PLANS DE LEÇONS POUR L'AGRÉGATION.

JULIEN BERNIS

Date: 19 janvier 2017.

1. **101 : Groupe opérant sur un ensemble. Exemples et applications.**

I. Qu'est-ce qu'une action de groupe ?

Définition. [Ulmer, 2005] Définition d'une action de groupe.

Proposition. Morphisme structurel de l'action.

Exemples d'actions.

(1) $\mathcal{S}(X)$ agit naturellement sur X.

(2) L'action de G sur lui-même par conjugaison n'est ni fidèle ni transitive.

(3) G agit fidèlement et transitivement sur lui-même par translation.

(4) L'action de G sur une orbite est transitive.

Définition. Définition des orbites, des stabilisateurs. Définition d'une action transitive, définition d'une action fidèle. Rappeler la formule $\cap \mathrm{Stab}_G(x) = \mathrm{Ker}(\rho)$.

Exemples.

(1) $\mathcal{S}(X)$ agit fidèlement et transitivement sur X.

(2) $\mathrm{GL}(V)$ agit naturellement sur V.

(3) G agit sur lui même par translation et conjugaison.

II. Dénombrement.

II.1. *Formule des classes.*

Proposition. La relation être dans la même orbite est une relation d'équivalence sur X.

Exemple. Orbites de $\mathrm{GL}_2(\mathbb{C})$ sous l'action de conjugaison par $\mathrm{GL}_2(\mathbb{C})$: Les homothéties, les matrices diagonalisables à valeurs propres distinctes, les matrices trigonalisables.

Principe de conjugaison. Le cardinal du stabilisateur est constant le long d'une orbite : $\mathrm{Stab}_G(g \cdot x) = g\mathrm{Stab}_G(x)g^{-1}$.

Proposition. On a $|G| = |\mathcal{O}_x||\mathrm{Stab}_G(x)|$.

Formule des classes. Soit $(x_1, \cdots, x_r)$ un système de représentant d'orbites alors on a : $|X| = \sum\limits_{i=1}^{r} \frac{|G|}{\mathrm{Stab}_G(x_i)}$

Application. [Caldero and Germoni, 2013] Calcul du cardinal des matrices diagonalisables de $\mathrm{GL}_n(\mathbb{F}_q)$.

II.2. *Points fixes de l'action.*

Définition. [Ulmer, 2005] On dit que $x \in X$ est un point fixe sous l'action de G lorsque $gx = g$ pour tout $g \in G$. L'ensemble des points fixes est noté X^G.

Exemple. Le centre de G est l'ensemble des points fixes de G pour l'action de G sur lui-même par conjugaison.

Formule de Burnside. On note r le nombre d'orbites de X sous l'action de G. Alors on a $r = \frac{1}{|G|} \sum_{g \in G} |X^{<g>}|$.

Application. Si G est un sous groupe fini non trivial de $\mathrm{SO}_3(\mathbb{R})$, alors G est isomorphe à l'un des groupes suivants : $\mathbb{Z}/m\mathbb{Z}$ avec $m \geq 2$, D_m, $\mathcal{A}_4$, $\mathcal{S}_4$ ou $\mathcal{A}_5$.

Remarque. Les résultats sur les p groupes de la partie suivante reposent sur cette formule.

III. L'action pour mieux comprendre le groupe

Action de translation du groupe G sur lui même : **Théorème de Cayley.** Tout groupe fini G d'ordre n est isomorphe à un sous-groupe transitif de $\mathcal{S}_n$.

Action par conjugaison. **Définition.** Définition du centralisateur d'un élément.

Exemple. Détermination des classes de conjugaison des éléments de D_n et des centralisateurs.

Action de $\mathrm{Aut}(G)$ sur les sous groupes de G. **Définition.** Définition d'un sous-groupe caractéristique.

Exemple. Le groupe dérivé et le centre de G sont des sous-groupes caractéristiques.

Application. Si H est distingué dans G et si K est un sous-groupe caractéristique de H alors K est distingué dans G.

Définition. Un p groupe est un groupe dont l'ordre de tout élément est une puissance de p.

Exemple. D_4 est un 2 groupe.

Proposition. Si G est un p groupe qui agit sur X fini, alors on a : $|X^G| \equiv |X|$ modulo p.

Théorème de Cauchy. Soit G un groupe fini d'ordre divisible par un nombre premier p. Alors il existe un élement d'ordre p dans G.

Autre application. Un p groupe fini est un groupe fini dont l'ordre est une puissance de p.

Centre d'un p groupe. Le centre d'un p groupe fini n'est jamais trivial. En particulier un p groupe fini d'ordre non premier n'est jamais un groupe simple.

Corollaire. Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

IV. Les actions pour mieux comprendre l'ensemble.

IV.1. *Polynômes*

Polynômes symétriques [Gourdon, 1994b] Définition, exemples, résultats de structure.

IV.2. *Espaces de matrices.*

Première action. [Caldero and Germoni, 2013] $\mathrm{GL}_n(\mathbb{K})$ agit par conjugaison sur $\mathrm{M}_n(K)$. Des matrices dans la même orbite sont dites semblables.

Condition d'appartenance à une même orbite. Des matrices sont semblables si et seulement si elles ont même réduction de Frobenius.

Deuxième action. [Caldero and Germoni, 2013] $\mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_m(\mathbb{K})$ agit par conjugaison sur $\mathrm{M}_{n,m}(K)$. Des matrices dans la même orbite sont dites équivalentes.

Condition d'appartenance à la même orbite. Des matrices sont semblables si et seulement si elles ont même rang.

Troisième action. [Caldero and Germoni, 2013] $\mathrm{GL}_n(\mathbb{K})$ agit par conjugaison sur $\mathrm{S}_n(K)$. Des matrices dans la même orbite sont dites congruentes.

Classification des formes quadratiques. [Perrin, 1996]

(1) Sur $\mathbb{C}$ même rang.
(2) Sur $\mathbb{R}$ même signature.
(3) Sur $\mathbb{F}_q$ de caractéristique différente de 2, par le fait que le discriminant soit un carré ou pas dans $\mathbb{F}_q$.

IV.3. *Géométrie.*

Classification affine des coniques affines. [Audin, 2012] On fait agir le groupe des transformations affines sur les coniques. On obtient 8 (ou 9) coniques affines. Deux coniques sont dans la même orbite lorsque leur formes quadratiques après changement de repère ont même signature.

Classification euclidienne des coniques non dégénérés. On fait agir le groupe des isométries sur l'ensemble des coniques non dégénérées. On obtient une infinité d'orbites qu'on peut répartir en 3 catégories.

Définition. Définition d'une droite projective $\mathbb{P}(\mathbb{K})$. Définition du groupe linéaire projectif et du groupe spécial projectif. Action fidèle et transitive de $\mathbb{P}SL$ sur $\mathbb{P}^1(\mathbb{K})$.

Définition. Définition de l'ensemble des droites hyperboliques $\mathcal{D}_h$ sur le demi plan de Poincarré.

Proposition.

(1) Le groupe $\mathbb{P}SL_2(\mathbb{R})$ agit transitivement sur le demi plan de Poincarré.

