aY - bX$ et $a'Y - b'X$ sont premiers entre eux.
- Soient $R(X, Y) \in k[X, Y]$ homogène et $[a : b] \in P^2(k)$ tel que $R(a, b) = 0$. Alors $aY - bX | R(X, Y)$.

(Ce sont les versions projectifs des théorèmes : si $P(a) = 0$, alors $X - a | P(X)$, et si $a \neq a'$, alors $X - a$ et $X - a'$ sont premiers entre eux)

Démonstration. Le premier point est évident. Pour le deuxième : on suppose par exemple que $b \neq 0$. On a alors $R(a/b, 1) = 0$, donc il existe $Q(T) \in k[T]$ tel que $R(T, 1) = (T - a/b)Q(T)$. Ce qui donne $R(X/Y, 1) = (X/Y - a/b)Q(X/Y)$ puis $bR(X, Y) = (bX - aY)Y^{\deg R - 1}Q(X/Y)$, avec $Y^{\deg R - 1}Q(X/Y) \in k[X, Y]$. □

théorème

Théorème. Soient k un corps infini et $P(X, Y, Z), Q(X, Y, Z)$ deux polynômes homogènes de degrés respectifs p et q. On suppose que $V(P, Q) := \{[x : y : z] \in P^2(k) : P(x, y, z) = Q(x, y, z) = 0\}$ est de cardinal $\geq pq + 1$, alors P et Q on un facteur commun non trivial (homogène).

Démonstration. Quitte à changer les variable, on suppose que . On note $R(X, Y) = Res_Z(P, Q)$. D'après le lemme R est homogène de degré $p \deg_Z Q + q \deg_Z P - \deg_Z P . \deg_Z Q \leq pq$ (le polynôme nul est homogène) : en effet, on a

$$\begin{aligned} R(\lambda X, \lambda Y) &= Res_Z(P(\lambda X, \lambda Y, Z), Q(\lambda X, \lambda Y, Z)) \\ &= Res_Z(\lambda^p P(X, Y, \lambda^{-1} Z), \lambda^q Q(X, Y, \lambda^{-1} Z)) \\ &= \lambda^{p \deg_Z Q + q \deg_Z P - \deg_Z P . \deg_Z} Res_Z(P(X, Y, Z), Q(X, Y, Z)) \end{aligned} .$$

On prend une partie S de $V(P, Q)$ à $pq + 1$ éléments. On considère l'ensemble des droites qui passent par deux points S. Comme k est infini, il existe un point M qui n'est sur aucune de ces droites (cf lemme sur les unions de sous-espace vectoriels). Quitte à appliquer une homographie (un élément de $PGL_3(k)$), on peut supposer que $M = [0 : 0 : 1]$.

Pour $[a : b : c] \in V(P, Q)$, on a $R(a, b) = 0$, car $P(a, b, Z)$ et $Q(a, b, Z)$ ont c pour racine commune. Donc $aY - bX | R(X, Y)$.

Soient $[a : b : c] \neq [a' : b' : c'] \in S$. Si $[a' : b'] = [a : b]$, alors les points $[a : b : c]$, $[a' : b' : c']$, $[0 : 0 : 1]$ seraient alignés, ce qui n'est pas le cas par choix de $M = [0 : 0 : 1]$.

Donc $R(X, Y)$ est divisible par $\prod_{[a:b:c] \in S}(aY - bX)$, ce qui implique $R(X, Y) = 0$ car $\deg R \leq pq$ et $\prod_{[a:b:c] \in V(P,Q)}(aY - bX) = pq$
Donc $P(X, Y, Z)$ et $Q(X, Y, Z)$ ont un facteur commun dans $k[X, Y][Z]$. □

Remarque.
- Ce développement a été proposé par Samuel Le Fourn.
- La preuve est peut-être plus simple dans le cas affine (les deux lemmes deviennent inutiles).

8 Probabilité pour que deux nombres soient premiers entre eux

Leçons concernées
- 110 - Nombres premiers. Applications.
- 145 - Méthodes combinatoires, problèmes de dénombrement.

Théorème. Pour $n \in \mathbb{N}$, on note

$$p_n = \frac{1}{n^2} \sharp\{(a,b) \in [1,n]^2 \mid pgcd(a,b) = 1\}.$$

Alors $\lim_{n\to+\infty} p_n = \frac{6}{\pi^2}$.

Démonstration. Soit $n \in \mathbb{N}$. On note A_n le nombre de couples de $[1,n]$ premiers entre-eux

$$A_n = \Big\{(a,b) \in [1,n]^2 \mid pgcd(a,b) = 1\Big\}.$$

On note $p_1, \dots, p_k$ les nombres premiers dans $[1,n]$, et pour $i \in [1,k]$, on note

$$U_k = \Big\{(a,b) \in [1,n]^2 \mid p_i | pgcd(a,b)\Big\}.$$

On a alors $A_k = {}^c\bigcup_{i=1}^k U_k$. Par fomule de la crible on a

$$\operatorname{Card}\bigcup_{i=1}^k U_k = \sum_{I\subset[1,k]} (-1)^(1 + \operatorname{Card} I) \operatorname{Card}\bigcap_{i\in I} U_i.$$

Or pour $I \subset [1,n]$, on note $d_I = \prod_{i\in I} p_i$, on a

$$\bigcap_{i\in I} U_i = (d_I.\mathbb{N} \cap [1,n]) \times (d_I.\mathbb{N} \cap [1,n]),$$

qui est de cardinal $E(n/d_I)^2$. On en déduit que

$$\begin{array}{rcl} \operatorname{Card}\bigcup_{i=1}^k U_k & = & -\sum_{I\subset[1,k]} \mu(d_I) E\left(\frac{n}{d_I}\right)^2 \\ & = & -\sum_{d=2}^n \mu(d) E\left(\frac{n}{d}\right)^2 \end{array}.$$

Comme $\operatorname{Card} A_n = n^2 - \operatorname{Card}\bigcup_{i=1}^k U_k$, on en déduit que

$$\boxed{\operatorname{Card} A_n = \sum_{d=1}^n \mu(d) E\left(\frac{n}{d}\right)^2}.$$

La proportion de couples de nombres premiers entre-eux dans $[1,n]$ est alors

$$r_n = \sum_{d=1}^n \frac{\mu(d)}{n^2} E\left(\frac{n}{d}\right)^2.$$

En dominant par le terme général par $1/d^2$, on en déduit que

$$\lim_{n\to+\infty} r_n = \sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2}.$$

En calculant on a

$$\begin{array}{rcl} \left(\sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2} \sum_{d=1}^{+\infty}\right)\left(\frac{\mu(d)}{d^2}\right) & = & \sum_{d,n=1}^{+\infty} \frac{\mu(d)}{(nd)^2} \\ & = & \sum_{d,p\geq 1, d|p} \frac{1}{p^2}\mu(d) \end{array}.$$

En utilisant le fait que $\sum_{d|p} \mu(d) = 1$ si $p = 1$ et 0 sinon, on en déduit que

$$\lim_{n\to+\infty} r_n = \zeta(2)^{-1} = \frac{6}{\pi^2}$$

□

Remarque. Voir [FGN, Alg 1, Ex 4.32].

9 Polynômes cyclotomiques

Leçons concernées
- 113 - Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
- 116 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Préliminaires

Théorème. Pour tout $n \in \mathbb{N}$, $\phi_n(X)$ est à coefficients entiers.

Démonstration. On raisonne par récurrence et on applique le lemme de Gauss à

$$X^n - 1 = \phi_n(X)\left(\prod_{d|n, d\neq n} \phi_d\right).$$

□

Lemme. Pour p un nombre premier ne divisant pas n, le polynôme $X^n - 1$ est sans facteurs carrés dans $\mathbb{F}_p[X]$.

Démonstration du lemme. Si p ne divise pas n, alors $(X^n - 1)' = nX^{n-1}$ est premier avec $X^n - 1$. □

Théorème

Théorème. Pour tout $n \in \mathbb{N}$, $\phi_n(X)$ est irréductible.

Démonstration. On note $P_0(X)$ le polynôme minimal de $e^{2i\pi/n}$. Montrons que toute les racines primitives $n$em de 1 sont racine de $P_0(X)$.

Lemme. Soit $P(X)$ un facteur irréductible unitaire de $\phi_n(X)$ dans $\mathbb{Q}[X]$ (aussi dans $\mathbb{Z}[X]$), x une racine de $P(X)$ (x est alors une racine primitive de l'unité) et p un nombre premier ne divisant pas n. Alors x^p est aussi racine de $P(X)$.

Démonstration du lemme. Comme x^p est aussi une racine primive de l'unité, x^p est racine de $\phi_n(X)$. Soit $Q(X)$ le polynôme minimal de x^p. Alors $Q(X)$ est dans $\mathbb{Z}[X]$ et est un facteur de $\phi_n(X)$. Comme x annule $Q(X^p)$ et que $P(X)$ est le polynôme minimal de x, on en déduit que $P(X)|Q(X^p)$. Donc dans $\mathbb{F}_p[X]$

$$P(X) \mod p | Q(X^p) \mod p = Q(X)^p \mod p.$$

On en déduit que $P(X) \mod p$ et $Q(X) \mod p$ admettent un facteur commun dans $\mathbb{F}_p[X]$. Si $P(X) \neq Q(X)$, alors $P(X)Q(X) \mod p | \phi_n(X) \mod p$, ce qui contredit le lemme précédent. □

Alors d'après le lemme, pour tout k entier premier avec n, le nombre $e^{2ik\pi/n}$ est racine de $P_0(X)$ et donc $P_0(X)$ contient toutes les racines primitives de l'unité. Donc $\phi_n(X) = P_0(X)$ est irréductible. □

Remarque. Voir [[Gou94a], Chap II Pb 9].

Preuve pour le cas $n = p$ premier

Proposition. Pour tout $p \in \mathbb{N}$ premier, $\phi_p(X)$ est irréductible.

Démonstration. Le polynôme

$$\phi_p(X) = \frac{X^p-1}{X-1} = \frac{(Y+1)^p-1}{Y} = \sum_{k=1}^{p} \binom{p}{k} Y^{k-1}$$

est irréductible par critère d'Eisenstein. □

10 Polynômes irréductibles sur les corps finis

Leçons concernées
- ? ? ?

Soit $q = p^N$ et K un corps de cardinal de q. Pour $n \in \mathbb{N}$, on note $I(K,n)$ l'ensemble des polynômes irréductibles unitaires de degré n de $k[X]$.

Théorème (Décomposition en irréductibles)**.** La décomposition de $X^{q^n} - X$ en irréductibles est

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

Démonstration. Si $d|n$, $P \in I(K,d)$. Alors le corps $K[T]/P(T)$ est de cardinal q^d, donc $x^{q^d} = x$ pour tout $x \in K[T]/P(T)$. Comme $x^{q^n} = (x^{q^{d\cdots}})^{q^d}$, on en déduit que $x^{q^n} = x$ puis que P divise $x^{q^n} - x$.

Réciproquement si T est un diviseur irréductible de $X^{q^n} - X$ de degré d. On note $n = qd + r$ la division euclidienne de n par d. Les polynômes $X^{q^d} - X$ et $X^{q^n} - X$ sont nuls sur $K[T]/P(T)$. Donc pout tout $x \in K[T]/Q(T)$, $x^{q^n} = x^{q^n} = \left((x^{q^{d\cdots}})^{q^d}\right)^{q^r}$, et on en déduit que $X^{q^r} - X$ est nuls sur $K[T]/P(T)$ de cardianal $q^d > q^r$. Donc $\deg(X^{q^r} - X) = 0$ puis $r = 0$.

Comme $pcgd(X^{q^n} - X, (X^{q^n} - X)') = pgcd(X^{q^n} - X, -1) = 1$, le polynôme $X^{q^n} - X$ est sans facteurs carrés, d'où le résultat. □

Théorème (Dénombrement)**.** On a
- Pour tout $n \in \mathbb{N}$, $q^n = \sum_{d|n} d|I(K,d)|$.
- Pour tout $n \in \mathbb{N}$, $I(K,n) \neq \emptyset$.
- Pour tout $n \in \mathbb{N}$, $I(K,n) = \frac{1}{n} \sum_{d|n} \mu_{n/d} q^d$.
- On a $|I(1,K)| = q$.
- Si $Caract(K) \neq 2$, $|I(2,K)| = \frac{q(q-1)}{2}$

Démonstration. Le premier point vient du théorème précédent. Le troisième point vient de la formule d'inversion de Möbius.

Pour le deuxième remarque d'abord que $q^d \geq dI(K,d)$. On en déduit alors que

$$nI(K,n) = q^n - \sum_{d|n, d<n} dI(K,d) \geq q^n - \sum_{0 \geq d<n} q^d > 0.$$

On a $I(1,K) = \{X - a | a \in K\}$, donc est de cardinal q. Si $Caract(K) \neq 2$, alors $I(2,K) = \{(X-a)^2 - b | a \in K, b \notin K^2\}$, donc est de cardinale $q.\frac{q-1}{2}$. □

Remarque. Voir [[Gou94a], Chap 2, Sujet d'étude 1].

11 Théorème de Kronecker

Leçons concernées
- ? ? ?

Théorème (Kronecker)**.** Soit $P \in \mathbb{Z}[X]$ irréductible tel que ses racines soient de module ≤ 1. Alors $P(X) = X$ ou $P(X)$ est un polynome cyclotomique.

Démonstration. Si $P(X) \neq X$, alors toutes ses racines $r_1, \dots, r_d$ sont non nulles. Comme le produit $r_1 \dots r_d$ est dans $\mathbb{Z}^*$, on en déduit que tous les r_i sont de module 1.

Montrons que l'un des r_i est racine $n$iem de l'unité, ce qui revient à dire que $\pi_k := (r_1^k - 1) \dots (r_d^k - 1)$ est nulle pour un certain k. Comme π_k est symétrique en les r_i, c'est donc un polynôme en les coefficients de $P(X)$. On en déduit que $\pi_k \in \mathbb{Z}$. Comme $|r_1^k - 1| \leq 2$, on a

$$|r_1^k - 1| = \frac{|\pi_k|}{|r_2^k - 1| \dots |r_d^k - 1|} \geq \frac{|\pi_k|}{2^{d-1}}.$$

Supposons que $\pi_k \neq 0$ pour tout k, alors $|r_1^k - 1| \geq 2^{1-d}$. Donc $r_1^{\mathbb{Z}}$ n'est pas dense dans le cercle unité, ce qui implique que r_1 est racine de l'unité.

On en déduit que $P(X)$ est le polynôme minimal d'une racine de l'unité, donc c'est un polynôme cyclotomique. □

Applications. Soit $B \in \mathcal{M}_n(\mathbb{Z})$ et $k \in \mathbb{N}_{\geq 2}$. On pose $A = I_N + kB$ et on suppose que A est d'ordre fini m. Alors si $k \leq 3$, on a $m = 1$ et si $k = 2$, on a $m = 1$ ou $m = 2$.

Démonstration. .[A completer]. □

Remarque.
- Remerciement à Samuel Le Fourn pour avoir trouver l'application.
- Voir [[Gou94a], Chap 1, Sujet d'étude 1], [FGN, Alg 1, Ex 5.28].

12 Théorème de Wedderburn

Leçons concernées
- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 112 - Corps finis. Applications.

Théorème (Wedderburn)**.** Tout corps fini est commutatif.

Démonstration. Soit K corps fini et Z son centre. On note $q = \sharp Z$ et $n = [K : Z]$. Pour $x \in K$ on note $C(x)$ son commutant et $d(x) = [C(x) : Z]$. On fait agir K^* sur lui-même par conjugaison et on note $Orb(x)$ l'orbite de x. On a alors

$$\sharp Orb(x) = \frac{\sharp K^*}{\sharp (C(x)-\{0\})} = \frac{q^n-1}{q^{d(x)-1}} = \prod_{d|n, d\nmid d(x)} \Phi_d(q).$$

D'autre part l'équation aux classes donne

$$\sharp K^* = \sharp Z^* + \sum_{x\in T} \sharp Orb(x),$$

où T est une famille de représentants de $K^* - Z^*$. L'équation précédente se réécrit

$$q^n - 1 = q - 1 + \sum_{x\in T} \frac{q^n-1}{q^{d(x)-1}}.$$

Or pour tout $x \in T$, on a $d(x) < n$ et $\Phi_n(q) | \frac{q^n-1}{q^{d(x)-1}}$. On en déduit que $\Phi_n(q)|q-1$. ce qui donne

$$q - 1 = |\Phi_n(q)| = \prod_{k\wedge n=1} |q - e^{2ik\pi/n}|.$$

Comme

$$\forall \zeta \in \mathbb{U}, \prod_{\zeta\in\mathbb{U}}, |q-\zeta| \geq dist(q, \mathbb{U}) = |q-1|,$$

avec égalité si et seulement si $\zeta = 1$, celà donne

$$q - 1 \geq \prod_{k\wedge n=1} |q - e^{2ik\pi/n}| \geq (q-1)^{\phi(n)} \geq q - 1.$$

On en déduit que $\forall k \wedge n = 1, e^{2ik\pi/n} = 1$, ce qui n'est possible que si $n = 1$.

□

Remarque. Voir [[Gou94a], Chap II Pb 10], [Per96].

13 Triplets Pythagoriciens et théorème de Fermat pour $n = 4$

Leçons concernées

- 109 - Anneaux Z/nZ. Applications.
- 110 - Nombres premiers. Applications.
- 111 - Anneaux principaux. Applications.

Triplets Pythagoriciens

Théorème. Soient $x, y, z \in \mathbb{N}^*$ vérifiant $x^2 + y^2 = z^2$. On suppose que (x, y, z) sont premiers entres eux globalement (et donc aussi deux-à-deux), alors il existe $u, v \in \mathbb{N}^*$ premiers entre eux tels que

$$\{x, y\} = \{2uv, u^2 - v^2\} \text{ et } z = u^2 + v^2.$$

Démonstration. Les nombres (x, y) ne peuvent pas tous les deux être impairs, car sinon

$$x^2 + y^2 \mod 4 = 1 + 1 \mod 4 = 2 \mod 4,$$

ce qui est absurde car $2 \mod 4$ n'est pas un carré. De plus (x, y) ne sont pas tous les deux pairs car sinon x, y et z seront divisibles par 2.

On suppose par exemple que x est pair et y impair. On en déduit que z est impair et que

$$\frac{x^2}{4} = \frac{z+y}{2}.\frac{z-y}{2}.$$

On note $d = pgcd\Big((z+y)/2, (z-y)/2\Big)$. Alors d divise $z + y$ et $z - y$ donc divise $z \wedge y = 1$. On en déduit que $(z + y)/2$ et $(z - y)/2$ sont premiers entre eux et comme leur produit est un carré, on en déduit que ce sont eux-même des carrés. Il suffit alors de prendre $u = \sqrt{(z + y)/2}$ et $v = \sqrt{(z - y)/2}$. □

Théorème de Fermat pour $n = 4$

Théorème. L'équation $x^4 + y^4 = z^4$ n'a pas de solutions dans $\mathbb{N}^*$.

Démonstration. On montre le résultat plus fort : $x^4 + y^4 = z^2$ n'a pas de solutions. Si ce n'est pas le cas, on choisit une solution (x, y, z) tel que z soit minimal. Les nombres (x, y, z) sont alors premiers entre eux. On en déduit que (x^2, y^2, z) est un triplet Pythagorien, donc il existe $u, v \in \mathbb{N}^*$ premiers entre eux tels que, quitte à inverser x et y :

$$x^2 = 2uv,\ y^2 = u^2 - v^2,\ z = u^2 + v^2.$$

On note $d = pgcd(y, u, v)$, alors d divise $2uv = x$ et $u^2 + v^2 = z$, donc $d = 1$. On en déduit de $y^2 = u^2 - v^2$ que (v, y, u) est un triplet Pythagoricien. Donc il existe $a, b \in \mathbb{N}^*$ tel que (on rappelle que y est impaire)

$$u = 2ab,\ y = a^2 - b^2,\ v = a^2 + b^2.$$

De $x^2 = 2uv$ en en déduit que $x^2/4 = ab(a^2 + b^2)$. Le triplet $(a, b, a^2 + b^2)$ sont premiers entre-eux deux-à-deux : en effet, (a, b) le sont par construction et si p est un nombre premier divisant a et $a^2 + b^2$, alors p divise leur différence b^2 et donc p divise $pcgd(a, b) = 1$. Comme leur produit $ab(a^2 + b^2) = x^2/4$ est un carré en on déduit que se sont chacun des carrés. En posant $x' = \sqrt{a}$, $y' = \sqrt{b}$ et $z' = \sqrt{a^2 + b^2}$, on obtient $z'^2 = x'^4 + y'^4$, avec $z' = \sqrt{v} < z$, ce qui contredit la minimalité de z. □

Remarque. Voir [[Com98], Chap 12.7]

14 Théorème de Dirichlet

Leçons concernées
- 109 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 110 - Nombres premiers. Applications.
- 113 - Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

Théorème (Forme faible)**.** Soit $m\mathbb{N}_{\geq 2}$. Alors il existe une infinité de nombres premiers congrues à 1 mod m.

Démonstration.

Lemme. Soient $m \in \mathbb{N}$ et $a\mathbb{N}$. Si p est un nombre premier divisant $\Phi_m(a)$, alors soit $p|m$ soit $p = 1 \mod m$.

Démonstration du lemme. L'hypothèse $\Phi_m(a) = 0 \mod p$ donne $\bar{a}^m = 0$ dans $\mathbb{F}_p$. Supposons que p ne divise pas m, alors le polynôme $X^m - 1$ est à racines simples. On en déduit que $\bar{a}$ est racine simple de $X^m - 1$, donc est d'ordre m : car sinon il existerait $d|m$ tel que $\Phi_d(a) = 0$ et comme $\Phi_m(X)\Phi_d(X)|X^m - 1$ celà contredit le fait que a est racine simple. Le nombre m divise alors le cardinal de $\mathbb{F}_p^*$, c'est à dire que $p = 1 \mod m$. □

Supposons qu'il existe qu'un nombre fini de nombres premiers $p_1, \ldots, p_k$ congrues à 1 mod m. On note $a = m.\prod_{i=1}^{k} p_i$. On a alors $\Phi_m(a) = \Phi_m(0) \mod a$. Or $\Phi_m(0) = 1$: en effet, $\Phi_1(X) = X - 1$ et $X^m - 1 = (X - 1)\prod_{d|m,d>1} \Phi_d(X)$, ce qui permet de montrer par récurrence sur m que $\Phi_m(0) = 1$. Donc $\Phi_m(a) = 1 \mod a$. Si q est un nombre premier divisant m ou du type p_i (c'est-à-dire divisant a), alors $\Phi_m(a) = 1 \mod q$. Donc si l est un nombre premier divisant $\Phi_m(a)$ (existe car $\Phi_m(a) > 2$), alors l ne divise pas m est n'est pas du type p_i. Ce qui contredit le lemme. □

Remarque. Voir [[Com98], Chap 4 Sec 12.6]

15 Transcendance de e et π

Références [Gourdon : Chapitre 2, Sujet d'etude 2], [Chambert-Loir, Alg. Corp.], [FGN, Alg 1, Ex 5.48]

Leçons concernées
- 239 - Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

Théorème (Lindeman, 1882)**.** Le nombre π est transcendant.

Démonstration. .[A completer] □

Théorème (Hermite, 1873)**.** Le nombre e est transcendant.

Démonstration. (Rapide, Cf FGN) Si e est algébrique, alors il existe $n \in \mathbb{N}$ et $(a_0, \dots, a_n)$ des entiers tel que $a_0 \neq 0$ et $\sum_{i=0}^{n} a_i e^i = 0$.

Lemme. Soit $P(X) \in \mathbb{R}[X]$ de degré $\leq q$. On note $Q(X) = \sum_{i=0}^{q} P^{(i)}(X)$ et $I(t,P) = \int_0^t e^{t-u}P(u)du$. Alors on a

$$I(t,P) = e^t Q(0) - Q(t).$$

Démosntration du lemme. Il suffit de remrquer que $\frac{d}{dt}(e^{-t}Q(t)) = e^{-t}P(t)$. □

Pour $p \in \mathbb{N}$, on note $P_p(X) = X^{p-1}(X-1)^p \dots (X-n)^p$, et on définit $Q_p(X)$ comme dans le lemme. On pose

$$J_p = a_0 I(0, P_p) + \dots + a_n I(n, P_p)$$

D'après lemme et en tenant compte du fait que $\sum_{i=0}^{n} a_i e^i = 0$ on a

$$J_p = -\sum_{i=0}^{n} a_i Q_p(i).$$

Comme $Q_p(X) = \sum_{i=0}^{(n+1)p-1} P^{(i)}(X)$, on en déduit que $\forall i \in [0,n], (p-1)! | Q_p(i)$ [y réfléchir]. Donc $(p-1)! | J$.

On montre de même que $J_p = -a_0(p-1)!(-1)^{np}(n!)^p \mod p!$ [y réfléchir]. Donc si p est un nombre premier assez grand, $p!$ ne divise pas J_p. En particulier $J_p \neq 0$ et $|J| \geq (p-1)!$

Avec l'expression intégrale de I, on a

$$\forall i \in [0,n], |I(i)| \leq e^n \|P_p\|_\infty^{[0,n]} \leq e^n n^{p-1} n^{np}.$$

Donc en posant $M = \sum_{i=0}^{n} |a_i|$, on a

$$|J| \leq (Me^n) n^{p-1} n^{np},$$

Ce qui est absurde car $|J| \geq (p-1)!$. □

Troisième partie

Développements d'analyse et de probabilité

Chapitre 5

Topologie et calcul différentiel

1 Théorème d'Hadamard-Levy

Leçons concernées
- 204 - Connexité. Exemples et applications.
- 214 - Applications du théorème d'inversion locale et du théorème des fonctions implicites.
- 215 - Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.
- 220 - Équations différentielles $X' = f(t, X)$. Exemples d'études qualitatives des solutions.
- 221 - Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

• -A Lemme préliminaire

Lemme. Une application continue propre vers un espace métrique est une application fermée.

Preuve lemme. On raisonne par critère séquentiel. Soit $f : X \to Y$ continue propre. Soit F un fermé de X et $(x_n)_{n\in\mathbb{N}}$ une suite de F telle que $(f(x_n))_{n\in\mathbb{N}}$ converge vers $y \in Y$. Alors la suite $(x_n)_{n\in\mathbb{N}}$ est à valeur dans $f^{-1}(\{x_n : n \in \mathbb{N}\} \cup \{y\})$ et on peut extraire une sous-suite de $(x_n)_{n\in\mathbb{N}}$ convergente dans F puisque F est fermé. On en déduit que $y \in f(F)$. □

Remarque. Le lemme est aussi vrai si l'espace d'arrivé est seulement topologique [Exercice].

• -B Théorème

Théorème (Hadamard-Levy)**.** Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ une application C^k avec $k \geq 2$. Si f est une immersion propre, alors f est un C^k difféomorphisme.

Démonstration. Il suffit de montrer que f est bijective.

• Surjectivité : par théorème de l'application ouverte $f(\mathbb{R}^n)$ est ouvert. D'après le lemme $f(\mathbb{R}^n)$ est fermé. Donc par connexité, on a $f(\mathbb{R}^n) = \mathbb{R}^n$.

• Injectivité : montrons que $f^{-1}(a)$ est un singleton pour tout $a \in \mathbb{R}^n$. On le fait par exemple pour $a = 0$. On considère le champ de vecteurs $X(x) = -x$ sur l'espace d'arrivé et le pull-back de X par f (existe car Df est inversible), noté Y :

$$Y(y) = Df_y^{-1}.\Big(X(f(y))\Big).$$

On note $\Phi_X(t, x)$ et $\Phi_Y(t, y)$ leurs flots (existe car f est C^2 et Y est C^1). Comme on a [y réfléchir]

$$f(\Phi_Y(t, y)) = \Phi_X(t, f(y)) = e^{-t} f(y),$$

le flot Φ_Y est complet : en effet, pour $y \in \mathbb{R}^n$ et $T > 0$, l'ensemble $f(\Phi_Y([-T, T], y)) = e^{-[T,T]} f(y)$ est borné et $\Phi_Y([-T, T], y)$ l'est aussi puisque f est propre, donc la solution $\Phi_Y(., y)$ ne peut pas exploser en temps fini.

On pose $\mathcal{E} = f^{-1}(0)$ et pour $z \in \mathcal{E}$ on note

$$V_z = \Big\{y \in \mathbb{R}^n \mid \lim_{t\to+\infty} \Phi_Y(t, y) = z\Big\}.$$

Par continuité du flot, l'ensemble V_z est un ouvert [y réfléchir], et contient z donc est aussi non vide. Les $(V_z)_{z\in\mathcal{E}}$ sont clairement disjoints. D'après le lemme suivant $\mathbb{R}^n$ est l'union des V_z pour $z \in \mathcal{E}$, donc par connexité $\mathcal{E} = f^{-1}(0)$ est un singleton.

Lemme. Pour $y \in \mathbb{R}^n$, il existe $z \in \mathcal{E}$ tel que $\lim_{t\to+\infty} \Phi_Y(t, y) = z$.

Démonstration du lemme. L'ensemble $\mathcal{E}$ est discret car f est localement injective et est compact car f est propre. Donc $\mathcal{E}$ est fini. On peut choisir $r > 0$ tel que les ouverts $(U_z)_{z\in\mathcal{E}} := (B(z, r))_{z\in\mathcal{E}}$ soient disjoints et tel que $f_{|U_z}$ est un difféomorphisme sur son image pour tout $z \in \mathcal{E}$. Il existe V voisinage de 0 tel que $f^{-1}(V) \subset \bigcup_{z\in\mathcal{E}} U_z$: car sinon il existerait une suite $(y_n)_{n\in\mathbb{N}}$ de $\mathbb{R}^n \setminus \bigcup_{z\in\mathcal{E}} U_z$ tel que $\lim_{n\to+\infty} f(y_n) = a$, et en extrayant une sous-suite convergente (possible car f est propre), celà contredit qu'aucun des $z \in \mathcal{E}$ n'est valeur d'adhérence de $(y_n)_{n\in\mathbb{N}}$.

Comme $\lim_{t\to+\infty} f(\Phi_Y(y, t)) = a$, il existe $T > 0$ tel que : $\forall t > T, f(\Phi_Y(y, t)) \in V$. On a donc

$$\forall t > T, \Phi_Y(y, t) \in f^{-1}(V) \subset \bigcup_{z\in\mathcal{E}} U_z.$$

Comme les $(U_z)_{z\in\mathcal{E}}$ sont des ouverts disjoints, par connexité il existe $z_0 \in \mathcal{E}$ tel que : $\forall t > T, \Phi_Y(y, t) \in U_{z_0}$. Donc on a

$$\begin{aligned} \Phi(y, t) &= f^{-1}_{|U_{z_0}}(f(\Phi_Y(y, t))) \\ &= f^{-1}_{|U_{z_0}}(e^{-tf(y)})) \\ &\xrightarrow{t\to+\infty} z_0 \end{aligned}$$

□

□

Remarque. On consultera par exemple [[ZQ96] CHap. X, Th V.3] ou [[GT98], Part II, Chap. 2, Ex. 30].

2 Théorème de Brouwer et théorème de Schauder

Leçons concernés
- 203 - Utilisation de la notion de compacité.
- 206 - Théorèmes de point fixe, exemples et applications.
- 214 - Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.
- 215 - Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.

Théorème de Brouwer

Théorème (Brouwer)**.** Soient $n \in \mathbb{N}^*$, B_n la boule unité de $\mathbb{R}^n$ et $f : \bar{B}_n \to \bar{B}_n$ une application continue. Alors f admet un point fixe.

Démonstration. • Montrons que si le théorème est vrai pour les fonctions C^1 (au sens la fonction peut se prolonger de façon C^1 sur un voisinage de $\bar{B}_n$ vers $\mathbb{R}^n$) alors il est vrai pour toute fonction continue.

Soit f continue. Par théorème de Stone-Weierstrass, pour $k \in \mathbb{N}$ il existe P_k polynôme tel que $\|f - P_k\|_\infty^{\bar{B}_n} \leq \frac{1}{k}$. Alors le polynôme $Q_k := \frac{P_k}{1+1/k}$ préserve la boule unité et on a

$$\|f - Q_k\|_\infty = \left\| \frac{k}{k+1}(f - P_k) + \frac{1}{k+1} f \right\| \leq \frac{2}{k+1} \xrightarrow{k \to +\infty} 0. \tag{5.1}$$

On note $x_k \in \bar{B}_n$ un point fixe de Q_k et en extrayant une sous-suite convergente, on obtient un point fixe de f.

• On montre le lemme de non rétraction.

Lemme. Il n'existe pas de rétraction de $\bar{B}_n$ à $\mathbb{S}^{n-1}$ de classe C^1.

Démonstration du lemme. Soit $g : \bar{B}_n \to \mathbb{S}^{n-1}$ une rétraction C^1. On définit l'homotopie entre Id et g

$$\begin{array}{rccc} H: & [0,1] \times \bar{B}_n & \longrightarrow & \bar{B}_n \\ & (t,x) & \longmapsto & H_t(x) = tg(x) + (1-t)x \end{array}, \tag{5.2}$$

et on note $P(t) = \int_{B_n} JH_t(x)dx$. Alors P est une fonction polynomiale et $P(0) = Vol(B_n)$, $P(1) = 0$ ($Jg = 0$ car sinon $g(B_n)$ serait d'intéreur non vide).

Montrons qu'il existe $t_0 > 0$ tel que pour tout $t \in [0, t_0], H_t : B_n \to B_n$ est un C^1-difféomorphisme. On pose $M = sup_{x \in \bar{B}_n} \|Dg(x)\|$. Alors on a

$$\forall t \in [0, 1/(2M+2)], \forall x \in B_n, \|DH_t(x) - x\| = t\|Dg(x) - x\| \leq \frac{1}{2}, \tag{5.3}$$

donc $JH_t(x) \neq 0$ et comme $JH_1(x) = 1$, on a $JH_t(x) > 0$. Pour $t \leq t_0$, H_t est injective car $H_t - Id$ est une contraction.

L'ensemble $H_t(B_n)$ est ouvert et inclus dans B_n par théorème de l'application ouverte. Pour montrer que H_t est surjective il suffit de montrer que $H_t(B_n)$ est un fermé de B_n. Soit $(y_p)_{p \in \mathbb{N}} = (H_t(x_p))_{p \in \mathbb{N}}$ une suite de $H_t(B_n)$ convergeant vers $y \in B_n$. On peut supposer que $(x_p)_{p \in \mathbb{N}}$ converge vers $x \in \bar{B}_n$ avec $H_t(x) = y$. On a $x \in B_n$ car sinon $x \in \mathbb{S}^{n-1}$ et $H_t(x) = x = y \notin B_n$. D'où $y \in H_t(B_n)$ et par théorème d'iversion globale $H_t : B_n \to B_n$ est un difféormorphisme.

On en déduit que pour $t \in [0, t_0]$, $P(t) = \int_{B_n} JH_t(x)dx = Vol(H_t(B_n)) = Vol(B_n)$, donc $P(t)$ est constant ce qui contredit $P(1) = 0$. □

• Soit $f : \bar{B}_n \to \bar{B}_n$ de classe C^1. On définit l'application

$$\begin{array}{rccc} g: & \bar{B}_n & \longrightarrow & \mathbb{S}^{n-1} \\ & x & \longmapsto &]f(x), x) \cap \mathbb{S}^{n-1} \end{array} \tag{5.4}$$

(existe car $]f(x), x)$ est un connexe non borné et la boule est strictement convexe). Il reste à montrer que g est C^1 pour appliquer le lemme de non-rétraction. Pour $x \in \bar{B}_n$ il existe un unique $\lambda(x) \geq 1$ tel que $g(x) = \lambda(x)(x - f(x)) + f(x)$. On a alors

$$1 = \|g(x)\|^2 = \lambda(x)^2 \|x - f(x)\|^2 + 2\lambda(x)\langle x - f(x), f(x)\rangle + \|f(x)\|^2. \tag{5.5}$$

On pose

$$\delta(x) = \langle x - f(x), f(x)\rangle^2 + (1 - \|f(x)\|^2)\|x - f(x)\|^2 \geq 0. \tag{5.6}$$

le discriminant réduit. Si $\delta(x) = 0$ alors $\|f(x)\| = 1$ ($\|x - f(x)\| = 0$ est impossible) et $\langle x - f(x), f(x)\rangle = 0$ ce qui donne $1 = \|x\|^2 = \|x - f(x)\|^2 + \|f(x)\|^2$ d'où $\|x - f(x)\| = 0$ ce qui est absurde. Donc $\delta(x) > 0$ et

$$g(x) = \frac{1}{\|x - f(x)\|^2}(-\langle x - f(x), f(x)\rangle + \sqrt{\delta(x)})(x - f(x)) + f(x), \tag{5.7}$$

(on rappelle que $\lambda(x) \geq 1$). Donc g peut être prolongé de façon C^1 sur un voisinage de $\bar{B}_n$. □

Corollaire. Soient C un convexe compact de $\mathbb{R}^n$ et $f : C \to C$ une fonction continue. Alors f admet un point fixe.