(2) Le groupe $\mathbb{P}SL_2(\mathbb{R})$ agit transitivement sur $\mathcal{D}_h$.

2. **102 : Groupe des nombre complexes de module 1. Sous-groupes des racines de l'unité. Applications.**

I. Groupe des nombres complexes de module 1.

I.1. *Propriétés.*

Définition. L'application $|\cdot| : \mathbb{C}^* \to \mathbb{R}_+^*$ est un morphisme de groupe de noyau U. U est le cercle unité du plan complexe.

Décomposition polaire 1. [Mneimné and Testard, 1986] L'application $U \times \mathbb{R}_+^* \to \mathbb{C}^*$ définie par $(u, r) \mapsto ru$ est un homéomorphisme.

Exponentielle. L'application $\exp(i\cdot) : \mathbb{R} \to U$ est un morphisme de groupes. Son noyau est $2\pi\mathbb{Z}$.

Décomposition polaire 2. Tout nombre complexe non nul z s'écrit $z = r\exp(i\theta)$ avec $r \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}/(2\pi\mathbb{Z})$.

Définitions. Définition du cosinus et du sinus. Formules d'Euler et de Moivre.

I.2. *Sous-groupes de U.*

Proposition. Un sous-groupe de U est dense ou fini.

Proposition. Le sous-groupe engendré par $\exp(i\theta)$ est dense si et seulement si $\theta \notin 2\pi\mathbb{Q}$.

Application. $\sin(n)$ est dense dans $[-1, 1]$.

II. Racines de l'unité.

II.1. *Structure de groupe cyclique.*

Définition. [Perrin, 1996] L'application $U \to U$, $z \mapsto z^n$ est un morphisme de groupe. Son noyau est le groupe des racines n-ièmes de l'unité, noté U_n.

Proposition. L'application $\mathbb{Z}/n\mathbb{Z} \to U$, $k \mapsto \exp(\frac{2ik\pi}{n})$ est un isomorphisme de groupes. U_n est donc un groupe cyclique. Il est engendré par les éléments de l'ensemble $U_n^* = \{\exp(\frac{2ik\pi}{n}) | \text{p.g.c.d}(k, n) = 1\}$, appelé racines primitives n-ièmes de l'unité.

Proposition. $U_d \subset U_n$ si et seulement si $d|n$.

Proposition. $U_n = \bigcup_{d|n} U_d$ et $|U_n^*| = \varphi(n)$.

II.2. *Polynômes cyclotomiques.*

Définition. [Perrin, 1996] Définition du n-ième polynôme cyclotomique. Il est unitaire de degré $\varphi(n)$.

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

Exemples. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$ etc

Irréductibilité les polynômes cyclotomiques sur $\mathbb{Z}$.

Application. Soit ω une racine primitive n-ième de l'unité, on a alors $[Q(\omega) : \mathbb{Q}] = \varphi(n)$.

Théorème de Kronecker. [ORAUX X-ENS ALGEBRE 1]

III. Applications

III.1. *Groupe diédral*

Remarque. [Ulmer, 2005] Les éléments de U_n sont les sommets du polygône régulier à n côtés P_n.

Définition. Pour $n \geq 3$, le groupe diédral D_n est le groupe des isométries du plan affine qui laissent invariant P_n.

Proposition. Le groupe diédral est d'ordre $2n$ et il est engendré par la symétrie axiale $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et la rotation d'angle $\theta = \frac{2\pi}{n}$, $r = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$.

Proposition. Le groupe $\langle r \rangle$ est isomorphe à U_n et il est distingué dans D_n. On a les relations $r^n = e$, $s^2 = e$, et $srs = r^{-1}$

Application. Détermination des caractère irréductibles de degré 1 de D_n. $\chi(s)^2 = \chi(s^2) = \chi(e) = 1$ d'où $\chi(s) = \pm 1$ et $\chi(r) = \pm 1$.

Groupe dérivé. Le groupe dérivé de D_n est $\langle r^2 \rangle$. C'est $\langle r \rangle$ si et seulement si n est impair.

III.2. *Représentations linéaires des groupes finis.*

Remarque. Si A est une matrice unitaire, alors $Spec(A) \subset U$.

Proposition. [Serre, 1967] Soit G un groupe fini et ρ une représentation linéaire de G. Alors pour tout $g \in G$, $\rho(g)$ est diagonalisable et ses valeurs propres sont dans U.

Application. [Ulmer, 2005] On définit $\mathrm{Ker}(\chi) = \{g \in G | \chi(g) = \chi(e)\}$. On a $\mathrm{Ker}(\rho) = \mathrm{Ker}(\chi)$.

Proposition. Si χ est le caractère d'une représentation de degré n, on a pour tout $g \in G$, $\chi(g^{-1}) = \overline{\chi(g)}$.

III.3. *Transformée de Fourier discrète.*

Remarque. Lorsque le groupe G est commutatif, on note $\hat{G}$ l'ensemble de ses caractères irréductibles qui sont tous de degré 1.

Proposition. [Peyré, 2004] Soit G un groupe fini de cardinal n. Les éléments de $\hat{G}$ sont les morphismes de G dans le groupe des racines n-ième de l'unité.

Cas du groupe cyclique. Soit $G = 1, g_0, \cdots, g_0^{n-1}$ un groupe cyclique et ω une racine primitive n-ième de l'unité. Par exemple $\omega = \exp(\frac{2i\pi}{n})$. Alors les éléments de G sont les $\chi_j : G \mapsto \mathbb{C}^*$ définis pour $j \in \{0, \cdots, n-1\}$ par : $\chi_j(g_0^k) = (\omega^j)^k$

Conséquence. Pour le choix $\omega = \exp(\frac{2i\pi}{n})$, la table de caractères de $\mathbb{Z}/n\mathbb{Z}$ est une matrice de Vandermonde qui contient des racines n-ièmes de l'unité : $V(1, \omega, \cdots, \omega^{n-1})$

Définition. Définition de la transformée de Fourier discrète.

Formule d'inversion.

Conséquence. La transformée de Fourier discrète est un isomorphisme d'espace vectoriels.

3. 103 : Exemples et applications des notions de sous-groupes distingués et de sous-groupes quotients.

I. Sous-groupes distingués.

Définition. [Ulmer, 2005] On dit que H sous-groupe de G est distingué, lorsque pour tout $h \in H$ et tout $g \in G$, on a : $ghg^{-1} \in H$. On note $H \triangleleft G$.

Définition. On appelle automorphisme intérieur les applications $(\sigma_g)_{g \in G}$, définies par $\sigma_g(h) = ghg^{-1}$. L'ensemble des automorphismes intérieurs est noté $\mathrm{Int}(G)$.

Remarque. $H \triangleleft G$ si et seulement si H est stable par les automorphismes intérieurs.

Exemples.

(1) $\{e\}$ est distingué.

(2) Dans un groupe abélien, tout sous groupe est distingué.

(3) Principe de conjugaison : $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$.

Contre-exemple. [Beck et al., 2004] $GL_2(Z)$ n'est pas distingué dans $GL_2(\mathbb{R})$.