Démonstration. .[A completer] □

Théorème de Schauder

Théorème (Schauder)**.** Si C est un convexe fermé borné d'un Banach et $f : C \to C$ continue tel que $f(C)$ est relativement compact, alors f admet un point fixe.

Démonstration. Soit $\varepsilon > 0$. Comme $T(C)$ est relativement compact il existe $y_1, \ldots, y_n \in T(c)$ tels que $T(C) \subset \bigcap_{i=1}^n B(y_i, \varepsilon)$.

On prend une famille $\phi_i : \bigcup_{i=1}^n B(y_i, \varepsilon) \to [0, 1]$ une partition de l'unité associée à cette union (prendre par exemple $\phi_i(x) = (\varepsilon - \|x_i - x\|)_{>0} / \sum_j (\varepsilon - \|x_j - x\|)_{>0}$). On pose $E = vect(y_1, \ldots, y_n)$. Alors $C \cap E$ est un convexe fermé borné de E. On définit

$$\begin{array}{rccc} P : & T(C) & \longrightarrow & C \cap E \\ & x & \longmapsto & \sum_{i=1}^n \phi_i(x) y_i \end{array} . \tag{5.8}$$

Alors pour $x \in T(C)$, on a $\|P(x) - x\| \leq \varepsilon$: en effet, puique (distinguer les cas $x \in B(y_i, \varepsilon)$ et $x \notin B(y_i, \varepsilon)$)

$$\|P(x) - x\| \leq \sum_{i=1}^n \phi(x)\|x - y_i\| \leq \sum_{i=1}^n \phi(x)\varepsilon = \varepsilon. \tag{5.9}$$

Comme $C \cap E$ est un convexe compact en dimension finie, l'application $C \cap E \to C \cap E, x \mapsto P(f(x))$ admet un point fixe x_0 et on a $\|x_0 - f(x_0)\| = \|P(f(x_0)) - f(x_0)\| \leq \varepsilon$.

On prend alors une suite $(x_n)_{n\in\mathbb{N}}$ telle que $\|x_n - f(x_n)\| \leq 1/n$, et quitte à extraire on peut supposer que $(f(x_n))_{n\in\mathbb{N}}$ converge vers l, on en déduit que $(x_n)_{n\in l}$ converge vers l et que $f(l) = l$. □

Remarque. Voir : [[GT96] Sec II.2.7], [[GT98] Sec I.2.7], [[CLF], Ex ? ?] ou [[Rou], ? ?].

3 Différentiablitité de la distance et théorème Motzkin

Leçons concernées
- 144 - Problèmes d'angles et de distances en dimension 2 ou 3.
- 203 - Utilisation de la notion de compacité.
- 215 - Applications différentiables définies sur un ouvert de Rn. Exemples et applications.

Différentiabilité de la distance

Théorème. Soit F un fermé de $\mathbb{R}^n$ non trivial, et :

$$\begin{array}{rccc} \phi: & \mathbb{R}^n & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & dist(x,F)^2 \end{array}.$$

Soit $x \in \mathbb{R}^n$. Alors ϕ est différentiable en x si et seulement si la distance est atteinte en un seul point $y \in F$. Auquel cas on a $\nabla\phi(x) = 2(x-y)$.

Démonstration. Supposons que ϕ soit différentiable en x. On prend y un point y tel que $dist(x,f) = dist(x,F)$. On a alors

$$\forall h \in \mathbb{R}^n, \phi(x+h) \leq dist(x+h,y)^2.$$

On en déduit que la fonction $h \mapsto \phi(x+h) - dist(x+h,y)$ atteint un maximum en $h=0$, donc par théorème des extrema liées sa différentielle est nulle en $h=0$, ce qui donne $\nabla\phi(x) = 2(x-y)$. Donc $\boxed{y \text{ est unique}}$.

Réciproquement. Pour $h \in \mathbb{R}^n$, on note

$$A(x+h)\{f \in F \mid dist(x+h,f) = dist(x+h,F)\}.$$

Supposons que $A(x) = \{y\}$.

Lemme. On a $\lim_{h\to 0} dist(A(x+h),y) = 0$.

Démonstarion du lemme. Supposons le contraire : il existe alors une suite (h_n) tendant vers 0 et $\delta > 0$ tel que $dist(A(x+h_n),y) \geq \delta$. On note

$$G = \left\{ f \in F \mid dist(f,y) \geq \delta \right\} \subset F \setminus \{y\}.$$

On a alors $dist(x+h_n,F) = dist(x+h_n,G)$ et faisant tendre n vers $+\infty$, on a $dist(x,F) = dist(x,G)$, ce qui contredit la fait que $A(x)$ est un singleton. □

Soit $h \in \mathbb{R}^n$. D'une part, comme $\phi(x+h) \leq dist(x+h,f)^2$, on a

$$\phi(x+h) - \phi(x) \leq |x+h-f_0|^2 - |x-f_0|^2 = 2\langle x-y,h\rangle + |h|^2.$$

Et d'autre part, pour $y_h \in A(x+h)$, on a

$$\begin{array}{rcl} \phi(x+h) - \phi(x) & = & |x+h-y_h|^2 - |x-y|^2 \\ & = & |x-y_h|^2 + 2\langle x-y,h\rangle + |h|^2 - |x-y|^2 \end{array}$$

Or $|x-f_h|^2 \leq |x-y|^2$ et $\langle x-y_h,h\rangle = \langle x-y,h\rangle + \langle y-y_h,h\rangle$ et d'après le lemme $y-y_h = o(1)$. On en déduit donc que

$$\phi(x+h) - \phi(x) \geq 2\langle x-y,h\rangle + o(h).$$

Ce qui montre que ϕ est différentiable en x et que $\nabla\phi(x) = 2(x-y)$. □

Remarque. La preuve se trouve dans [[GT98] Part. I, Chap 1, Ex. 2].

Théorème de Motzkin

Proposition. Soit F un fermé de $\mathbb{R}^n$. On suppose que pour tout $x \notin F$, il existe H un hyperplan ne contenant pas x et tel que F est inclus dans le demi plan délimité par H et ne contenant pas x. Alors F est convexe.

Démonstration. .[Exercice] □

Corollaire. Soit F un fermé de $\mathbb{R}^n$. On suppose que pour tout $x \notin F$ et $f \in F$ tel que $d(x, f) = d(x, F)$, on a

$$\forall y \in x + \mathbb{R}_+(x - f), d(y, F) = d(y, x) + d(x, f).$$

[Dessin]. Alors f est convexe.

Démonstration. .[Exercice]. □

Théorème (Motzkin)**.** Soit F un fermé de $\mathbb{R}^n$. On suppose que pour tout $x \in \mathbb{R}^n$ la distance de x à F est atteinte en un seul point. Alors F est convexe.

Démonstration. On note $f : \mathbb{R}^n \setminus F \to \mathbb{R}$ la fonction distance à F. Alors le champs de gradient ∇f est continue et unitaire (cf théorème ci dessus). Soit $x \notin F$ et X une solution tel que $X(0) = x$ (Th. de Cauchy-Peano). On a

$$\tfrac{d}{dt} f(X(t)) = \langle \nabla f(X(t)), X'(t) \rangle = 1,$$

donc $f(X(t)) = f(x) + t$. Comme le champs de gradient est unitaire, X est Lipchitzien, et comme f croit, X reste dans $\mathbb{R}^n \setminus F$. Donc X est définie sur $\mathbb{R}_+$ (on peut appliquer le principe d'explosion en temps fini). Comme

$$f(x) + t = f(X(t)) = d(X(T), p(X(t))) \leq d(X(T), p(x)) \leq d(X(T), x) + d(x, p(x)) \leq t + f(x),$$

on en déduit qu'on a égalité partout, donc $P(X(t)) = P(x)$ et $d(X(t), x) = t$. Or

$$t = d(X(t), x) \leq \textstyle\int_0^t |X'(s)| ds \leq t,$$

donc $X'(s)$ est de direction constante et $X(t) \in x + \mathbb{R}_+(x - p(x))$. On conclut avec le corollaire, □

Remarque. La preuve se trouve dans [[GT98], Part. II, Chap 2, Ex. 31].

4 Etude de $y'(x) = y^2(x) - x$

Leçons concernées
- 220 - Équations différentielles $X' = f(t, X)$, exemples d'études qualitatives des solutions.
- 229 - Fonctions monotones. Fonctions convexes. Exemples et applications.

On s'intéresse à l'équation différentielle

$$y'(x) = y^2(x) - x := f(x, y).$$

Cette équation vérifie les hypothèses de Cauchy-Lipchitz. Pour $a \in \mathbb{R}$, on note $y_a(x)$ le flot : c'est la solution vérifiant $y_a(0) = a$ et on note I_a son intervalle de définition.

Domaine de croissance et de convexité de y

Toutes les dérivées de y s'expriment en fonction de x et y, et on a

$$y' \geq 0 \iff x \leq y^2.$$

De plus, on a $y''(x) = 2y(x)(y^2 - x) - 1$, donc

$$y'' \geq 0 \iff \begin{cases} y > 0 \text{ et } x \geq y^2 - \frac{1}{2y} \\ \text{ou } y < 0 \text{ et } x \leq y^2 - \frac{1}{2y} \end{cases}.$$

On définit les fonctions

$$\Gamma_+ : \begin{array}{ccc} [0, +\infty[& \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sqrt{x} \end{array} \text{ et } \Gamma_- : \begin{array}{ccc} [0, +\infty[& \longrightarrow & \mathbb{R} \\ x & \longmapsto & -\sqrt{x} \end{array},$$

si bien que

$$\forall x > 0, y'(x) < 0 \iff \Gamma_-(x) < y(x) < \Gamma_+(x).$$

On définit aussi les fonctions

$$C_+ : \mathbb{R} \to \mathbb{R},\ C_-^1 : \mathbb{R} \to \mathbb{R} \text{ et } C_-^1 : \mathbb{R} \to \mathbb{R},$$

définis implicitement par l'équation $x = y^2 - \frac{1}{2y}$. Donc

$$y'' \geq 0 \iff y \text{ est au dessus de } C_+ \text{ ou entre } C_-^1 \text{ et } C_-^2.$$

Proposition.
- La fonction C_+ est une barrière inférieure.
- Les focntions C_-^1 et C_-^2 forment un entonnoir.
- Les fonctions Γ_+ et Γ_- forment un entonnoir.

Démonstration. Pour le premier point : soit $x_0 \in \mathbb{R}$ et $y_0 = C_+(x_0)$. On a alors $x_0 = 2y_0 - \frac{1}{2y_0}$, ce qui donne

$$f(x_0, y_0) = y_0^2 - x_0 = \frac{1}{2y_0},$$

et

$$\frac{dC_+}{dx}(x_0) = \left(\frac{d}{dy}_{|y=y_0}(y^2 - 1/2y)\right)^{-1} = \left(2y_0 + \frac{1}{2y_0^2}\right)^{-1} \leq f(x_0, y_0).$$

Ce qui prouve que C_+ est une barrière inférieure.

On fait de même pour les autres points. □

Corollaire. Si y passe entre Γ_- et Γ_+, alors y est décroissante et définie pour tous les x positifs.

Démonstration. La décroissance vient de la discussion ci-dessus. Si y a une durée de vie finie, alors par décroissance de y et le fait que $y > \Gamma_-$, la solution y admettrait une limite finie, ce qui est absurde. □

Étude de y_a avec $a < 0$

On se fixe $a < 0$.
La proposition suivante détermine le comportement de y_a pour $x < 0$.

Proposition. On a $I_a \subset]1/a, +\infty[$.

Démonstration. Celà vient du lemme suivant.

Lemme. On a $\forall x \in]1/a, +\infty[\cap I_a, y(x) \leq \frac{1}{1/a-x}$.

Démonstration. Pour $x \in I_a \cap]-\infty, 0]$, on a $y'(x) \geq y^2(x)$, donc $\int_x^0 \frac{y'(x)}{y^2(x)} dx \geq -x$ et en primitivant on obtient $y(x) \leq \frac{1}{1/a-x}$. On fait de même pour $x \in I_a \cap [0, +\infty[$, en minorant $y'(x) \geq y^2(x)$. □

□

On étudie maintenant le cas $x > 0$.

Proposition. Il existe $x^1 \in \mathbb{R}_+$ tel que $y_a(x^1) = \Gamma_-(x^1)$.

Démonstration. Si ce n'est pas le cas alors y_a reste en dessous de Γ_-. La solution y_a est alors croissante et concave, donc admet une limite finie ou $+\infty$, ce qui est absurde car $\Gamma_- \to -\infty$. □

On en déduit que $I_a \supset]0, +\infty[$.

Proposition. Il existe $x^2 > x^1$ tel que $y_a(x^2)$ entre dans l'entoinnoir C_-.

Démonstration. Comme y_a est dans l'entonnoir Γ, elle est décroissante. Si elle ne coupe pas C_- alors est concave, ce qui implique $y_a(x) < -\alpha x + \beta$ pour un certain $\alpha > 0$ et $\beta \in \mathbb{R}$, et celà contredit $y(x) > \Gamma_-(x) = -\sqrt{x}$. □

Proposition. $y_a(x) = -\sqrt{x} + o(1)$.

Démonstration. . [? ? ?] □

Proposition. Soit une solution $z(x)$ qui passe à $x = x^0 > 0$ en $z(x^0) = y^0 < \Gamma_-(x^0)$, alors elle est définie pour $x = 0$, i.e. la solution z est du type y_b avec $b < 0$.

Démonstration. On prend $c < 0$ tel que $\frac{1}{c-x^0} = y^0$. On a alors d'une part par la proposition [?]

$$y_c(x^0) \leq \frac{1}{c-x^0} \leq z(y_0)$$

et d'autre part

$$z(y_0) \leq y_0(y_0),$$

car la solution y_0 entre dans l'entonnoir Γ en $x = 0$. Comme les courbes intégrales ne se coupent pas on a $y_c(x) \leq z(x) < y_0(x)$ pour x tel que $z(x)$ existe. On en déduit que z est borné pour $x \in [0, x^0]$ donc z existe pour $x = 0$ et $z(0) < y_0(0) = 0$. □

Étude de y_a avec $a \geq 0$ et $x \geq 0$

On définit les deux grandeurs suivantes

$$a^* = sup\Big\{a \in [0, +\infty[| y_a \text{ coupe } \Gamma_+\Big\},$$

$$a^{*\prime} = inf\Big\{a \in]-\infty, a_+] | y_a \text{ coupe } C_+\Big\}.$$

Proposition. On a
- a^* et $a^{*\prime}$ sont dans $]0, a_+[$.
- La solution y_{a^*} ne coupe pas Γ_+.
- La solution $y_{a^{*\prime}}$ ne coupe pas C_+.
- $a^* = a^{*\prime}$.

Démonstration. Soit a tel que y_a coupe Γ_+, il existe $r > 0$ tel que $y_0(r) < \Gamma_+(r)$. Par continuité du flot il existe $\varepsilon > 0$ tel que $\forall b \in [a-\varepsilon, b+\varepsilon], y_b(x_0) < \Gamma_+(r)$. Donc $\{a \in [0, a_+] | y_a \text{ coupe } \Gamma_+\}$ est ouvert (de $[0, +\infty[$) contenant 0, et c'est un intervalle (utiliser le fait que $a < b \Rightarrow y_a \leq y_b$), donc c'est $[0, a^*[$. En particulier y_{a^*} ne coupe pas Γ_+.

On montre de même que $\{a \in]-\infty, a_+] | y_a \text{ coupe } C_+\} =]a^{*\prime}, a_+]$.

Pour $a \in [0, a^*]$ et $b \in]a^{*\prime}, a_+]$, y_a coupe Γ_+ et y_b coupe C^+, donc il existe x tel que $y_a(x) < \Gamma_+(x) < y_b(x)$ et on en déduit $a < b$. Donc $a* \leq a^{*\prime}$. On a $y'_{a^{*\prime}}(x) - y'_{a^*}(x) = y^2_{a^{*\prime}}(x) - y^2_{a^*}(x)$, donc si $a* < a^{*\prime}$, $y_{a^{*\prime}} - y_{a^*}$ serait sctrictement croissant, ce qui contredit $y_{a^{*\prime}}(x) - y_{a^*}(x) \to 0$.

□

Proposition. Si $a \in [0, a^*]$ alors $I_a \subset [0, +\infty[$.

Démonstration. La solution y_a est majoré par C_+ et minorée par Γ_-, donc si I_a est majoré y_a serait bornée ce aui est absurde. □

Proposition. Il existe $A > a^{*\prime}$ tel que

$$\forall a \leq A, \text{ l'intervalle } I_a \text{ soit majoré.}$$

Démonstration. Soit $a > 0$ et $b < a^2$. Alors $\forall x \in I_a \cap [0, b], y'_a(x) \geq y^2_a(x) - b$. On note $\phi :]1, +\infty[\to]-\infty, 0[, x \mapsto \frac{1}{2} \ln \frac{x-1}{x+1}$ (c'est l'expression de argth) et $\psi = \phi^{-1} :]-\infty, 0[\to]1, +\infty[$, si bien que ψ vérifie $\psi' = \psi^2 - 1$ et $\lim_{x \to 0} \psi(x) = +\infty$. La solution de $y' = y^2_a(x) - b$, $y(0) = a$ est $x \mapsto \Psi(x, a, b) := \sqrt{b}\psi\left(\sqrt{b}x + \phi\left(\frac{a}{\sqrt{b}}\right)\right)$ (on a $\frac{a}{\sqrt{b}} > 1$). Donc $\forall x \in I_a \cap [0, b], y_a(x) \geq \Psi(x, a, b)$ avec $\lim_{x \to X(a,b)} \Psi(x, a, b) = +\infty$ et $X(a, b) = -\phi\left(\frac{a}{\sqrt{b}}\right) = \frac{-1}{2} \ln\left(1 - \frac{2}{x+1}\right)$.

On a cherche alors à quelle condition sur a, $\exists b \leq a^2, X(a, b) \leq b$. En calculant numériquement on trouve que $a \geq 1.4$ suffit ($a_+ = (1/2)^{1/3} = 0,79...$), et on a $I_a \subset]-\infty, X(a, b)[$ avec b tel que $X(a, b) \leq b$. □

On note $a_* = inf\{a \in \mathbb{R} | I_a \text{ est majoré}\}$. On alors $0 < a^* \leq a^{*\prime} \leq a_*$ et $a^{*\prime} < a_+$.

Étude de y_a avec $a \geq 0$ et $x \leq 0$

On se fixe $a \geq 0$.

Proposition. La solution y_a s'annule pour un temps $x \in \mathbb{R}_-$.

Démonstration. Si $a \leq a_+$, alors sur $I_a \cap]-\infty, 0]$ y_a est croissante concave donc y_a tend vers $-\infty$ quand $x \to inf(I_a)$. Donc en particulier la solution s'annule.

Si $a > a_+$. Montrons que y_a coupe C_+. Si ce n'est pas le cas alors y_a est croissante convexe minoré par 0 donc admet une limite en $-\infty$ et $\lim_{x \to -\infty} y'_a(x) = 0$, ce qui est absurde car $y'_a(x) = y^2_a(x) - x$. Donc y_a coupe C_+ et par même raisonnement que ci-dessus y_a tend vers $-\infty$. □

Proposition. L'intervalle I_a est minoré.

Démonstration. .[A completer] □

Remarque.
- Ce développement a été proposé par Matthias Moreno.
- L'étude est faite dans [[CLF], Ex ?].
- C'est le développement que j'ai présenté à l'oral d'analyse.

5 Théorème de Tietze et théorème d'Uryshon

Leçons concernées
- 202 - Exemples de parties denses et applications.
- 207 - Prolongement de fonctions. Exemples et applications.

Théorème d'Urysohn

Définition. Un espace topologique X est dit normal si X est séparé et si pour tout E et F fermé disjoint, E et F admettent des voisinage ouverts disjoints.

Lemme. Soient X un espace normal, F un fermé et O un ouvert contenant F. Alors il existe V un ouvert tel que

$$F \subset V \subset \overline{V} \subset O.$$

Démonstration. Comme X est normal, il existe V voisinage de F et W voisinage de O^c disjoints. On a alors

$$F \subset V \subset \overline{V} \subset W^c \subset O.$$

□

Théorème (Urysohn)**.** Soit X un espace topologique normal et $F \subset O$ un fermé inclus dans un ouvert. Alors il existe $f : X \to [0,1]$ continue tel que $f = 0$ sur F et $f = 1$ sur O^c.

Démonstration. On commence par construire une famille $(O_r)_{r\in\mathbb{Q}\cap[0,1]}$ vérifiant

$$F \subset U_0 \text{ et } \overline{U_1} \subset O,$$

$$\text{et } \forall r, s \in \mathbb{Q} \cap [0,1], r < s \Longrightarrow \overline{U}_r \subset U_s.$$

On indexe $\mathbb{Q} \cap [0,1]$ par $(x_n)_{n\in\mathbb{N}}$. On prend U_{x_0} un ouvert tel que

$$F \subset U_{x_0} \subset \overline{U}_{x_0} \subset O.$$

Suppsons constuite la suite $U_{x_0}, ..., U_{x_{n-1}}$. On définit alors U_{x_n} de la façon suivante : on partitionne $[0,1]$ en

$$[0,1] = [0, y_0] \cup [y_0, y_1] \cup ... \cup [y_{n-1}, 1],$$

avec $\{y_1, ..., y_{n-1}\} = \{x_0, ..., x_{n-1}\}$. On a alors

$$F \subset U_{y_0} \subset \overline{U}_{y_0} \subset U_{y_1} \subset ... \subset U_{y_n} \subset \overline{U}_{y_{n-1}} \subset O.$$

Par convention on note $y_{-1} = 0$, $y_n = 1$, $\overline{U}_{y_{-1}} = F$ et $U_{y_n} = O$. Il existe alors $k \in [-1, n-1]$ tel que $x_n \in]y_k, y_{k+1}[$. On prend alors U_{x_n} tel que

$$\overline{U}_{y_k} \subset U_{x_n} \subset \overline{U}_{x_n} \subset U_{y_{k+1}}.$$

On définit alors la fonction :

$$\begin{array}{rccc} f: & X & \longrightarrow & [0,1] \\ & x & \longmapsto & inf\Big(\{r \in \mathbb{Q} \cap [0,1] \mid x \in U_r\} \cup \{1\}\Big). \end{array}$$

On a alors $f = 0$ sur F et $f = 1$ sur O. Montrons que f est continue. Soit $x \in X$.
- Si $f(x) = 0$, alors $x \in \bigcap_{r>0} U_r$. On en déduit que pour tout $r > 0$, U_r est un voisinage de x tel que $f(U_r) \leq r$. Ce qui prouve que f est continue en x.
- Si $f(x) = 1$, alors $x \in \bigcap_{r<1} U_r^c$. On en déduit que pour tout $r < 1$, $\overline{U_r}^c$ est un voisinage de x tel que $f(U_r) \geq r$.
- Si $f(x) \in]0,1[$. Pour tout $r, s \in \mathbb{Q}\cap]0,1[$ tel que $f(x) \in]r, s[$, on choisit $r', s' \in \mathbb{Q}\cap]0,1[$ tel que $f(x) \in]r', s'[$, $[r', s'] \subset]r, s[$. Comme $f(x) > r'$ on a $x \notin U_{r'}$ donc a fortiori $x \notin \overline{U}_r$. Comme $f(x) < s'$ on a $f(x) \in U_s$ [faire un dessin ?]. On en déduit que $U_s \setminus \overline{U}_r$ est un voisinage de x tel que $f\Big(U_s \setminus \overline{U}_r\Big) \in [r, s]$.

□

Corollaire. Soit X espace localement compact et séparé. Si K est un compact de X, alors il existe une fonction continue à support compact valant 1 sur K.

Démonstration. On démontre d'abord le lemme suivant.

Lemme. Pour X espace localement compact et K un compact de X, il existe un voisinage U de K relativement compact.

Démonstration du lemme. Pour $x \in K$, il existe U_x voisinage ouvert de x relativement compact. Par compacité de K on trouve alors un ouvert $U = \bigcup_{x \in I} U_x$ relativement compact avec I fini. □

Soit U un voisinage relativement compact de K. La fermeture de U est alors normal, donc il existe une fonction $f : \overline{U} \to [0,1]$ valant 1 sur K et 0 sur $\overline{U} \setminus U = \partial U$. On prolonge alors f par 0 sur $X \setminus \overline{U}$. On vérifie ensuite aisément que la fonction f est continue en tout point de ∂V. □

Théorème de Tietze

Théorème (Tietze)**.** Soient X un espace normal et A un fermé de X. Si $f : A \to [-1,1]$ est continue, alors il existe $g : X \to \mathbb{R}$ telle que $g(A) \subset [-1,1]$ et $g_{|A} = f$, $inf(g) = inf(f)$ et $sup(g) = sup(f)$.

Démonstration. On montre d'abord le lemme suivant.

Lemme. Soit $a > 0$ et $h : A \to [-a,a]$ continue. Alors il existe $k : F \to [-a/3, a/3]$, telle que

$$\forall x \in A, |f(x) - g(x)| \leq \tfrac{2a}{3}.$$

Démonstration du lemme. On note $F_1 = f^{-1}([-a, -a/3])$, $F_3 = f^{-1}([a/3, a])$ et $F_2 = F - (F_1 \cup f_3)$. Alors F_1 et F_3 sont des fermés disjoint donc par théorème d'Uryshon, il existe $g : X \to [-a/3, a/3]$ tel que $g = -a/3$ sur F_1 et $g = a/3$ sur F_3. Pour $x \in F_1$ on a $f(x) \in [-a, -a/3]$ et $g(x) = -a/3$, donc $|f(x) - g(x)| \leq 2a/3$. De même pour $x \in F_3$, on a $|f(x) - g(x)| \leq 2a/3$. Pour $x \in F_2$, on a $f(x), g(x) \in [-a/3, a/3]$, donc $|f(x) - g(x)| \leq 2a/3$. □

On crée alors aisément par récurrence une suite $(g_n)_{n \in \mathbb{N}^*} \in C^0(X, [-1,1])$ tel que pour tout $n \in \mathbb{N}^*$
- La fonction g_n est à valeur dans $[-2^{n-1}/3^n, 2^{n-1}/3^n]$.
- Pour tout $x \in A$, on a $|f(x) - \sum_{k=1}^{n} g_n(x)| \leq (2/3)^n$.

La série $\sum_{n \geq 1} g_n$ converge alors normalement sur X, est à valeur dans $\sum_{n=1}^{\infty} \frac{2^{n-1}}{3^n} = 1$ et sa somme est f sur A.

□

Remarque. On consultera par exemple [[Lan93], Th 4.2 et Th 4.4], [[Gou94b], Chap 1, Ex 10], [[Coh80], Ex ? ?], [[CLF], Anal 1, Ex 1.3].

6 Théorème de Jordan

Leçons concernées
- 139 - Applications des nombres complexes à la géométrie.
- 203 - Utilisation de la notion de compacité.
- 204 - Connexité. Exemples et applications.
- 216 - Étude métrique des courbes. Exemples.
- 245 - Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$.

Théorème (de Jordan)**.** Le complémentaire d'une courbe fermé simple C^2 dans $\mathbb{C}$ a deux composantes connexes.

Démonstration. Soit $\gamma : \mathbb{S}^1 \to \mathbb{C}$ un chemin fermé sans point double (i.e γ est injective). Quitte à renormaliser, on peut supposer que $\forall t \in I, |\Gamma'(t)| = 1$. On identifie $\mathbb{S}^1$ à $\mathbb{R}$ modulo $\mathbb{Z}$.

Lemme (Voisinage epsilon)**.** Il existe $\varepsilon > 0$ tel que l'application suivante est une bijection sur le voisinage ε de γ

$$\begin{array}{rccc} \phi : & \mathbb{S}^1 \times]-\varepsilon, \varepsilon[& \longrightarrow & \mathbb{C} \\ & (t, r) & \longmapsto & \gamma(t) + ir\gamma'(t) \end{array}.$$

Démonstration. Soit $t_0 \in \mathbb{S}^1$. Alors l'application $\phi : (t, r) \mapsto \gamma(t) + ir\gamma'(t)$ est une immersion en $(t_0, 0)$ car les dérivées partielles

$$\frac{\partial \phi}{\partial t}(t_0, 0) = \gamma(t_0) \text{ et } \frac{\partial \phi}{\partial r}(t_0, 0) = i\gamma'(t_0),$$

sont libres. Il existe alors ε_t et U_t un voisinage de t telle que $\phi : U_t \times]\varepsilon_t, \varepsilon_t[\to \mathbb{C}$ soit un homéomorphisme sur son image. Par compacité il existe une famille finie $(t_1, \dots, t_p)$ tel que $\mathbb{S}^1 = \bigcup_{i=1}^p U_{t_i}$.

On note

$$d = inf\Big\{ |\gamma(s) - \gamma(t)| \ : \ s, t \text{ n'appartiennent pas à un même ouvert } U_{t_i} \Big\}.$$

Alors $d > 0$, car $(\mathbb{S}^1 \times \mathbb{S}^1) \setminus (\bigcap_{i=1}^p U_i \times U_i)$ est compact. On prend alors

$$\varepsilon = \min(\tfrac{d}{3}, \varepsilon_{t_1}, \dots, \varepsilon_{t_1}).$$

On vérifie alors que ε convient : soient $(t, r), (t', r')$ tels que $\phi(t, r) = \phi(t', r')$. S'il existe U_{t_i} tel que $t, t' \in U_(t_i)$, alors $(t, r) = (t', r')$ par injectivité de ϕ. Sinon, on a $d(\gamma(t), \gamma(t')) \geq 3\varepsilon$, ce qui donne

$$d(\phi(t, r), \phi(t', r')) \geq d(\gamma(t), \gamma(t')) - \|ir\gamma'(t)\| - \|ir'\gamma'(t')\| \geq \varepsilon.$$

□

Montrons que $\mathbb{C} \setminus \Gamma$ a au plus 2 composantes connexes. Les ensembles $V_+ := \phi(\mathbb{S}^1 \times]0, \varepsilon[)$ et $V_- := \phi(\mathbb{S}^1 \times]0, \varepsilon[)$ sont connexes. On note C_+ et C_- leur composantes connexes respectives dans $\mathbb{C} \setminus \gamma$. Soit $z \in \mathbb{C} \setminus \gamma$ et z_0 la projection de z_0 sur γ. Alors $]z, z_0[$ est un connexe de $\mathbb{C} \setminus \gamma$ et rencontre soit $V_+ \cup V_-$. Donc z est soit dans C_+ soit dans C_-.

Soit $\gamma : I \to \mathbb{C}$ un chemin fermé sans point double. Quitte à appliquer une similitude et à renormaliser, on peut supposer que $I = [0, 1]$, $\forall t \in I, |\Gamma'(t)| = 1$. Pour $r \in \mathbb{R}$ on note $\Gamma_r(t) = \Gamma(t) + ir\Gamma'(t)$ (Γ_r est un chemin fermé).

Montrons que $\mathbb{C} \setminus \gamma$ a au moins deux composantes connexes. Il suffit de trouver deux points qui n'ont pas le même indice. quitte à appliquer une similitude, on peut supposer que $\gamma(0) = 0$ et $\gamma(0) = 1$. Pour $x \in]0, \varepsilon[\subset \mathbb{C} \setminus \Gamma$, on a

$$Ind(ix, \Gamma) - Ind(-ix, \Gamma) = \tfrac{1}{2i\pi} \int_\Gamma \tfrac{1}{z - ix} - \tfrac{1}{z + ix} dz = \tfrac{x}{\pi} \int_{-1/2}^{1/2} \tfrac{\gamma'(t)}{\gamma(t)^2 + x^2} dt.$$

Comme $\Gamma(t)^2 = t^2 + o(t)$, il existe $\delta > 0$ tel que $|t| \leq \delta \Longrightarrow \operatorname{Re} \Gamma(t)^2 \geq \frac{t^2}{2}$. D'une part, on a

$$\lim_{x \to 0} \tfrac{x}{\pi} \int_{\delta \leq |t| \leq 1/2} \tfrac{\Gamma'(t)}{\Gamma(t)^2 + x^2} dt = 0.$$

(Minoner $|\Gamma(t)|$). D'autre part, on a

$$\tfrac{x}{\pi} \int_{|t| \delta} \tfrac{\Gamma'(t)}{\Gamma(t)^2 + x^2} dt = \tfrac{1}{\pi} \int_{|t| \leq \delta} \tfrac{\Gamma'(t)/x}{(\Gamma(t)/x)^2 + 1} dt = \tfrac{1}{\pi} \int_{|u| \leq \delta x^{-1}} \tfrac{\Gamma'(u)}{(\Gamma(xu)/x)^2 + 1} du.$$

Or $|(\Gamma(xu)/x)^2 + 1| \geq \operatorname{Re}(\Gamma(xu)/x)^2 u^2 + 1 \geq u^2/2 + 1$, donc on peut dominer par $\frac{1}{1+u^2}$ et on en déduit que

$$\lim_{x\to 0} \frac{x}{\pi} \int_{\mathbb{R}} \frac{\Gamma'(u)}{(\Gamma(xu)/xu)^2 u^2+1} \mathbf{1}_{|u|\leq x^\delta} du = \frac{1}{\pi} \int_{\mathbb{R}} \frac{du}{1+u^2} = 1.$$

Donc pour x assez petit $Ind(ix, \Gamma) \neq Ind(-ix, \Gamma)$. □

Remarque. Voir [[GT98], Sec 2.28].

7 Densité des fonctions continues nulle part dérivables

Leçons concernées
- 201 - Espaces de fonctions. Exemples et applications.
- 202 - Exemples de parties denses et applications.
- 228 - Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.

Théorème. L'ensemble des fonctions dérivables nulle part de $C([0,1],\mathbb{R})$ est dense.

Démonstration. f n'est dérivable pas dérivble en x si et seulement si $\frac{f(x+h)-f(x)}{h}$ n'a pas de limite quand $h \to 0$. En particulier c'est le cas si

$$\forall n \in \mathbb{N}, \forall k \in \mathbb{N}, \exists |h| \leq \tfrac{1}{k}, \left|\tfrac{f(x+h)-f(x)}{h}\right| > n.$$

Pour $n, k \in \mathbb{N}$ et $x \in [0,1]$, on note

$$U_{n,k}(x) = \Big\{ f \in C([0,1],\mathbb{R}) | \exists |h| \leq \tfrac{1}{k}, \left|\tfrac{f(x+h)-f(x)}{h}\right| > n \Big\}.$$

L'ensemble $U := \bigcap_{n=1}^{+\infty} \bigcap_{k=1}^{+\infty} \bigcap_{x\in[0,1]} U_{n,k}(x)$ est alors formé de fonctions dérivables nulle part. On va montrer que U est dense.

Soient $n, k \in \mathbb{N}$. Montrons que $U_{n,k} := \bigcap_{x\in[0,1]} U_{n,k}(x)$ est ouvert. On note

$$F_{n,k} = \Big\{ f \in C([0,1],\mathbb{R}) | \exists x \in [0,1], \forall |h| \leq \tfrac{1}{k}, |f(x+h) - f(x)| \leq n|h| \Big\}.$$

Soit $(f_i)_{i\in\mathbb{N}}$ une suite de $F_{n,k}$ convergeant vers une fonction $f \in C([0,1],\mathbb{R})$. Pour tout $i \in \mathbb{N}$, il existe $x_i \in [0,1]$ tel que $\forall |h| \leq k^{-1}, |f_i(x_i + h) - f_i(x_i)| \leq n|h|$. On extrait une sous-suite de (x_n) convergeant vers x, on a alors en passant a la limite $\forall |h| \leq k^{-1}, |f(x+h) - f(x)| \leq n|h|$. Donc $F_{n,k}$ est fermé et $U_{n,k}$ est ouvert.