On peut obtenir de nombreux groupes distingués grâce aux morphismes de groupe. **Proposition.**

(1) Soit $f \in \mathrm{Hom}(G, G')$, alors pour tout $H' \triangleleft G'$, on a $f^{-1}(H') \triangleleft G$. En particulier, $\mathrm{Ker}(f) \triangleleft G$

(2) Soit $f \in \mathrm{Hom}(G, G')$, alors pour tout $H \triangleleft G$, on a $f(H) \triangleleft f(G)$. En particulier si f est surjectif : $f(H) \triangleleft G'$.

Exemples.

(1) $SL_n(\mathbb{K})$ est distingué dans $GL_n(\mathbb{K})$ comme noyau du déterminant.

(2) $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ comme noyau de la signature.

Attention. Si $K \triangleleft H$ et $H \triangleleft G$ on a pas nécessairement $K \triangleleft G$.

Définition. Un sous-groupe H de G est dit caractéristique lorsqu'il est stable par les automorphismes de G.

Proposition. Un sous-groupe caractéristique est stable par les automorphismes dont par les automorphismes intérieurs, donc est distingué.

Proposition.

(1) Si K est caractéristique dans H et que H est caractéristique dans G alors K est caractéristique dans G.

(2) Si K est caractéristique dans H et que H est distingué dans G alors K est distingué dans G.

I.1. *Deux sous-groupes distingués important.*

Définition. [Ulmer, 2005] Définition du centre du groupe G, noté $Z(G)$.

Proposition. [Ulmer, 2005] Le centre de G est le noyau de l'application $\sigma : G \to \mathrm{Int}(G)$ définie par $\sigma(g) = \sigma_g$. A ce titre c'est un sous-groupe caractéristique donc distingué de G.

Exemples. [Perrin, 1996]

(1) Le centre de $GL_n(\mathbb{K})$ est l'ensemble des homothéties.

(2) Le centre de $SL_n(\mathbb{K})$ est égal à $Z(GL_n(\mathbb{K})) \cap SL_n(\mathbb{K})$

(3) Pour $n \geq 3$, on a $Z(\mathcal{S}_n) = \{Id\}$

Définition. On appelle groupe dérivé du groupe G le sous-groupe de G engendré par les commutateurs. Il est noté $\mathcal{D}(G)$.

Proposition.

(1) $\mathcal{D}(G) = \{e\}$ est un sous-groupe caractéristique de G.

(2) On a $\mathcal{D}(G) = \{e\}$ si et seulement si G est abélien.

Exemples. [Ulmer, 2005] [Perrin, 1996]

(1) $\mathcal{D}(\mathcal{S}_n) = \mathcal{A}_n$ et $\mathcal{D}(\mathcal{A}_n) = \mathcal{A}_n$ pour $n \geq 2$.

(2) $\mathcal{D}(GL_n(\mathbb{K})) = SL_n(\mathbb{K})$ sauf si $n = 2$ ou $\mathbb{K} = \mathbb{F}_2$.

(3) $\mathcal{D}(SL_n(\mathbb{K})) = SL_n(\mathbb{K})$ sauf si $n = 2$ ou $\mathbb{K} = \mathbb{F}_2$ ou $\mathbb{K} = \mathbb{F}_3$.

II. Groupe quotient, théorèmes d'isomorphismes

II.1. *Classes modulo un sous-groupe.*

Définition. [Ulmer, 2005] Soit $H \lhd G$. On définit la relation d'équivalence sur G par $x\mathcal{R}_H y \Leftrightarrow y^{-1}x \in H$. La classe d'équivalence d'un élément x est notée xH et est appelée classe à gauche. On définit de même les classes à droite comme les classes de $x\mathcal{R}'_H y \Leftrightarrow x^{-1}y \in H$. On note G/H l'ensemble des classes à gauche. On appelle indice de H noté $[G : H]$ le cardinal de G/H.

Remarque. Si le groupe est abélien, les classes à droite et à gauche coïncident.

Théorème de Lagrange. Si G est fini, on a $|G| = |H|[G : H]$.

Application. Si $[G : H] = 2$ alors $H \lhd G$.

Exemple. Dans le groupe diédral D_n, $\langle r\rangle$ est d'ordre 2 donc il est distingué dans D_n.

II.2. *Groupe quotient*

Définition. Si $H \triangleleft G$, G/H est muni d'une structure de groupe via $(gH)(g'H) = (gg'H)$. On appelle alors G/H le groupe quotient de G par H. L'application de projection canonique $\pi : G \to G/H$ est un morphisme surjectif de groupes, de noyau H.

Exemple. $n\mathbb{Z} \triangleleft \mathbb{Z}$ donc $\mathbb{Z}/n\mathbb{Z}$ est un groupe.

Propriété universelle du quotient. Soit G_1 et G_2 deux groupes. Soit $H \triangleleft G_1$ et $\varphi : G_1 \to G_2$ un morphisme de groupes. Alors les propriétés suivantes sont équivalentes :

(1) $H \subset \mathrm{Ker}(\varphi)$

(2) Le morphisme φ se factorise à travers G_1/H. Il existe un unique morphisme de groupes $\overline{\varphi} : G_1/H \to G_2$ tel que $\varphi = \overline{\varphi} \circ \pi$.

De plus $\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi)$ et $\mathrm{Ker}(\overline{\varphi}) = \mathrm{Ker}(\varphi)/H$.

Exemple. Il existe un isomorphisme entre $\mathbb{P}SL_2(\mathbb{R})$ et $\mathbb{P}GL_2^+(\mathbb{R})$.

Corollaire. Théorème d'isomorphisme. On a donc $\mathrm{Im}(\varphi) \cong G_1/\mathrm{Ker}(\varphi)$.

Applications.

(1) On a $\mathbb{K}^* \cong GL_n(\mathbb{K})/SL_n(\mathbb{K})$. On peut par exemple en déduire le cardinal de $SL_n(\mathbb{F}_q)$.

(2) On a en caractéristique différente de 2 : $(\mathbb{F}_q^*)^2 \cong \mathbb{F}_q^*/\{\pm 1\}$. On en déduit qu'il y a $\frac{q-1}{2}$ carrés dans $\mathbb{F}_q^*$.

(3) On a $\mathcal{S}_n/\mathcal{A}_n \cong \{\pm 1\}$

Théorème de Frobenius-Zoltarev [Beck et al., 2004]

Troisième théorème d'isomorphisme. Soient $K \subset H \subset G$ trois groupes. Supposons que H et K soient distingués dans G. Alors on a : $\frac{G/K}{H/K} \cong G/H$.

II.3. *Groupes simples*

Définition. Définition d'un groupe simple.

Remarque. Il est important de connaître les groupes simples. En effet ce plan a montré qu'il est possible d'étudier un groupe en le dévissant par des morphismes dont le noyau est un sous-groupe distingué. Les groupes simples constituent donc les briques élémentaires pour construire des groupes.

Exemple. Un groupe cyclique d'ordre $p \in \mathcal{P}$ est simple.

Contre-exemple. Le groupe de Klein est distingué dans $\mathcal{A}_4$. $SO_{2n}(\mathbb{R})$ n'est pas simple.

Proposition. $\mathcal{A}_5$ est simple pour $n \geq 5$

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

4. **104 : Groupes finis. Exemples et applications.**

I. Généralités.

Définition. Soit G un groupe. G est dit fini lorsque son cardinal, noté $|G|$, vérifie $|G| < +\infty$

Exemples. Le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$, Le groupe diédral D_n, Le groupe symétrique et symétrique alterné, $\mathcal{S}_n$ et $\mathcal{A}_n$, Le groupe linéaire et le groupe spécial linéaire sur un corps fini $GL_n(\mathbb{F}_q)$ et $SL_n(\mathbb{F}_q)$.

Définition. [Ulmer, 2005] Soit $H \triangleleft G$. On définit la relation d'équivalence sur G par $x\mathcal{R}_H y \Leftrightarrow y^{-1}x \in H$. La classe d'équivalence d'un élément x est notée xH et est appelée classe à gauche. On définit de même les classes à droite comme les classes de $x\mathcal{R}'_H y \Leftrightarrow x^{-1}y \in H$. On note G/H l'ensemble des classes à gauche. On appelle indice de H noté $[G : H]$ le cardinal de G/H.

Remarque. Si le groupe est abélien, les classes à droite et à gauche coïncident.

Théorème de Lagrange. Si G est fini, on a $|G| = |H|[G : H]$.

Application. Si $[G : H] = 2$ alors $H \triangleleft G$.

Proposition. Propriété universelle du quotient.

Applications. [Perrin, 1996]

(1) Il y a $\frac{q-1}{2}$ carrés dans $\mathbb{F}_q^2$.

(2) Cardinal de $SL_n(F_q)$

Remarque. Enfin, l'étude des groupes finis peut être faite à travers l'étude des **représentations linéaires** de ce groupe et de sa **table de caractères**.

II. Groupes symétriques et alternés.

Écriture en produit de cycles à supports disjoints. Toute permutation $\sigma \in \sigma_n$ s'écrit comme produit de cycles de longueur supérieure ou égale à 2 dont les supports sont disjoints deux à deux. Cette décomposition est unique à ordre près et à écriture près de chaque cycle.

Exemple. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix} (6)$.

Définition. On appelle type d'une permutation σ, que l'on note $[l_1, l_2, \cdots l_m]$ la liste des cardinaux des cycles de σ.

Proposition. Une permutation σ a pour ordre p.p.c.m.(l_i).

Exemple. La permutation précédente a pour ordre 6.

Principe de conjugaison pour les permutations. Deux permutations sont conjugués dans σ_n si et seulement si elles ont même type. En particulier on a :

$$\omega \begin{pmatrix} i_1 & \cdots & i_l \end{pmatrix} \omega^{-1} = \begin{pmatrix} \omega(i_1) & \cdots & \omega(i_l) \end{pmatrix}.$$

Exemple. Il y a 5 types possibles de permutations dans σ_4 : l'identité $[1,1,1,1]$, les transpositions $[1,1,2]$, les doubles transpositions $[2,2]$, les 3 cycles $[1,3]$ et les 4 cycles $[4]$. L'action de conjugaison donne une partition des 24 élements de σ_4 en cinq orbites de cardinal respectif 1, 6, 3, 8 et 6.

II.1. *Groupe symétrique alterné.*

Proposition. Définition de la signature d'une permutation.

Exemple. La signature d'une transposition vaut -1.

Proposition. La signature est l'unique morphisme de groupes non trivial de σ_n sur $\{\pm 1\}$. Une permutation est paire lorsqu'elle se décompose en un nombre pair de transpositions et impaire sinon.

Définition. Le noyau du morphisme ε est appelé groupe alterné et est noté $\mathcal{A}_n$. C'est un sous-groupe distingué de σ_n de cardinal $\frac{n!}{2}$.

Proposition. [Peyré, 2004] Pour $\mathcal{S}_4$ on a :

	1	(1,2)	(1,2,3)	(1,2,3,4)	(1,2)(3,4)
Id	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_2	2	0	-1	0	2
χ_C	3	-1	0	1	-1
χ_3'	3	1	0	-1	-1

III. Actions de groupes

Proposition. A toute action d'un groupe sur un ensemble X il correspond un unique morphisme $\varphi : G \to \mathcal{S}(X)$ défini par $g \to \mathcal{S}_g$ avec $\mathcal{S}_g(x) = g \cdot x$. On appelle ce morphisme le morphisme structurel de l'action. L'action est dites fidèle lorsque ce morphisme est injectif.

En faisant opérer un groupe fini sur lui même par translation on obtient. **Conséquence.** Théorème de Cayley. Tout groupe fini G d'ordre n est isomorphe à un sous-groupe transitif de $\mathcal{S}_n$.

Proposition.

(1) La relation être dans la même orbite est une relation d'équivalence sur X.
(2) Le cardinal du stabilisateur est constant le long d'une orbite : $\mathrm{Stab}_G(g\cdot x) = g\mathrm{Stab}_G(x)g^{-1}$.
(3) $|G| = |\mathcal{O}_x||\mathrm{Stab}_G(x)|$.

Formule des classes. Soit $(x_1, \cdots, x_r)$ un système de représentant d'orbites alors on a : $|X| = \sum_{i=1}^{r} \frac{|G|}{\mathrm{Stab}_G(x_i)}$

Application. [Caldero and Germoni, 2013] Calcul du cardinal des matrices diagonalisables de $\mathrm{GL}_n(\mathbb{F}_q)$.

IV. Groupe abélien finis.

IV.1. *Groupes cycliques*

Proposition. Un groupe monogène est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$. Dans le second cas on dit qu'il est cyclique.

Exemples.

(1) Le groupe des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

(2) Le groupe des inversibles d'un corps fini est cyclique.

Proposition. [Perrin, 1996] On a l'équivalence entre :

(1) s est premier avec n

(2) s est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

(3) $s \in (\mathbb{Z}/n\mathbb{Z})^*$ groupe des éléments inversibles pour la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Application. [Perrin, 1996] On a l'isomorphisme $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \approx (\mathbb{Z}/n\mathbb{Z})^*$

Proposition. Dans un groupe cyclique, il existe exactement un sous groupe d'ordre d pour chaque diviseur d de l'ordre du groupe.

Application. [Beck et al., 2004] Théorème de Frobenius Zoltarev.

Caractères. [Peyré, 2004] Caractères du groupe $\mathbb{Z}/n\mathbb{Z}$. Isomorphisme non canonique entre G et $\hat{G}$.

Application. Définition de la transformée de Fourier discrète.

Théorème de structure des groupes abéliens finis. [Peyré, 2004] (admis)

Application. Pour un groupe abélien fini, on a $G \cong \hat{G}$

V. Quelques groupes finis en géométrie.

Définition. [Audin, 2012] On appelle isométrie affine toute application affine qui préserve la distance. On note $Isom(\mathcal{E})$ le groupe des isométries affines.

Exemples.

(1) Les translations sont des isométries.

(2) Les symétries orthogonales sont des isométries.

Définition. On définit le sous-groupe des déplacements, noté $Isom^+(\mathcal{E})$ comme le noyau du déterminant.

Proposition.

(1) Le groupe d'isométries du tétraèdre est $\mathcal{S}_4$. Le groupe des déplacements du tétraèdre est $\mathcal{A}_4$.