Montrons que $U_{n,k}$ est dense. Soit $f \subset C([0,1],\mathbb{R})$ et $r > 0$. On cherche un élément de $\bar{B}(f,r) \cap U_{n,k}$ sous la forme

$$g = f + r \sin \omega x \text{ avec } N \in \mathbb{N}.$$

On fixe $x \in [0,1]$. Pour $h \in \mathbb{R}$, on a

$$|g(x+h) - g(x+h)| \leq r|\sin\omega(x+h) - \sin\omega x| - |f(x+h) - f(x)|.$$

Il existe $\eta > 0$ tel que $\forall |h| \leq \eta, |f(x+h) - f(x)| \leq \frac{r}{2}$. Pour tout $\omega > \frac{2\pi}{\omega}$ il existe $|h_\omega| \leq \frac{2\pi}{\omega} (\leq \eta)$ tel que

$$r|\sin\omega(x+h) - \sin\omega x| \geq r.$$

On a alors

$$\forall \omega > \tfrac{2\pi}{\eta}, |g(x+h_\omega) - g_N(x)| \geq \tfrac{r}{2} \geq \tfrac{r\omega}{4\pi}|h|.$$

On prend alors ω tel que $\frac{r\omega}{4\pi} \geq n$ et $\frac{2\pi}{N} \leq \frac{1}{k}$.

Par théorème de Baire U est donc dense. □

Remarque.
- Voir [[Gou94b] Annexe A, Ex 4], [[GT96], Part I Chap 2, Ex 2].
- On pourra aussi consulter [http ://epubl.ltu.se/1402-1617/2003/320/LTU-EX-03320-SE.pdf].

8 Immersion propre

Leçons concernées
- 203 - Utilisation de la notion de compacité.
- 214 - Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.
- 217 - Sous variétés de $\mathbb{R}^n$. Exemples.

Théorème. Soient M, N deux sous-variétés. Soit $f : M \to N$ une immersion propre de classe C^p dont le cardinal des fibres non vides est constante à $k \in \mathbb{N}^*$. Alors f est un revêtement sur son image à k feuillets (en particulier son image est une sous-variété).

Démonstration. Soit $y \in \operatorname{Im} f$. On note $x_1, \dots, x_k$ les antécédents de y par f. Comme f est une immersion, pour $i \in [1, k]$ il existe U_i un voisinage de x_i tel que $f : U_i \to f(U_i)$ soit un C^p-difféomorphisme. Quitte à réduire les $(U_i)_{i\in[1,k]}$ on peut les supposer tous disjoints.

Lemme. Il existe un voisinage V de y tel que

$$f^{-1}(V) \subset \bigcup_{i=1}^{k} U_i.$$

Démonstration du lemme. Si ce n'était pas le cas, alors il existerait une suite $(x_n)_{n\in\mathbb{N}}$ de M tel que $\lim_{n\to+\infty} f(x_n) = y$ et $\forall n \in \mathbb{N}, x_n \notin \bigcup_{i=1}^{k} U_i$. Comme f est propre, quitte à extraire on peut supposer que $(x_n)_{n\in N}$ converge. Sa limite est alors un antécédant de y, ce qui est absurde. □

Lemme. Pour tout $i_0 \in [1, k]$, l'application $f : f^{-1}(V) \cap U_{i_0} \to V$ est une bijection.

Démonstration du lemme. L'application est injective et à valeur dans V. Soit $z \in V$ et $u_1, \dots, u_k$ ses antécédants. Alors d'après le lemme 1

$$\forall j \in [1, k], u_i \in \bigcup_{i=1}^{k} U_i.$$

Comme les $(U_i)_{i\in[1,k]}$ sont disjoints et que f est injective sur chaque U_i, on en déduit que exactement un des $(u_j)_{j\in[1,k]}$ est dans U_{i_0}. □

On en déduit que pour tout $i \in [1, k]$, $f : f^{-1}(V) \cap U_{i_0} \to V$ est un difféomorphisme, c'est-à-dire que f est un revêtement. □

Exemple. L'application

$$\begin{array}{rccc} f : & \mathbb{S}^2 & \longrightarrow & \mathbb{S}^5 \\ & (x, y, z) & \longmapsto & (x^2, y^2, z^2, \sqrt{2}yz, \sqrt{2}xz, \sqrt{2}xy) \end{array}.$$

définit un plongement de $\mathbb{P}^1(\mathbb{R})$ dans $\mathbb{S}^5$.

Remarque. C'est un exercice non corrigé du [[Lau01]].

9 Théorème d'inversion locale et du rang constant

Leçons concernées
- 206 - Théorèmes de point fixe, exemples et applications.
- 214 - Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.
- 215 - Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.

Théorème d'inversion locale

Théorème. Si $f : E \to F$ une fonction C^k, avec $k \geq 1$, entre $\mathbb{R}$-espace vectoriel de dimension finie (ou entre ouverts) et $x_0 \in E$. Si $Df(x_0)$ est inversible alors f réalise un C^k difféomorphisme entre un voisinage ouvert de x_0 vers un voisinage ouvert de $f(x_0)$.

Démonstration. Quitte à remplacer f par $x \mapsto Df(x_0)^{-1}.(f(x+x_0)-f(x_0))$, on peut supposer $E = F$, $x_0 = 0$, $f(x_0) = 0$ et $Df(x_0) = Id_E$. Pour $y \in F$ on pose

$$\begin{array}{rccc} \phi_y : & E & \longrightarrow & E \\ & x & \longmapsto & x - f(x) + y \end{array},$$

si bien que

$$\forall x, y \in E, f(x) = y \iff \phi_y(x) = x.$$

Comme $D\phi_y(x) = dx - Df(x)$ il existe $r > 0$ tel que

$$\forall y \in F, \forall x \in B(0,r), ||D\phi_y(x)|| \leq \tfrac{1}{2}.$$

Pour $y \in F$ et $x \in E$, on a $||\phi_y(x)|| \leq ||y|| + ||x - f(x)||$, donc si $||x|| \leq r$ et $||y|| < r/2$ on a $||\phi_y(x)|| < r$ (bien remarquer les inégalités srictes et larges). On applique alors le théorème du point fixe à paramètre à la fonction

$$\begin{array}{rccc} \phi : & B(0,r/2) \times \bar{B}(0,r) & \longrightarrow & \bar{B}(0,r) \\ & (y,x) & \longmapsto & \phi_y(x) \end{array},$$

et on en déduit que : pour tout $y \in B(0,r/2)$ il existe un unique $g(y) \in \bar{B}(0,r)$ tel que $\phi_y(g(y)) = g(y)$ soit $f(g(y)) = y$. Or ϕ_y envoie $B(\bar{0},r)$ dans $B(0,r)$, donc en fait $g(y) \in B(0,r)$. Celà veut dite que f est bijective de $U := f^{-1}(B(0,r/2)) \cap B(0,r)$ (ouvert) vers $V := B(0,r/2)$ de bijection réciproque g continue.

Il reste à montrer que g est différentiable et de classe C^k. Soit $a \in U$. On pose $b = f(a)$ et $L = Df(a)$ et on écrit

$$f(a+h) = f(a) + L.h + ||h||\varepsilon(h).$$

Pour k tel que $b+k \in V$ on pose $h_k = g(b+k) - g(a)$ (ce qui équivaut à $k = f(a+h_k) - f(a)$). On a donc $k = L.h_k + ||h_k||\varepsilon(h_k)$, ce qui donne

$$g(b+k) - g(a) = h_k = L^{-1}.k - ||h_k||L^{-1}.\varepsilon(h_k).$$

Il faut montrer que $||h_k||L^{-1}.\varepsilon(h_k)) = o(||k||)$. Par inégalité triangualire, on a

$$||h_k|| \leq ||L^{-1}||.||k|| + ||L^{-1}||.||\varepsilon(h_k)||.||h_k||.$$

Comme l'application $k \to h_k$ est continue, pour k assez petit on a

$$||L^{-1}||.||\varepsilon(h)|| \leq 1/2,$$

ce qui donne $||h|| \leq 2||L^{-1}||.||k||$, puis

$$||h||.||L^{-1}.\varepsilon(h)|| \leq 2||L^{-1}||.||L^{-1}.\varepsilon(h)||.||k||,$$

avec $2||L^{-1}||.||L^{-1}.\varepsilon(h)|| \xrightarrow{k \to 0} 0$. Ce qui prouve que g est différentiable en a de différentielle L^{-1}.

Il reste à montrer que g est de classe C^k. On a $Dg(y) = [Df(g(y))]^{-1}$, on montre alors que g est C^k par récurrence sur k. □

Théorème du rang constant

Théorème. Soient $f : E \to F$ C^k, $a \in E$ tel que $rg(Df)$ est constant au voisinage de a. On note $T_a f$ l'application tangente de f en a. Alors il existe $\Phi : U \to U'$ un C^k-difféomorphisme entre deux voisinages de a et $\Psi : U \to U'$ un C^k-difféomorphisme entre deux voisinages de $f(a)$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} U & \xrightarrow{f} & V \\ {\scriptstyle\Phi}\downarrow{\scriptstyle\sim} & & {\scriptstyle\sim}\downarrow{\scriptstyle\Psi} \\ U' & \xrightarrow[T_a f]{} & V' \end{array}$$

De plus on a $D_a\Phi = Id_E$ et $D_{f(a)}\Psi = Id_F$.

Démonstration. On se ramène au cas $a = 0$ et $f(a) = 0$. On note $L = D_a f$, E' un supplémentaire de $\ker L$ dans E, F' un supplémentaire de $\operatorname{Im} L$ dans F et $\tilde{L} = L^{Im\,L}_{E'}$. L'application $\tilde{L} : E' \to \operatorname{Im} L$ est alors un isomophisme et on a les décompositions :

$$\begin{aligned} E &= \ker L \oplus E', \\ F &= \operatorname{Im} L \oplus F'. \end{aligned}$$

On note aussi $f = (f_1, f_2)$ la décomposition de f sur $F = \operatorname{Im} L \oplus F'$. On considère :

$$\begin{array}{rccc} \Phi : & \ker L \oplus E' & \longrightarrow & \ker L \oplus E' \\ & (x, y) & \longmapsto & (x, \tilde{L}^{-1} f_1(x, y)) \end{array}.$$

$$\ker L \oplus E' \longrightarrow \ker L \oplus \operatorname{Im} L \longrightarrow \ker L \oplus E'$$

$$(x, y) \longrightarrow (x, f_1(x, y)) \longrightarrow (x, \tilde{L}^{-1} f_1(x, y))$$

On a alors $D_a\Phi = Id_{\ker f} \oplus \tilde{L}$, donc est localement inversible en a. De plus le diagramme suivant commute :

$$\begin{array}{ccc} \ker L \oplus E' & \xrightarrow{f_1} & \operatorname{Im} L \oplus F' \\ {\scriptstyle\Phi}\downarrow & \nearrow_{L} & \\ \ker L \oplus E' & & \end{array}$$

Le diagramme suivant commute aussi :

$$\begin{array}{ccc} \ker L \oplus E' & \xrightarrow{f=(f_1,f_2)} & \operatorname{Im} L \oplus F' \\ {\scriptstyle\Phi}\downarrow & \nearrow_{(\tilde{L},f_2)} & \\ \ker L \oplus E' & & \end{array}$$

Comme (L, f_2) est de rang constant au voisinage de $a = 0$, il existe U' voisinage de a tel que $D_1 f_2 = 0$. La fonction f_2 ne dépend alors pas de la première variable : $\forall (x, y) \in U', f_2(x, y) = f_2(0, y)$. On pose alors :

$$\begin{array}{rccc} \Psi : & \operatorname{Im} L \oplus F' & \longrightarrow & \operatorname{Im} L \oplus F' \\ & (x', y') & \longmapsto & (x', y' - f_2\left(0, \tilde{L}^{-1}(x')\right)) \end{array}.$$

On a alors $D_{f(a)}\Psi = Id_F$, donc Ψ est un C^k-difféomorphisme au voisinage de $f(a)$. De plus le diagramme suivant commute :

$$\begin{array}{ccc} & & \operatorname{Im} L \oplus F' \\ & \nearrow_{(\tilde{L},f_2)} & {\scriptstyle\Psi}\downarrow \\ U' \subset \ker L \oplus E' & \xrightarrow[L]{} & \operatorname{Im} L \oplus F' \end{array}$$

Au bilan le diagramme suivant commute :

$$\begin{array}{ccc} \Phi^{-1}(U') \subset \ker L \oplus E' & \xrightarrow{f_1} & \operatorname{Im} L \oplus F' \\ \Big\downarrow{\scriptstyle \Phi} & & \Big\downarrow{\scriptstyle \Psi} \\ U' \subset \ker L \oplus E' & \xrightarrow[L]{} & \operatorname{Im} L \oplus F' \end{array}$$

Pour conclure on se restreint à des ouverts où Φ et Ψ sontdes difféomorphisme. □

10 Toute hypersurface compacte est définie par une équation globale

Leçons concernées
- 203 - Utilisation de la notion de compacité.
- 214 - Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.
- 217 - Sous variétés de $\mathbb{R}^n$. Exemples.
- 225 - Étude locale de surfaces. Exemples.

Théorème. Toute hypersurface H de $\mathbb{R}^n$ compacte C^k est définie par une équation globale C^k.

Démonstration. Pour tout $x \in H$, il existe V_x voisinage de x dans H et $N_x : V_x \to S$ un champ de vecteur orthogonal de classe C^k.

Lemme (Voisinage epsilon)**.** Pour $\varepsilon > 0$, on note

$$V_\varepsilon(H) = \Big\{ x \in \mathbb{R}^n : d(x,H) < \varepsilon \Big\}.$$

Alors il existe $\varepsilon > 0$ tel que l'application suivante soit bijective

$$\begin{array}{rccc} \phi : & V \times]-\varepsilon,\varepsilon[& \longrightarrow & V_\varepsilon(H) \\ & (y,t) & \longmapsto & y + tN_y(y) \end{array}.$$

Démonstration. Pour $X \in H$, on peut choisir $\varepsilon_x > 0$ et diminuer V_x pour que l'application suivante soit injective

$$\begin{array}{rccc} \phi_x : &]-\varepsilon_x,\varepsilon_x[\times]-\varepsilon_x,\varepsilon_x V_x & \longrightarrow & \mathbb{R}^n \\ & (t,y) & \longmapsto & y + tN_x(y) \end{array}.$$

Par compacité, il existe I une partie finie de H tel que $H = \bigcup_{x\in I} V_x$, et on note $\varepsilon = \min_{x\in I} \varepsilon_x$. On note :

$$\delta = \min \Big\{ d(x,y) \mid x, x' \in H \text{ et } x, x' \text{ ne sont pas dans le même ouvert} \Big\}.$$

On prend alors $\varepsilon = \min(\varepsilon_1, \delta/4)$. □

On note $\lambda : \mathbb{R} \to \mathbb{R}$ une fonction C^∞ impaire strictement croissante $[-\varepsilon/2, \varepsilon/2]$ telle que $\lambda'(0) = 1$ et $\lambda(t) = \varepsilon/2$ si $t > 1$. Pour $x \in I$, on note $U_x = \{y + tN_x(y) \mid y \in V_x, t \in]-\varepsilon,\varepsilon[\}$ et :

$$\begin{array}{rccc} f_x : & U_x & \longrightarrow & \mathbb{R} \\ & y + tN_x(y) & \longmapsto & \phi(t) \end{array}.$$

On a pour $\alpha \leq \varepsilon$:

$$\{y + tN_x(y) \mid x \in I, y \in V_x, |t| \leq \alpha\} = \{z \in \mathbb{R}^n \mid d(z,H) \leq \alpha\}.$$

Donc en posant $U_0 = \{z \in \mathbb{R}^n \mid d(z,H) > \varepsilon/2\}$, on a $\mathbb{R}^n = \bigcup_{x\in I} U_x \cup U_0$. On note $f_0 : U_0 \to \mathbb{R}$ la fonction constante à 1. On a alors une famille $(f_i : U_i \to \mathbb{R})_{i\in[0,N]}$ qui vérifie la propriété

$$\forall i,j \in [0,N], \exists e \in \{-1,1\}, \forall x \in U_i \cap U_j, f(x_i) = ef(x_j)f.$$

On note X l'ensemble des $x \in \mathbb{R}^n$ tel que : il existe une suite de boule $B_1, \dots, B_p$ centré sur $[0,x]$. vérifiant
- $0 \in B_1$, $x \in B_l$.
- $\forall l \in [1,p], B_l \cap B_{l+1} \neq \emptyset$ et $(B_1 \cup \dots \cup B_{l-1}) \cap B_{l+1} = \emptyset$.

Montrons que $X = \mathbb{R}^n$. Soit $x \in \mathbb{R}^n$. Il est clair que $X \cap [0,x]$ est un ouvert de $[0,x]$, donc $x \in E$.

On suppose que $0 \notin U_1 \cup \dots \cup U_N$. Pour $x \in \mathbb{R}^n$, on définit $f(x)$ de la façon suivante : on prend une suite de boules $B_1, \dots, B_p$ comme dans le paragraphe précédent. On définit l'application $g : \bigcup_{l=1}^p B_p \to \mathbb{R}$ par : $g = f_{i_1} = f_0$ sur B_1, et pour tout $l \in [2,p]$, sur B_l $g = +f_{i_l}$ si $g = f_{i_l}$ sur $B_{l-1} \cap B_l$ et $g = -f_{i_l}$ si $g = -f_{i_l}$ sur $B_{l-1} \cap B_l$. On pose alors $f(x) = g(x)$.

Montrons que $f(x)$ est indépendant de la suite de boule. Soient $B_1, ..., B_p$ et $B'_1, ..., B'_{p'}$ deux suites et g, g' les fonctions associées. Alors $\bigcup B_l \cap \bigcup B'_l$ est un ouvert contenant $[0,x]$, donc contient Ω un voisinage connexe ouvert de $[0,x]$. On note :

$$E_+ = \{y \in \Omega \mid g = +g' \text{sur un voisinage de } y \text{ dans } \Omega\}.$$

$$E_- = \{y \in \Omega \mid g = -g' \text{sur un voisinage de } y \text{ dans } \Omega\}.$$

Alors E_+, E_- forment une partition de Ω_x en deux ouverts disjoints. Donc $E_+ = \Omega$ et $g = g'$ sur Ω.

La fonction f est C^k, car pour $f = \pm f_i$ localement. Et H est le niveau régulier de f pour 0.

□

Remarque. Voir [GT98] [Sec I.2.30].

11 Loi de groupe sur $\mathbb{R}$

Leçons concernées
- 220 - Équations différentielles $X' = f(t, X)$. Exemples d'études qualitatives des solutions.
- ? ? ?

Théorème. Si $*$ est une loi de groupe sur $\mathbb{R}$(non nécessairement commutative) tel que $(x, y) \mapsto x * y$ est C^1, alors il existe un C^1-difféomorphisme ϕ tel que $\phi(x * y) = \phi(x) + \phi(y)$.

Démonstration. Analyse : on note $L_x(y) = x * y$ et e l'élément neutre. Alors en dérivant $\phi(x*y) = \phi(x)+\phi(y)$ par rapport à y, on obtient

$$\phi'(x * y).L'_x(y) = \phi'(y).$$

En évaluant en $y = e$, celà donne

$$\phi'(x).L'_x(e) = \phi'(e).$$

Comme L_x est un C^1-difféomorphisme (car sa réciproque est $L_{x'}$ avec $x' * x = e$), on en déduit que $L'_x(e) \neq 0$, puis

$$\phi(x) = \phi'(e) \int_e^x \frac{dy}{L'_y(e)}.$$

Synthèse : réciproquement, si on définit ϕ de cette façon. Alors

$$\phi'(x).L'_x(e) = \phi'(e).$$

En dérivant $\phi(x * y)$ par rapport à y on obtient

$$\frac{d}{dy}\phi(x * y) = \phi'(x * y).L_x(y) = \phi'(e)\frac{L_x(y)}{L'_{x*y}(e)}$$

D'autre part en dérivant $L_x \circ L_y(z) = L_{x*y}(z)$ par rapport à z, on a

$$L'_x(y * z).L'_y(z) = L'_{x*y}(z),$$

et en évaluant en $z = e$, on trouve

$$L'_x(y).L'_y(e) = L'_{x*y}(e).$$

On en déduit que $\frac{d}{dy}\phi(x*y) = \frac{d}{dy}\phi(y)$, et on en déduit que $\phi(x*y)-\phi(x*e) = \phi(y)-\phi(e)$, soit $\phi(x*y)-\phi(x) = \phi(y)$. □

Remarque. Voir [[Rou], Ex 24]

12 Théorème de dérivabilité de Lebesgue

Leçons concernées

...

Théorème. Soit $f : [a, b] \to \mathbb{R}$ continue et à variation bornée. Alors f est dérivable sur un ensemble de mesure pleine (f est la différence de deux fonctions croissante donc est mesurable).

Démonstration. On peut se restreindre au cas f croisant. On note :

$$f^+(x) = \limsup_{y\to x} \frac{f(y)-f(x)}{y-x},\ f^-(x) = \liminf_{y\to x} \frac{f(y)-f(x)}{y-x}.$$

$$\begin{cases} A^+ = \{x \in [a, b] \mid f^+(x) = +\infty\}, \\ A^+ = \{x \in [a, b] \mid f^-(x) = -\infty\}, \\ B = \{x \in [a, b] \mid -\infty < f^-(x) < f^+(x) < +\infty\}. \end{cases}$$

Il s'agit de montrer que $\lambda(A^+) = \lambda(A^-) = \lambda(B) = 0$.

Montrons que $\mu(A^+) = 0$. On se fixe $K > 0$. Pour tout $x \in A^+$, il existe u_x tel que $f(u_x) - f(x) \geq K(u_x - x)$. on pose alors $a = \min(x, u_x)$ et $b_x = \max(x, u_x)$.

Lemme (Vitali)**.** Si $(B(x_n, r_n))_{n\in I}$ est une famille finie de boule, alors il existe $J \subset I$ tel que $(B(x_n, r_n))_{n\in J}$ soient disjointes et :

$$\bigcup_{n\in I} B(x_n, r_n) \subset \bigcup_{n\in J} B(x_n, 3r_n).$$

En particulier :

$$\lambda\left(\bigcup_{n\in I} B(x_n, r_n)\right) \leq 3^{dim}\lambda\left(\bigcup_{n\in J} B(x_n, r_n)\right).$$

Démonstration. On raisonne par récurrence sur $Card(I)$. On prend n_0 tel que r_{n_0} soit maximal, on pose :

$$I' = \{n \in I | B(x_n, r_n) \cap B(x_{n_0}, r_{n_0}) = \emptyset\}.$$

Par hypothèse de récurrence il existe $J' \subset I$ tel que $(B(x_n, r_n))_{n\in J'}$ soient disjoints et :

$$\bigcup_{n\in I} B(x_n, r_n) \subset \bigcup_{n\in J'} B(x_n, 3r_n).$$

On prend alors $J = J' \sqcup \{n_0\}$. Si $n \in I$, alors :

$$B(x_n, r_n) \subset \bigcup_{n\in J'} B(x_n, 3r_n) \subset \bigcup_{n\in J} B(x_n, 3r_n),$$

et sinon on a $r_n \leq r_{n_0}$ et $B(x_n) \cap B(x_{n_0}, r_{n_0}) \neq \emptyset$, donc :

$$B(x_n, r_n) \subset B(x_{n_0}, 3r_{n_0}) \subset \bigcup_{n\in J} B(x_n, 3r_n).$$

□

Retour au théorème : il existe une partie finie $I \subset [a, b]$ telle que

$$\lambda\left(\bigcup_{x\in I}[a_x, b_x]\right) \geq \lambda\left(\bigcup_{x\in A^+}[a_x, b_x]\right) \geq 1/2\lambda(A^+).$$

Par le lemme de Vitali il existe $J \subset I$ tel que $([a_x, b_x])_{x\in I}$ soient disjoints et on a alors :

$$\sum_{x\in I} f(b_x) - f(a_x) \geq K \sum_{x\in I} b_x - a_x \geq K/6\lambda(A^+),$$

et ce pour tout $K > 0$. Comme f est à variations bornée on en déduit que $\boxed{\lambda(A^+) = 0}$. On montre de même que $\boxed{\lambda(A^-) = 0}$.

On suppose que $\lambda(B) > 0$. Il existe alors $\beta < \alpha$ tels que :

$$C := \{x \in [a, b] \mid -\infty < f^-(x) < \beta < \alpha < f^+(x) < +\infty\}.$$

Quitte à ajouter à f une fonction affine, on peut suppose $\alpha = -\beta$. Pour $\sigma = (s_1, ..., s_n)$ une subdivision de $[a, b]$, on note :

$$S_\sigma = \sum_{i=1}^n |f(s_{i+1}) - f(s_i)|.$$

Lemme. Si $\sigma = (a_0 < x_1 < y_1 < x_2 < y_2 < ... < x_n < y_n < b_0)$ est tel que :
- $f(a_0) \leq f(b_0)$.
- Il existe $k > 0$ tel que $\forall i \in [1, n] f(y_i) - f(x_i) < -k(y_i - x_i)$.

Alors $S_\sigma \geq S_{a_0,b_0} + k \sum_{i=1}^n y_i - x_i$.

Démonstration. On raisonne par récurrene sur n. Si $n = 1$, alors :

$$\begin{array}{rcl} S_\sigma & = & |f(a_0) - f(x_1)| + f(x_1) - f(y_1) + |f(y_1) - f(b_0)| \\ & \geq & |f(a_0) - f(x_1)| + |f(y_1) - f(b_0)| + k(y_1 - x_1) \\ & \geq & f(b_0) - f(a_0) + k(y_1 - x_1), \end{array}$$

car on a $f(b_0) - f(a_0) \leq |f(a_0) - f(x_1)| + |f(y_1) - f(b_0)|$

Pour n quelconque. On note :

$$\sigma' = (a_0 < x_1 < y_1 < x_2 < y_2 < ... < x_{n-1} < y_{n-1} < b_0).$$

Alors

$$\begin{array}{rcl} S_\sigma & = & S_\sigma - |f(b_0) - f(y_{n-1})| + \\ & & |f(x_n) - f_{y_{n-1}}| + f(x_n) - f(y_n) + |f(y_n) - f(b_0)| \\ & \geq & f(b_0) - f(a_0) + k \sum_{i=1}^n y_i - x_i + |f(x_n) - f_{y_{n-1}}| \\ & & + |f(y_n) - f(b_0)| - |f(b_0) - f(y_{n-1})| \\ & \geq & f(b_0) - f(a_0) + k \sum_{i=1}^n y_i - x_i \end{array}$$

[A completer] □

On part de σ. Pour $x \in C \setminus \sigma$, on prend $[a_x, b_x]$ tel que $[a_x, b_x] \cap \sigma = \emptyset$ et :

$$\begin{cases} f(b_x) - f(a_x) \leq -\alpha(b_x - a_x) & \text{si } f(\sigma_i + 1) \geq f(\sigma_i) \text{avec } x \in [\sigma_i, \sigma_{i+1}] \\ f(b_x) - f(a_x) \geq \alpha(b_x - a_x) & \text{si } f(\sigma_i + 1) \leq f(\sigma_i) \text{avec } x \in [\sigma_i, \sigma_{i+1}] \end{cases}.$$

Comme précédemment, on peut extraire un famille finie $I \subset C \setminus \sigma$ telle que $([a_x, b_x])_{x \in I}$ soient disjoints et :

$$\lambda\left(\bigcup_{x \in I} [b_x, a_x]\right) \geq \frac{1}{6} \lambda(C).$$

On prend alors $\sigma' = \sigma \cup I$ et on a :

$$S_{\sigma'} \geq S_\sigma + \frac{\alpha}{6} \lambda(C).$$

Comme $\lambda(C) > 0$, en réitérant l'opération celà contredit le fait que f est à variation bornée. □

Remarque. Voir [GT98] [Sec I.1.9].

13 Théorème fondamental des courbes

Leçons concernées
– ? ? ?

Théorème. Soient $c(s)$ et $t(s)$ fonctions C^∞, $\gamma_0 \in \mathbb{R}^3$, $\overrightarrow{T}_0, \overrightarrow{N}_0, \overrightarrow{\beta}_0$ une base orthonormée directe. Alors il existe une unique courbe birégulière $\gamma(s)$ paramétré par longueur d'arc, de courbure c, de torsion t tel que $\gamma(0) = \gamma_0$, $\overrightarrow{T}(0) = \overrightarrow{v}_0$ et $\overrightarrow{N}(0) = \overrightarrow{a}_0$.

Démonstration. On note M_0, la matrice de $(\overrightarrow{T}_0, \overrightarrow{N}_0, \overrightarrow{\beta}_0)$ dans la base canonique et $A(s)$ la matrice

$$A(s) = \begin{pmatrix} 0 & -c(s) & 0 \\ c(s) & 0 & \tau(s) \\ 0 & -\tau(s) & 0 \end{pmatrix}.$$

On considère la solution $M(s) \in \mathcal{M}_3(\mathbb{R})$ de

$$\begin{cases} \frac{dM(s)}{ds} = M(s)A(s) \\ M(0) = M_0 \end{cases}.$$

Alors pour tout s, on a $M(s) \in SO_3(\mathbb{R})$: en effet, puisque $M_0 \in SO_3(\mathbb{R})$ et (en utilisant le fait que A est antisymétrique)

$$\frac{d}{ds}(M.{}^tM) = M.{}^t(MA) + (MA).{}^tM = 0.$$

On note alors $(\overrightarrow{T}(s), \overrightarrow{N}(s), \overrightarrow{\beta}(s))$ la base orthonormée directe définie par la matrice $M(s)$, et $\gamma(s)$ la solution de (la fonction $\overrightarrow{T}$ est C^∞)

$$\begin{cases} \frac{d\gamma(s)}{ds} = \overrightarrow{T}(s) \\ \gamma(0) = \gamma_0 \end{cases}.$$

On vérifie alors aisément que la courbe γ est l'unique solution du problème. □

Remarque.
– Si c et τ sont de classe C^1, alors le théorème est aussi vrai.
– Voir par exemple [BGL87].

14 Équation de la chaleur

Leçons concernées
– ? ? ?

Théorème. On note $D = \mathbb{R}\times]0,+\infty[$ et $\bar{D} = \mathbb{R}\times[0,+\infty[$. On se donne $h \in C^0_{2\pi}(\mathbb{R})$. On considère l'équqtion

$$\begin{cases} \partial_t - \partial^2_{x^2} u = 0 & \text{si } (x,t) \in D, \\ u(0,t) = u(\pi,t) = 0 & \text{si } t \in [0,+\infty[, \\ u(x,0) = h(x) & \text{si } x \in \mathbb{R}, \end{cases}$$

où u est une fonction de $C^0_{2\pi}(\bar{D}) \cap C^2(D)$. Alors cette équation admet une unique solution.

Démonstration. Soit u une telle solution. Alors pout tout $t \geq 0$, la fonction $u(.,t)$ est périodique et

$$\forall t \geq 0, \forall x \in \mathbb{R}, u(x,t) = \textstyle\sum_{n\in\mathbb{Z}} c_n(t) e^{-inx},$$

avec

$$c_n(t) = \textstyle\int_0^{2\pi} u(y,t) e^{-iny} \frac{dy}{2\pi}$$

On a pour $t > 0$

$$\tfrac{d}{dt} c_n(t) = \textstyle\int_0^{2\pi} \frac{\partial}{\partial t} u(y,t) e^{-iny} \frac{dy}{2\pi} = \int_0^{2\pi} \frac{\partial^2}{\partial x^2} u(y,t) e^{-iny} \frac{dy}{2\pi},$$

ce qui donne $\frac{d}{dt} c_n(t) = -n^2 c_n(t)$. En utilisant le fait que c_n est continue sur $\mathbb{R}_+$, on en déduti que

$$\forall t \geq 0, c_n(t) = \hat{h}(n) e^{-n^2 t}.$$

On pose alors pour $x \in \mathbb{R}$ et $t > 0$,

$$k_t(x) = \textstyle\sum_{n\in\mathbb{Z}} e^{-n^2 t} e^{inx}.$$

et on a $u(x,t) = (k_t * f)(x)$ [vérifer Fubini].

Réciproquement : cette solution est bien C^2 et vérifie (1). Il reste à montrer qu'elle est continue en $t = 0$. Montrer que $(k_t)_{t>0}$ est une famille d'unités approchées (en regroupant les termes en n et $-n$, on voit que k_t est réel). L'intégrale de k_t vaut 1 d'après sont développement en série de Fourier. Il reste à montrer que k_t est postif.

Lemme. Si h est C^2, alors $k_t * h$ converge uniformément vers h.

Démonstration du lemme. On a

$$|u(x,t) - h(x)| = |\textstyle\sum_{n\in\mathbb{Z}} e^{-n^2 t} \hat{h}(n) e^{inx} - \hat{h}(n) e^{inx}| \leq \sum_{n\in\mathbb{Z}} |1 - e^{-n^2 t}||\hat{h}(n)|.$$

Donc

$$\|u(x,t) - h(x)\|_\infty \leq \textstyle\sum_{n\in\mathbb{Z}} |1 - e^{-n^2 t}||\hat{h}(n)|,$$

et comme $h \in C^2$, on a $\hat{h}(n) = o(n^{-2})$ et donc on peut appliquer la convergence dominée. □

Lemme. Si h est C^2 positive, alors $k_{t_0} * h$ est positif.

Démonstration du lemme. Si $u(x_0,t_0) < 0$. On pose $v(x,t) = e^{-t} u(x,t)$, alors comme u est continue et est positive, sur $\mathbb{R}\times\{0\}$, on en déduit que v atteint un minimum sur $\mathbb{R}\times]0,t_0[$ (on rapelle que $u(,t)$ est périodique). Soit (x_1,t_1) ce minimum. On a alors $\partial_x v(x_1,t_1) = 0$. Or

$$\partial_x v(x_1,t_1) = -e^{-t_1} u(x_1,t_1) + e^{-t_1} \partial_t u(x_1,t_1) = -e^{-t_1} u(x_1,t_1) + e^{-t_1} \partial_{xx} u(x_1,t_1) = -v(x_1,t_1) + \partial_{xx} v(x_1,t_1).$$

Comme $\partial_{xx} v(x_1,t_1) \geq 0$ et $-v(x_1,t_1) > 0$ c'est absurde. □

En prenant $(h_n)_{n\in\mathbb{N}}$ une suite d'unités approchée, on en déduit que $k_t = \lim_{n\to+\infty} k_t * h(n)$ est positif. □

Remarque. Voir par exemple [[ZQ96], Chap IV, Sec VI.3], [[Gou94b], Anal, Chap V, Pb 5], [[DM72], Chap ? ?]

15 Théorie de Floquet

Leçons concernées
- 221 - Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.
- ? ? ?

On considère $A : \mathbb{R} \to \mathcal{M}_n(\mathbb{C})$ continue, T-périodique et l'équation différentielle

$$x'(t) = A(t)x(t).$$

On note $R : \mathbb{R} \to \mathcal{M}_n(\mathbb{C})$ sa résolvante.

Théorème (Floquet)**.**
- Pour $x_0 \in \mathbb{C}^n$, la solution partant de x_0 en $t = 0$ est T-périodique si et seulement si $x_0 \in \ker(R(T) - I_n)$.
- Il existe $S : \mathbb{R} \to \mathcal{M}_n(\mathbb{C})$ T-périodoque et $F \in \mathcal{M}_n(\mathbb{R})$ tel que
$$\forall t \in \mathbb{R}, R(t) = S(t)exp(tF).$$
- Si $1 \notin Spec(R(T))$, alors pour $b : \mathbb{R} \to C^n$, l'équation
$$x'(t) = A(t)x(t) + b(t),$$
admet une unique solution T-périodique.