(2) Le groupe des déplacements du cube est $\mathcal{S}_4$. Le groupe des isométries du cube est $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Application. [Serre, 1967] Détermination d'un caractère irréductible de degré 3 de $\mathcal{S}_4$.

V.1. *Groupe diédral*

Remarque. [Ulmer, 2005] Les éléments de U_n sont les sommets du polygône régulier à n côtés P_n.

Définition. Pour $n \geq 3$, le groupe diédral D_n est le groupe des isométries du plan affine qui laissent invariant P_n.

Proposition. Le groupe diédral est d'ordre $2n$ et il est engendré par la symétrie axiale $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et la rotation d'angle $\theta = \frac{2\pi}{n}$, $r = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$.

Proposition. Le groupe $\langle r \rangle$ est isomorphe à U_n et il est distingué dans D_n. On a les relations $r^n = e$, $s^2 = e$, et $srs = r^{-1}$

Groupe dérivé. Le groupe dérivé de D_n est $\langle r^2 \rangle$. C'est $\langle r \rangle$ si et seulement si n est impair.

Définition. On appelle noyau du caractère l'ensemble : $\mathrm{Ker}(\chi) = \{g \in G | \chi(g) = \chi(e)\}$.

Proposition. Soit G un groupe fini ayant m classes de conjugaison et $\chi_1, \cdots, \chi_m$ les caractères irréductibles de G. Tout sous-groupe distingué H de G est de la forme $\bigcap_{j \in J} \mathrm{Ker}(\chi_j)$ avec $J \subset \{1, \cdots, m\}$.

Corollaire. Un groupe fini G est simple si et seulement si tout caractère irréductible non trivial de G a un noyau trivial.

Application. Application au groupe diédral D_6.

5. **105 : Groupe des permutations sur un ensemble fini. Applications.**

I. Groupes symétriques et alternés.

I.1. *Définitions et premières propriétés.*

Définition. [Ulmer, 2005] Soit X en ensemble fini. On note $\mathcal{S}(X)$ l'ensemble des bijections de X. $(\mathcal{S}(X), \circ)$ est appelé groupe symétrique de X. Pour $n \in \mathbb{N}^*$, on note $\mathcal{S}_n = \mathcal{S}(\{1, \cdots, n\})$. On a $|\mathcal{S}_n| = n!$

Proposition. Le groupe $\mathcal{S}(X)$ opère naturellement à gauche sur X par la relation $\mathcal{S} \cdot x = \mathcal{S}(x)$.

Proposition. Réciproquement, à toute action d'un groupe sur un ensemble X il correspond un unique morphisme $\varphi : G \to \mathcal{S}(X)$ défini par $g \to \mathcal{S}_g$ avec $\mathcal{S}_g(x) = g \cdot x$. On appelle ce morphisme le morphisme structurel de l'action. L'action est dites fidèle lorsque ce morphisme est injectif.

En faisant opérer le groupe sur lui même par translation on obtient. **Conséquence.** Théorème de Cayley. Tout groupe fini G d'ordre n est isomorphe à un sous-groupe transitif de $\mathcal{S}_n$.

Notation pour les permutations. Pour décrire $\sigma \in \mathcal{S}_n$, on note $\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$.

Exemple. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ et $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. On constate que $\rho\sigma \neq \sigma\rho$. Le groupe σ_3 n'est pas abélien.

I.2. *Orbites, cycles*

Définition.

(1) Définition des points fixes d'une permutation.
(2) Définition du support d'une permutation.

Proposition. Si deux permutations ont des supports disjoints, alors elles commutent.

Définition. Définition d'un cycle de longueur l dans une permutation. Un cycle de longueur 2 est appelé une transposition.

Exemple. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$. Il y a deux cycles (3) et $\begin{pmatrix} 1 & 4 & 2 & 5 \end{pmatrix}$ qu'on peut aussi écrire $\begin{pmatrix} 2 & 5 & 1 & 4 \end{pmatrix}$.

Écriture en produit de cycles à supports disjoints. Toute permutation $\sigma \in \sigma_n$ s'écrit comme produit de cycles de longueur supérieure ou égale à 2 dont les supports sont disjoints deux à deux. Cette décomposition est unique à ordre près et à écriture près de chaque cycle.

Exemple. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix} (6)$.

Définition. On appelle type d'une permutation σ, que l'on note $[l_1, l_2, \cdots l_m]$ la liste des cardinaux des cycles de σ.

Proposition. Une permutation σ a pour ordre $\mathrm{ppcm} l_i$.

Exemple. La permutation précédente a pour ordre 6.

Principe de conjugaison pour les permutations. Deux permutations sont conjugués dans σ_n si et seulement si elles ont même type. En particulier on a :

$$\omega \begin{pmatrix} i_1 & \cdots & i_l \end{pmatrix} \omega^{-1} = \begin{pmatrix} \omega(i_1) & \cdots & \omega(i_l) \end{pmatrix}.$$

Exemple. Il y a 5 types possibles de permutations dans σ_4 : l'identité $[1,1,1,1]$, les transpositions $[1,1,2]$, les doubles transpositions $[2,2]$, les 3 cycles $[1,3]$ et les 4 cycles $[4]$. L'action de conjugaison donne une partition des 24 élements de σ_4 en cinq orbites de cardinal respectif 1, 6, 3, 8 et 6.

Exemple. Exemple d'obtention d'une relation de conjugaison entre deux permutations du même type dans σ_6.

Proposition. Tout cycle d'ordre l peut s'écrire comme un produit de $l-1$ transpositions.

I.3. *Groupes alternés.*

Proposition. Définition de la signature d'une permutation.

Exemple. La signature d'une transposition vaut -1.

Proposition. La signature est l'unique morphisme de groupes non trivial de σ_n sur $\{\pm 1\}$. Une permutation est paire lorsqu'elle se décompose en un nombre pair de transpositions et impaire sinon.

Théorème de Frobenius Zoltarev. [Beck et al., 2004]

Définition. Le noyau du morphisme ε est appelé groupe alterné et est noté $\mathcal{A}_n$. C'est un sous-groupe distingué de σ_n de cardinal $\frac{n!}{2}$.

Exemple. Énumération des éléments de $\mathcal{A}_4$.

II. Générateurs et structures

Proposition.

(1) σ_n est engendré par les transpositions.

(2) $\mathcal{A}_n$ est engendré par les doubles transposition, et par les 3 cycles de la forme $\begin{pmatrix} 1 & i & j \end{pmatrix}$

Exemple. $\sigma = \begin{pmatrix} 3 & 1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix} \begin{pmatrix} 3 & 1 \end{pmatrix}$.

Remarque. On peut trouver d'autres systèmes de générateurs...

Théorème. $\mathcal{A}_n$ est simple pour $n \geq 5$.

Cas de $\mathcal{A}_4$ Le groupe de Klein est distingué dans $\mathcal{A}_4$.

Groupes dérivés. [Perrin, 1996]

(1) Pour $n \geq 5$, on a $D(\mathcal{A}_n) = \mathcal{A}_n$
(2) Pour $n \geq 2$, on a $D(\sigma_n) = \mathcal{A}_n$

Exemple. $D(\mathcal{A}_4)$ est isomorphe au groupe de Klein.