Démonstration. .[A ompleter] □

Remarque.
- Ce développement a été proposé par Élodie Bouchet.
- La preuve se trouve dans [[GT96], Part. I Chap 1 Ex. 3].

16 Sous-groupes de $\mathbb{R}^n$

Leçons concernées
- ? ? ?

On considère G un sous-groupe fermé de $\mathbb{R}^n$.

Proposition. Si G est discret, alors il existe $(e_1, \dots, e_p)$ une famille libre de $\mathbb{R}^n$ telle que

$$G = \bigoplus_{i=1}^{p} \mathbb{Z}e_i.$$

Démonstration. On montre la propriété par récurrence sur $\dim Vect(G)$. Le cas $\dim Vect(G) = 1$ est connu.

On prend $(f_1, \dots, f_p)$ une famille de G qui soit base de $Vect(G)$. On note $K = \bigoplus_{i=1}^{p} [0,1]f_i$. Comme G est discret, l'ensemble $K \cap G$ est fini [y réfléchir]. On prend alors $e_p \in K$ tel que sa composante sur f_p soit minimal et non nulle. On a alors

$$G = G' \oplus \mathbb{Z}e_p,$$

avec $G' = G \cap Vect(f_1, \dots, f_{p-1})$: en effet, la somme est directe car $(f_i)_{i\in[1,p]}$ est une base et $G' \oplus \mathbb{Z}e_p \subset G$. Soit $g \in G$, il existe $k \in \mathbb{Z}$ tel que $f_p^*(g - ke_p) \in [0, f_p^*(e_p)[$. Il existe $h \in G'$ tel que $g - ke_p - h \in K$. Par minimalité de $f_p^*(e_p)$, on en déduit que $g - ke_p - h = 0$. D'où $G = G' \oplus \mathbb{Z}e_p$.

On conclue alors par hypothèse récurrence. □

Théorème. Il existe deux sous-groupes H, D de G tels que
- H soit discret.
- D soit dense dans $Vect(D)$.
- $Vect(H) \cap Vect(D) = \{0\}$.
- $G = H \oplus D$.

Démonstration. Pour $r > 0$, on note $V_r = Vect(B(0,r) \cap G)$ et $V = \bigcap_{r>0} V_r$. Comme $(V_r)_{r>0}$ est une famille décroissante d'espace vectoriel, il existe $r_0 > 0$ tel que $V = V_{r_0}$. On prend alors $\boxed{D = V \cap G}$.

Lemme. Le groupe D est dense dans V.

Démonstration du lemme. Pour $r \in]0, r_0[$ et $x \in V$, comme $Vect(B(0,r) \cap D = V$ il existe $(e_1, \dots, e_p)$ une famille de $B(0,r) \cap D$ qui soit base de V. On a $\mathbb{Z}e_1 \oplus \cdots \mathbb{Z}e_p \subset D$. Comme le groupe $\mathbb{Z}e_1 \oplus \cdots \mathbb{Z}e_p$ rencontre $B(x, rp)$ (décomposer x sur la base $(e_1, \dots, e_p)$), on en déduit que D rencontre $B(x, rp)$. Ce qui montre que D est dense. □

On note F un supplémentaire de V dans E et $\pi : E \to F$ la projection sur F parallèlement à V.

Lemme. Le groupe $\pi(G)$ est discret.

Démonstration du lemme. Il suffit de montrer que $B(0, r_0/3) \cap \pi(G) = \{0\}$. Soit $g \in G$ tel que $\pi(g) \in B(0, r_0/3)$. Comme $g - \pi(g) \in V$, par densité de D il existe $h \in D$ tel que $\|g - \pi(g) - h\| \leq r_0/3$. On a alors $\|g - h\| \leq 2r_0/3$, donc $g - h \in B(0, r_0) \cap G \subset V$, puis $\pi(g) = 0$. □

D'après la proposition, il existe $(f_1, \dots, f_q)$ une famille de G tel que $(\pi(f_1), \dots, \pi(f_q))$ soit libre et $\pi(G) = \bigoplus_{i=1}^{q} \mathbb{Z}\pi(f_i)$. On note alors $\boxed{H = \bigoplus_{i=1}^{q} \mathbb{Z}f_i}$. Comme $(\pi(f_1), \dots, \pi(f_q))$ est une famille libre de F, on en déduit que $(f_j)_{j\in[1,q]}$ est libre (ce qui implique que H est discret) et que la somme $Vect(f_1, \dots, f_q) + V$ est directe. On montre ensuite aisément que $G = H + D$. □

Remarque. Voir [[GT96], Part. I, Chap 1, Ex. 1], [[AF77], Chap XI.2, Ex 23]

17 Théorèmes de Cauchy-Lipschitz et Cauchy-Peano

Leçons concernés
- 203 - Utilisation de la notion de compacité.
- 206 - Théorèmes de point fixe, exemples et applications.
- 220 - Equations différentielles $X' = f(t, X)$. Exemples d'études qualitatives des solutions.
- 221 - Equations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

Théorème de Chauchy-Lipschitz linéaire

Théorème. Soient E un Banach, I intervalle de $\mathbb{R}$, $A : I \to L_c(E)$ et $B : I \to E$ continues. Alors pour toute condition initiale $(t_0, X_0) \in I \times E$ le problème de Cauchy

$$\begin{cases} X'(t) = A(t)X(t) + B(t) \\ X(t_0) = X_0 \end{cases},$$

admet une unique solution (dans $C^1(I, E)$).

Démonstration. Soit T tels que $K := [t_0 - T, t_0 + T] \subset I$. Pour $f \in C^0([t_0 - T, t_0 + T], E)$, on note $\Phi(f) \in C^1([t_0 - T, t_0 + T], E)$ la fonction définie par

$$\Phi(f)(t) = X_0 + \int_{t_0}^{t} A(s)f(s) + B(s)ds.$$

Alors on a $\Phi(f) = f$ si et seulement si f est solution du problème sur $[t_0 - T, t_0 + T]$. On pose $Y_0 = \tilde{X}_0$ et $Y_{n+1} = \Phi(Y_n)$. On montre alors par récurrence sur $n \in \mathbb{N}$ que

$$\forall t \in, ||Y_{n+1}(t) - Y_n(t)|| \leq ||A||^n_{L^\infty(K)}.||Y_1 - Y_0||_{L^\infty(K)} \frac{|t-t_0|^n}{n!}.$$

Il s'en suit que Y_n est une suite de Cauchy dans $C([t_0 - T, t_0 + T_1], E)$ donc converge vers un point fixe de Φ dans $C([t_0 - T, t_0 + T_1], E)$.

Montrons l'unicité du point fixe sur $C^0([t_0 - T, t_0 + T_1], E)$. Il suffit de montrer que $\Psi : f \mapsto \Psi(f)$ avec $\Psi(f)$ avec $\Psi(f)(t) = \int_{t_0}^{t} A(s)f(s)ds$ n'a que 0 pour point fixe. Si f est point fixe de Ψ, alors on montre par récurrence sur $n \in \mathbb{N}$ que

$$\forall t \in K, ||f(t)|| \leq ||A||^n_{L^\infty(K)} \leq ||f||_{L^\infty(K)} \frac{|t-t_0|^n}{n!}.$$

D'où l'unicité en faisant tendre n vers $+\infty$.

Pour en déduire l'existence et l'unicité d'une solution, il suffit de recoller les solutions obtenue sur chaque compact $K \subset I$. □

A Théorème de Chauchy-Lipschitz avec hypothèse globalement Lipschitzien

Théorème. Soit E un Banach, $f : I \times E \to E$ une application globalement lipschitzienne : il existe $k > 0$ tel que

$$\forall (t, x, y) \in \mathbb{R} \times E \times E, ||f(t, x) - f(t, x)|| \leq k||x - y||.$$

Alors pour toute condition initiale $(t_0, x_0) \in I \times E$, le problème de Cauchy

$$\begin{cases} x'(t) = f(t, x(t)) \\ x(t_0) = f(t_0, x_0) \end{cases},$$

admet une unique solution dans $C^1(I, E)$.

Démonstration. Pour $x \in C^0(I, E)$, on note $\Phi(x) \in C^0(I, E)$ la fonction définie par

$$\Phi(x)(t) = x_0 + \int_{t_0}^{t} f(s, x(s))ds.$$

Montrons que l'une des itérée des Φ est contractante. Soient $x, y \in C^0(I, E)$. On montre alors par récurrence sur $n \in \mathbb{N}$ que

$$\forall t \in I, \|\Phi(x)(t) - \Phi(y)(t)\| \leq \frac{k(|t-t_0|)^n}{n!}\|x - y\|_\infty.$$

Donc Φ^n est contractante pour $\mathbb{N}$ tel que $\frac{k(l(I))^n}{n!} < 1$. □

Théorème de Chauchy-Lipschitz local (cas non-autonome)

Théorème. Soit E un Banach, Ω un ouvert de $\mathbb{R} \times E$, $f : \Omega \to E$ une application localement lipschitzienne : pour tout $(t_0, x_0) \in \Omega$ il existe un voisinage $]t - T, t + T[\times B(x_0, r) \subset U$ et $k > 0$ tels que

$$\forall t \in]t - t_0, t + t_0[, \forall x, y \in B(x_0, r),\ ||f(t, x) - f(t, x)|| \leq k||x - y||.$$

Alors pour toute condition initiale (t_0, x_0) le problème de Cauchy

$$\begin{cases} x'(t) = f(t, x(t)) \\ x(t_0) = f(t_0, x_0) \end{cases},$$

admet une unique solution local, c'est-à-dire qu'il existe I un intervalle contenant t_0 tel qu'il existe une unique fonction $x \in C^1(I, E)$ qui vérifie le problème de Cauchy.

Démonstration. Soient $T > 0$ et $r > 0$ comme dans l'hypothèse. Pour $u \in C([t_0 - T, t_0 + T], \bar{B}(x_0, r))$, on pose

$$\Phi(u)(t) = x_0 + \int_{t_0}^{t} f(s, u(s))ds.$$

On a $\forall t \in [t_0 - T, t_0 + T], ||\Phi(u)(t) - x_0|| \leq T||f||_{L^\infty([t_0-T,t_0+T]\times\bar{B}(x_0,r))}$. Quitte à réduire T, on peut supposer que $T||f||_{L^\infty([t_0-T,t_0+T]\times\bar{B}(x_0,r))} \leq r$. L'opérateur Φ stabilise alors $C([t_0 - T, t_0 + T], \bar{B}(x_0, r))$.

Montrons que pour un $T' \leq T$, Φ est une contraction de $C([t - T', t + T'], \bar{B}(x_0, r))$. Soient $T' < T$ et $u, v \in C([t - T_1, t + T_1], \bar{B}(x_0, r))$, alors

$$\forall t \in [t_0 - T, t_0 + T], ||\Phi(u)(t) - \Phi(v)(t)|| \leq \int_{|t_0,t|} |f(s, u(s)) - f(s, v(s))|ds \leq T_1 k||u - v||_\infty.$$

On prend alors $T_1 \leq k/2$. □

Théorème de Chauchy-Peano

Résultats préliminaires

Théorème (de Schauder)**.** Soit C convexe fermé d'un Banach et $T : C \to C$ continue tel que $T(C)$ est relativement compact. Alors Φ admet un point fixe.

Théorème (d'Ascoli)**.** Soit K espace métrique compact et E un espace métrique. Alors une famille H de $C(K, L)$ est relativement compact si et seulement si elle est uniformément-équicontinue et $\forall x \in K, \{f(x)|f \in H\}$ est relativement compact.

Théorème

Théorème (Cauchy-Peano)**.** Soit U un ouvert de $\mathbb{R}^n \times \mathbb{R}^n$, $f : U \to \mathbb{R}^n$ continue et $(t_0, x_0) \in U$. Alors l'équation $x'(t) = f(t, x(t)), y(t_0) = x_0$ admet une solution.

Démonstration. Par même argument qui ci-dessus il existe $T > 0$ et $r > 0$ tel que $\Phi : u \mapsto x_0 + \int_{t_0}^{t} f(s, u(s))ds$ soit un opérateur de $C([t_0 - T, t_0 + T], \bar{B}(x_0, r)])$ (fermé convexe) dans lui-même (on utilise la dimension finie pour dire que ϕ est borné sur les boules). Il reste à montrer que $\Phi(C([t_0 - T, t_0 + T], \bar{B}(x_0, r)]))$ est une famille uniformément-équicontinue. On note $M = sup_{[t_0-T,t_0+T]\times\bar{B}(x_0,r)}|f(s, x)|$. Alors pour $u \in \Phi(C([t_0 - T, t_0 + T, \bar{B}(x_0, r)]))$, $t, t' \in [t_0 - T, t_0 + T]$, on a $||\Phi(u)(t) - \Phi(u)(t')|| = || \int_{t'}^{t} f(s, u(s))ds|| \leq |t - t'|M$ inférieur à ε dès que $|t' - t| \leq \varepsilon/M$. □

18 Théorème de Glaeser

Leçons concernées
- 218 - Applications des formules de TAYLOR.
- 228 - Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.

Théorème. Soit $f : \mathbb{R} \to \mathbb{R}_+$ de classe C^2. Alors $\sqrt{f}$ est C^1 si et seulement si $f''(x) = 0$ aux points $x \in \mathbb{R}$ où $f = 0$.

Démonstration. Si $g := \sqrt{f}$ est C^1, alors on a $f'' = (g^2)'' = 2g'^2 + gg''$. Si x est un zéros de f, alors x est un zéro de g et on a

$$g(x) = 0 \text{ et } g'(x) = 0,$$

d'où $f''(x) = 0$.

Réciproquement, si $f' = 0$ aux points où $f = 0$. Alors $g := \sqrt{f}$ est C^1 sur $\{f \neq 0\}$. Soit $x \in \mathbb{R}$ tel que $f(x) = 0$. Alors par formule de Taylor-Young, on a

$$f(x + h) = f(x) + f'(x).h + \tfrac{1}{2}f''(x)h^2 + o(h^2) = o(h^2).$$

Donc $g(x + h) = o(h)$ et $g'(x)$ existe et vaut 0. Donc g est dérivable sur $\mathbb{R}$.

Il reste à montrer que g' est continue aux points $x \in \mathbb{R}$ tels que $f(x) = 0$. Soit x tel que $f(x) = 0$ et $h \in \mathbb{R}$ tel que $f(x + h) \neq 0$. On a alors

$$g'(x + h) = \tfrac{f(x+h)}{2\sqrt{f(x+h)}}.$$

Lemme. Pour $r > 0$, on note $M(r) = sup_{h\in[-r,r]}f''(x + h)$. On a alors

$$\forall h \in [-r, r], f'(x + h)^2 \leq 2f(x + h)M(2r).$$

Démonstration. On suppose que $x = 0$ pour simplifier les notations. Soit $h \in [-r, r]$. Le polynôme $P(T) = f(h) + f'(h)T + \frac{M(2r)}{2}T^2$ a pour discriminant $\Delta = f'(h)^2 - 2f(h)M(2r)$. Donc il suffit de montrer que $P(T)$ est positif. Le polynôme $P(T)$ atteint son minimum en $k := f'(h)/M(2r)$ (regarder le zéro de P'). Par accroissements finis, on a $|f'(h)| = |f'(h) - f'(0)| \leq rM(r)$, donc $k \in [-r, r]$. Par égalité de Taylor-Lagrange appliquée entre h et $h + k$, il existe $t \in [-r, r]$ tel que

$$f(h + k) = f(h) + f'(h)k + \tfrac{f''(h+t)}{2}k^2.$$

D'où $P(k) = f(h + k) + \frac{M(r)-f''(h+t)}{2}k^2 \geq 0$. □

On en déduit que $|g'(x + h)| \leq \sqrt{2M(2r)}$ si $h \in [-r, r]$ est tel que $f(x + h) \neq 0$, et c'est même vrai si $f(x + h) = 0$ (car $g'(x + h) = 0$). Comme $\lim_{h\to 0} f''(x + h) = 0$ par hypothèse, on en déduit que $\lim_{h\to 0} g'(x + h) = g'(x) = 0$. □

Remarque.
- Ce développement a été proposé par Irène Marcovici.
- La preuve se trouve dans [[GT98], Part. I, Chap 1, Ex. 11] et [FGN, Analyse 1, 4.33].

19 Ouverts étoilés de $\mathbb{R}^n$

Leçons concernées
– ? ? ?

Théorème. Si Ω est un ouvert étoilé de $\mathbb{R}^n$, alors Ω est C^∞-difféomorphe à $\mathbb{R}^n$.

Démonstration. .[A completer] □

Remarque. Voir [[GT96], Part. I Chap 2 Ex. 4]

Chapitre 6

Analyse fonctionnelle

1 Théorème d'interpolation de Riesz-Thorin

Leçons concernées
- 207 - Prolongement de fonctions. Exemples et applications.
- 208 - Espaces vectoriels normés, applications linéaires continues. Exemples.
- 213 - Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.
- 234 - Espaces L^p.
- 245 - Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$. Exemples et applications.

A Lemme des trois droites d'Hadamard

Lemme. Soit f continue bornée sur $D := \{\text{Re} \in [0,1]\}$ et holomorphe sur l'intérieur. Pour $t \in [0,1]$, on note

$$M_t = \sup_{\text{Re}(z)=t} |f(z)|.$$

Alors on a : $M_t \leq M_0^{1-t} M_1^t$.

Démonstration. • On montre dans un premier temps que $\|f\|_\infty \leq \max(M_0, M_1)$. Supposons d'abord que f tende vers 0 lorsque $|\operatorname{Im} z|$ tend vers $+\infty$. Alors on a $\|f(z)\|_\infty = \max(M_0, M_1)$: en effet, comme $\lim_{|\operatorname{Im} z|\to+\infty} |f(z)| = 0$, la borne $\sup\{|f(z)| : z \in D\}$ est atteinte en un point $z_0 \in D$ et par principe du maximum, le point z_0 est sur le bord.

On revient au cas général. Pour ε, on pose $g(z) = e^{\varepsilon z^2} f(z)$. Alors $|g(z)|$ tend vers 0 quand $|Imz| \to +\infty$, car

$$|g(z)| = e^{\varepsilon(x^2-y^2)}|f(z)| \leq e^{\varepsilon(1-y^2)}\|f\|_\infty.$$

Donc $\|g\|_\infty \leq \max(M_0, e^\varepsilon M_1)$, puis

$$\forall z \in \{\text{Re} \in [0,1]\},\ |f(z)| = e^{\varepsilon(-x^2+y^2)}|g(z)| \leq e^{\varepsilon(-x^2+y^2)} \max(M_0, e^\varepsilon M_1)$$

En faisant tendre ε vers 0, on obtient $\|f\|_\infty \leq \max(M_0, M_1)$.

• Soit $t \in [0,1]$. Pour $\lambda \in \mathbb{R}$, on pose $h(z) = e^{-\lambda t} f(z)$. Alors

$$M_t = \sup_{\text{Re}(z)=t} e^{\lambda t}|h(z)| \leq e^{\lambda t} \max\Big(\sup_{\text{Re}(z)=0} |h(z)|, \sup_{\text{Re}(z)=1} |h(z)|\Big) \leq e^{\lambda t} \max(M_0, e^{-\lambda} M_1).$$

En prenant $\lambda \in \mathbb{R}$ tel que $M_0 = e^{-\lambda} M_1$, on a $e^{\lambda t} \max(M_0, e^\lambda M_1) = M_0^{1-t} M_1^t$. Ce qui achève la preuve du lemme. □

B Théorème d'interpolation de Riesz-Thorin

Théorème (Riesz-Thorin)**.** Soient X, Y deux espaces mesurés, $p_0, p_1, q_0, q_1 \in]1, +\infty[$. On note $L^p(X)$ les fonctions L^p de X vers $\mathbb{C}$. Soit $T : L^{p_0}(X) \cup L^{q_0}(X) \subset \mathcal{M}(X) \longrightarrow \mathcal{M}(Y)$ un opérateur sur l'ensemble des fonctions mesurables tel que $T : L^{p_0}(X) \to L^{q_0}(Y)$ soit de norme $M_0 < +\infty$ et tel que $T : L^{p_1}(X) \to L^{q_1}(Y)$ soit de norme $M_1 < +\infty$. Pour tout $t \in [0,1]$, on note

$$\frac{1}{p_t} = \frac{1-t}{p_0} + \frac{t}{p_1} \text{ et } \frac{1}{q_t} = \frac{1-t}{q_0} + \frac{t}{q_1} \text{ (ce sont des moyennes harmoniques).}$$

Alors pour tout $t \in [0,1]$, l'opérateur T est prolongeable de $L^{p_t}(X) \to L^{q_t}(Y)$ de norme M_t vérifiant : $M_t \leq M_0^{1-t} M_0^t$.

Démonstration. Pour $p \in]1, +\infty[$, on note p' son conjugué. Comme $q_t < +\infty$, le dual de $L^{q_t}(Y)$ est $L^{q_t'}(Y)$. Il faut alors montrer que $M_t \leq M_0^{1-t} M_0^t$, avec

$$M_t = \sup \Big\{ |\langle g, T.f \rangle| : \|f\|_{p_t} = 1, \|g\|_{q_t'} = 1 \Big\},$$

où l'on peut prendre le sup sur l'ensemble des fonctions simples à support borné. Pour $z \in D$, on définit

$$\frac{1}{p_z} = \frac{1-z}{p_0} + \frac{z}{p_1} \text{ et } \frac{1}{q_z'} = \frac{1-z}{q_0'} + \frac{z}{q_1'}.$$

On prend $f \in \mathcal{M}(X)$ et $g \in \mathcal{M}(Y)$ des fonctions simples à support bornés (donc dans tous les L^r). On pose

$$f_z = |f|^{p_t/p_z} \frac{f}{|f(z)|} \text{ et } g_z = |g|^{q_t'/q_z'} \frac{g}{|g(z)|},$$

avec convention $f(z)/|f(z)| = 0$ si $f(z) = 0$. Pour $z \in D$, on pose $F(z) = \langle g_z, T.f_z \rangle$ (on rappelle que $T.f_z \in L^{q_0}(X)$ et que $g_z \in L^{q_0'}(Y)$). En développant les fonctions f et g en fonctions indicatrices, on voit que $F(z)$ est de la forme

$$F(z) = \sum_{j=1}^{k} a_j r_j^z,$$

avec $a_j \in \mathbb{C}$ et $r_j \in \mathbb{R}_+$. On en déduit que $F(z)$ est continue bornée sur D et holomorphe sur l'intérieur. Donc par lemme des trois droites, on a

$$|F(t)| \leq \sup_{Re(z)=0} |F(z)|^{1-t} \sup_{Re(z)=1} |F(z)|^t.$$

Pour $z \in D$, on a $|F(z)| \leq M_0 \|f_z\|_{q_0} \|g_z\|_{q_0'}$. Si $\mathrm{Re}(z) = 0$, alors

$$\|f_z\|_{p_0} = \|f^{Re(p_t/p_z)}\|_{p_0} = \|f^{p_t/p_0}\|_{p_0} = \|f\|_{p_t}^{p_t/p_0},$$

et de même $\|g_z\|_{q_0'} = \|g\|_{q_t'}^{q_t'/q_0'}$. D'où

$$\sup_{Re(z)=0} |F(z)| \leq M_0 \|f\|_{p_t}^{p_t/p_0} \|g\|_{q_t'}^{q_t'/q_0'}.$$

On montre de la même façon que si $\mathrm{Re}(z) = 1$, alors $\|f_z\|_{p_1} = \|f\|_{p_t}^{p_t/p_1}$ et $\|g_z\|_{q_1'} = \|g\|_{q_t'}^{q_t'/q_1'}$. Ce qui donne

$$\sup_{Re(z)=1} |F(z)| \leq M_1 \|f\|_{p_t}^{p_t/p_1} \|g\|_{q_t'}^{q_t'/q_1'}.$$

puis

$$|\langle g, T.f \rangle| = |F(t)| \leq M_0^{1-t} M_1^t \|f\|_{p_t} \|g\|_{q_t'}$$

□

Théorème. Le théorème est aussi vrai pour $p_0, p_1, q_0, q_1 \in [1, +\infty]$.

Démonstration. • Si $q_0, q_1 \in [1, +\infty[$, et $p_0, p_1 \in [1, +\infty]$. On a toujours $\|f_z\|_{p_0} = \|f\|_{p_t}^{p_t/p_0}$ et $\|f_z\|_{p_0} = \|f\|_{p_t}^{p_t/p_0}$ que p_0 et p_1 soient finis ou pas (distinguer tous les cas...). On obtient alors le résultat.

• Si q_0 ou q_1 est fini, alors q_t est fini, donc on peut raisonner par dualité comme précédemment.

• Si $q_0 = q_1 = +\infty$ et $p_0, p_1 \in [1, +\infty]$ (éventuellement tous les deux égaux à $+\infty$). On a donc $q_t = +\infty$. On doit montrer que pour toute fonction simple f, on a

$$\|Tf\|_\infty \leq M_0^{1-t} M_1^t \|f\|_{p_t}.$$

On pose comme précédemment $\frac{1}{p_z} = \frac{1-z}{p_0} + \frac{z}{p_1}$ (avec la convention $1/+\infty = 0$), $f_z = |f|^{p_t/p_z} \frac{f}{|f(z)|}$ et $F(z) = Tf_z$ (à valeur dans $L^\infty(Y)$!!!). En développant f en fonction indicatrice on en déduit que Tf_z s'écrit

$$Tf_z = \sum_{i=1}^{n} \sum_{j=1}^{k} a_j r_j^z h_i.$$

avec $a_j \in \mathbb{C}$ et $r_j \in \mathbb{R}_+$ et h_j des fonctions L^∞.

On admet le théorème des trois droites pour les fonctions holomorphes à valeurs dans $L^\infty(Y)$. On a alors

$$\|F(t)\|_\infty \leq \sup_{Re(z)=0} \|F(z)\|_\infty^{1-t} \sup_{Re(z)=1} \|F(z)\|_\infty^t.$$

On termine alors comme précédemment. □

Remarque. Le théorème est aussi valable pour les fonctions L^p de X vers $\mathbb{R}$ (il suffit de complexifier l'opérateur [y réfléchir]).

Remarque. Voir [Villani ?] ou [[ZQ96], Chap XI.4, Th II.6 et Chap XI.5, Th II.7].

2 Espaces de Bergman

Leçons concernées
- 201 - Espaces de fonctions. Exemples et applications.
- 205 - Espaces complets. Exemples et applications.
- 213 - Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.
- 234 - Espaces L^p.
- 239 - Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.
- 245 - Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$.

A Espaces de Bergman

Définition. Soit Ω ouvert de $\mathbb{C}$. L'*espace de Bergman* sur Ω est $A^2(\Omega) = \mathcal{H}(\Omega) \cap L^2(\Omega)$. On munit $A^2(\Omega)$ du produit scalaire hermitien de L^2.

Lemme. Soient K compact de Ω et $f \in A^2(\Omega)$. Alors

$$\|f\|_\infty^K \leq \frac{1}{\sqrt{\pi} dist(K, {}^c\Omega)} \|f\|_2.$$

Démonstration. Soient $a \in K$ et $R > 0$ tel que $B(a,R) \subset \Omega$. Pour $r \leq R$, on a par formule de Cauchy

$$f(a) = \frac{1}{2i\pi} \int_{C(a,r)} \frac{f(z)}{z-a} dz = \frac{1}{2\pi} \int_0^{2\pi} f(a + re^{it}) dt.$$

En intégrant sur $r \in [0,R]$ on obtient $\int_{r=0}^R \int_{t=0}^{2\pi} f(a+re^{it}) r dr dt = \pi R^2 f(a)$, ce qui donne

$$f(a) = \iint_{B(a,R)} f(z) \frac{d\lambda_2(z)}{\lambda_2(B(0,R))}.$$

En utilisant Hölder, on en déduit que

$$\|f(a)\| \leq \sqrt{\iint_{B(a,R)} |f(z)|^2 \frac{d\lambda_2(z)}{\lambda_2(B(0,R))}} \leq \frac{\|f\|_2}{\sqrt{\pi} R}.$$

En faisant tendre R vers $dist(K, {}^c\Omega)$, on obtient le résultat voulu. □

Théorème. L'espace $A^2(\Omega)$ est un Hilbert.

Démonstration. On va montrer que $A^2(\Omega)$ est fermé dans $L^2(\Omega)$. Soit $(f_n)_{n\in\mathbb{N}}$ une suite de $A^2(\Omega)$ convergeant vers $f \in L^2(\Omega)$. D'après lemme la suite $(f_n)_{n\in\mathbb{N}}$ est de Cauchy dans $C^0(K)$ pour tout compact K de Ω. Par théorème de Montel la suite $(f_n)_{n\in\mathbb{N}}$ converge uniformément sur tout compact vers une fonction holomorphe $g \in \mathcal{H}(\Omega)$. Nécessairement la limite simple est aussi la limite L^2, donc $f = g \in A^2(\Omega)$ (prendre une extraction qui converge presque partout). □

B Noyau de Bergmann

Théorème. Il existe $K : \Omega \times \Omega \to \mathbb{C}$ une fonction continue telle que pour tout $f \in A(\Omega)$ et $z \in \Omega$

$$f(w) = \int_\Omega K(w,z) f(z) dz.$$

Démonstration. Soit $w \in \Omega$. Comme l'application ev_w est continue, il existe $K(w,.) \in A(\Omega)$ telle que $ev_w = K(w,.)$.

Montrons que l'application suivante est continue :

$$\begin{array}{ccc} \Omega & \longrightarrow & A^2(\Omega) \\ w & \longmapsto & K(w,.) \end{array}.$$

Soit $w \in \Omega$ et $h \in \mathbb{C}$ tel que $w + h \in \Omega$. Alors on a

$$\|K(w+h,.) - K(w,.)\|_2 = \sup_{\|f\|_2=1} |\langle K(w+h,.) - K(w,.), f\rangle| = \sup_{\|f\|_2=1} |f(w+h) - f(w)|.$$

Par inégalité des accroissements finis, on a$|f(w+h)-f(w)| \leq \sup_{x\in[w,w+h]} |f'(x)|.|h|$, ce qui donne

$$\|K(w+h,.)-K(w,.)\|_2 = |h| \sup_{\|f\|_2=1} \sup_{x\in[w,w+h]} |f'(x)|.$$

On prend $R>0$ tel que $\overline{B}(w,2R)\subset\Omega$. D'après le formule de Cauchy et d'après le lemme, on a

$$\forall x \in B(w,R),\ |f'(x)| \leq \frac{2}{R}\|f\|_{C^0(C(x,R))} \leq \frac{2}{\sqrt{\pi}R^2}\|f\|_2.$$

On en déduit que $\|K(w+h,.)-K(w,.)\|_2$ tend vers 0 quand h tend vers 0.

L'application $K : \Omega\times\Omega \to A(\Omega)$ est alors continue car c'est la composée des deux applications suivantes qui sont continues

$$\begin{array}{ccc} \Omega\times\Omega & \longrightarrow & A^2(\Omega)\times\Omega \\ (w,z) & \longmapsto & (K(w,.),z) \end{array} \text{ et } \begin{array}{ccc} A^2(\Omega)\times\Omega & \longrightarrow & \mathbb{C} \\ (f,z) & \longmapsto & f(z) \end{array}.$$

(Pour la deuxième fonction, on montre la continuité à la main). □

C Exemple de $A(D)$

Théorème. Pour $n\in\mathbb{N}$, on note $e_n = \sqrt{\frac{n+1}{\pi}}z^n$. Alors $(e_n)_{n\geq 1}$ est une base hilbertienne de $A^2(D)$.

Démonstration. On vérifie aisément que c'est une famille orthonormée.

Il faut montrer que la famille $(z^n)_{n\in\mathbb{N}}$ est dense. Soit $f\in A^2(D)$ et $f(z)=\sum_{n=0}^{+\infty} a_n z^n$ son développement en série entière. Soit $R<1$. La famille $(z^n)_{n\in\mathbb{N}}$ forme une base orthogonale de $A^2(B(0,R))$. Comme la série de fonction $\sum_{n\in\mathbb{N}} a_n z^n$ converge uniformément vers f sur $B(0,R)$, on en déduit qu'elle converge en norme L^2 sur $B(0,R)$. En utilisant Pythagore, on en déduit que

$$\|f\|^2_{L^2(B(0,R))} = \sum_{n=0}^{+\infty} |a_n|^2 \|z^n\|^2_{L^2(B(0,R))}.$$

En faisant tendre R vers 1 et en utilisant la convergence monotone, on en déduit que

$$\|f\|_2^2 = \sum_{n=0}^{+\infty} |a_n|^2\|z^n\|_2^2.$$

La série $\sum_{n\in\mathbb{N}} a_n z^n$ est donc de Cauchy dans $L^2(D)$, car

$$\begin{array}{rcl} \forall q>p>0,\ \left\|\sum_{n=p}^{q} a_n z^n\right\|_2^2 & = & \sum_{n=p}^{q} |a_n|^2\|z^n\|_2^2 \\ & \leq & \sum_{n=p}^{+\infty} |a_n|^2\|z^n\|_2^2 \\ & \xrightarrow{p\to+\infty} & 0 \end{array}$$

Sa limite est nécessairement f. □

Corollaire. L'espace $A^2(D)$ est la complétion de $\mathbb{C}[X]$ pour la norme $L^2(D)$.

Proposition. Le noyau de Bergman de $A^2(D)$ est la fonction

$$K(w,z) = \frac{1}{\pi(1-\bar{w}z)^2}$$

Démonstration. Soit $w \in D$. Comme $(e_n)_{n\in\mathbb{N}} = \sqrt{\frac{n+1}{\pi}} z^n$ est une base hilbertienne, on a

$$K(w,.) = \sum_{n\in\mathbb{N}} \langle e_n, K(w,.)\rangle e_n = \sum_{n\in\mathbb{N}} \frac{n+1}{\pi} \langle z^n, K(w,.)\rangle z^n,$$

l'égalité étant au sens L^2, mais aussi partout d'après le lemme. Or $\langle z^n, K(w,.)\rangle = \bar{w}^n$, d'où

$$\forall z \in D, K(w,z) = \sum_{n\in\mathbb{N}} \frac{n+1}{\pi} (\bar{w}z)^n = \frac{1}{\pi(1-\bar{w}z)^2}.$$

□

Remarque. – Voir [[CLF], Ex ?].

3 Formule d'inversion de Fourier et de Fourier-Plancherel

Leçons concernées
- 205 - Espaces complets. Exemples et applications.
- 207 - Prolongement de fonctions. Exemples et applications.
- 208 - Espaces vectoriels normés, applications linéaires continues. Exemples.
- 213 - Espaces de HILBERT. Bases hilbertiennes. Exemples et applications.
- 234 - Espaces L^p, $1 \leq p \leq +\infty$.
- 235 - Suites et séries de fonctions intégrables. Exemples et applications.
- 240 - Transformation de FOURIER, produit de convolution. Applications.

Pour $f \in L^1(\mathbb{R})$, on note : $\mathcal{F}[f](p) = \int_{\mathbb{R}} f(x)e^{-ipx}\frac{dx}{\sqrt{2\pi}}$.

Lemme. Soient $f, g \in L^1(\mathbb{R})$. On a alors $\mathcal{F}[\mathcal{F}[f].g] = \check{f} * g$ partout.

Démonstration. Comme f et g sont L^1, en appliquant Fubini, on a pour $y \in \mathbb{R}$

$$\begin{array}{rcl} \mathcal{F}[\mathcal{F}(f).g](y) & = & \int_{\mathbb{R}} \left(\int_{\mathbb{R}} f(x)e^{-ipx}\frac{dx}{\sqrt{2\pi}}\right) g(p)e^{-ipy}\frac{dp}{\sqrt{2\pi}} \\ & = & \int_{\mathbb{R}} f(x)\left(\int_{\mathbb{R}} g(p)e^{-ip(y+x)}\frac{dp}{\sqrt{2\pi}}\right)\frac{dx}{\sqrt{2\pi}} \\ & = & \int_{\mathbb{R}} \check{f}(-x)\mathcal{F}[g]((x+y))\frac{dx}{\sqrt{2\pi}} \end{array}.$$

□

On note $h_n(x) = \frac{n}{\sqrt{2\pi}}e^{-(nx)^2/2}$ et $H_n(p) = e^{-(p/n)^2/2}$. Alors les (h_n) sont des unités approchés, et on a : $\mathcal{F}[h_n] = H_n$ et $\mathcal{F}[H_n] = h_n$. Donc pour $f \in L^1(\mathbb{R})$.

$$\mathcal{F}[\mathcal{F}[f].H_n] = \check{f} * h_n.$$

Théorème (Inversion de Fourier)**.** Si $f \in L^1(\mathbb{R})$ est telle que $\mathcal{F}[f] \in L^1(\mathbb{R})$, alors on a $\mathcal{F}[\mathcal{F}[f]] = \check{f}$.

Démonstration. Il suffit de passer à la limite dans la formule précédente. □

Théorème (Parseval)**.** Pour $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$, on a $\|\mathcal{F}[f]\|_2 = \|f\|_2$.

Démonstration. On note $g = f * \bar{\check{f}}$. On a alors $\mathcal{F}[g](p) = |\mathcal{F}[f](p)|^2$. Comme $\check{g} * h_n = \mathcal{F}[\mathcal{F}[g].H_n]$, en évaluant en 0, on obtient

$$(\check{g} * h_n)(0) = \int_{\mathbb{R}} |\mathcal{F}[f](p)|^2 H_n(p)\frac{dp}{\sqrt{2\pi}}.$$

En faisant tendre $n \to +\infty$ (par convergence monotone pour le membre de droite), on en déduit que

$$\check{g}(0) = \int_{\mathbb{R}} |\mathcal{F}[f](p)|^2 \frac{dp}{\sqrt{2\pi}}.$$

Or $\check{g}(0) = \int_{\mathbb{R}} f(x)\bar{\check{f}}(-x)\frac{dx}{\sqrt{2\pi}} = \int_{\mathbb{R}} |f(x)|^2 \frac{dx}{\sqrt{2\pi}}$, ce prouve le résultat. □

On considère $\Phi[f](p) = \lim_{n\to+\infty} \int_{-n}^{n} f(x)e^{-ipx}dx = \mathcal{F}[1_{[-n,n]}f]$.

Théorème (Prolongement)**.** Soit $f \in L^2(\mathbb{R})$
- Alors $\lim_{n\to+\infty}(p \mapsto \int_{-n}^{n} f(x)e^{-ipx}dx = \mathcal{F}[1_{[-n,n]}f])$ converge dans $L^2(\mathbb{R})$ et on note $\Phi[f]$ sa limite.
- Si $f \in L^1(\mathbb{R})$, alors $\Phi[f] = \mathcal{F}[f]$.
- On a $\|\Phi[f]\|_2 = \|f\|_2$.
- On a $\Phi[\Phi[f]] = \check{f}$.

Démonstration. Montrons que la suite $(\mathcal{F}[1_{[-n,n]}f])_{n\in\mathbb{N}}$ est de Cauchy dans $L^2(\mathbb{R})$. Pour $n \geq m \in \mathbb{N}$, on a par parseval

$$\begin{array}{rcl} \|\mathcal{F}[1_{[-n,n]}f] - \mathcal{F}[1_{[-m,m]}f]\|_2^2 & = & \|\mathcal{F}[(1_{[-n,n]} - 1_{[-m,m]})f]\|_2^2 = \|(1_{[-n,n]} - 1_{[-m,m]})f\|_2^2 \\ & \leq & \int_{\mathbb{R}\setminus[-m,m]} f^2 \\ & \xrightarrow{m\to+\infty} & 0 \end{array}.$$

Si $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$, alors la suite $(\mathcal{F}[1_{[-n,n]}f])_{n\in\mathbb{N}}$ converge simplement vers $\mathcal{F}[f]$. Donc $\Phi[f] = \mathcal{F}[f]$.

L'égalité $\|\Phi[f]\|_2 = \|f\|_2$, vient du fait $\|\mathcal{F}[1_{[-n,n]}f]\|_2 = \|1_{[-n,n]}f\|_2$ pour tout $n \in \mathbb{N}$.

Il suffit de montrer que $\Phi[\Phi[f]] = \check{f}$ pour $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$. Comme $f * h_n \in L^1(\mathbb{R})$ et $\mathcal{F}[f * h_n] = \mathcal{F}[f] * H_n \in L^1(\mathbb{R})$, on a donc

$$\Phi[\Phi[f * h_n]] = \mathcal{F}[\mathcal{F}[f * h_n]] = \check{f} * h_n.$$

Comme $\lim_{nto+\infty} f * h_n = f$ dans $L^2(\mathbb{R})$, on a donc $\lim_{nto+\infty} \Phi[\Phi[f * h_n]] = \Phi[\Phi[f]]$ dans $L^2(\mathbb{R})$ et $\lim_{n\to+\infty} f * \check{h}_n = \check{f}$ dans $L^2(\mathbb{R})$ (et aussi dans $L^1(\mathbb{R})$). □

Exemple (Question posée à l'oral Agreg 2010)**.** On a $\mathcal{F}[1_{[-1,1]}] = \sqrt{\frac{2}{\pi}}sinc$. Pour $p \neq \pm 1$, la limite $\lim_{A\to+\infty} \frac{1}{\pi}\int_{-A}^{A} 2sinc(x)e^{ipx}dx$ existe (intégrer par partie). D'après le théorème sa limite est $1_{[-1,1]}$ dans $L^2(\mathbb{R})$. D'où

$$\forall p \in\neq \pm 1, \lim_{A\to+\infty} \frac{1}{\pi}\int_{-A}^{A} 2sinc(x)e^{ipx}dx = \begin{cases} 1 & \text{si } |p| < 1 \\ 0 & \text{si } |p| > 1 \end{cases}.$$

Remarque. Voir [RDH75].

4 Équation de Poisson

Leçons concernées

- 215 - Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.
- 235 - Suites et séries de fonctions intégrables. Exemples et applications.
- 239 - Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.
- 241 - Suites et séries de fonctions. Exemples et contre-exemples.
- 243 - Convergence des séries entières, propriétés de la somme. Exemples et applications.
- 245 - Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$. Exemples et applications.
- 246 - Séries de FOURIER. Exemples et applications.

Cf notes de cours d'analyse.

Remarque. Voir [RDH75].

5 Inégalité de Kolmogorov

Leçons concernées
- ?218 -
- ? ? ?

Théorème. Soit $f : \mathbb{R} \to \mathbb{R}$ de classe C^n. Pour $k \in [0, n]$, note $M_k = sup_{x\in\mathbb{R}}|f^{(k)}(x)|$. On suppose que M_0 et M_n sont finis. Alors M_k est fini et $M_k \leq 2^{k(n-k)/2} M_0^{1-k/n} M_n^{k/n}$ pour tout $k \in [0, n]$.

Démonstration. On montre d'abord que M_k est fini pour tout k. [A completer]

On montre la majoration par récurrence sur n. Si $n = 1$ c'est clair. On montre d'abord que $M_1 \leq \sqrt{2M_0M_1}$. Soit $x \in \mathbb{R}$. Pour $h \leq 0$, on écrit

$$f(x + h) = f(x) + f'(x)h + \tfrac{h^2}{2} f''(\alpha),$$

$$f(x - h) = f(x) - f'(x)h + \tfrac{h^2}{2} f''(\beta).$$

On en déduit que

$$f'(x) = \tfrac{1}{2h}(f(x + h) - f(x - h)) + \tfrac{h}{4}(f''(\beta) - f''(\alpha)),$$

puis pour tout $h \geq 0$:

$$|f'(x)| \leq \tfrac{M_0}{h} + \tfrac{M_2 h}{2} = (\sqrt{\tfrac{M_0}{h}} - \tfrac{M_2 h}{2})^2 + \sqrt{2M_0M_2}).$$

En prenant $h = \sqrt{\frac{2M_0}{M_1}}$, on en déduit le résultat.

Supposons le résultat vrai au rang n. Soit $k \in [0, n]$. On a par hypothèse de récurrence

$$M_k \leq 2^{n(n-k)/2} M_0^{1-k/n} M_n^{k/n}.$$

D'après le cas $n = 2$, on a

$$M_n^2 \leq 2M_{n-1}M_{n+1},$$

et par hypothèse de récurrence, on a

$$M_{n-1} \leq 2^{(n-1)/2} M_0^{1/m} M_n^{1-1/m} .$$

Ce qui donne la majoration sur M_n^2

$$M_n^2 \leq 2^{(n-1)/2+1} M_0^{1/m} M_n^{1-1/m} M_{n+1},$$

puis en divisant (même si $M_n = 0$), la majoration sur M_n

$$M_n^{(m+1)/m} \leq 2^{(n-1)/2+1} M_0^{1/m} M_{n+1}.$$

En élévant ette inégalité à la puissance $k/(m + 1)$ et en réinjectant sur la majoration de M_k, on obtient le résultat. □

Remarque. Voir [FGN, Analyse 1, 4.36], [[Gou94b], Chap ?, Ex ?]

6 Inégalité isompérimétrique

Leçons concernées
- 219 - Problèmes d'extremums.
- 236 - Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables réelles.
- 246 - Séries de FOURIER. Exemples et applications.

Préliminaires

Théorème (Calcul d'aire par formule de Green-Riemann)**.** Soit D un domaine à bord C^1 simple fermé. Alors

$$Aire(D) = \int_\gamma xdy = -\int_\gamma ydx \frac{1}{2}\int_\gamma xdy - ydx.$$

Démonstration. .[A completer] □

Théorème

Théorème. Soit γ une courbe fermé C^1 sans point double de $\mathbb{C}$. On note L sa longueur et S la surface qu'elle définie. Alros on a

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

avec égalité si et seulement si γ est ne cercle.

Démonstration. On paramètre $\gamma : [0,1] \to \mathbb{C}$ de façon positive. Par formule de Green-Riemann, on a

$$S = \frac{1}{2}\int_0^1 x(t)y'(t)dt - x'(t)y(t)dt,$$

et on remarque alors que $S = \frac{1}{2}\int_0^1 \overline{\gamma(t)}\gamma'(t)dt$, soit

$$\boxed{S = \frac{1}{2}\langle \gamma(t), \gamma'(t)\rangle}.$$

Quitte à reparamétrer, on peut supposer que $\forall t \in [0,1], |\gamma(t)| = L$. On a alors

$$\boxed{L^2 = \|\gamma'\|^2}.$$

En développant $\gamma(t) = \sum_{n\in\mathbb{Z}} c_n e^{2i\pi nt}$ et $\gamma'(t) = \sum_{n\in\mathbb{Z}} 2i\pi n\ c_n e^{2i\pi nt}$ en série de fourier et en utilisant la Formule de Parseval (γ et γ' sont L^2 car continues), on a

$$\begin{array}{rcl} L^2 & = & \sum_{n\in\mathbb{Z}} 4\pi^2 n^2 |c_n|^2 \\ S & = & \sum_{n\in\mathbb{Z}} \pi n |c_n|^2 \end{array}$$

Comme pour tout $n \in \mathbb{Z}$, $n^2 \geq n$ avec égalité si et seulement si $n \in \{0,1\}$, on en déduit que

$$L^2 \leq 4\pi S,$$

avec égalité si et seulement si $\gamma(t)$ a pour développement $\gamma(t) = c_0 + c_1 e^{2i\pi t}$, c'est-à)dire aue cùest le cercle de centre c_0 et de rayon $|c_1|$. □

Remarque. Voir [[ZQ96], Th VI 3]

7 Dual de $L^p(X)$ pour $1 \leq p < 2$

Leçons concernées
- 201 - Espaces de fonctions. Exemples et applications.
- 205 - Espaces complets. Exemples et applications.
- 208 - Espaces vectoriels normés, applications linéaires continues. Exemples.
- 234 - Espaces L^p.

Théorème. Si $p \in]1,2[$ et $p' = (1-1/p)^{-1}$, alors l'application suivante est un isomorphisme d'espaces vectoriels normés

$$\begin{array}{rccc} T: & L^{p'}([0,1]) & \longrightarrow & L^{p^*}([0,1]) \\ & f & \longmapsto & T_f \int f \times . \, d\mu \end{array}.$$

Démonstration. Soit $f \in L^{p'}([0,1])$. Par Hölder on a $||T_f|| \leq ||f||$. On considère u mesurable à valeur dans $\{-1,1\}$ tel que $f = u|f|$ et on pose $\phi = u|g|^{p'-1}$. On a alors $||\phi||_p^p = ||\ |g|^{p'-1}\ ||_p^p = ||g^{p'}||^{p'} < +\infty$. On a alors $T_f(\phi) = \int |f|^{p'} = ||f||_{p'}||\phi||_p$. Donc $||T_f|| = ||f||_p$ et T est une isométrie.

Soit $R \in L^{p^*}([0,1])$. Pour $f \in L^p([0,1])$, on a $|R(g)| \leq ||R||\ ||g||_p \leq ||R||\ ||g||_2$. Donc $R_{|L^2}$ est continue et il existe ($L^2([0,1])$ est un Hilbert) $f \in L^2([0,1])$ tel que $R_{|L^2} = \int f \times\ .\, dx$ sur $L^2([0,1])$.

Montrons que $f \in L^{p'}([0,1])$. Soit u tel que $f = u|f|$ et $g_n = u|f|^{p'-1}\chi_{|f|\leq n} \in L^\infty([0,1])$. On a alors

$$R(g_n) = \int f g_n = \int f^{p'}\chi_{|f|\leq n} \leq ||R||\ ||g_n||_p = ||R||\left(\int |f|^{p'}\chi_{|f|\leq n}\right)^{1/p},$$

soit

$$\left(\int f^{p'}\chi_{|f|\leq n}\right)^{1/p'} \leq ||R||,$$

et par théorème de convergence monotone $\left(\int f^{p'}\right)^{1/p'} \leq ||R||$. Donc $f \in L^{p'}([0,1])$.

On a $R(g) = T_f(g)$ sur $L^2([0,1])$ dense dans $L^p([0,1])$ donc $R = T_f$.

□

Remarque. Voir [HL98], [BCL83], [ZQ96].

8 Méthode de Laplace et des phases stationnaires

Leçons concernées
- 218 - Applications des formules de TAYLOR.
- 239 - Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

Méthode de Laplace

Soient $\phi, f : [a, b[\to \mathbb{R}$ deux fonctions telles que
- ϕ est de classe C^2.
- f mesurable continue en a et telle que $f(a) \neq 0$.

On note $F(t) = \int_a^b e^{-t\phi(x)} f(x)dx$. On veut étudier l'équivalent en $+\infty$ de F.

On suppose que $F(t_0)$ existe pour un t_0 et que ϕ est croissante. Ce qui implique que $F(t)$ existe pour $t > t_0$, car

$$|e^{-t\phi(x)} f(x)| \leq e^{(t_0-t)\phi(a)} |e^{-t_0\phi(x)} f(x)|.$$

Proposition. Si $\phi : [0, b[\to \mathbb{R}, x \mapsto x$, alors

$$F(t) \sim \tfrac{f(0)}{t}.$$

Démonstration. On commence par remarquer que pour tout $\alpha > 0$

$$\int_0^\alpha e^{-tx} dx = \tfrac{1}{t} \int_0^{t\alpha} e^{-u} du \sim \tfrac{1}{t}.$$

Comme f est continue en a, il existe $M > 0$ et $\alpha > 0$ telle que $|f(x)| < M$ sur $[0, \alpha]$. D'une part, on a par convergence dominée

$$\int_0^\alpha e^{-tx} f(x)dx = \tfrac{1}{t} \int_a^{t\alpha} e^{-u} f(\tfrac{u}{t})du \sim \tfrac{f(0)}{t}.$$

Et d'autre part on a

$$\int_\alpha^b |e^{-tx} f(x)|dx \leq e^{(t_0-t)\alpha} \int_\alpha^b |e^{-t_0\phi(x)} f(x)|dx = o(t^{-1}),$$

ce qui permet de conclure. □

Proposition. Si $\phi'(a) > 0$, alors

$$F(t) \sim \tfrac{1}{\phi'(a)} \tfrac{e^{-t\phi(a)} f(a)}{t}.$$

Démonstration. On écrit $\phi(a + h) = \phi(a) + \phi'(a)h + \varepsilon(h)h$. Alors

$$F(t) = e^{-t\phi(a)} \int_0^{b-a} e^{-th(\phi'(a)+\varepsilon(h))} f(a + h)dh.$$

Or, on a

$$\int_0^{b-a} e^{-th(\phi'(a)+\varepsilon(h))} f(a + h)dh = \int_0^{(b-a)t\phi'(a)} e^{-u(1+\frac{1}{\phi'(a)}\varepsilon(\frac{u}{t\phi'(a)}))} f(a + \tfrac{u}{t\phi'(a)})dh \tfrac{1}{t\phi'(a)}.$$

En utilisant la convergence dominée, on en déduit que cette intégrale est équivalente à $f(a)/(\phi'(a)t)$. □

Proposition. Si $\phi : [0, b[\to \mathbb{R}, x \mapsto x^2$, et si $F(t_0)$ existe pour un t_0, alors

$$F(t) \sim \tfrac{\sqrt{\pi}}{2} \tfrac{f(0)}{\sqrt{t}}.$$

Démonstration. On a

$$\int_0^b e^{-tx^2} f(x)dx = \int_0^{\sqrt{t}b} e^{-y^2} f\Big(\tfrac{y}{\sqrt{t}}\Big) \tfrac{dy}{\sqrt{t}}.$$

On en déduit le résultat comme précédemment. □

Proposition. Si $\phi'(a) = 0$, $\phi''(a) > 0$, alors

$$F(t) \sim \sqrt{\tfrac{\pi}{2\phi''(a)}} \tfrac{e^{-t\phi(a)} f(a)}{\sqrt{t}}.$$

Démonstration. .[A completer] □

Application à la fonction Γ

On rappelle que la fonction Γ est définie par

$$\forall t > -1,\ \Gamma(t+1) = \int_0^{+\infty} x^t e^{-x} dx.$$

Pour $t > -1$, la fonction $x \mapsto e^{-x}x^t$ atteint son maximum en $x = t$, ce qui amène à faire le changement de variable $x = t(u+1)$

$$\Gamma(t+1) = \int_{-1}^{+\infty} t^t (u+1)^t e^{-t(u+1)} t du = t^{t+1} \int_{-1}^{+\infty} e^{-t\phi(u)} du,$$

avec $\phi(u) = 1 + u - ln(u+1) = 1 + u^2/2 + o(u^2)$. On vérifie aisément que ϕ est coissante sur $[0, +\infty[$ et décroissante sur $]-1, 0]$, ce qui permet d'appliquer le théorème précédent :

$$\int_0^{+\infty} e^{-t\phi(u)} du \simeq \sqrt{\tfrac{\pi}{2t}} e^{-t},$$

$$\int_{-1}^{0} e^{-t\phi(u)} du = \int_0^1 e^{-t\phi(-v)} dv \simeq \sqrt{\tfrac{\pi}{2t}} e^{-t}.$$

On en déduit que

$$\Gamma(t+1) \simeq \sqrt{2\pi t} \left(\tfrac{t}{e}\right)^t.$$

Méthode des phases stationnaires

[A completer]

Remarque.
- Ce développement a été proposé par Anne-Laure Mouly.
- Voir [[Rou], Ex 113], [[ZQ96], Chap IX, Sec VI].

9 Fonctions Lipschitziennes

Leçons concernées
- 201 - Espaces de fonctions. Exemples et applications.
- 228 - Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.
- 234 - Espaces L^p.

Théorème. Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction k-lipschitzienne. Alors il existe $g \in L^\infty(\mathbb{R})$ tel que $f(x) = f(0) + \int_0^x g(t)dt$.

Démonstration. On définit la fonction

$$T : C_c^\infty(\mathbb{R}) \to \mathbb{R}, \phi \mapsto -\int_{\mathbb{R}} f\phi'.$$

Montrons que T est continue pour la norme L^1. Soit $\phi \in C_c^\infty(\mathbb{R})$, alors on a

$$-\int_{\mathbb{R}} f\phi' = \lim_{h\to 0} -\int_{\mathbb{R}} f(t)\frac{\phi(t+h)-\phi(t)}{h}dt,$$

(dominer par $|f|1_{supp(\phi)}||\phi'||_\infty$). Or pour $h \in \mathbb{R}$

$$\left|\int_{\mathbb{R}} f(t)\frac{\phi(t+h)-\phi(t)}{h}dt\right| = \left|\int_{\mathbb{R}} \frac{f(t-h)-f(t)}{h}\phi(t)\right| \leq k\int_{\mathbb{R}} |\phi|dt.$$

Donc $T(f) \leq k||\phi||_1$ et T se prolonge sur $L^1(\mathbb{R})$ de façon continue.

Pour $n \in \mathbb{N}$, T est continue sur $L^2([-n,n]) \subset L^1(\mathbb{R})$. Il existe donc un unique $g_n \in L^2([-n,n])$ tel que

$$\forall f \in L^2([-n,n]), T(f) = \int_{\mathbb{R}} g_n f.$$

On peut définir $g = sup_n\ g_n$. On prend u à valeur dans $\{-1,1\}$ tel que $g = u|g|$. Soit $\varepsilon > 0$. On note $A_n = \{|g_n| \geq k+\varepsilon\}$ et $A = \{|g| \geq k+\varepsilon\}$. On a alors $u1_{A_n} \in L^2([-n,n])$ et

$$T(u1_{A_n}) = \int g_n u\chi_{A_n} = \int_{A_n} |g| \geq (k+\varepsilon)\lambda(A_n).$$

D'autre part $|T(u1_{A_n})| \leq k||u1_{A_n}||_1 \leq k\lambda(A_n)$, donc $\lambda(A_n) = 0$ puis $A = 0$ (car A est limite croissante des A_n). Donc $||g||_\infty \leq k$. Pour $\phi \in C_c^\infty(\mathbb{R})$ et $n \in \mathbb{N}$ tel que $supp(\phi) \subset [-n,n]$ on a $T(\phi) = \int g_n\phi = \int g\phi$, donc $T(h) = \int gh$ pour $h \in L^1(\mathbb{R})$.

On note $G(x) = \int_0^x g(t)dt$. Alors pour $\phi \in C_c^\infty(\mathbb{R})$, on a

$$\begin{array}{rcl}
\int_{\mathbb{R}} G(x)\phi'(x)dx &=& \int_{x=0}^{+\infty}\int_{t=0}^{x} g(t)\phi'(x)dtdx - \int_{x=-\infty}^{0}\int_{t=x}^{0} g(t)\phi'(x)dtdx \\
&=& \int_{t=0}^{+\infty}\int_{x=t}^{\infty} g(t)\phi'(x)dxdt - \int_{t=-\infty}^{0}\int_{x=-\infty}^{t} g(t)\phi'(x)dxdt \\
&=& \int_{t=0}^{+\infty} g(t)(-\phi(t))dt - \int_{t=-\infty}^{0}\phi(t)dxdt \\
&=& -\int_{t=-\infty}^{+\infty} g(t)\phi(t)dt \\
&=& -T(\phi) \\
&=& -\int_{\mathbb{R}} f(x)\phi'(x)dx
\end{array}.$$

Donc si on pose $H = G - f$ on a $\forall\phi \in C_c^\infty(\mathbb{R}), \int_{\mathbb{R}} H\chi' = 0$. On note $I : C_c^\infty(\mathbb{R}) \to \mathbb{R}, \phi \mapsto \int\phi$. Si $I(\phi) = 0$ alors ϕ est du type $\phi = \psi'$ avec $\psi \in C_c^\infty(\mathbb{R})$ donc $\int_{\mathbb{R}} H\phi = 0$ et $\ker I \subset \ker \int H.$, Donc il existe λ tel que $\int H. = \lambda I$.

Il reste à montrer que $H = \lambda$ On pose $F = H - \lambda$. Soit $n \in \mathbb{N}$ et $\theta \in C_c^\infty(\mathbb{R})$ valant 1 sur $[-n,n]$. On prend (ρ_k) des unités approchés dasn $C_c^\infty(\mathbb{R})$. Alors $F\theta * \rho_k \xrightarrow{L^1(\mathbb{R})} F\theta$ et $f\theta * \rho_k(x) = \int_{\mathbb{R}} F(y)(\theta(x)\rho(x-y))dy = 0$ car $\theta(x)\rho(x-y) \in C_c^\infty(\mathbb{R})$. Donc $F\theta = 0$ puis $F = 0$. □

Remarque. La preuve a été prise sur la liste de développement de Brice Loustau.

10 Injection de Sobolev

Leçons concernées
- ? ? ?

Lemme. Soit $f \in L^1_{loc}(\mathbb{R})$ tel que

$$\forall \phi \in C^0_c(\mathbb{R}), \int_{\mathbb{R}} f(x)\phi(x)dx = 0.$$

Alors $f = 0$.

Démonstration. .[A completer] □

Lemme. Soit $f \in L^1_{loc}(\mathbb{R})$ tel que

$$\forall \phi \in C^0_c(\mathbb{R}), \int_{\mathbb{R}} f(x)\phi'(x)dx = 0.$$

Alors f est constante.

Démonstration. .[A completer] □

Définition. Soit I un intervalle de $\mathbb{R}$. L'espace de Sobolev $H^1(I)$ est l'ensemble des $f \in L^2(I)$ tel que

$$\exists f' \in L^2(I), \forall \phi \in C^0_c(I), \int_I f(x)\phi'(x)dx = -\int_I f'(x)\phi(x)dx,$$

auquel cas f' est unique et s'appelle la dérivée faible de f.

Proposition. L'espace $H^1(I)$ munie de la norme $\|f\|^2_{H^1} = \|f\|^2_{L^2} + \|f'\|^2_{L^2}$ est une Hilbert.

Démonstration. .[A completer] □

Proposition. L'espace $H^1([0,1])$ est inclus dans $C^0([0,1])$ avec injection compacte.

Démonstration. .[A completer] □

Remarque.
- Ce développement a été proposé par Sébastien Alvarez.
- Voir [RDH75].

11 Réduction des opérateurs autoadjoints compact dans un Hilbert

Leçons concernées
- 213 -
- ? ? ?

Théorème. Soit H une Hilbert séparable et T un endomorphisme auto-adjoint compact. Alors il existe une base hilbertienne de vecteurs propre pour T.

Démonstration. On commence par le lemme suivant.

Lemme. La norme de T est atteinte en un vecteur propre.

Démonstration du lemme. Soit $(x_n)_{n\in\mathbb{N}}$ sur suite de vecteurs de norme 1 tel que

$$\lim_{n\to+\infty}\langle x_n, T.x_n\rangle = \|T\|.$$

Quittte à extraire, on peut supposer que $(T.x_n)_{n\in\mathbb{N}}$ converge fortement vers y et que $(x_n)_{n\in\mathbb{N}}$ converge faiblement vers x. On a alors $\langle x, y\rangle = \|T\|$: en effet

$$|\langle x_n, T.x_n\rangle - \langle x - y\rangle| \leq |\langle x_n, T.x_n - y\rangle| + |\langle x_n - x, y\rangle| \xrightarrow{n\to+\infty} 0.$$

Pour $h \in H$, on a

$$\langle x, T.h\rangle = \lim_{n\to+\infty}\langle x_n, T.h\rangle,$$

et comme T est autoadjoint, on en déduit que

$$\langle T.x, h\rangle = \lim_{n\to+\infty}\langle T.x_n, h\rangle = \langle y, h\rangle,$$

D'où $T.x = y$ puis $\langle x.T.x\rangle = \|T\|$.

Le vecteur x est alors vecteur propre : en effet la forme quadratique $x \mapsto \|T\|.\|x\|^2 - \langle x.T.x\rangle$ est positive, donc son cône coïncide avec son noyau. Donc x est dans le noyau, ce qui donne $T.x = \|T\|x$. □

On note E la somme hilbertienne des sous-espace propre de T. Si $E \neq H$, alors $T_{|E^\perp}$ $E^\perp$ ($\neq 0$ car E est fermé) admet un vecteur propre ce qui est absurde. □

Remarque. Voir [[GT96], Part. II, Chap 3, Ex. 13].

12 Autour la fonction Γ et de la fonction ζ

Leçons concernées

- 207 - Prolongement de fonctions. Exemples et applications.
- 230 - Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.
- 245 - Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$.
- 247 - Exemples de problèmes d'interversion de limites.

13 Théorème de représentation conforme

Leçons concernées
- 203 - Utilisation de la notion de compacité.
- 219 - Problèmes d'extremums.
- 245 - Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$.

Théorème. Soit Ω ouvert simplement connexe de complémentaire non vide et $z_0 \in \Omega$. Alors il existe un unique biholomorphisme $f : \Omega \to D$ tel que $f(z_0) = 0$ et $f'(z_0) \in \mathbb{R}_+$.

Démonstration. **Unicité :** si f et g sont deux tels fonctions alors fg^{-1} est un biholomorphisme de D qui fixe 0 et tel que $fg^{-1}(0) \in \mathbb{R}_+$, donc lemme de Schwarz $fg^{-1} = Id_D$.

Existence : On note $E = \{f : \Omega \to D | f \text{holomorphe injective et } f(z_0) = 0\}$. Montrons que E est non vide. Soit $a \notin \Omega$, Comme $z - a$ ne s'annule pas sur Ω simplement connexe, il existe $f : \Omega \to \mathbb{C}$ tel que $f(z)^2 = z - a$. On note $z_1 = f(z_0)$, alors $-z_1 \notin \overbrace{f(\Omega)}$, car sinon il existe (y_n) tel que $f(y_n) \to -z_1$ donc $f(y_n)^2 = y_n - a \to z_1^2 = z_0 - a$ soit $y_n \to z_0$ puis $f(y_n) \to f(z_0) = z_1$. Donc il existe $r > 0$ tel que $B(-z_1, r) \cap f(\Omega) = \emptyset$ et l'application $\frac{r}{f(z)+z_1}$ est injective à valeur dans D et en composant par un biholomorphime de D on obtient un élément de E.

Par formule de Cauchy $M := sup_{f\in E}|f'(z_0)| < +\infty$ ($M \neq 0$ car les fonctions sont injectives). On prend (f_n) une suite de E tel que $|f_n'(z_0)| \to M$. Par lemme de Montel il existe une extraction qui cnverge uniformément sur tout compact vers une fonction f. Par lemme de Hurwitz f est injective ou constante mais comme $|f'(z_0)| = M \neq 0$, f est injective, et par théorème de l'application ouverte $f(\Omega)$ est un ouvert inclus dans $\bar{D}$, donc f est dans E.

Montrons que f est surjective. S'il existe $a \in D \setminus f(\Omega)$, alors on pose $\phi_a(z) = \frac{a-z}{1-\bar{a}z}$ et on a $\phi_a'(z) = \frac{1-|a|^2}{(1-\bar{a}z)^2}$. Comme $\phi_a \circ f$ ne s'annule pas sur Ω simpleemnt connexe, il existe $g : \Omega \to D$ tel que $g^2 = \phi_a \circ f$. La fonction g est alors injective. En dérivant on a $2g(z_0)g'(z_0) = \phi_a'(0)f'(z_0) = (1 - |a|^2)M$. Or $g(z_0)^2 = \phi_a(0) = a$, donc $|g'(z_0)| = \frac{1-|a|^2}{2\sqrt{|a|}}M$. On pose $h = \phi_{g(z_0)} \circ g$ qui est dans E. On a alors $h'(z_0) = \phi'_{g(z_0)}(g(z_0))g'(z_0) = \frac{1}{1-|g(z_0)|^2}\frac{1-|a|^2}{2\sqrt{|a|}}M = \frac{1}{1-|a|}\frac{1-|a|^2}{2\sqrt{|a|}}M = \frac{1+|a|}{2\sqrt{|a|}}M$ avec $\frac{1+|a|}{2\sqrt{|a|}} > 1$ (car $(1 - \sqrt{|a|})^2 > 0$) ce qui contredit la maximalité de M. □

Remarque. Voir [CT61].

14 Un truc sur les fonctions convexes

Leçons concernées
- 228 - Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.
- 229 - Fonctions monotones. Fonctions convexes. Exemples et applications.

Théorème. Soit $f : \mathbb{R}_+ \to \mathbb{R}$ C^1 et convexe. On suppose qu'il existe $a \in \mathbb{R}$ tel que

$$\forall x \in \mathbb{R}, f(x) = f(0) + f'(0)x + \tfrac{a}{2}x^2 + o(x^2).$$

Alors f' est dérivable en 0, et $f''(0) = a$.

Démonstration. On se ramène au cas $f(0) = f'(0) = 0$, en remplaçant f par

$$f(x) - (f(0) + f'(0)x)$$

Ce qui ne change pas la convexité car la dérivée est toutjours croissante. On note $\varepsilon(x)$ tel que $g(x) = \frac{a^2}{2} + \varepsilon(x)x^2$.

Soit $x > 0$. On cherche à évaluer le taux d'accroissement

$$\tfrac{f'(x)-f'(0)}{x-0} = \tfrac{f'(x)}{x}.$$

Soient $y < x$ et $z > x$. Par convexité on a

$$\tfrac{f(x)-f(y)}{x-y} \leq f'(x) \leq \tfrac{f(z)-f(x)}{z-x}.$$

Puis

$$\tfrac{1}{x}\tfrac{f(x)-f(y)}{x-y} - a \leq \tfrac{f'(x)}{x} - a \leq \tfrac{1}{x}\tfrac{f(z)-f(x)}{z-x} - a.$$

Or

$$f(x) - f(y) = \Big(\tfrac{a}{2}(1 - (y/x)^2) + \varepsilon(x) - \varepsilon(y)(y/x)\Big)x^2.$$

Donc en notant $\lambda = y/x < 1$, on a $x - y = x(1 - x)$ puis

$$\tfrac{1}{x}\tfrac{f(x)-f(y)}{x-y} - a = \tfrac{a}{2}(\lambda - 1) + \tfrac{\varepsilon(x)-\varepsilon(\lambda x)\lambda^2}{1-\lambda}.$$

Pour $\eta > 0$, il existe $\lambda < 1$ tel que

$$\tfrac{a}{2}(\lambda - 1) \geq -\eta.$$

Il existe $r > 0$ tel que pour tout $x \in]0, r[$

$$\tfrac{\varepsilon(x)-\varepsilon(\lambda x)\lambda^2}{1-\lambda} \geq -\eta.$$

En posant $y = \lambda x$, on a donc

$$\tfrac{f'(x)}{x} - a \geq \tfrac{1}{x}\tfrac{f(x)-f(y)}{x-y} - a \geq -2\eta.$$

En travaillant avec z on a de même

$$\tfrac{f'(x)}{x} - a \leq 2\eta.$$

D'où $\lim_{x\to 0^+} \frac{f'(x)}{x} = a$. □

15 Fonction log-convexe et fonction Γ

Leçons concernées
- 229 - Fonctions monotones et fonctions convexes.
- 245 - Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$, exemples et applications.

Théorème. Soit $f : \mathbb{R}_+^* \to \mathbb{R}_+^*$ vérifiant
- $\forall x \in \mathbb{R}_+^*, f(x+1) = xf(x)$.
- $f(1) = 1$.
- f est log-convexe.

Alors $f = \Gamma$.

Démonstration. Montrons que f est unique. Pour $x > 0$ et $n \in \mathbb{N}$ on a $f(x+n) = (x+n-1)...(x+1)xf(x)$, et $f(n+1) = n!$. Pour $n \geq 2$ et $x > 0$, en comparant les taux d'accroissement on a

$$\frac{1}{(n-1)-n}(\log f(n-1) - \log f(n)) \leq \frac{1}{(n+x)-n}(\log f(n+x) - \log f(n)) \leq \frac{1}{(n+1)-n}(\log f(n+1) - \log f(n)).$$

Soit

$$\log(n-1) \leq \frac{1}{x}(\log f(n+x) - \log(n-1)! \leq \log n.$$

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

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

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

A droite on a $f(x) \leq \frac{(n-1)!n^x}{(x+n-1)...(x+1)x} = \frac{n!n^x}{(x+n)...(x+1)x}\frac{x+n}{n}$, et à gauche en changeant n en $n+1$, on obtient $\frac{n!n^x}{(x+n)...(x+1)x} \leq f(x)$. Donc par théorème des gendarmes.

$$\forall x > 0, f(x) = \lim_{n\to+\infty} \frac{n!n^x}{(x+n)...(x+1)x}.$$

D'où l'unicité.