Proposition. Pour $n \geq 5$, les sous groupes distingués de σ_n sont $\{Id\}$, $\mathcal{A}_n$, et σ_n.

Table de caractère de σ_4

III. Applications.

III.1. *Formes alternées, déterminant.*

Proposition. [Gourdon, 1994b] L'ensemble des formes linéaires n alternées sur un $\mathbb{K}$ ev de dimension n est un espace vectoriel de dimension 1.

Proposition. Formule du déterminant.

Application. Déterminant par blocs d'une matrice triangulaire supérieure par blocs.

III.2. *Polynômes symétriques.*

Définition. [Gourdon, 1994b] Un polynôme $P \in A[X_1, \cdots, X_n]$ est dit symétrique lorsque pour toute permutation $\sigma \in \sigma_n$, on a :

$$P(X_{\sigma(1)}, \cdots, X_{\sigma(n)}) = P(X_1, \cdots, X_n).$$

Exemple. $P(X, Y, Z) = XY + XZ + YZ$ est symétrique.

Définition. Définition des polynômes symétriques élémentaires.

Théorème. Tout polynôme symétrique P peut s'écrire comme un unique polynôme Φ évalué en les polynômes élémentaires.

III.3. *Matrices de permutations*

[Beck et al., 2004]

III.4. *Groupe des isométries d'un polyèdre régulier.*

Proposition. [Caldero and Germoni, 2013]

(1) Le groupe des isométries d'un triangle est isomorphe à σ_3
(2) Le groupe des isométries d'un tétraèdre est isomorphe à σ_4 et celui des isométries positives à $\mathcal{A}_4$.
(3) Le groupe des isométries du cube est isomorphe à $\sigma_4 \times \mathbb{Z}/2\mathbb{Z}$, les positives à σ_4.

Table de caractètre de $\mathcal{S}_4$. [Peyré, 2004] **Exemple 4.** Pour $\mathcal{S}_4$ on a :

	1	(1,2)	(1,2,3)	(1,2,3,4)	(1,2)(3,4)
Id	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_2	2	0	-1	0	2
χ_C	3	-1	0	1	-1
χ_3'	3	1	0	-1	-1

6. 106 : Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.

On travaille sur E un $\mathbb{K}$-espace vectoriel de dimension finie avec $\mathbb{K}$ un corps commutatif.

I. Structure et propriétés de $GL(E)$.

Définition. [Perrin, 1996] Définition de $GL(E)$.

Proposition. La donnée d'une base de E définit un isomorphismes (non canonique) de $GL(E)$ sur $GL_n(\mathbb{K})$.

Remarque. Cet isomorphisme permet l'utilisation des outis de calcul matriciel pour étudier le groupe linéaire.

Proposition. Le déterminant est un morphisme de groupe surjectif de $GL(E)$ sur $\mathbb{K}^*$. Son noyau est appelé groupe spécial linéaire et est noté $SL(E)$. On a donc $SL(E) \triangleleft GL(E)$.

Application. Par le théorème d'isomorphisme, on peut déduire le cardinal de $SL_n(\mathbb{F}_q)$ de celui de $GL_n(\mathbb{F}_q)$

I.1. *Générateurs*

Définition et caractérisation des dilatations

Définition et caractérisation des transvections

Proposition.
— $SL_n(\mathbb{K})$ est engendré par les transvections.
— $GL_n(\mathbb{K})$ est engendré par les transvections et les dilatations.

Application. Connexité par arcs de $GL_n^-(\mathbb{R})$ et $GL_n^+(\mathbb{R})$.

Groupe dérivé. Groupes dérivés de $GL(E)$ et de $SL(E)$.

Application. [Beck et al., 2004] Théorème de Frobenius-Zoltarev.

I.2. *Un peu de projectif*

Centres. Le centre de $GL(E)$ est l'ensemble des homothéties. Le centre de $SL(E)$ est constitué des homothéties de rapport une racine n-ième de l'unité.

Définitions. Groupe projectif linéaire et groupe projectif spécial linéaire.

Application. Cardinal de $\mathbb{P}GL_n(\mathbb{F}_q)$ et $\mathbb{P}SL_n(\mathbb{F}_q)$.

Proposition. $\mathbb{P}GL_2(\mathbb{C})$ est l'ensemble des homographies. Les homographies conservent le birapport, c'est à dire laissent stables les cercles/droites de $\mathbb{P}^1(\mathbb{C})$.

Proposition. Action transitive de $\mathbb{P}SL_2(\mathbb{R})$ sur le demi-plan de Poincarré et sur les droites hyperboliques.

Remarque. [Perrin, 1996] On a un isomorphisme $\mathbb{P}SL_2(\mathbb{C}) \cong \mathbb{P}GL_2(\mathbb{C})$ mais on a seulement $\mathbb{P}SL_2(\mathbb{R}) \cong \mathbb{P}GL_2^+(\mathbb{R})$.

II. Sous-groupes de $GL(E)$

II.1. *Sous-groupes finis et sous-groupes remarquables*

Définition. [Beck et al., 2004] Définition des matrices de transposition et des matrices de permutation.

Proposition. Soit $\varphi : \mathcal{S}_n \to GL_n(\mathbb{K})$ définie par $\varphi(\sigma) = P_\sigma$. Alors φ est un morphisme de groupes injectif. Le groupe des matrices de permutations est donc un sous-groupe de $GL_n(\mathbb{K})$, isomorphe à $\mathbb{S}_n$.

Sous-groupe abélien de $GL_n(\mathbb{K})$. [Beck et al., 2004] Supposons $\mathbb{K}$ algébriquement clos. Soit $G < GL_m(\mathbb{K})$ un sous-groupe tel que $|G|$ soit premier avec $car(\mathbb{K})$. Alors G est codiagonalisable.

Contre-exemples.

(1) Contre-exemple lorsque le corps n'est pas algébriquement clos.
(2) Contre-exemple lorsque le cardinal du groupe n'est pas premier avec la caractéristique du corps.

Théorème de Burnside. [ORAUX X-ENS ALGB 2]. Un sous-groupe de $GL_n(\mathbb{C})$ est fini si et seulement si il est d'exposant fini.

Passons à quelques sous-groupes remarquables.

Définitions.

(1) Définition du groupe orthogonal.
(2) Définition du groupe unitaire.
(3) Définition du groupe spécial orthogonal.

Proposition. Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $GL_n(\mathbb{K})$ est un ouvert dense de $M_n(\mathbb{K})$.

Théorème de Cartan/Von Neumann. [GONNORD-TOSEL Calcul différentiel] [**?**] Tout sous-groupe fermé de $GL_n(\mathbb{R})$ est une sous-variété de $GL_n(\mathbb{R})$ donc une sous-variété de $M_n(\mathbb{R})$.

Application. $O_n(\mathbb{R})$, $SO(n(\mathbb{R})$ et $SL_n(\mathbb{R})$ sont des sous-variétés. Donner aussi leur plan tangents en I_n.

II.2. *Groupe orthogonal.*

Théorème. Théorème de réduction des endomorphismes orthogonaux.