La fonction Γ est log-convexe car $\Gamma(s) = ||t||_s^s$ pour la mesure $e^{-t}\frac{dt}{t}$, et vérifie les deux autres conditions. □

Remarque. Voir [[RDH75], espace L^p, notes historiques].

16 Polynômes orthogonaux dans $L^2(I,\rho)$

Leçons concernées
- 201 - Espaces de fonctions. Exemples et applications.
- 202 - Exemples de parties denses et applications.
- 213 - Espaces de HILBERT. Bases hilbertiennes. Exemples et applications.
- 239 - Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.
- 240 - Transformation de FOURIER, produit de convolution. Applications.

Théorème. Soit I un intervalle de $\mathbb{R}$ et ρ une fonction poids sur I tel que

$$\int_I e^{\alpha x}\rho(x)dx < +\infty,$$

pour un certain $\alpha > 0$. Alors $\mathbb{C}[X]$ est dense dans $L^2(I,\rho)$.

Démonstration. Soit $f \in L^2(I,\rho)$. On définit

$$\begin{array}{rccc} TF[f]: & \{|\operatorname{Im}| < \alpha/2\} & \longrightarrow & \mathbb{C} \\ & z & \longmapsto & \int_I f(x)e^{izx}\rho(x)dx \end{array}.$$

La fonction $TF[\phi]$ est alors holomorphe (utiliser Wierstrass et le fait que les fonctions f et $e^{ax/2}$ sont dans $L^2(I,\rho)$). On a alors pour $n \in \mathbb{N}$

$$TF[\phi]^{(n)}(0) = i^n \int_I f(x)x^n\rho(x)dx.$$

Donc si $f \in \mathbb{R}[X]^\perp$, alors $TF[f] = 0$. Par injection de la transformée de Fourier on en déduit que $f(x)\rho(x) = 0 \in L^1(\mathbb{R})$, puis que $f = 0 \in L^2(I,\rho)$. □

Remarque.
- Si on prend $\rho = x^{-\ln x}$ et $I = \mathbb{R}_+$, alors $f(x) = \sin(2\pi \ln x)$ est orthogonal à $\mathbb{R}[X]$ (faire le changement de variable $y = \ln x$).
- La preuve se trouve dans [[BMP04], Chap. 3, Ex 3.7].

17 Sous-espaces fermés de $L^2(\mathbb{R})$ invariant par translations

Leçons concernées
- 201 - Espaces de fonctions. Exemples et applications.
- 205 - Espaces complets. Exemples et applications.
- 213 - Espaces de HILBERT. Bases hilbertiennes. Exemples et applications.
- 234 - Espaces L^p.
- 240 - Transformation de FOURIER, produit de convolution. Applications.

Théorème. Les sous-espaces fermés stables par translations de $L^2(\mathbb{R})$ sont du type $TF[L^2(X)]$ avec $X \subset \mathbb{R}$ une partie mesruable.

Démonstration. Soit E un sous-espace de $L^2(\mathbb{R})$ stable par translation. On note $\hat{E} = TF(E)$. Alors $\hat{E}$ est un sous-espace de $L^2(\mathbb{R})$ stable par multiplication par $e^{ip.\alpha}$. On note P la projection orthogonale sur $\hat{E}$. Alors pour tout $f, g \in L^2(\mathbb{R})$, on a :

$$\langle f - Pf, \overline{Pg} e^{ip.\alpha} \rangle = 0.$$

Ce qui signifie que $TF[(f - Pf).Pg] = 0$ ($(f - Pf).Pg \in L^1(\mathbb{R})$). Donc :

$$f.Pg = Pf.Pg,$$

et en echangeant les rôles de f, g, on obtient :

$$f.Pg = Pf.g.$$

On prend $g \in L^2(\mathbb{R})$ strictement positive, par exemple $g(p) = e^{-|p|}$, alors pour tout $f \in L^2(\mathbb{R})$:

$$Pf = \tfrac{Pg}{g} f.$$

Donc P est la multiplication par $\phi = Pg/g$ et on en déduit que $\phi^2 = \phi$ (appliquer $P = \phi$ à $g > 0$). Donc $\phi = 0$ ou 1 presque partout et on note $X = \phi^{-1}(1)$, si bien que $\phi = 1_X$. On en déduit que :

$$f \in \hat{E} \Leftrightarrow Pf = f \Leftrightarrow f_{X^c} = 0.$$

Réciproquement si $X \subset \mathbb{R}$, alors $L^2(X)$ est un sous-espace fermé car complet et stable par multiplication par $e^{ip.\alpha}$, donc $TF[L^2(X)]$ est stable par translation. De plus on a $L^2(X) = L^2(Y)$ si et seulement si $X \delta Y$ est de mesure nulle, car si $L^2(X) \subset L^2(Y)$ alors $1_{X \setminus Y} \in L^2(X) \subset L^2(Y)$, donc $X \setminus Y \cap Y$ est de mesure nulle.

□

Remarque. Voir [[RDH75], Th 9.16]

18 Théorème d'Anossov et de Grobman-Hartman

Leçons concernées
- 206 - Théorèmes de point fixe. Exemples et applications
- 220 - Équations différentielles $X' = f(t, X)$, exemples d'études qualitatives des solutions.
- 221 - Équations différentielles linéaires, exemples et applications.

Préliminaires

Soit E un Banach sur $\mathbb{R}$ ou $\mathbb{C}$ et T un automorphisme hyperbolique de E, c'est-à-dire que
- T est linéaire et continue.
- Il existe deux supplémentaires fermés E_+ et E_- tels qu'il existe $\lambda > 1$ vérifiant
$$||T.X|| \geq \lambda||X|| \text{ sur } E_+ \text{ et } ||T.X|| < 1/\lambda||X|| \text{ sur } E_-.$$

Perturbation du point fixe d'un automorphisme hyperbolique

[Gonnord Topo II.2.10]

Théorème. Il existe $k > 0$ tel que pour toute fonction $f \in Lip_k(E, E)$, $T + f$ admet un unique point fixe.

Démonstration. Soit $k > 0$ et $f \in Lip_k(E, E)$, alors pour $x = (u, v) = E_+ \oplus E_-$, on a

$$\begin{aligned}(T + f)(x) = x &\Leftrightarrow u = T.u + f_+(u, v) \text{ et } v = T.v + f_-(u, v)\\ &\Leftrightarrow u = T^{-1}.u - T^{-1}.f_+(u, v) \text{ et } v = T(v) + f_-(u, v)\end{aligned}$$

Comme $T^{-1}_{|E_+}$ et $T_{|E_-}$ sont contractants pour k assez petit, l'application

$$\begin{array}{rcl} E & \longrightarrow & E \\ (u, v) & \longmapsto & \Big(T^{-1}.u - T^{-1}.f_+(u, v), T(v) + f_-(u, v)\Big) \end{array},$$

est contractante. □

Théorème d'Anossov

[Gonnord Topo II.2.11]

Théorème. Il existe $\varepsilon > 0$ tel que pour toute fonction $f \in Lip_k(E, E)$, $T+f$ et T soient homéomorphiquement conjuguées : il existe $h : E \to E$ un homéomorphisme tel que

$$T + f = h \circ T \circ h^{-1}.$$

Démonstration.

Lemme. Soient $g, h \in Lip_k(E, E)$. Alors pour k assez petit l'équation

$$(g + T) \circ (Id + u) = (Id + u) \circ (h + T),$$

admet une unique solution pour $u \in C^0_b(E, E)$.

Démonstration du lemme. On a

$$(g + T) \circ (Id + u) = (Id + u) \circ (h + T) \Leftrightarrow g \circ (Id + u) + T.u = h + u \circ (h + T).$$

Pour $k < 1/||T^{-1}||$, $(h + T)$ est bijective, donc

$$(g + T) \circ (Id + u) = (Id + u) \circ (h + T) \Leftrightarrow A(u) + B(u) = u,$$

avec

$$\begin{aligned}A(u) &= T.g \circ (h + T)^{-1},\\ B(u) &= g \circ (Id + u) \circ (h + T)^{-1} - h \circ (h + T)^{-1}.\end{aligned}$$

L'application A est alors linéaire bijective et continue (car A est $||T||$-lipchitzienne). On note

$$F_+ = \{v \in C_b^0(E,E) \mid v(E) \subset E_+\},$$
$$F_- = \{v \in C_b^0(E,E) \mid v(E) \subset E_-\}.$$

Alors F_+ et F_- sont fermés, $C_b^0(E,E) = F_+ \oplus F_-$, et

$$||A(v)||_\infty \geq \lambda||v||_\infty \text{ sur } F_+ \text{ et } ||A(v)||_\infty < 1/\lambda||v||_\infty \text{ sur } F_-.$$

Donc A est un automorphisme hyperbolique. Comme f_1 est k-lipchitzienne, B est aussi k-lipchitzienne.

Donc par théorème précédent, $A(u) + B(u) = u$ admet une unique solution. □

En appliquant le lemme à $(g,h) = (f,0)$ il existe $u \in C_b^0(E,E)$ tel que

$$(f+T) \circ (Id+u) = (Id+u) \circ T,$$

puis en l'appliquant à $(g,h) = (0,f)$ il existe $v \in C_b^0(E,E)$ tel que

$$T \circ (Id+v) = (Id+v) \circ (f+T).$$

On en déduit que $(f+T)\circ(Id+u)\circ(Id+v) = (Id+u)\circ(Id+v)\circ(f+T)$. Comme $(Id+u)\circ(Id+v) = Id+u+v+u\circ v$, avec $u+v+u\circ v \in C_b^0(E,E)$, par unicité pour le cas $(g,h) = (f,f)$ on en déduit que $(Id+u)\circ(Id+v) = Id$. On déduit de même que :

$$\text{On en déduit que } T \circ (Id+v) \circ (Id+u) = (Id+v) \circ (Id+u)T,$$

puis que $(Id+v)\circ(Id+u) = Id$. On prend alors $h = (Id+u)$. □

Théorème de Grobman-Hartmann

[GT Calcul Diff, II.2.12]

Théorème. Soit E un Banach et $f : E \to E$ de classe C^k. On suppsoe que $f(0) = 0$ et que $Df(0)$ est hyperbolique, alors il existe $h : E \to E$ un homéomorphisme tel que $h(0) = 0$

$$f = h^{-1} \circ Df(0) \circ h,$$

au voisiange de 0

Démonstration. On note $\varepsilon(x) = f(x) - Df(0).x$. Alors il existe $R > 0$ tel que ε soit k-lipchitzienne sur $B(0,2R)$. On pose

$$g : \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & \begin{cases} \varepsilon(x) & , \text{ si } ||x|| \leq R \\ \varepsilon\left(R\frac{x}{||x||}\right) & , \text{ sinon} \end{cases} \end{array}.$$

Alors g est k-lipchitzienne [y réfléchir]. En appliquant le théorème d'Anossov il existe un homéomorphisme h tel que

$$Df(0) + g = h^{-1} \circ Df(0) \circ h.$$

sur E. En évaluant en 0 on a $h(0) = Df(0).h(0)$, donc $h(0) = 0$ car $Df(0)$ est hyperbolique. On en déduit ensuite que

$$f = h^{-1} \circ Df(0) \circ h.$$

sur $B(0,R)$. □

Théorème de la variété stable et de la variété instable

[GT Calcul Diff, II.2.13]
On considère $X : \mathbb{R}^n \to \mathbb{R}^n$ un champ de vecteur tel que 0 est point hyperbolique, c'est-à-dire que
– $X(0) = 0$.
– $Spec(DX(0)) \cap i\mathbb{R} = \emptyset$.
(A ne pas confondre avec les automorphismes hyperboliques). En conséquence $e^t DX(0)$ est un automorpshime hyperbolique. On considèr l'équation différentielle

$$y(t) = X(y(t)),$$

et on note Φ sont flot.

Théorème (Variété stable)**.** Il existe des constante $C, \eta > 0$ une sous variété W_s (variété stable) passant par 0 tel que : pour tout $x \in W_s$ et $t > 0$, $\Phi_t(x)$ existe et appartient à W_s et de plus

$$|\Phi_t(x)| \leq Ce^{-\eta t}|x|.$$

Démonstration. Idées : si on note V_1 la variété stable de $exp(DX(0))$, alors on montre que : pour $v \in V_1$ assez proche de 0, il existe un unique $x_v \in \mathbb{R}^n$ tel que $\pi_{V_1}(x_v) = v$ et $\lim_{t\to+\infty} \Phi_t(x_v) = 0$. L'application $v \mapsto x_v$ sera alors le paramétrage de la variété stable. □

Linéarisation d'un champ de vecteurs hyperbolique

[GT Calcul Diff, II.2.14]
On considère le champ de vecteur précédent. On note $A = DX(0)$.

Théorème (Grobman-Hartman)**.** Il existe un homéomorphisme (difféo ?) $h : \Omega \to \Omega'$ entre deux ouverts de 0 tels que

$$\forall x \in U, \forall t \text{ convenable}, \phi_t(h(x)) = h(e^{tA}x).$$

19 Théorème d'Helly

Leçons concernées
- 229 - Fonctions monotones et fonctions convexes.
- 241 - Suites et séries de fonctions. Exemples et contre-exemples.

Théorème (de Helly)**.** Soit $f_n : I \to \mathbb{R}$ une suite de fonctions croissantes. On suppose que $\forall x \in I, (f_n(x))$ est bornée, alors il existe une extraction convergent simplement.

Démonstration. Comme $\forall x \in I, (f_n(x))$ est bornée, par processus diagonale on peut trouver une extraction qui converge simplement sur les rationnelles. On note g sa limtie définie sur les rationnels. g est croissant.

On prolonge g de la façon suivante : $g(x) = sup\{g(y)|y \in \mathbb{Q} \cap I, y \leq x\}$. Si $x_0 \in \mathbb{Q} \cap I$ et $x < x_0$ alors $g(x) \leq g(x_0)$ et si $x > x_0$ alors $g(x_0) \geq g(x)$ de même si $x_0 \notin \mathbb{Q}$. Donc g est croissante sur I.

Montrons que la convergense est simple là g est continue. Pour $z \in I$ où g est continue, et $x, y \in \mathbb{Q} \cap I$ tel que $x \leq z \leq y$, alors $f_n(x) \leq f_n(z) \leq f_n(y)$, donc $g(x) \leq liminf(f_n(z)) \leq limsup(f_n(z)) \leq g(y)$. Par continuité de g on obtient $liminf(f_n(z)) \leq limsup(f_n(z)) = g(z)$.

On note D l'ensemble des points de discontinuités de g, dénombrable car g est croissante. On réextrait alors une suite pour faire converger la suite sur D.

□

20 Un résultat sur les fonctions à dérivées bornées

Leçons concernées
- 201 - Espaces de fonctions. Exemples et applications.
- 228 - Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.
- 245 - Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$.

Théorème. Soit $f : \mathbb{R} \to \mathbb{R}$, C^∞ tel que $f'(0) = 1$ et $\forall \in \mathbb{N}, \forall x \in \mathbb{R}, |f^{(n)}(x)| \leq 1$. Alors $f = \sin$.

Démonstration. On pose $F(z) = \sum_{n=0}^{+\infty} \frac{f^{(n)}(0)}{n!} z^n$. Comme les dérivées de f sont uniformément bornées, par formule de Taylor on a $f = F$ sur $\mathbb{R}$. On se fixe $a \in R$, alors $\left(\frac{F}{\cos}\right)'(a) = Res(g, a)$ avec $g(z) = \frac{1}{(z-a)^2} \frac{F(z)}{\cos z}$. Les pôles de g sont a et $\frac{\pi}{2} + n\pi$ avec résidu $\frac{1}{(\frac{\pi}{2}+n\pi-a)}(-1)^{n+1} F(\frac{\pi}{2} + n\pi)$. Pour $n \in \mathbb{N}$, on note γ_n le bord du carré $[-n\pi, n\pi] \times [-ni\pi, ni\pi]$. On a alors $\frac{1}{2i\pi} \int_{\gamma_n} g(z)dz = Res(g, a) + \sum_{k=-n}^{n-1} Res(g, \frac{\pi}{2} + k\pi)$. Comme $F(x + iy) = \sum_{j=1}^{+\infty} \frac{f^{(j)}(x)}{n!} (iy)^j$, on a $|F(x + iy)| \leq e^{|y|}$, donc $|g(z)| \leq \frac{e^{|y|}}{\sqrt{\cos^2 x + \sinh^2 y}} \frac{1}{|x-a+iy|^2}$. On en déduit $\lim_{n\to+\infty} \int_{\gamma_n} g(z)dz = 0$, soit :

$$\left(\frac{F}{\cos}\right)'(a) = \sum_{k=-\infty}^{+\infty} \frac{1}{(\frac{\pi}{2} + n\pi - a)} (-1)^n F(\frac{\pi}{2} + n\pi). \tag{6.1}$$

En prenant $a = 0$, (6.1) donne $\left(\frac{F}{\cos}\right)'(0) = F'(0) = 1$, donc :

$$\begin{array}{rcl} 1 & = & \sum_{k=-\infty}^{+\infty} \frac{1}{(\frac{\pi}{2}+n\pi-a)} (-1)^n F(\frac{\pi}{2} + n\pi) \\ & = & \sum_{k=-\infty}^{+\infty} \frac{1}{(\frac{\pi}{2}+n\pi-a)} \end{array}.$$

Et en prenant $f = \sin$ et $a = 0$, (6.1) donne $1 = \sum_{k=-\infty}^{+\infty} \frac{1}{(\frac{\pi}{2}+n\pi-a)}$. Donc $\forall k \in \mathbb{Z}, (-1)^n F(\frac{\pi}{2} + n\pi) = 1$. Donc $\left(\frac{F}{\cos}\right)'(a) = \sum_{k=-\infty}^{+\infty} \frac{1}{(\frac{\pi}{2}+n\pi-a)} = \left(\frac{F}{\cos}\right)'(a)$ (en spécialisant $f = \sin$).

Donc $f = \sin + \lambda \cos$ avec $\lambda \in \mathbb{R}$. Comme $f(\frac{\pi}{2}) = \sin \frac{\pi}{2} + \lambda \cos \frac{\pi}{2} = 1$ et que f est bornée par 1 on en déduit $f'(\pi/2) = -\lambda = 0$. □

Remarque. Ce développement a été proposé par François Lê.

21 Sous-espaces fermés de L^p, théorème de Grothendieck

Leçons concernées

–
– 201 - Espaces de fonctions. Exemples et applications.
– 208 - Espaces vectoriels normés, applications linéaires continues. Exemples.
– 213 - Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.
– 234 - Espaces L^p.

Théorème (Grothendieck)**.** Soit Ω un espace mesuré de mesure finie et $p \in]1, \infty[$. Si F est un sous-espace $L^p \cap L^\infty$ fermé dans L^p, alors F est de dimension finie.

Démonstration. Montrons que les normes L^p et L^∞ sont équivalentes sur F. Comem Ω est de mesure finie on a $||f||_2 \leq \sqrt{\mu(\Omega)}||f||_\infty$. On considère la graphe Γ de l'injection $F \to L^\infty$. Soit (f_n, f_n) une suite de Γ convergeant vers $(f, g) \in F \times L^\infty$, alors f_n converge vers g dans L^∞ donc converge p.p., et en extrayant une suite convergeant p.p. vers f on obtient $f = g$. Donc Γ est fermé et il existe C tel que $||f||_\infty \leq C||f||_p$ sur F.

Montrons que $F \subset L^2$ et que l'injection $(F, ||.||_2) \to L^p$ est continue. On a $F \subset L^\infty \subset L^2$. Si $p \leq 2$ alors $L^2 \to L^p$ est continue. Si $p \geq 2$, alors $||f||_p \leq ||f||_2^{2/p}||f||_\infty^{1-2/p}$ et comme la norme L^2 et L^∞ coïncident la conclusion découle.

Soit $n \in \mathbb{N}$ et $(f_1, ..., f_n)$ une famille orthonormale de F. On considère les f_i comme des fonctions. On prend $C > 0$ tel que $||.||_\infty \leq \alpha||.||_2$ sur F. On note $E = \text{Vect}(f_1, ..., f_n)$. Montrons qu'il existe $\Omega' \subset \Omega$ de mesure pleine tel que $\forall f \in E, \forall x \in \Omega', |f(x)| \leq ||f||_\infty$. Comme E est de dimension finie, E est séparable. Il existe alors $(g_l)_{l\in\mathbb{N}}$ une famille dénombrable dense dans E. Pour $l \in \mathbb{N}$, comme le sup essentiel est atteint il existe Ω_l de mesure pleine tel que $sup_{x\in\Omega_l}|g_l| = ||g_l||_\infty$. On prend alors $\Omega' = \cap_{l\in\mathbb{N}}\Omega_l$ de mesure pleine et on a $\forall l \in \mathbb{N}, \forall x \in \Omega', |g_l(x)| \leq ||g_l||_\infty$. Soit $x \in \Omega'$, comme on est en dimension finie $E \to \mathbb{R}, g \mapsto x$ est continue et $E \to \mathbb{R}, g \mapsto ||g||_\infty$ est une norme en dimension finie. Par densité on a donc

$$\forall x \in \Omega', \forall g \in E, |g(x)| \leq ||g||_\infty \leq C||f||_2.$$

Pour $x \in \Omega'$, on note $\forall t \in \Omega, f_x(t) = \frac{\bar{f}_1(x)f_1(t)+...+\bar{f}_1(x)f_1(t)}{\sqrt{|f_1(x)|^2+...+|f_1(x)|^2}}$ ($= 0$ si $|f_1(x)|^2 + ... + |f_1(x)|^2 = 0$). Alors $||f_x||_2 = 1$ (car f_i est une base orthonormée) ou $f = 0$, donc et $f_x(x)^2 = |f_1(x)|^2 + ... + |f_1(x)|^2 \leq C^2$, et en intégrant sur Ω' on obtient $||f_1||_2^2 + ... + ||f_n||_2^2 = n \leq C\mu\Omega$. Donc $\dim F \leq C\mu\Omega$. □

Remarque. Voir [[Rud95], Chap ?]

22 Théorème d'Ascoli et de Riesz-Frechet-Kolmogorov

Leçons concernées
- 201 - Espaces de fonctions. Exemples et applications.
- 203 - Utilisation de la notion de compacité.
- 234 - Espaces L^p.
- 235 - Suites et séries de fonctions intégrables. Exemples et applications.
- 241 - Suites et séries de fonctions. Exemples et contre-exemples.

Théorème d'Ascoli

Proposition. Soient K un métrique compact et E métrique. Si $(f_n : K \to E)_{n\in\mathbb{N}}$ est une suite équicontinue convergeant simplement vers f, alors la convergence est uniforme.

Démonstration. On montre d'abord que f est continue. Soit $x \in K$ et $\varepsilon > 0$. Il existe $r > 0$ tel que

$$\forall n \in \mathbb{N}, \forall y \in B(x, r), d(f_n(y), f_n(x)) \leq \varepsilon$$

En passant à la limite, on a

$$\forall y \in B(x, r), d(f(y), f(x)) \leq \varepsilon$$

Soit $\varepsilon > 0$. Comme K est compact, la famille $(f_n)_{n\in\mathbb{N}}$ est uniformément équicontinue, et la fonction f est uniformément continue. Il existe $\eta > 0$ tel que

$$\forall x, y \in K, |x - y| \leq \eta \Longrightarrow |f(x) - f(y)| \leq \varepsilon \text{ et } \forall n \in \mathbb{N}, |f_n(x) - f_n(y)| \leq \varepsilon.$$

On prend $(x_1, \ldots, x_p)$ dans K tel que $K = \subset B(x_i, \eta)$. On a alors pour $n \in \mathbb{N}$, $x \in K$ et $i \in [1, p]$ tel que $x \in B(0, x)$

$$|f(x) - f_n(x)| \leq |f(x) - f(x_i)| + |f(x_i) - f_n(x_i)| + |f_n(x_i) - f_n(x)|.$$

On conclut alors aisément. □

Proposition. Soient K métrique compact et E complet. Si $(f_n : K \to E)_{n\in\mathbb{N}}$ est une suite équicontinue convergeant simplement sur une partie dense, alors elle converge partout.

Démonstration. Soit D un ensemble dense sur lequel $(f_n)_{n\in\mathbb{N}}$ converge simplement. Soit $x \in K$. On a alors pour tout $n, m \in \mathbb{N}$ et $y \in D$

$$|f_n(x) - f_m(x)| \leq |f_n(x) - f_n(y)| + |f_n(y) - f_m(y)| + |f_m(y) - f_m(x)|.$$

On montre alors aisément que $(f_m(x))_{n\in\mathbb{N}}$ est de Cauchy. □

Théorème (Ascoli)**.** Soient K métrique compact et E métrique. Une famille F de $C^0(K, E)$ est relativement compact si et seulement si elle vérfie les deux conditions suivantes
- F est équicontinue.
- $\forall x \in K, (f(x))_{f\in F}$ est relativement compact dans E.

Démonstration. Supposons que $(f_i)_{i\in I}$ vérifie les deux conditions. Soit $(f_n)_{n\in\mathbb{N}}$ une suite de F. Comme F est ponctuellement relativement compact, par extraction diagonale, on extrait une sous-suite qui converge simplement sur une partie dense dénombrable. Cette sous-suite converge alors uniformément.

Si F est relativement compact. On note G son adhérence. Soit $x \in K$. Alors $(g(x))_{g\in G}$ est compact (image d'un compact par une application continue), donc $(f(x))_{f\in F}$ est relativement compact. Soit $\varepsilon > 0$. Comme G est compact, il existe $(g_1, \ldots, g_p)$ tel que $G \subset \bigcup_{i=1}^{p} B(q, \varepsilon)$. Soit $x \in K$. Pour $y \in K$ et $g \in G$ et $i \in [1, p]$ tel que $g \in B(g_i, \varepsilon)$, on a

$$|g(y) - g(x)| \leq |g(y) - g_i(y)| + |g_i(y) - g_i(x)| + |g_i(x) - g(x)|.$$

On montre alors aisément que G, et donc a fortiori F, est équicontinue. □

Théorème de Riesz-Frechet-Kolmogorov

Théorème (Riesz-Fréchet-Kolmogorov)**.** Soit K compact de $\mathbb{R}^n$. Soit F un sous-ensemble de $L^p(\Omega)$ avec $p < +\infty$. On suppose que

- F est bornée.
- $\forall \varepsilon > 0, \exists \eta > 0, \forall ||h|| \leq \eta, \forall f \in F, ||\tau_h f - f||_{L^p(K)} \leq \varepsilon$, avec $\tau_h f(x) = f(x+h)$.

Alors $F_{|K} = \{f_{|K} | f \in F\}$ est relativement compact dans $L^p(K)$.

Démonstration. On prend $M_p > 0$ tel que $\forall f \in F, ||f||_p \leq M_p$. Soit (ρ_n) des unités approchées C^∞ telles que $supp(\rho_n) \subset B(0, 1/n)$. Pour $n \in N$ on note $F^n := \{\rho_n * f | f \in F\} \subset C(\mathbb{R}^n, \mathbb{R})$.

Soit $n \in \mathbb{N}$, montrons que $F^n_{|K}$ est relativement compact dans $C(K, \mathbb{R})$. Par inégalité de Young, pour $f \in F$,

$$\begin{aligned} ||\rho_n * f||_{L^\infty(K)} &\leq ||\rho_n * f||_{L^\infty(\mathbb{R}^n)} \\ &\leq ||\rho_n||_{L^{p'}(\mathbb{R}^n)} ||f||_{L^p(\mathbb{R}^n)} \\ &\leq ||\rho_n||_{L^{p'}(\mathbb{R}^n)} M_p \quad . \end{aligned}$$

Donc $F^n_{|K}$ est uniformément bornée (pour la norme uniforme). Pour $x, y \in K$ et $f \in F$,

$$|\rho_n * f(x) - \rho_n * f(y)| \leq \int_{\mathbb{R}^n} |f(t)| \, |\rho_n(x-t) - \rho_n(y-t)| dt \quad .$$

Comme $t \mapsto \rho_n(x-t) - \rho_n(y-t) = 0$ est à support dans $x + B(0,1/n) \cup y + B(0,1/n) \subset K_n := K + B(0,1/n)$ et que $|\rho_n(x-t) - \rho_n(y-t)| \leq ||\rho_n||_{Lip} \, |x-y|$, on a

$$\begin{aligned} |\rho_n * f(x) - \rho_n * f(y)| &\leq \int_{K_n} |f(t)| \, |x-y| \, ||\rho_n||_{Lip} dt \\ &\leq |x-y| \, ||\rho_n||_{Lip} \, ||f||_{L^1(K_n)} \\ &\leq |x-y| \, ||\rho_n||_{Lip} \, ||f|_{L^p(K_n)} \, \mu(K_n)^{1/p'} \\ &\leq |x-y| \, ||\rho_n|| M_p \mu(K_n)^{1/p'} \quad . \end{aligned}$$

Donc $F^n_{|K}$ est uniformément Lipschitzienne. Donc par Ascoli $F^n_{|K}$ est relativement compact dans $(C(K, \mathbb{R}), ||.||_\infty)$.

L'ensemble $adh_{C(K,\mathbb{R})}(F^n_{|K})$ pour la topologie $||.||_\infty$ est compact et comme l'injection

$$(C(K, \mathbb{R}), ||.||_\infty) \to (L^p(K), ||.||_p)$$

est continue, il est aussi compact pour la topologie $||.||_p$. Donc $F^n_{|K}$ est relativement compact dans $L^p(K)$.

Soit $\varepsilon > 0$, $\delta > 0$ comme dans l'hypothèse. Soit $n \in \mathbb{N}$ tel que $\frac{1}{n} \leq \delta$. Montrons que $\forall f \in F, ||\rho_n * f - f||_{L^p(K)} \leq \varepsilon$. On a

$$\begin{aligned} ||\rho_n * f - f||^p_{L^p(K)} &= \int_K \left(\int_{B(0,1/n)} \rho_n(t)(f(x-t) - f(x)) dt \right)^p dx \\ &\leq \int_K \int_{B(0,1/n)} \rho_n(t) |f(x-t) - f(x)|^p dt dx \\ &\quad \text{(Hölder pour la mesure de proba)} \rho_n(y) dy \\ &= \int_{B(0,1/n)} \rho_n(t) ||\tau_t f - f||^p_{L^p(K)} dt \\ &\leq \varepsilon^p \quad . \end{aligned}$$

Montrons que $adh(F_{|K})$ est précompact, étant aussi complet on en déduira que $adh(F)$ est compact. Soit $\varepsilon > 0$ et $n \in \mathbb{N}$ tel que $1/n \leq \delta$. Comme $F^n_{|K}$ est relativement compact, il existe $f_1, ..., f_n \in L^p(K)$ tel que $F^n_{|K} \subset \bigcup_{i=1}^n B(f_i, \varepsilon)$, et comme $\forall f \in F, ||\rho_n * f - f||_{L^p(K)} \leq \varepsilon$, on a alors $adh(F) \subset \bigcup_{i=1}^n B(f_i, 2\varepsilon)$. □

Remarque. Voir [[BCL83], Th ?].

23 Fonction $\wp$ de Weierstrass

Leçons concernées

- 201 - Espaces de fonctions. Exemples et applications.
- 230 - Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.
- 241 - Suites et séries de fonctions. Exemples et contre-exemples.
- 245 - Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$.

[A completer]

Remarque. Voir [[CLF], Anal ?]

Chapitre 7

Suites et séries

1 Théorème de Tauber et d'Abel

Leçons concernées

- 207 - Prolongement de fonctions. Exemples et applications.
- 223 - Convergence des suites numériques. Exemples et applications.
- 224 - Comportement asymptotique de suites numériques. Rapidité de convergence. Exemples.
- 230 - Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.
- 243 - Convergence des séries entières, propriétés de la somme. Exemples et applications.

Théorème d'Abel non-tangentiel

Théorème. Soit $\sum a_n z^n$ une série entière de rayon de convergence R de somme f. Si pour $|z_0| = R$, la série $\sum a_n z_0^n$ converge vers S, alors pour tout $\alpha \in]0, \pi/2[$,

$$\lim_{z \to z_0} f(z) = S,$$

où la limite est prise pour z tendant vers z_0 en restant dans le secteur d'angle 2α et de bissectrice $[0, z_0]$.

Démonstration. On peut supposer que le RCV vaut 1 et que $z_0 = 1$. On note $S = \sum_{n=0}^{+\infty} a_n$ et $R_k = \sum_{n=k+1}^{+\infty} a_n$. Alors par transformation d'Abel, on a

$$f(z) - S = \sum_{n=0}^{+\infty} a_n(z^n - 1) = \sum_{n=0}^{+\infty} R_n(z^{n+1} - z^n) = (z-1)\sum_{n=0}^{+\infty} R_n z^n.$$

Soit $\varepsilon > 0$. Il existe $N \in \mathbb{N}$ tel que $\forall n \geq N, |R_n| \leq \varepsilon$. On a alors

$$\begin{array}{rcl} |f(z) - S| & \leq & |z-1| \sum_{n=0}^{N} R_n z^n + \varepsilon |z-1| \sum_{n=N+1}^{+\infty} |z|^n \\ & \leq & |z-1| \sum_{n=0}^{N} R_n z^n + \varepsilon \frac{|z-1|}{1-|z|}. \end{array}$$

On note $r = |1 - z|$ et $\rho = |z|$, si z est dans le secteur d'angle 2α, alors on a

$$\rho^2 \leq (r \sin\alpha)^2 + (1 - r\cos\alpha)^2 = 1 - 2r\cos\alpha + r^2.$$

Ce qui donne

$$\frac{r}{1-\rho} \leq \frac{r}{1 - \sqrt{1 - 2r\cos\alpha + r^2}} = \frac{1}{\cos\alpha + o(1)},$$

qui est bornée indépendamment de ε. On en déduit que $|f(z) - S| \to 0$ dans le secteur. □

Remarque. La preuve se trouve dans [[Gou94b], Chap IV.4, Ex 10].

Théorèmes tauberiens

Théorème (Tauberien faible)**.** Soit $\sum a_n z^n$ de RCV $R < +\infty$ et $|z_0| = R$. Si sa somme f vérifie $\lim_{r\to 1} f(rz_0) = S \in \mathbb{C}$ et si $a_n = o(1/n)$ alors la série $\sum a_n z_0^n$ converge vers S.

Démonstration. On peut supposer que le RCV vaut 1 et que $z_0 = 1$. On note $S_n = \sum_{k=0}^n a_k$. On prend $M > 0$ un majorant de $(a_n/n)_{n\in\mathbb{N}}$. On a pour $x \in [0, 1[$,

$$f(x) - S_n = \sum_{k=0}^n a_k(x^k - 1) + \sum_{k=n+1}^{+\infty} a_k x^k,$$

$$\begin{array}{rrl} |f(z) - S_n| & \leq & \sum_{k=0}^n |a_k|(x-1).(x^{k-1} + ... + x + 1) + \sum_{k=n+1}^{+\infty} |a_k| x^k \\ \text{donc} & \leq & n(1-x)M + \sum_{k=n+1}^{+\infty} \frac{|ka_k|}{n} z^k \\ & \leq & n(1-x)M + \frac{sup_{k\geq n+1}|ka_k|}{n(1-x)} \end{array}.$$

On note $\lambda = n(1-x)$ (i.e. $x = 1 - \lambda/n$). Ce qui donne

$$|S_n - f(1-\lambda/n)| \leq \lambda M + \frac{sup_{k\geq n+1} ka_k}{\lambda}.$$

Pour $\varepsilon > 0$, on fixe λ tel que $\lambda M < \varepsilon$ et puis N tel que $\forall n \geq N, \lambda^{-1}\ sup_{k\geq n+1}|ka_k| < \varepsilon$. □

Remarque. La preuve se trouve dans [[Gou94b], Chap IV.4, Ex 11].

Théorème (de Tauber fort)**.** Soit $\sum a_n z^n$ de RCV $R = 1$. Si sa somme f vérifie $\lim_{r\to 1} f(r) = S \in \mathbb{C}$ et si $a_n = O(1/n)$ alors $\sum_{n=1}^{+\infty} a_n z_0^n = S$.

A compléter. . □

Exemple. ? ? ?

Remarque. La preuve se trouve dans [[Gou94b], Chap IV.4, Prob 20].

Théorèmes tauberien de Fejer

[ZQ, Chap III, Ex 4]

Théorème. Soit $\sum_{n\in\mathbb{N}} a_n z^n$ une série entière de rayon de convergence 1 et de somme f. On suppose que f est prolongeable par continuité sur $\bar{D}$. Alors la série converge uniformément sur $\bar{D}$

Démonstration. On note $g(e^{it}) = f(e^{it})$. La fonction g est alors continue sur $\mathbb{S}^1$ et on a $c_n(g) = a_n$ pour $n \in \mathbb{Z}$ (passer à la limite sous l'intégrale).

Lemme. la suite $S_N(e^{it}) = \sum_{n\in[-N,N]} a_n e^{int}$ converge uniformément vers g sur $\mathbb{S}^1$.

Démonstration du lemme. Par théorème de Fejer, la suite $(N^{-1}(S_0, \ldots, S_{N-1}))_{N\in\mathbb{N}}$ converge uniformément vers g. Or on a

$$\tfrac{1}{N}\sum_{p=0}^{N-1} S_p(e^{it}) = \sum_{n=0}^{N-1}(a_n - \tfrac{n}{N}a_n)e^{int}.$$

Il suffit de montrer que $\frac{1}{N}\sum_{n=0}^{N-1} n|a_n|$ tend vers 0.

Si on note $A = f(F)$, bornée car $f(\bar{D})$ est compact, on a

$$\begin{array}{rcl} \lambda_2(A) & = & \iint |Jf(z)| d\lambda_2(z) = \iint |f'(z)|^2 d\lambda_2(z) = \int_0^1 \int_0^{2\pi} |f(re^{it})|^2 r dr d\theta \\ & = & \int_0^1 2\pi \sum_{n=1}^{+\infty} n^2 |a_n|^2 r^{2n-1} dr \\ & = & \pi \sum_{n=1}^{+\infty} n^2 |a_n|^2. \end{array}.$$

L'avant dernière égalité vient de Parseval et la dernière vient de Fubini-Tonelli. En particulier $\sum_{n=1}^{+\infty} n^2|a_n|^2 < +\infty$.

Pour $p \in [0, N-1]$, on a en appliquant Cauchy-Schwarz

$$\begin{array}{rcl} \frac{1}{N}\sum_{n=0}^{N-1} n|a_n| & = & \frac{1}{N}\sum_{n=0}^{N-1} n|a_n| + \frac{1}{N}\sum_{n=p+1}^{N-1} \sqrt{n}.\sqrt{n}|a_n| \\ & \leq & \frac{1}{N}\sum_{n=0}^{N-1} n|a_n| + \frac{1}{N}\left(\sum_{n=p+1}^{N-1} n\right)^{1/2}\left(\sum_{n=p+1}^{N-1} n|a_n|^2\right)^{1/2} \\ & \leq & \frac{1}{N}\sum_{n=0}^{N-1} n|a_n| + \left(\sum_{n=p+1}^{+\infty} n|a_n|^2\right)^{1/2} \end{array}.$$

On en déduit que $\lim_{N\to+\infty} \frac{1}{N}\sum_{n=0}^{N-1} n|a_n| = 0$. □

Soient $p < q \in \mathbb{N}$. On a alors par principe du maximum

$$\|S_p - S_q\|_{L^\infty(\bar{D})} = \|S_p - S_q\|_{L^\infty(\mathbb{S}^1)},$$

Donc la suite $(S_n)_{n\in\mathbb{N}}$ converge uniformément sur $\bar{D}$ et sa limite est nécéssairement f. □

Remarque. – Le preuve se trouve dans [[ZQ96]].
– On y trouverea aussi un exemple où la série ne converge pas normalement sur $\bar{D}$.

2 Formule d'Euler Mac Laurin et applications

Leçons concernées
- 218 - Applications des formules de TAYLOR.
- 223 - Convergence des suites numériques. Exemples et applications.
- 236 - Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables réelles.
- 238 - Méthodes de calcul approché d'intégrales.
- 239 - Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

Formule d'Euler-MacLaurin

Soit $g \in C^p([0,1])$. En intégrant par partie, on a

$$\int_0^1 g(t)dt = \left[\left(t-\tfrac{1}{2}\right)g(t)\right]_0^1 - \int_0^1 \left(x-\tfrac{1}{2}\right)g'(x)dx,$$

où $t-1/2$ est la primitive de 1 d'intégrale 0 sur $[0,1]$. Ce qui donne un estimation de l'erreur de la méthode des trapèzes sur $[0,1]$

$$\tfrac{1}{2}(g(0)+g(1)) = \int_0^1 g(t)dt - \int_0^1 B_1(t)g'(t)dt,$$

avec $B_1(t) = 1/2 - x$. En notant B_2 la primitive de $2B_1$ d'intégrale 0 sur $[0,1]$, on a $AB2(0) = B_2(1) := b_2$ (car B_1 est d'intégrale nulle) et

$$\tfrac{1}{2}(g(0)+g(1)) = \int_0^1 g(t)dt + \tfrac{b_2}{2}(g'(1)-g'(0)) - \int_0^1 \tfrac{B_2(t)}{2}g^{(2)}(t)dt.$$

Pour tout $k \in \mathbb{N}$, on posant B_k la primitive de kB_{k-1} d'intégrale 0 sur $[0,1]$, on en déduit par récurrence que

$$\tfrac{1}{2}(g(0)+g(1)) = \int_0^1 g(t)dt + \sum_{k=2}^p (-1)^k \tfrac{b_k}{k!}(g^{(k-1)}(1) - g^{(k-1)}(0)) - (-1)^p \int_0^1 \tfrac{B_p(x)}{p!}g^{(p)}(t)dt,$$

avec $b_k = B_k(0) = B_k(1)$. Pour k pair (resp. impair), la fonction B_k est paire (resp. impaire) autour de $1/2$. Donc pour $k \geq 3$ impair $a_k = 0$.

On en déduit la formule d'Euler-Mac-Laurin.

Théorème (Formule d'Euler-Maclaurin)**.** Pour $g : [0,1] \to \mathbb{R}$ de classe C^2p, on a

$$\tfrac{1}{2}(g(0)+g(1)) = \int_0^1 g(t)dt + \sum_{k=1}^{2p} \tfrac{b_{2k}}{2k!}(g^{(2k-1)}(1) - g^{(2k-1)}(0)) - \int_0^1 \tfrac{B_{2p}(x)}{2p!}g^{(2p)}(t)dt.$$

Corollaire. Soient $f \in C^{2p}([a,b])$, avec $a, b \in \mathbb{Z}$, on note

$$T(f) = \tfrac{1}{2}f(a) + f(a+1) + ...f(b-1) + \tfrac{1}{2}f(b),$$

la somme des trapèze relativement à la subdivision $a < a+1 < \cdots < b-1 < b$. Alors on a

$$T(f) = \int_0^1 f(t)dt + \sum_{k=1}^p \tfrac{b_{2k}}{2k!}(g^{(2k-1)}(b) - g^{(2k-1)}(a)) - \int_0^1 \tfrac{B_{2p}(t)}{2p!}g^{(2p)}(t)dt,$$

où l'on a compléter B_k de façon $\mathbb{Z}$-périodique.

Démonstration. Il suffit de sommer la formule précédente sur chaque intervalle $[i, i+1]$ ($i \in [a, b-1]$). □

Remarque. Voici quelques valeurs des b_k :
- $B_1(t) = t - 1/2$.
- $B_2(t) = t^2 - t + 1/6$, $b_2 = 1/6$.
- $B_3(t) = t^3 - 3/2.t^2 + 1/2.t$.
- $B_4(t) = t^4 - 2.t^3 + t^2 - 1/30$, $b_4(t) = -1/30$

Corollaire. Si f est une fonction C^∞ et T-périodique, alors la méthodes trapèzes pour calculer $\in_0^T f(t)dt$ converge à l'ordre p pour tout $p \in \mathbb{N}$.

Applications à la méthode de Romberg

[A completer]

Application à la recherche de développement asymptotique

Constante γ d'Euler

On sait que

$$\sum_{k=1}^{n} \frac{1}{k} = \ln n + \gamma + R_n,$$

avec $R_n = o(1)$. En ramarquant que R_n est le reste de la série convergente $\sum_{k\geq 2} \frac{1}{k} - \ln k + \ln(k-1)$, dont le terme général est équivalent à $1/2k^2$, on en déduit que

$$\sum_{k=1}^{n} \frac{1}{k} = \ln n + \gamma + \frac{1}{2n} + o(n^{-1}).$$

On va maintenant utiliser la formule d'Euler-MacLaurin pour avoir un développment asymptotique. On pose $f(x) = \frac{1}{x}$. La formule donne alors sur $[1, n]$ à l'ordre $p \in \mathbb{N}$ (on rappelle que $f^{(k)}(t) = (-1)^k k!/t^{k+1}$)

$$\begin{array}{rcl} \sum_{k=1}^{n} \frac{1}{k} & = & \frac{1}{2}(f(1)+f(n)) + \int_1^n f(x)dx + \sum_{k=1}^{p} \frac{b_{2k}}{2k!}(f^{(2k-1)}(n) - f^{(2k-1)}(1)) - \int_1^n \frac{B_{2p}(t)}{2p!} f^{(2p)}(t)dt \\ & = & \frac{1}{2} + \frac{1}{2n} + \ln n + \sum_{k=1}^{p} \frac{b_{2k}}{2k!}(\frac{-(2k-1)!}{n^{2k}} + (2k-1)!) - \int_1^n \frac{B_{2p}(t)}{2p!} \frac{2p!}{t^{2p+1}} dt \end{array}.$$

Ce qui donne pour tout $p \in \mathbb{N}$ (utiliser le fait que B_{2p} est bornée)

$$\boxed{\sum_{k=1}^{n} \frac{1}{k} = C + \ln n + \frac{1}{2n} + \sum_{k=1}^{p-1} -\frac{b_{2k}}{2kn^{2k}} + O(\frac{1}{n^{2p}})},$$

avec C une constante, qui vaut γ par définition. Si on prend $p = 3$, on obtient

$$\sum_{k=1}^{n} \frac{1}{k} = \ln n + \gamma + \frac{1}{2n} + \sum_{k=1}^{p-1} -\frac{1}{12n^2} + \frac{1}{60n^4} + O(\frac{1}{n^6}),$$

Formule de Stirling

[A completer]

Remarque. Voir [Dem06].

3 Théorème de Stone-Weierstrass

Leçons concernées
- 201 - Espaces de fonctions. Exemples et applications.
- 202 - Exemples de parties denses et applications.
- 203 - Utilisation de la notion de compacité.
- 208 - Espaces vectoriels normés, applications linéaires continues. Exemples.
- 241 - Suites et séries de fonctions. Exemples et contre-exemples.
- 249 - Suites de variables de BERNOULLI indépendantes.
- 252 - Loi binomiale. Loi de POISSON. Applications.

Stone-Wierstrass

Remarque. On peut voir par exemple [HL98], [[Gou94b], Chap IV, Sec 3, Ex 7], [[CLF] Anal 1, Ex 1.5].

Lemme. Soit $\sum_{n\in\mathbb{N}} a_n x^n$ une série entière à coefficients positifs dont les coefficients de rayon de convergence $R < +\infty$ et de somme S. On suppose que S admet une limtie finie en R. Alors $\sum_{n=0}^{+\infty} a_n R^n = S(R)$ (et donc il y a convergence normale de la série sur $[-R, R]$).

Démonstration. C'est la convergence monotone. □

Théorème (Stone-Weierstrass)**.** Soit K un compact de $\mathbb{R}^n$. Toute sous-$\mathbb{R}$-algèbre unitaire séparante de $C^0(K, \mathbb{R})$ est dense.

Démonstration. Soit A une sous-$\mathbb{R}$-algèbre unitaire séparante de $C^0(K, \mathbb{R})$. On note B l'adhérence de A.

Lemme. Il existe une suite de $\mathbb{R}[X]$ convergeant uniformément vers $x \mapsto |x|$ sur $[-1, 1]$.

Démonstration du lemme. [A completer]. □

Lemme. L'algèbre B est stable par inf et sup et $|.|$, c'est-à-dire que
- Si $f, g \in B$, alors $inf(f, g) \in B$ et $sup(f, g) \in B$.
- Si $f \in B$, alors $|f| \in B$.

Démonstration du lemme. Comme pour tout $f, g \in C^0(K, \mathbb{R})$, on a

$$inf(f, g) = \tfrac{1}{2}((f + g) - |f - g|) \text{ et } sup(f, g) = \tfrac{1}{2}((f + g) + |f - g|),$$

il suffit de montrer que B est stable par $|.|$. Soit $f \in B$, et $(P_n(X))_{n\in\mathbb{N}}$ une suite de polynôme qui converge vers $|X|$ sur $[-1, 1]$. On a pour $n \in \mathbb{N}$

$$\left\| \|f\|_\infty P\left(\tfrac{f}{\|f\|_\infty}\right) - |f| \right\|_\infty \leq \|f\|_\infty \left\| P\left(\tfrac{f}{\|f\|_\infty}\right) - \tfrac{|f|}{\|f\|_\infty} \right\|_\infty \leq \|f\|_\infty \|P_n(X) - |X|\|_\infty^{[-1,1]}.$$

Ce qui prouve que la suite $(\|f\|_\infty P(\frac{f}{\|f\|_\infty}))_{n\in\mathbb{N}}$ converge uniformément vers f et c'est une suite de B puisque chaque terme est polynôme en f. □

Montrons que B est dense, il résultera que A est dense. Soit $f \in C^0(K, \mathbb{R})$.

• Comme B est une algèbre séparante (car A l'est), pour tout $x, y \in K$ et $a, b \in \mathbb{R}$ tel que $x \neq y$, il existe $h \in B$ tel que $h(x) = a$ et $h(y) = b$: en effet, on prend g tel que $g(x) \neq g(y)$ et $h(t) = \frac{b-a}{g(y)-g(x)}(g(t) - g(x)) + a$.

• Soit $\varepsilon > 0$ et $x \in K$. Montrons qu'il existe $g_x \in B$ telle que $g_x(x) = f(x)$ et $g_x(y) \leq f(y) + \varepsilon$. Pour $y \in K$, on prend $h \in B$ tel que $h(x) = f(x)$ et $h(y) = f(y) + \frac{\varepsilon}{2}$. Par continuité, il existe V_y un voisinage de y tel que $h(t) \leq f(t) + \varepsilon$ sur V_y. Par compacité, il existe une famille finie $(y_1, \ldots, y_n)$ de K tel que $(V_{y_i})_{i\in[1,n]}$ recouvre K. Il suffit alors de prendre $g_x = inf(h_{y_1}, \ldots, h_{y_n})$ qui dans B d'après le lemme.

• De la même manière pour $x \in K$, il existe U_x un voisinage de x tel que $g_x \geq f - \varepsilon$ sur U_x. On extrait alors une famille finie $(x_1, \ldots, x_m)$ telle que $(U_{x_j})_{j\in[1,m]}$ recouvre K, et on pose $g = sup(g_{x_1}, \ldots, g_{x_m})$. Comme $g_{x_i} \leq f + \varepsilon$ pour tout $i \in [1, m]$, on a $g \leq f + \varepsilon$, et par construction de g $g \geq f - \varepsilon$. Ce qui prouve que f est adhérent à B. □

Théorème (Stone-Weierstrass complexe)**.** Soit K un compact et A une sous-$\mathbb{C}$-algèbre unitaire de $C^0(K, \mathbb{C})$ séparante et autoadjoint (c'est-à-dire si $f \in A$, alors $\bar{f} \in A$). Alors A est dense.

Démonstration. Comme A est stable par conjugaison, elle est aussi stable par partie réelle et partie imaginaire. On note B la sous-algèbre de $C^0(K,\mathbb{R})$ engendré par les parties réelles et imaginaires des éléments de A. Alors B sépare aussi les points (clair), donc B est dense dans $C^0(K,\mathbb{R})$. Il en vient que $B+iB$ est dense dans $C^0(K,\mathbb{C})$. On conclut remarquant que $B+iB=A$ (facile). □

Théorème de Weierstrass

Point de vu probabiliste

Remarque. Voir [[ZQ96], Chap XIII, Sec II.1.c].

Soit $f:[0,1]\to\mathbb{R}$ une fonction continue. Soit $x\in[0,1]$ et $(X_n^{(x)})_{n\in\mathbb{N}}$, une suite de v.a.i.i.d. loi de Bernoouilli de paramètre x. Pour $n\in\mathbb{N}$, on note $S_n^{(x)}=X_1^{(x)}+\cdots+X_n^{(x)}$ et

$$P_n(x)=E\Big[f(\tfrac{S_n^{(x)}}{n})\Big] \text{ (polynômial en } x).$$

Pour $\delta>0$, on note $\omega(\delta)=\sup\{|f(x)-f(y)| \mid |x-y|\leq\delta\}$ le module de continuité de f.

Théorème. On a : $\|f-P_n(x)\|_\infty\leq\frac{3}{2}\omega(\frac{1}{\sqrt{n}})$.

Démonstration. On a pour tout $x\in[0,1]$, $n\in\mathbb{N}$ et $\delta>0$:

$$|f(x)-P_n(x)|\leq E\Big[|f(x)-f(\tfrac{S_n^{(x)}}{n})|\Big]\leq E\Big[\omega\left(|x-\tfrac{S_n^{(x)}}{n}|\right)\Big].$$

Lemme. Pour $h,\lambda>0$ tel que $h\in[0,1]$ et $\lambda h\in[0,1]$, on a : $\omega(\lambda h)\leq(\lambda+1)\omega(h)$.

Démonstration du lemme. Si $\lambda\leq1$, c'est évident, car $\omega(\lambda h)\leq\omega(h)$.
Si $\lambda\geq1$. Pour $h,k>0$, on a $\omega(k+h)\leq\omega(h)+\omega(k)$, car

$$sup_{|x,y|\leq k+h}|f(x)-f(y)|\leq sup_{|x,y|\leq k+h}sup_{z,|x-z|\leq h,|y-z|\leq k}|f(x)-f(z)|+|f(z)-f(y)|.$$

On note $\lambda=n+\alpha$, avec $\alpha\in[0,1]$. On a alors

$$\omega(\lambda h)\leq\omega(nh)+\omega(\alpha h)\leq(n+1)\omega(h)\leq(\lambda+1)\omega(h).$$

□

En prenant $h=\frac{1}{\sqrt{n}}$ et $\lambda=\sqrt{n}|x-S_n/n|$ (c'est une v.a), on en déduit que

$$|f(x)-P_n(x)|\leq\omega(\tfrac{1}{\sqrt{n}})E\Big[\sqrt{n}|x-\tfrac{S_n^{(x)}}{n}|\Big].$$

Il reste à évaluer $E\Big[\sqrt{n}|x-\frac{S_n^{(x)}}{n}|\Big]$. Par Hölder, on a

$$E\Big[|x-\tfrac{S_n^{(x)}}{n}|\Big]\leq\sqrt{E\Big[|x-\tfrac{S_n^{(x)}}{n}|^2\Big]}=\sqrt{Var(S_n^{(x)}/n)}=\tfrac{1}{2n},$$

ce qui donne le résultat. □

Preuve sans le point de vu probabiliste

[Groudon, Anal, Chap IV, Sec 3, Ex 7]

Soit $f:[0,1]\to\mathbb{R}$ une fonction continue. Pour $n\in\mathbb{N}$ et $l\in[0,n]$, on note

$$R_n^l(X)=\tbinom{n}{l}x^l(1-x)^{n-l}.$$

$$P_n(X)=\textstyle\sum_{k=0}^n f(\frac{k}{n})R_n^k(X).$$

Pour $x\in[0,1]$ et $n\in\mathbb{N}$, on remarque que $P_n(x)$ est le barycentre des points $(f(\frac{k}{n}))_{k\in[0,n]}$ pondérés par les coefficients $(R_n^k(x))_{k\in[0,n]}$.

Soit $n\in\mathbb{N}$, $x\in[0,1]$ et $\delta>0$. On a alors

$$\begin{array}{rcl} |f(x)-P_n(x)| & \leq & \sum_{k=0}^n |f(\frac{k}{n})||1-R_n^k(x)| \\ & \leq & \sum_{|k/n-x|\leq\delta} |f(\frac{k}{n})-f(x)|R_n^k(x) + \sum_{|k/n-x|\geq\delta} |f(\frac{k}{n})-f(x)|R_n^k(x) \end{array}.$$

En notant $\omega(\delta) = \sup\{|f(x)-f(y)| \mid |x-y|\leq\delta\}$ le module de continuité de f, on obtient

$$|f(x)-P_n(x)| \leq \omega(\delta) + 2\|f\|_\infty \sum_{|k/n-x|\geq\delta} \sum_{|k/n-x|\geq\delta} R_n^k(x)$$

Comme $(\frac{k/n-x}{\delta})^1 \geq 1$ pour $|k/n-x|\geq\delta$, on en déduit que

$$\sum_{|k/n-x|\geq\delta} R_n^k(x) \geq \frac{1}{\delta^2} \sum_{k=0}^n (\frac{k}{n}-x)^2 R_n^k(x).$$

Lemme. Pour $x\in[0,1]$ et $n\in\mathbb{N}$, on a

$$\sum_{k=0}^n (\frac{k}{n}-x)^2 R_n^k(x) = \frac{x(1-x)}{n} \text{ (c'est une variance).}$$

Démonstration du lemme. On a

$$\sum_{k=0}^n (\frac{k}{n}-x)^2 R_n^k(x) = \frac{x(1-x)}{n} = \sum_{k=0}^n (\frac{k}{n})^2 R_n^k(x) - 2x\sum_{k=0}^n \frac{k}{n} R_n^k(x) + x^2 \sum_{k=0}^n R_n^k(x).$$

En définissant la fonction

$$\Phi(a,b) = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} = (a+b)^n.$$

On en déduit que

$$\sum_{k=0}^n k R_n^k(x) = x\frac{\partial\Phi}{\partial a}(x,1-x) = nx,$$

$$\sum_{k=0}^n k^2 R_n^k(x) = x\frac{\partial}{\partial a}\left(a\frac{\partial\Phi}{\partial a}\right)(x,1-x) = n^2x^2 + nx(1-x),$$

Ce qui fournit le résultat. □

On a donc pour tout $x\in[0,1]$, $n\in\mathbb{N}$ et $\delta>0$

$$|f(x)-P_n(x)| \leq \omega(\delta) + \frac{\|f\|_\infty}{2n\delta^2}.$$

On en déduit que pour tout $n\in\mathbb{N}$, et $\delta>0$

$$\|f-P_n\|_\infty \leq \omega(n) + \frac{\|f\|_\infty}{2n\delta^2}.$$

Comme f est uniformément continue, $\omega(\delta) \xrightarrow{\delta\to 0} 0$, ce qui montre que $(P_n)_{n\in\mathbb{N}}$ tend uniformément vers f.

Remarque. La preuve plus longue car on a du recalculer la variance d'une loi binomiale implicitement via sa fonction génératrice, ce qui est plus facile à faire si on sait que c'est une somme de Bernouilli indépendantes.

4 Théorème de Borel

Leçons concernées
- 207 - Prolongement de fonctions. Exemples et applications.
- 228 - Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.
- 241 - Suites et séries de fonctions. Exemples et contre-exemples.

Théorème. Soient $n \in N$ et $(c_\alpha)_\alpha$ une suite de réels où α parcours $\mathbb{N}^n$. Alors il existe $f \in \mathbb{C}^\infty(\mathbb{R}^n, \mathbb{R})$ telle que pour tout α, $\partial_{x^\alpha} f(0) = c_\alpha$.

Démonstration.

Lemme. Pour $g \in \mathbb{C}^\infty(\mathbb{R}^n, \mathbb{R})$ et $m \in \mathbb{N}$ tel que

$$\forall |\alpha| \leq m, \partial_{x^\alpha} g(0) = 0,$$

il existe $(h_k)_{k\in\mathbb{N}}$ une suite de fonctions $\mathbb{C}^\infty(\mathbb{R}^n, \mathbb{R})$ nulles sur un voisinage de 0 convergeant vers g en norme C^m.

Démonstration. On prend ϕ une fonction $C^\infty(\mathbb{R}^n, \mathbb{R})$ tel que $\phi(x) = 0$ si $|x| \leq 1$ et $\phi(x) = 1$ si $|x| > 2$. On pose alors

$$\forall k \in \mathbb{N}, h_k(x) = \phi(kx)g(x).$$

Pour $|\alpha| \leq m$ et $\varepsilon > 0$, on a :

$$\begin{aligned} \|\partial_{x^\alpha} h_k - \partial_{x^\alpha} g\|_\infty^{\mathbb{R}^n} &= \|\partial_{x^\alpha} h_k - \partial_{x^\alpha} g\|\|_\infty^{B(0,3/k)} \\ &\leq \|\partial_{x^\alpha} h_k\|_\infty^{B(0,3/k)} + \|D^\alpha g\|_\infty^{B(0,3/k)}. \end{aligned}$$

Comme g est plate en 0, on a $\lim_{k\to+\infty} \|\partial_{x^\alpha} g\|_\infty^{B(0,3/k)} = 0$. On a :

$$\partial_{x^\alpha} h_k(x) = \sum_{\lambda+\mu=\alpha} \binom{|\alpha|}{\lambda} \partial_{x^\lambda}\phi(kx)\partial_{x^\mu} g(x).$$

Donc

$$\|\partial_{x^\alpha} h_k\|_\infty^{B(0,3/k)} \leq \sum_{\lambda+\mu=\alpha} \binom{|\alpha|}{\lambda} k^{|\lambda|} \max_{\lambda\leq\alpha} \|\partial_{x^\lambda}\phi\|_\infty \|\partial_{x^\mu} g(x)\|_\infty^{B(0,3/k)}.$$

Or pour tout $\mu \leq \alpha$, $\partial_{x^\mu} g(x) = o(x^{m-|\mu|})$ (Taylor-Young). Donc $\lim_{k\to+\infty} \|\partial_{x^\alpha} h_k\|_\infty^{B(0,3/k)} = 0$. □

Soit $(c_\alpha)_\alpha$ une suite de réels. On note $g_m(x) = \sum_{|\alpha|=m} \frac{c_\alpha}{\alpha!} x^\alpha$. Pour tout $m \in \mathbb{N}$ il existe h_m C^∞ nulle sur un voisinage de 0 tel que $\|g_{m+1} - h_m\|_{C^m} \leq 1/2^m$. On pose alors $f(x) = g_0(x) + \sum_{m=0}^\infty g_{m+1}(x) - h_m(x)$. La série converge normalement en norme C^m pour tout m, donc f est bien définie et est C^∞. En dérivant termes-à-termes on a $\partial_{x^\alpha} f(x) = \partial_{x^\alpha} f(x) = c_\alpha$. □

Remarque. La preuve se trouve dans [[GT98], Sec I.1.23] et [[Rou], Ex 116].

5 Théorèmes de Bernstein

Références [Gourdon, Anal, Chap IV, Sec 4, Ex 8], [Gourdon, Anal, Chap IV, Sec 5, Ex 6].

Leçons concernées
- ? ? ?

Théorème de Bernstein pour les séries entières

[Gourdon, Anal, Chap IV, Sec 4, Ex 8]

Théorème. Soit $f :]-a, a[\to \mathbb{R}$. On suppose que

$$\forall k \in \mathbb{N}, \forall x \in]-a, a[, f^{(2k)}(x) \leq 0.$$

Alors f est développable en série entière utour de 0 avec un rayon de convergence $\geq a$.

Démonstration. □

Théorème de Bernstein pour les séries de Fourier

[Gourdon, Anal, Chap IV, Sec 5, Ex 6]

Théorème. Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction 2π-périodique α-höldérienne avec $\alpha > 1/2$. Alors sa série de Fourier converge normalement vers f.

Rapide. La fonction f en particulier continue, donc dans $L^2([0, 2\pi])$. On note $\rho_n = \sqrt{|c_n| + |c_{-n}|}$. Il suffit alors de montrer

$$\sum_{n\in\mathbb{N}} \rho_n < +\infty.$$

Soit $h > 0$, par parseval appliqué à $x \mapsto f(x + h) - f(x - h)$, on a

$$4\sum_{n\in\mathbb{N}} \rho^2 \sin^2(nh) = \frac{1}{2\pi} \int_0^{2\pi} |f(x + h) - f(x - h)|dx.$$

En utilisant le fait de f est höldérienne ($|f(x - y)| \leq C|x - y|^\alpha$), on en déduit la majoration

$$\sum_{n\in\mathbb{N}} \rho^2 \sin^2(nh) \leq \frac{C^2\pi^{2\alpha}}{42^{2\eta\alpha}}.$$

Soit $q \in \mathbb{N}$. On prend $h = \frac{\pi}{2^{q+1}}$. Alors pour $n \in [2^{q-1} + 1, 2^q]$, on a $nh \in [\pi/4, \pi/2]$, donc $\sin^2(nh) \geq 1/2$. D'où

$$\sum_{n=2^{q-1}+1}^{2^q} \rho_n^2 \leq 2\sum_{n=2^{q-1}+1}^{2^q} \rho^2 \sin^2(nh) \leq \frac{C^2\pi^{2\alpha}}{2^{2\alpha q}}.$$

En appliquant Cauchy-Schwarz on en déduit que

$$\sum_{n=2^{q-1}+1}^{2^q} \rho_n \leq 2^{(q-1)/2} \left(\frac{C^2\pi^{2\alpha}}{2^{2\alpha q}}\right) = O(\frac{1}{2^{(\alpha-1/2)q}}).$$

On en déduit que $\sum_{n\in\mathbb{N}} \rho_n < +\infty$, et que la série de Fourier de f converge normalement. Comme f est continue, alors sa limite est f (utilier le théorème Fejer). □

Inéglité de Bernstein

Théorème. Soit $\lambda > 0$ et $\lambda_1, \dots, \lambda_N \in [-\lambda, \lambda]$. On note E l'ensemble des focntions qui sont combinaisons linéaires de $(e^{i\lambda_i t})_{i\in[1,n]}$. Alors pour $f \in E$, on a : $\|h'\|_\infty \leq \lambda \|h\|_\infty$.

Démonstration. Quitte à dilater, on peut supposer $\lambda = \pi/2$. On note alors S la fonction 2π-périodique impaire telle que $S(x) = x$ sur $[0, \pi/2]$ et $S(x) = \pi - x$ sur $[\pi/2, \pi]$ (c'est la fonction triangle).Le développement en série de Fourier de S est

$$S(x) = \sum_{l=0}^{+\infty} b_{2l+1} \sin((2l+1)x).$$

avec $b_{2l+1} = \frac{4(-1)^p}{\pi(2l+1)^2}$ (à vérifier). Ce qui donne $c_l = \frac{-2i(-1)^l}{\pi(2l+1)^2}$ et $c_{-l} = \frac{2i(-1)^l}{\pi(2l+1)^2}$. Ce qui donne

$$S(x) = \sum_{l=0}^{\infty} c_{2l+1} e^{i(2l+1)x} + c_{-(2l+1)} e^{-i(2l+1)x},$$

et en évaluant en $x = \pi/2$, on en déduit que

$$\sum_{m\in\mathbb{Z}} |c_m| = \tfrac{\pi}{2}.$$

Soit $h(t) = \sum_{k=1}^n a_k e^{i\lambda_k t}$. On a alors

$$h'(t) = \sum_{k=1}^n i a_k S(\lambda_k) e^{i\lambda_k t} = \sum_{l\in\mathbb{Z}} i c_l \sum_{k=1}^n i a_k e^{i(n+t)\lambda_k} = \sum_{l\in\mathbb{Z}} i c_l h(n+t).$$

On conclut avec le fait que $\sum_{m\in\mathbb{Z}} |c_m| = \pi/2$. □

6 Méthodes de Newton

Références [Chambert-Loir Analyse 2 ?], [Rouviere ?]

Leçons concernées
- 218 - Applications des formules de TAYLOR.
- 223 - Convergence des suites numériques. Exemples et applications.
- 224 - Comportement asymptotique de suites numériques. Rapidité de convergence. Exemples.
- 226 - Comportement d'une suite réelle ou vectorielle définie par une itération $u_{n+1} = f(u_n)$. Exemples.
- 232 - Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.

7 Formule sommatoire de Poisson

Leçons concernées
- 240 - Transformation de FOURIER, produit de convolution. Applications.
- 241 - Suites et séries de fonctions. Exemples et contre-exemples.
- 246 - Séries de FOURIER. Exemples et applications.

Théorème

Pour $f \in L^1(\mathbb{R})$, on définit la transformée de Fourier de f par

$$\hat{h}(p) = \int_{\mathbb{R}} f(x)e^{-2i\pi px}dx.$$

Théorème. Soit $f \in L^1(\mathbb{R})$. On suppose que
- f est continue.
- $\sum_{n\in\mathbb{Z}} |\hat{(f)}(n)| < +\infty$.
- Il existe $M > 0$ et $\alpha > 1$ tel que

$$\forall x \in \mathbb{R}, |f(x)| \leq \frac{M}{(1+|x|)^\alpha}.$$

Alors $\sum_{n\in\mathbb{Z}} f(n)$ converge absolument et on a

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{N}} \hat{f}(n).$$

Démonstration. On définit la fonction $G : \mathbb{R} \to \mathbb{C}$ par

$$g(x) = \sum_{n\in\mathbb{Z}} f(x+n)$$

D'après l'hypothèse de majoration sur f, la série définissant G converge normalement sur tout compact, donc G est bien définie et continue. De plus G est évidemment 1-périodique. Pour $m \in \mathbb{Z}$, le $n$em coefficient de Fourier de G sont

$$c_m(G) = \int_0^1 G(x)e^{-2i\pi mx}dx = \int_0^1 \sum_{n\in\mathbb{Z}} f(x+n)e^{-imx}dx.$$

Comme la série de fonctions $\sum_{n\in\mathbb{Z}} f(x+n)e^{-2i\pi mx}$ converge nromalement sur le compact $[0,1]$, on en déduit que

$$c_m(G) = \sum_{n\in\mathbb{Z}} \int_0^1 f(x+n)e^{-imx}dx.$$

Après changement de variable, on obtient

$$c_m(G) = \sum_{n\in\mathbb{Z}} \int_n^{n+1} f(y)e^{-2i\pi my}dx = \hat{f}(m).$$

Donc $\sum_{n\in\mathbb{Z}} c_n(G)(n)| < +\infty$ et donc la série de Fourier de G converge normalement vers G. En évaluant en 0, on obtient la formule. □

Remarque. Si on prend $TF[f](p) = \frac{1}{\sqrt{2\pi}} \int_0^{2\pi} f(p)e^{ipx}dx$, on obtient

$$\sum_{n\in\mathbb{Z}} TF[f](n) = \sqrt{2\pi} \sum_{n\in\mathbb{Z}} f(2n\pi).$$

Applications

Développement eulérien de coth

Théorème. Pour $a \in \mathbb{R}_{>0}$, on a

$$\frac{\pi}{a} coth(\pi a) = \sum_{n\in\mathbb{Z}} \frac{1}{a^2+n^2}.$$

Démonstration. Pour $x \in \mathbb{R}_>0$, on a

$$\begin{array}{rcl} coth(x) & = & \frac{1+e^{-2x}}{1-e^{-2x}} = 2\frac{1}{1-e^{-2x}} - 1 = 2\sum_{n=0}^{+\infty} e^{-2nx} - 1 \\ & = & \sum_{n=0}^{+\infty} e^{-2x|n|} \end{array}.$$

Ce qui donne $coth(\pi a) = \sum_{n\in\mathbb{Z}} f(n)$ avec $f(x) = e^{-2\pi a|x|}$ (dans $L^1(\mathbb{R})$ car $a > 0$). On a alors

$$\hat{f}(p) = \int_0^{+\infty} e^{-2\pi ax+2i\pi px}dx + \int_0^{+\infty} e^{-2ax-2i\pi px}dx = \frac{a}{\pi(a^2+p^2)}.$$

Comme f vérifie les hypothèses du théorème on en déduit que

$$coth(\pi a) = \sum_{n\in\mathbb{Z}} e^{-2a|n|} = \frac{a}{\pi}\sum_{n\in\mathbb{Z}} \frac{1}{a^2+n^2}.$$

□

Remarque. Par principe du prolongement analytique la formule est vraie pour $a \in \mathbb{C} \setminus i\mathbb{Z}$.