Application. $SO_n(\mathbb{R})$ est connexe par arcs.

Définition. Définition d'une symétrie orthogonale par rapport à un sous-espace. Cas particulier des réflexions et des renversements.

Théorème.

(1) Tout élement de O_n peut s'écrire comme produit de n réflexions orthogonales.

(2) Tout élément de SO_n pour $n \geq 3$ peut s'écrire comme produit de n renversements.

Application. Simplicité de $SO_3(\mathbb{R})$.

Remarque. En dimension paire, $\{\pm I_n\}$ est distingué dans $SO_n(\mathbb{R})$.

Théorème. $O_n(\mathbb{R})$ est un groupe compact.

Application. [Mneimné and Testard, 1986] On peut étendre la décomposition polaire à $M_n(\mathbb{R})$ mais la décomposition polaire n'est plus injective.

7. 107 : Représentations et caractères d'un groupe fini sur un $\mathbb{C}$ espace vectoriel.

I. Représentations.

I.1. *Représentations*

Définition. [Serre, 1967] On appelle représentation linéaire du groupe G tout morphisme $\rho : G \to GL(V)$. La dimension de l'espace vectoriel V est appelé degré de la représentation.

Exemples.

(1) La représentation triviale de degré 1 donnée par $\forall g \mathbb{G}, \rho(g) = Id$.
(2) Si $|G| = n$. Soit $(e_t)_{t \in G}$ une base de $\mathbb{C}^n$ indexée par G. Alors on définit la représentation régulière définie par : $\rho(g)(e_t) = e_{gt}$.
(3) Plus généralement, si on dispose d'une action de groupe de G sur un ensemble fini X et soit $(e_x)_{x \in X}$ une base d'un espace vectoriel de dimension $|X|$ alors on appelle représentation par permutation l'application définie par $\rho(g)(e_x) = e_{g.x}$.

Sous-répésentations. Soit V un représentation de G et W un sous-espace vectoriel de V stable par la famille $(\rho(g))_{g \in G}$. $\rho^W : G \to GL(W)$ est alors une représentation. On dit que W est une sous représentation de V.

Exemple. Dans le cas de la représentation régulière $\rho : G \to GL_(V)$, on pose $W = Vect(x)$ avec $x = \sum_{s \in G} e_s$. Alors W est une sous représentation.

I.2. *Théorème de Maschke.*

Théorème du supplémentaire stable. Soit $\rho : G \to GL_(V)$ une représentation linéaire et W une sous-représentation. Alors il existe W_0 sous-représentation telle que $V = W \oplus W_0$.

Définition. On dit qu'une représentation $\rho : G \to GL_(V)$ avec $V \neq \{0\}$ est irréductible lorsqu'il n'existe pas de sous-représentations triviales (V ou $\{0\}$).

Exemple. Toute représentation de degré 1 est irréductible.

Théorème de Maschke. Toute représentation est somme directe de représentations irréductibles.

II. Introduction des caractères.

II.1. *Caractère d'un groupe fini*

Existence du produit d'espaces vectoriels. Soient V_1 et V_2 deux espaces vectoriels. On appelle produit tensoriel de V_1 et V_2 un espace vectoriel W muni d'une application $(x_1, x_2) \mapsto x_1.x_2$ linéaire en chacune des variables et vérifiant la propriété : Si (e_i^1) est une base de V_1 et (e_j^2) est une base de V_2

alors la famille $(e_i^1 e_j^2)_{i,j}$ est une base de W. Un tel espace existe et est unique à isomorphisme près. On note $W = V_1 \otimes V_2$.

Définition. Étant donnés deux représentations $\rho_1 : G \to GL_(V_1)$ et $\rho_2 : G \to GL_(V_2)$. On définit le produit tensoriel des deux représentations par $\rho(s)(x_1.x_2) = \rho_1(s)(x_1)\rho_2(s)(x_2)$. On définit ainsi une représentation de G dans $V_1 \otimes V_2$.

Définition. Soit $\rho : G \to GL_(V)$ une représentation linéaire d'un groupe fini. On appelle caractère de la représentation, que l'on note $\chi_\rho : G \to \mathbb{C}$ ou χ l'application définie pour tout $g \in G$ par $\chi(g) = Tr(\rho(g))$.

Exemple. Pour la représentaion régulière on a $\chi(g) = 0$

Propriétés. Si n désigne le degré de la représentation :

(1) $\chi(e) = n$

(2) $\chi(s^{-1}) = \overline{\chi(s)}$

(3) Le caractère est constant le long des classes de conjugaison : $\chi(tst^{-1}) = \chi(s)$. On dit que le caractère est une fonction centrale.

(4) Le caractère de la somme directe est la somme des caractères.

(5) Le caractère de la représentation produit tensoriel est le produit des caractères.

II.2. *Lemme de Schur et applications*

Lemme de Schur. Soient $\rho_1 : G \to GL_(V_1)$ et $\rho_2 : G \to GL_(V_2)$ deux représentations irréductibles de G, et soit $f : V_1 \to V_2$ une application linéaire telle que pour tout $g \in G$, $\rho_2(g) \circ f = f \circ \rho_1(g)$, alors :

(1) Si ρ_1 et ρ_2 ne sont pas isomorphes, alors $f = 0$

(2) Si $V_1 = V_2$ et $\rho_1 = \rho_2$, f est une homothétie.

Conséquence. Soient φ et ψ deux fonctions de G à valeurs dans $\mathbb{C}$, on pose $\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum\limits_{g \in G} \varphi(g)\overline{\psi(g)}$. On a ainsi définit un produit scalaire hermitien qui vérifie les propriétés suivantes :

(1) Si χ est le caractère d'une représentation irréductible, alors $\langle \chi, \chi \rangle = 1$.

(2) Si χ et χ' sont deux caractères irréductibles non isomorphes, alors $\langle \chi, \chi' \rangle = 0$.

Corollaire. Soit $\rho : G \to V$ une représentation de caractère χ. Si $V = W_1 \oplus \cdots W_k$, est une décomposition en somme directe de représentations irréductibles, alors pour tout caractère irréductible χ' d'une représentation W, le nombre des W_i isomorphes à W est égal à $\langle \chi, \chi' \rangle$.

Corollaire. Deux représentations ayant le même caractère sont isomorphes.

Proposition. Toute représentation est isomorphe à une somme directe $V = \oplus m_i W_i$ où $m_i = \langle \chi, \chi_i \rangle$. Le caractère s'écrit $\chi = \sum\limits_{i=1}^{k} m_i \chi_i$ où les χ_i sont des caractères irréductibles. En particulier $\langle \chi, \chi \rangle = \sum\limits_{i=1}^{k} m_i^2$.

Corollaire. $\langle \chi, \chi \rangle$ est un entier strictement positif qui vaut 1 si et seulement si la représentation est irréductible.

Remarque. Les caractères irréductibles forment une base orthonormée de l'espace vectoriel des fonctions centrales sur G.