Fonction θ de Jacobi

Définition. On définit la fonction theta de Jacobi par

$$\begin{array}{rccc} \theta: & \{\mathrm{Re} > 0\} & \longrightarrow & \mathbb{R} \\ & z & \longmapsto & \sum_{n\in\mathbb{Z}} e^{-\pi n^2 z} \end{array}.$$

La série converge normaelement sur tout compact de $\{\mathrm{Re} > 0\}$

Théorème. On a la relation suivante

$$\forall t \in \mathbb{R}_{>0}, \theta(t) = \frac{1}{\sqrt{t}}\theta(\frac{1}{t}).$$

Démonstration. Appliquer la formule sommatoire de Poisson à une Gaussienne. □

Remarque. Voir [[ZQ96], Chap IV, Sec IV, Th 9 + Ex 13,14,15]

8 Suites equireparties

Leçons concernées

- 202 - Exemples de parties denses et applications.
- 223 - Convergence des suites numériques. Exemples et applications.
- 224 - Comportement asymptotique de suites numériques. Rapidité de convergence. Exemples.
- 236 - Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables réelles.

Définition

Définition. Une suite $(x_n)_{n\in\mathbb{N}}$ de $[0,1]$ est *équirépartie* si pour tout $[a,b] \mod \mathbb{Z} \subset [0,1]$, on a

$$\text{Card}\left\{m \in [1,n] : x_m \in [a,b] \mod \mathbb{Z}\right\} \simeq_{n\to+\infty} nl([b,a]).$$

Critère de Weyl

Théorème. Soit $(x_n)_{n\in\mathbb{N}}$ une suite de $[0,1]$. Alors on a équivalence entre

(i) $(x_n)_{n\in\mathbb{N}}$ est équirépartie.

(ii) Pour toute fonction f réglée, on a
$$\lim_{n\to+\infty} \frac{1}{n}\sum_{m=1}^{n} f(x_m) = \int_0^1 f(x)dx.$$

(iii) Pour toute fonction $f \in C^0_{1-per}(\mathbb{R})$, on a
$$\lim_{n\to+\infty} \frac{1}{n}\sum_{m=1}^{n} f(x_m) = \int_0^1 f(x)dx.$$

(iv) Pour tout $m \in \mathbb{N}$, on a $\sum_{m=1}^{n} e^{2i\pi x_m} = o(n)$.

Démonstration. $(i) \Longrightarrow (ii)$: Soit f Riemann-intégrable. La propriété est clairement vraie si f est en escalier. Soient $(\phi_k)_{k\in\mathbb{N}}$ une suite de fonctions en escaliers convergent uniformément vers f. On a alors pour $n \in \mathbb{N}$ et $k \in \mathbb{N}$:

$$\begin{aligned}\left|\frac{1}{n}\sum_{m=1}^{n} f(x_k) - \int_0^1 f(x)dx\right| &\leq \left|\frac{1}{n}\sum_{m=1}^{n} f(x_k) - \phi(x_k)\right| + \int_0^1 |f(x) - \phi(x)dx| + \left|\frac{1}{n}\sum_{m=1}^{n} \phi_k(x_k) - \int_0^1 \phi(x)dx\right| \\ &\leq \|f-\phi_k\|_\infty + \|f-\phi_k\|_\infty + \left|\frac{1}{n}\sum_{m=1}^{n} \phi_k(x_k) - \int_0^1 \phi(x)dx\right|\end{aligned}.$$

Ce qui donne facilement le résultat.

$(ii) \Longrightarrow (iii)$: c'est clair

$(iii) \Longrightarrow (iv)$: c'est clair car la fonction $e^{2im\pi x}$ est continue d'intégrale nulle.

$(iv) \Longrightarrow (iii)$: on approxime f uniformément par des polynômes trigonométriques.

$(iii) \Longrightarrow (ii)$: On approxime les fonctions $1(x \in [\alpha,\beta])$ par des fonctions continue.

$(ii) \Longrightarrow (i)$: on prend la fonction indicatrice $!(x \in [a,b])$.

□

Exemple. Si $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, alors $(n\alpha \mod 1)$ est équirépartie.

Remarque. Voir [FGN, Anal 2, E 1.29], [[CLF], Anal, Ex 7.4]

9 Théorème de Dini

Leçons concernées
- 229 - Fonctions monotones et fonctions convexes.

Théorème (Dini 1)**.** Soit $f_n : [a,b] \to \mathbb{R}$ une suite de fonctions convergeant simplement vers f. On suppose que les f_n sont croissantes (non nécessairement continues) que f est continue. Alors la convergence est uniforme.

Démonstration. On voit facilement que f est croissante. Soit $\varepsilon > 0$ et $x \in [a,b]$. Par continuité de f, il existe $\eta > 0$ tel que

$$\forall y \in [x-\eta, x+\eta], |f(y) - f(x)| \leq \varepsilon.$$

Par convergence de $(f_n)_{n\in\mathbb{N}}$, il existe $n_x \in \mathbb{N}$ tel que

$$\forall n \leq n_x, |f(x-\eta) - f_n(x-\eta)| \leq \varepsilon \text{ et } |f(x+\eta) - f_n(x+\eta)| \leq \varepsilon.$$

Alors pour $n \geq n_x$ et $y \in [x-\eta, x+\eta]$, on a

$$\begin{array}{rcl} f(y) - f_n(y) & \leq & f(x+\eta) - f_n(x-\eta) \text{ par croissance} \\ & = & (f(x+\eta) - f(x-\eta)) + (f(x-\eta) - f_n(x-\eta)) \\ & & +(f_n(x-\eta) - f_n(x-\eta)) \\ & \leq & 4\varepsilon \end{array}.$$

Et de même on montre que $f(y) - f_n(y) \geq 4\varepsilon$. Par compacité de $[a,b]$, il existe $x_1, \ldots, x_p \in [a,b]$ tel que $[a,b] \subset \bigcup_{i=1}^{p} [x_i - \eta_{x_i}, x_i + \eta$
On pose alors $n_0 = \max(n_{x_1}, \ldots, n_{x_p})$ et on en déduit que $\forall n \geq n_0, ||f - f_n||_\infty \leq 4\varepsilon$. □

Théorème (Dini 2)**.** Soit K compact, $f_n : K \to \mathbb{R}$ une suite de fonctions convergeant simplement vers f. On suppose que la suite $(f_n)_{n\in\mathbb{N}}$ est croissante et que les $(f_n)_{n\in\mathbb{N}}$ et f sont continues. Alors la convergence est uniforme.

Démonstration. Soit $\varepsilon > 0$. Pour $n \in \mathbb{N}$, on pose

$$V_n(\varepsilon) = \{x \in X | f(x) - f_n(x) < \varepsilon\}.$$

Alors V_n est un ouvert de X et par compacté il existe $n_1, \ldots, n_p \in \mathbb{N}$ tel qe $X = \bigcup_{i=1}^{p} V_{n_i}(\varepsilon)$. On pose $n_0 = \max n_1, \ldots, n_p$. Alors pour $n \geq n_0$ et $x \in X$, il existe $i_0 \in [1,p]$ tel que $x \in V_{n_{i_0}}(\varepsilon)$ et on a

$$f(x) - f_n(x) \leq f(x) - f_{n_{i_0}}(x) \leq \varepsilon.$$

Ce qui montre que $\forall n \geq n_0, ||f - f_n||_\infty \leq \varepsilon$. □

10 Théorème ergodique de Von Neumann

Leçons concernées
- 208 - Espaces vectoriels normés, applications linéaires continues. Exemples.
- 213 - Espaces de HILBERT. Bases hilbertiennes. Exemples et applications.

Théorème

Théorème. Soient H un Hilbert et T un endomorphisme de norme ≤ 1. Pour $n \in \mathbb{N}$, on note

$$T_n = \frac{1}{n} \sum_k = 0^{n-1} T^k.$$

On note aussi P le projecteur orthogonal sur $\ker(T - Id)$. Alors la suite $(T_n)_{n\in\mathbb{N}}$ convege simplement vers P.

Démonstration. Soit $x \in H$. On a

$$x \in \ker(T - Id) \iff Tx = x \iff \langle x, Tx\rangle = \|x\|^2.$$

Comme $\|T^*\| = \|T\| \leq 1$, on a aussi

$$x \in \ker(T^* - Id) \iff T^*x = x \iff \langle x, T * x\rangle = \|x\|^2.$$

D'où $\ker(T^* - Id) = \ker(T - Id)$. On en déduit que $H = \overline{\mathrm{Im}(T - Id)} \oplus \ker(T - Id)$ et que

$$\forall x \in \ker(T^* - Id), \forall n \in \mathbb{N}, T_n x = p(x).$$

Si $x = Ty - y \in \mathrm{Im}(T - Id)$, alors on a

$$T_n x = \frac{1}{n}(T^n y - y) \xrightarrow{n\to+\infty} 0.$$

On montre ensuite que $T_n x \xrightarrow{n\to+\infty} 0$ pour $x \in \overline{\mathrm{Im}(T - Id)}$ (faire avec les ε). □

Exemple

Proposition. Soit $f \in L^2([0, 1])$ et $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Alors on a

$$\frac{1}{n} \sum_{k=0}^{n-1} f(. + \alpha k) \xrightarrow{n\to+\infty}^{L^2} \int_0^1 f(t)dt.$$

Démonstration. On définit

$$\begin{array}{rccc} T : & L^2([0, 1]) & \longrightarrow & L^2([0, 1]) \\ & f & \longmapsto & f(. + \alpha) \end{array}.$$

Il s'agit alors de voir que $\ker(T - Id) = \mathbb{C}$ (ou $\mathbb{R}$). On a

$$\forall n \in \mathbb{Z}, c_n(Tf) = e^{-2i\pi n\alpha} c_n(f).$$

Donc si $f \in \ker(T - Id)$, pour $n \in \mathbb{Z}^*$, on a

$$(1 - e^{-2i\pi n\alpha})c_n(f) = 0.$$

Comme $\alpha \notin \mathbb{Q}$, on a donc $c_n(f) = 0$. □

Remarque. Voir [[BMP04], Chap 3, Ex 3.6], [[CLF], Anal 1, Ex 9.2].

11 Théorème de Polya

Leçons concernées

- 223 - Convergence des suites numériques. Exemples et applications.
- 238 - Méthodes de calcul approché d'intégrales.
- 238b - Méthodes de calcul approché d'intégrales et d'une solution d'une équation différentielle.

Remarque. Voir [Dumas].

12 Critère de Kitai d'hypercyclicité

Leçons concernées
- 202 - Exemples de parties denses et applications.
- 226 - Comportement d'une suite réelle ou vectorielle définie par une itération $u_{n_1} = f(u_n)$. Exemples.

Préliminaires

On note E un $\mathbb{C}$-espace vectoriel normé (ou métirque complète) séparable et S une partie dénombrable dense.

Définition. Soit $T \in L_c(E)$. Un vecteur $x \in E$ est dit hypercyclique si son orbite est dense dans E. On note $HC(T)$ l'ensemble des vecteurs hypercycliques.

Proposition. Soit $T \in L_c(E)$.
- L'ensemble $HC(T)$ est une G_δ.
- Si $HC(T)$ est non vide, alors $HC(T)$ est dense.

Démonstration. .[A completer]. □

Proposition. Si ${}^tT$ admet un vecteur propre (ce qui est le cas si E est de dimension finie), alors T n'est pas hypercyclique.

Démonstration. .[A completer]. □

Théorème

Théorème (Kitaï)**.** Soit $T \in L_c(E)$. On supose qu'il existe X, Y deux partie dense de E et S une application telle que :
- $\forall y \in Y, TS.y = y$.
- $\forall x \in X, T^n.x \xrightarrow{n\to+\infty} 0$.
- $\forall y \in Y, S^n.y \xrightarrow{n\to+\infty} 0$.

Alors T est hypercyclique.

Démonstration. .[A completer]. □

Exemples

Exemple. On considère Ω un ouvert de $\mathbb{C}$, et on prend $E = \mathcal{H}(\Omega)$ munie de la métrique usuelle. Alors la dérivation est hypercyclique.

Démonstration. On prend $X = Y = \mathbb{C}[z]$. □

Exemple. On prend $E = \mathcal{H}(\mathbb{C})$. Alors la translation par 1, $T.f(z) = f(z+1)$, est hypercyclique.

Démonstration. On prend $X = e^{-z}\mathbb{C}[z]$ et $Y = e^z\mathbb{C}[z]$. □

Exemple. On prend $E = l^2$, $\lambda > 1$ et T définit par $\begin{cases} (T.x)_n = \lambda x_{n-1} \\ \tau(x)_0 = 0 \end{cases}$. Alors T est hypercyclique.

Démonstration. On prend $X = l^0$ et $y = l^2$. □

Remarque. Voir [[GT96], Chap II.2.14]

13 Suite logistique

Leçons concernées
– ? ? ?

Remarque. Voir [http ://www.math.u-psud.fr/ perrin/Conferences/logistiqueDP.pdf].

Chapitre 8

Probabilités

1 Marche aléatoire sur $\mathbb{Z}^d$

Leçons concernées
- 235 - Suites et séries de fonctions intégrables. Exemples et applications.
- 242 - Utilisation en probabilités de la transformation de FOURIER ou de LAPLACE et du produit de convolution.
- 249 - Suites de variables de BERNOULLI indépendantes.
- 251 - Indépendance d'événements et de variables aléatoires. Exemples.
- 252 - Loi binomiale. Loi de POISSON. Applications.

Théorème. Soit $d \in \mathbb{N}^*$. On considère X la loi unirforme sur $\{\varepsilon e_i : \varepsilon \in \{-1,1\}, i \in [1,d]\}$ avec $(e_i)_{i\in[1,d]}$ la base canonique de $\mathbb{Z}^d$. On considère $(X_k)_{k\in\mathbb{N}}$ une suite de v.a.i.i.d. de loi celle de X. On considère la marche aléatroire $S_n = \sum_{k=1}^n X_k$ ($n \in \mathbb{N}$, et $S_0 = 0$).
- Si $d \leq 2$, alors p.s. la suite $(S_n)_{n\in\mathbb{N}}$ passe une infinité de fois par 0 (et même par tous les points de $\mathbb{Z}^d$).
- Si $d \geq 3$, alors p.s. on a $\lim_{n\to+\infty} S_n = \infty$.

Démonstration. La fonction caractéristique Φ_X de X est

$$\begin{array}{rccc} \Phi_X : & \mathbb{R}^n & \longrightarrow & \mathbb{C} \\ & t = (t_i)_{i\in[1,d]} & \longmapsto & E[e^{i\langle t,x\rangle}] = \sum_{i=1}^d \frac{1}{d}\cos t_i \end{array},$$

et celle de S_n est $\Phi_{S_n} = \Phi_X^n$.

Pour $x \in \mathbb{Z}^d$, on note $E_x = E\Big[\text{Card}\{n \in \mathbb{N} : S_n = 0\}\Big]$ le nombre moyen de passage en x. On a alors

$$E_x = \sum_{n=0}^\infty P(S_n = x).$$

Lemme. On a : $\forall x \in \mathbb{Z}^d, E_0 < +\infty \Longleftrightarrow E_x < +\infty$.

Démonstration du lemme. Soit $x \in \mathbb{Z}^d$. On définit la v.a. sur $\mathbb{N}$: $N_x = \inf\{n \in \mathbb{N} : S_n = x\}$. En conditionnant, on a alors (en fait, il faudrait garder que les évènements de probabilité non nul...)

$$\begin{array}{rcl} E_x & = & \sum_{n=0}^{+\infty}\Big(\sum_{p=0}^{+\infty} P(S_n = x|N_x = p)P(N_x = p)\Big) + P(S_n = x|N_x = +\infty)P(N_x = +\infty) \\ & = & \sum_{n=0}^{+\infty}\sum_{p=0}^{n} P(S_n = x|N_x = p)P(N_x = p) \\ & = & \sum_{n=0}^{+\infty}\sum_{p=0}^{n} P(S_n - S_p = 0|N_x = p)P(N_x = p) \end{array}$$

Or par indépendance, on a $P(S_n - S_p = 0|N_x = p) = P(S_{n-p} = 0)$. En appliquant Fubini, on obtient

$$\begin{array}{rcl} E_x & = & \sum_{p=0}^{+\infty}\sum_{n=p}^{+\infty} P(S_{n-p} = 0)P(N_x = p) = \sum_{p=0}^{+\infty}\sum_{m=0}^{+\infty} P(S_m = 0)P(N_x = p) \\ & = & E_0.(1 - P(N_x - +\infty)). \end{array}$$

On conclut en remarquant que $P(N_x = +\infty) < 1$ (considérer un chemin de longeur fini qui passe par x). □

Pour $x \in \mathbb{Z}^d$, on note p_x la probabilité de passer au moins une fois en x pour un $n \geq 1$.

Lemme. On a : $E_0 < +\infty \Longleftrightarrow p_0 < 1$.

Démonstration du lemme. Pour $m \in \mathbb{N}$, la probabilité de passer au moins m fois au point 0 est p_0^m : en effet, si on note F_m l'évènement {retourner au moins m fois en 0} et N_m le premier temps où l'on est revenu en 0 pour la $m$em fois, alors pour $m \geq 2$, on a (là aussi il faudrait garder que les évènements de probabilité non nul...)

$$\begin{array}{rcl} P(F_m) & = & \sum_{N\in[1,+\infty]} P(F_m|N_{m-1}=N)P(N_{m-1}=N) \\ & = & \sum_{N\in[1,+\infty[} p_0 P(N_{m-1}=N) \\ & = & p_0 P(N_{m-1}<+\infty) \\ & = & p_0 P(F_{m-1}). \end{array}$$

La probabilité de retourner exactement m fois en 0 est alors $p_0^m - p_x^{m+1}$ et la probabilité de retourner une infinité de fois en 0 est $p_0^{+\infty}$ (car l'évènement {retourner une infinité de fois} est l'intersection décroissante des évènements {retourner au moins m fois}). Donc on obtient

$$E_0 = \sum_{m=0}^{+\infty} m(p_0^m - p_0^{m+1}) + (+\infty)p_0^{+\infty} = (1-p_0)\sum_{m=0}^{+\infty} m p_0^m + (+\infty)p_0^{+\infty},$$

avec les conventions : $(1-p)\sum_{m=0}^{+\infty} mp^m = 0$ si $p = 1$ et $(+\infty)p^{+\infty} = +\infty$ si $p = 1$ et 0 si $p < 1$, ce qui permet de conclure. □

Proposition. – Si $E_0 = +\infty$, alors p.s. la suite $(S_n)_{n\in\mathbb{N}}$ passe une infinité de fois par 0.
– Si $E_0 < +\infty$, alors p.s. on a $\lim_{n\to+\infty} S_n = \infty$.

Démonstration de la proposition. Si $E_0 = +\infty$, alors d'après ce qui précède pour tout $x \in \mathbb{Z}^d$, l'évènement $\Big\{S_n \neq 0 \text{ une nombre infinité de fois}\Big\}$ est de probabilité $p_0^{+\infty} = 1$.

Si $E_0 < +\infty$, alors pour tout $x \in \mathbb{Z}^d$, l'évènement $\Big\{S_n \neq x \text{ une nombre infitnité de fois}\Big\}$ est de probabilité $p_0^{+\infty}p_x = 0$. On note F l'évènement

$$F = \bigcup_{x\in\mathbb{Z}^d} \Big\{S_n \neq x \text{ sauf un nombre fini de fois}\Big\}.$$

Alors F est de probabilité 1. Soit $\omega \in F$. Pour tout $R > 0$, l'ensemble $B_{\mathbb{Z}^d}(0,R)$ est fini, donc la suite $(S_n(\omega))_{n\in\mathbb{N}}$ ne passe qu'un nombre fini de fois dans $B_{\mathbb{Z}^d}(0,R)$. D'où $\lim_{n\to+\infty} S_n(\omega) = \infty$. □

Lemme. On a

$$E_0 = \int_{[-\pi,\pi]^2} \frac{1}{1-\Phi_X(t)^2} dt.$$

Démonstration du lemme. Pour $n \in \mathbb{N}$, la probabilité de l'évènement $\{S_n = 0\}$ est (la série de Fourier de S_n est finie)

$$\begin{array}{rcl} P(S_n=0) & = & \hat{\Phi}_{S_n}(0) = \int_{[-\pi,\pi]^d} \Phi_{S_n}(t)dt \\ & = & \int_{[-\pi,\pi]^d} \Phi_X(t)^n dt. \end{array}$$

En remarquant que $P(S_n = 0) = 0$ si n est impaire, on a

$$\begin{array}{rcl} E_0 & = & E\left[\sum_{n=0}^{\infty} 1(S_n=0)\right] = \sum_{n=0}^{\infty} P(S_{2n}=0) \\ & = & \sum_{n=0}^{\infty} \int_{[-\pi,\pi]^d} \Phi_X(t)^{2n} dt \end{array}$$

Par théorème de Fubini-Tonelli, on en déduit le résultat. □

Proposition. Si $d \leq 2$, alors $E_0 = +\infty$ et si $d \geq 3$, alors $E_0 < +\infty$.

Démonstration de la proposition. Il suffit d'étudier l'intégrabilité de $(1-\Phi_X(t)^2)^{-1}$ aux points $t = (0,\dots,0)$ et $t = (\pi,\dots,\pi)$.

En $t = 0$: comme $\cos u = 1 - \frac{1}{2}u^2 + o(u^2)$, on en déduit que

$$\begin{array}{rcl} 1-\Phi_X(t)^2 & = & 1 - \left(\frac{1}{d}\sum_{i=1}^d 1 - \frac{1}{2}t_i^2 + o(t_i^2)\right)^2 = 1 - \left(1 - \frac{1}{2d}\|t\|_2^2 + o(\|t\|_2^2)\right)^2 \\ & \sim & \frac{1}{d}\|t\|_2^2 \end{array}$$

Donc $(1-\Phi_X(t)^2)^{-1}$ est intégrable en 0 si et seulement si $2 < d$.

On fait de même en $t = (\pi,\dots,\pi)$. □

Le théorème découle des deux propositions. □

Remarque. Si $E_0 = +\infty$, a-t-on $p_x = 1$ pour tout $x \in \mathbb{Z}^d$?

Remarque.
- Ce développement a été proposé par Élodie Bouchet.
- La preuve se trouve dans [[DM72], Chap ?].

2 Processus de Galton-Watson

Leçons concernées
- 226 - Comportement d'une suite réelle ou vectorielle définie par une itération $u_{n+1} = f(u_n)$. Exemples.
- 229 - Fonctions monotones. Fonctions convexes. Exemples et applications.
- 235 - Suites et séries de fonctions intégrables. Exemples et applications.
- 242 - Utilisation en probabilités de la transformation de FOURIER ou de LAPLACE et du produit de convolution.
- 251 - Indépendance d'événements et de variables aléatoires. Exemples.

On note X une variable aléatoire L^1 sur $\mathbb{N}$. Elle représente le nombre de descendant d'un individu. On suppose qu'après une génération chaque individu meurt et donne naissance X descendants.

Soit $(X_n^k)_{n,k\in\mathbb{N}}$ une suite de v.a.i.i.d. de loi celle de X. Pour $\omega \in \Omega$, on note $Z_0(\omega) = 1$ et $Z_n(\omega)$ le nombre d'individu à la génération n. La variable $X_n^k(\omega)$ représente alors le nombre de descendant du $k$em individu, s'il existe, à la génération n. On a alors

$$Z_{n+1}(\omega) = \sum_{k=1}^{Z_n(\omega)} X_n^k(\omega).$$

On remarque que si $Z_n(\omega) = 0$ pour un certain n, alors $Z_m(\omega) = 0$ pour tout $m \geq n$.

Théorème. Si $E[X] \leq 1$, alors la population s'éteint :

$$P(\exists n \in \mathbb{N}, Z_n = 0) = 1,$$

et si $E[X] > 1$, alors la population survie avec probabilité > 0 :

$$P(\exists n \in \mathbb{N}, Z_n = 0) < 1,$$

Démonstration. On note Φ_X la fonction génératrice de X.

Lemme. On a pour tout $n \in \mathbb{N}$: $\Phi_{Z_n} = \Phi_X^{(n)}$ (composée n fois).

Démonstration du lemme. On a pour $n \in \mathbb{N}$ et $|z| < 1$:

$$\begin{aligned} \Phi_{Z_n}(z) &= E[z^{Z_n}] = E[z^{\sum_{k=1}^{Z_n} X_n^k}] \\ &= \sum_{p=0}^{+\infty} E[z^{\sum_{k=1}^{p} X_n^k} \mid Z_n = p] P(Z_n = l) \end{aligned}$$

Comme les $(X_n^k)_{k\in\mathbb{N}}$ et Z_n sont indépendantes, on a.

$$\Phi_{Z_n}(z) = \sum_{p=0}^{+\infty} E[z^X]^l P(Z_n = l) = \Phi_{Z_n}(\Phi_X(z)).$$

□

Soit $n \in \mathbb{N}$. On a $P(Z_n = 0) = \Phi_{Z_n}(0) = \Phi_X^n(0)$. Comme la suite d'évèmements $(\{Z_n = 0\})_{n\in\mathbb{N}}$ est croissante, on a

$$P(\exists n \in \mathbb{N}, Z_n = 0) = \lim_{n\to+\infty} P(Z_n = 0) = \lim_{n\to+\infty} \Phi_X^n(0).$$

La fonction Φ_X sur $[0, 1]$ est croissante et convexe (car les coefficients de sa série sont positifs), donc la suite $(P(Z_n = 0))_{n\in\mathbb{N}}$ converge vers une limite que l'on note P. On note $p_i = P(X = i)$.

• 1er cas : $p_0 + p_1 = 1$. Alors $\Phi_X(z) = p_0 + p_1 z$. Si $p_0 = 0$, alors $E[X] = 1$ et le processus est déterministe p.s., et si $p_0 > 0$, alors $E[X] < 1$ et 1 est le seul point fixe de Φ_X. D'où $P = 1$.

• 2em cas : $p_0 + p_1 > 1$. Alors Φ_X est strictement convexe. Comme la v.a. X est L^1, la série $\sum_{i=0}^{+\infty} ip_i x^i$ converge normalement sur $[0, 1]$ et on a $\Phi'_X(1) = E[X]$.

Si $E[X] \leq 1$, alors par stricte convexité $\Phi_X(x) < x$ sur $[0, 1[$, et donc 1 est le seul point fixe. D'où $P = 1$.

Si $E[X] > 1$, alors Φ_X admet un unique point fixe x_0 dans $[0, 1[$ (faire un dessin ?). L'intervalle $[0, x_0]$ est alors stable par Φ_X et x_0 est le seul point fixe. Donc $P = x_0 < 1$. □

Remarque. La preuve se trouve dans [Cotrell, Chap ?].

3 Nombre de cycles d'une permutation

Leçons concernées
– ? ? ?

Remarque. Voir [[Dur96], Cha I.5, Exem 5.8].

4 Séries entières avec coupure

Leçons concernées
- 243 - Convergence des séries entières, propriétés de la somme. Exemples et applications.
- 251 - Indépendance d'événements et de variables aléatoires. Exemples.

A Préliminaires

Théorème (Loi du 0-1 de Kolmogorov)**.** Si $(F_n)_{n\in\mathbb{N}}$ et une suite de tribus indépendantes sur un espace de probabilité Ω, et si F est sa tribu queue, alors pour tout $A \in F$, on a $P(A) = 0$ ou $P(A) = 1$.

Proposition. Soient $f(z) = \sum_{n=0}^{+\infty} a_n z^n$ une série entière de RCV 1 et I un arc fermé de $\mathbb{S}^1$. Alors tous les points de I sont réguliers si et seulement si : il existe $C > 0$ et $\rho \in]0, 2[$ tel que pour tout $a \in I$, on a

$$\forall k \in \mathbb{N}, |f^{(k)}(a/2)/k!| \leq C\rho^k.$$

Démonstration. Supposons que f est régulière en tout point de I. On prend U un ouvert un voisinage de I sur lequel f est holomorphe. Comme on a

$$\bigcap_{r>1/2} I/2 + \bar{B}(0, r) = I/2 + \bar{B}(0, 1/2) \subset D \cup U,$$

avec $\bigcap_{r>1/2} I/2 + \bar{B}(0, r)$ une intersection décroissante de compacts, il existe $r > 1/2$ tel que $I/2 + \bar{B}(0, r) \subset D \cup U$. Par formle de Cauchy on a alors

$$|f^{(k)}(a/2)/k!| \leq r^{-k}\|f\|_{L^\infty(I/2+\bar{B}(0,r))}.$$

Réciproquement, si f vérie les conditions, alors pour tout $a \in I$, la série $\sum_{k\in\mathbb{N}} \frac{f^{(k)}(a/2)}{k!} y^k$ est holomorphe sur $B(a/2, \rho^{-1})$. Donc f est holomorphe sur $I/2 + B(0, \rho^{-1}) \supset I$. □

Remarque. Il suffit de se limiter à C un entier, ρ un rationnel et a un point rationnel.

B Théorème

Théorème. Soit $\sum a_n z^n$ une SE de RCV=1. Alors il existe $(e^{i\theta_n})_{n\in\mathbb{N}}$ tel que la série $\sum a_n e^{i\theta_n} z^n$ soit singulière en tout points de $\mathbb{S}^1$ (i.e. $\mathbb{S}^1$ est coupure de la série).

Démonstration. On considère une suite $(X_n)_{n\in\mathbb{N}}$ de variables aléatoires sur $\mathbb{S}^1$ i.i.d uniformément distribué. On va montrer qu'avec probbilité 1, le cercle est coupure de la série $f^\omega(z) = \sum_{n\geq 0} a_n X_n z^n$.

Pour I un arc fermé de $\mathbb{S}^1$, on note A_I l'évènement

$$A_I = \Big\{\omega \in \Omega : \sum a_n X_n(\omega) z^n \text{ est régulière en tout point de } I\Big\}.$$

Montrons que A_I est dans la tribu asymptique. Soit $N \in \mathbb{N}$. On note $f_N^\omega(z) = \sum_{n\geq N} a_n X_n(\omega) z^n$. On a alors

$$\forall \omega \in \Omega, \forall a \in I, a \text{ est point régulier de } f^\omega \iff a \text{ est point régulier de } f_N^\omega.$$

Pour tout $a \in I$, $k \in \mathbb{N}$, l'application $\omega \mapsto f_N^{\omega\,(k)}(a/2)$ est $\sigma(Z_N, \dots)$-mesurable. Le lemme [?] montre alors que A_I est dans $\sigma(Z_N, \dots)$. Donc A_I est dans la tribu asymptotique.

D'après la loi du 0-1, on a $P(A_I) = 0$ ou 1 pour tout arc fermé I. Si $I = e^{i\alpha} I'$ (i.e. si I et I' ont même longueur), alors $P(A_I) = P(A_{I'})$ [y réfléchir].

S'il existe I tel que $P(A_I) = 1$, alors on prend $I_1, \dots, I_p$ de même longueur que I recouvrant le cercle. Pour $\omega \in A_{I_1} \cap \dots \cap A_{I_p}$, la série $\sum a_n e^{i\theta_n} z^n$ a pour rayon de convergence 1 et est sans point singulier, ce qui est absurde.

Donc pour tout I, $P(A_I) = 0$. On prend alors $(I_{n\in\mathbb{N}})$ la famille d'arc à bornes rationnels, et on a $P(\bigcup_{n\in\mathbb{N}} I_n) = 0$. Pour $\omega \in \Omega \setminus \bigcup_{n\in\mathbb{N}} I_n$, la série $\sum a_n e^{i\theta_n} z^n$ est singulière en tout point de $\mathbb{S}^1$. □

Remarque. Voir [[ZQ96], Chap XIII, Sec III.1].

Bibliographie

[AF77] J.M. Arnaudies and H. Fraysse. *Cours de mathématiques. 2, Analyse.* Dunod, 1977.

[AJ06] F. Apéry and J.P. Jouanolou. Élimination : le cas d'une variable. *Hermann, Collection Méthodes*, 2006.

[Ale99] M. Alessandri. Thèmes de géometrie. *Groupes en situation geometrique, Dunod*, 1999.

[Arn69] J.M. Arnaudiès. *Les cinq polyèdres réguliers de ([R])[sup] 3 et leurs groupes : avec, en première, une étude des déplacements de ([R])[sup] 3.* Centre de Documentation Universitaire, 1969.

[Aud06] M. Audin. *Geometrie.* EDP Sciences Editions, 2006.

[AZ03] M. Aigner and GM Ziegler. Proof from THE BOOK, 2003.

[BCL83] H. Brezis, P.G. Ciarlet, and J.L. Lions. *Analyse fonctionnelle : theorie et applications.* Masson, paris, 1983.

[Ber77] M. Berger. *Geometrie.* Cedic, 1977.

[BGL87] M. Berger, B. Gostiaux, and S. Levy. *Differential geometry : manifolds, curves, and surfaces.* springer-Verlag New York, 1987.

[BMP04] V. Beck, J. Malick, and G. Peyré. *Objectif agrégation : mathématiques.* H & K, 2004.

[Cal06] J. Calais. *Eléments de théorie des anneaux : anneaux commutatifs.* Ellipses, 2006.

[CL05] A. Chambert-Loir. *Algebre corporelle.* Éditions École Polytechnique, 2005.

[CLF] A. Chambert-Loir and S. Fermigier. Agregation de mathematiques, analyse 1, 2 et 3, exercices.

[Coh80] D.L. Cohn. *Measure theory.* Birkh
"auser, 1980.

[Com98] F. Combes. *Algèbre et géométrie.* Bréal, 1998.

[CT61] H.P. Cartan and R. Takahashi. *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes.* Hermann, 1961.

[Dem97] M. Demazure. *Cours d'algèbre : primalité, divisibilité, codes.* Cassini, 1997.

[Dem06] J.P. Demailly. *Analyse numérique et équations différentielles.* L'Editeur : EDP Sciences, 2006.

[DM72] H. Dym and H.P. McKean. *Fourier series and integrals.* Academic Press New York, 1972.

[Dur96] R. Durrett. *Probability : theory and examples.* Citeseer, 1996.

[Esc00] J.P. Escofier. *Théorie de Galois.* Dunod, 2000.

[FG95] S. Francinou and H. Gianella. *Exercices de mathématiques pour l'agrégation : Algèbre.* Masson, 1995.

[Gob96] R. Goblot. *Algèbre commutative.* Masson, 1996.

[Gou94a] X. Gourdon. *Les maths en tête : algebre.* Ellipse, 1994.

[Gou94b] X. Gourdon. Les maths en tête analyse, 1994.

[GT96] S. Gonnord and N. Tosel. *Thèmes d&analyse pour l&Agrégation.[1]. Topologie et analyse fonctionnelle.* Ellipses-Marketing, 1996.

[GT98] S. Gonnord and N. Tosel. Calcul différentiel, 1998.

[HL98] F. Hirsch and G. Lacombe. *Eléments d'analyse fonctionnelle.* Masson, 1998.

[Lan93] S. Lang. *Real and functional analysis.* Springer, 1993.

[Lau01] F. Laudenbach. *Calcul différentiel et intégral.* Ecole Polytechnique, 2001.

[Mic] A. Michel. Agrégation de mathématiques. Thèmes de géométrie. Groupes en situation géométrique.

[MT86] R. Mneimné and F. Testard. *Introduction à la théorie des groupes de Lie classiques.* Hermann, 1986.

[Per96] D. Perrin. *Cours d'algébre*. Ellipse, 1996.

[RBB06] J.J. Risler, P. Boyer, and P. Boyer. *Algèbre pour la Licence 3 : groupes, anneaux, corps*. Dunod, 2006.

[RDH75] W. Rudin, N. Dhombres, and F. Hoffman. *Analyse reelle et complexe*. Masson, 1975.

[Rou] F. Rouvière. Petit guide de calcul différentiel à l'usage de la licence et de l'agrégation. Deuxième édition revue et commentée.

[Rud95] W. Rudin. Analyse fonctionnelle. *Ediscience international*, 1995.

[Sam61] P. Samuel. On unique factorization domains. *Illinois J. Math*, 5 :1–17, 1961.

[Ser70] J.P. Serre. *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1970.

[ZQ96] C. Zuily and H. Queffélec. *Éléments d'analyse pour l'agrégation*. Masson, 1996.