Théorème. Le nombre de représentations irréductibles de G est égal au nombre des classes de conjugaison de G. Soit $s \in G$, on note $c(s)$ le cardinal de la classe de conjugaison de s. On a :

(1) $\frac{1}{|G|} \sum_{i=1}^{k} \chi_i(s)\overline{\chi_i(s)} = c(s)$

(2) $\frac{1}{|G|} \sum_{i=1}^{k} \chi_i(s)\overline{\chi_i(g)} = 0$ si g n'est pas conjugué à s.

III. TABLE DE CARACTÈRES ET UTILISATIONS

III.1. *Premiers exemples.*

Définition. Soit G un groupe fini et c le nombre de classes de conjugaison de G. La table de caractère de G est le tableau $c \times c$ dont les coefficients sont les valeurs des caractères irréductibles sur les classes de conjugaison de G. En particulier les lignes du tableau forment une famille orthogonale.

Exemple 1. Pour le groupe $\mathbb{Z}/2\mathbb{Z}$, on a :

	1	-1
1	1	1
χ	1	-1

Pour le groupe $\mathbb{Z}/3\mathbb{Z}$, on a en notant $w = \exp(\frac{2i\pi}{3})$:

	0	1	2
χ_0	1	1	1
χ_1	1	w	w^2
χ_2	1	w^2	w

Exemple 2. Pour $\mathcal{S}_3$ on a :

	1	(1,2)	(1,2,3)
Id	1	1	1
χ_ε	1	-1	1
χ	2	0	-1

Exemple 4. Pour $\mathcal{S}_4$ on a :

	1	(1,2)	(1,2,3)	(1,2,3,4)	(1,2)(3,4)
Id	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_2	2	0	-1	0	2
χ_C	3	-1	0	1	-1
χ_3'	3	1	0	-1	-1

III.2. *Caractères et sous-groupes distingués.*

Lemme. [Ulmer, 2005] Soit G un groupe fini et $\rho : G \to GL(V)$ une représentation de caractère χ. On a :

(1) $|\chi(g)| \leq \chi(e)$

(2) $\chi(g) = \chi(e)$ si et seulement si $g \in \mathrm{Ker}(\rho)$.

Définition. On appelle noyau du caractère l'ensemble : $\mathrm{Ker}(\chi) = \{g \in G | \chi(g) = \chi(e)\}$.

Proposition. Soit G un groupe fini ayant m classes de conjugaison et $\chi_1, \cdots, \chi_m$ les caractères irréductibles de G. Tout sous-groupe distingué H de G est de la forme $\bigcap_{j \in J} \mathrm{Ker}(\chi_j)$ avec $J \subset \{1, \cdots, m\}$.

Corollaire. Un groupe fini G est simple si et seulement si tout caractère irréductible non trivial de G a un noyau trivial.

Application. Application au groupe diédral D_6.

8. 108 : Exemples de parties génératrices d'un groupe. Applications.

Principales utlités des parties génératrices d'un groupe.

(1) Informations sur la structure du groupe
(2) Étude des morphismes et des actions de groupes
(3) Étude des propriétés du groupe

I. Partie génératrice d'un groupe.

Définition. [Ulmer, 2005] Soit $X \subset G$ un sous-ensemble d'un groupe. Il existe un plus petit sous-groupe de G contenant X, noté $\langle X \rangle$, appelé sous-groupe engendré par X.

Définition. Un groupe est dit de type fini s'il contient une partie génératrice finie. Un groupe est dit monogène lorsqu'il existe $g \in G$ tel que $G = \langle g \rangle$.

Exemples.
(1) Dans $\mathbb{Z}/4\mathbb{Z}$, on a $\langle 1 \rangle = \mathbb{Z}/4\mathbb{Z}$ et $\langle 2 \rangle = \{0, 2\}$.
(2) $(\mathbb{Q}, +)$ est engendré par $\{\frac{1}{p}, p \in \mathcal{P}\}$.

Définition. Définition du groupe dérivé comme groupe engendré par les commutateurs.

I.1. *Groupes cycliques*

Proposition. Un groupe monogène est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$. Dans le second cas on dit qu'il est cyclique.

Proposition. [Perrin, 1996] On a l'équivalence entre :
(1) s est premier avec n
(2) s est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$
(3) $s \in (\mathbb{Z}/n\mathbb{Z})^*$ groupe des éléments inversibles pour la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$

Application. [Perrin, 1996] On a l'isomorphisme $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \approx (\mathbb{Z}/n\mathbb{Z})^*$

Proposition. Dans un groupe cyclique, il existe exactement un sous groupe d'ordre d pour chaque diviseur d de l'ordre du groupe.

Théorème chinois.

II. Groupes symétriques et alternés

Définition. [Ulmer, 2005] Définition de σ_n et $\mathcal{A}_n$.

Proposition. Décomposition d'une permutation en produit de cycles à supports disjoints.

Exemple. Un exemple.

Proposition.

(1) Les transpositions engendrent σ_n

(2) Les 3 cycles engendrent $\mathcal{A}_n$

(3) Les doubles transposition engendrent $\mathcal{A}_n$

Application. [Ulmer, 2005] [Perrin, 1996] Démonstration de la simplicité de $\mathcal{A}_\backslash$

III. Groupes diédraux.

Définition. [Ulmer, 2005] Le groupe diédral D_n est le sous-groupe des isométries du plan affine qui laissent le polygône régulier à n côtés centré en 0 invariant.

Proposition. Le groupe diédral D_n est d'ordre $2n$ et il est engendré par la rotation d'angle $\frac{2\pi}{n}$ et par la symétrie d'axe (Ox).

Application. Détermination des classes de conjugaison de D_n et du centre de D_n.

IV. Groupe linéaire

IV.1. *Groupe linéaire et groupe spécial linéaire*

Définition. [Perrin, 1996] Définition du groupe spécial linéaire.

Caractérisation des dilatations

Caractérisation des transvections

Théorème. Les transvections engendrent le groupe spécial linéaire, les transvections et les dilations engendrent le groupe linéaire.

Application. GL_n^- est connexe par arcs.

Application. Calcul du groupe dérivé du groupe linéaire et du groupe spécial linéaire.

Application. [Beck et al., 2004] Théorème de Frobenius Zoltarev.

IV.2. *Groupe orthogonal euclidien*

Théorème. Le groupe orthogonal est engendré par les réflexions et le groupe spécial orthogonal par les renversements.

Application. [Caldero and Germoni, 2013] $\mathrm{SO}_3(\mathbb{R})$ est un groupe simple.

IV.3. *Droite projective.*

Définition. [Caldero and Germoni, 2013] [Audin, 2012] Définition de la droite projective $\mathbb{P}^1(\mathbb{C})$.

Définition. Définition du groupe des homographies $\mathbb{P}GL_2(\mathbb{C})$.

Définition. Définition de $\mathbb{P}GL_2(\mathbb{R})$ et $\mathbb{P}SL_2(\mathbb{R})$

Proposition. $\mathbb{P}SL_2(\mathbb{R})$ est engendré par $z \mapsto \frac{-1}{z}$ et $z \mapsto az + b$ avec $a > 0$ et $b \in \mathbb{R}$.

Application. L'action de $\mathbb{P}SL_2(\mathbb{R})$ sur le demi plan de Poincarré est transitive et l'action de $\mathbb{P}SL_2(\mathbb{R})$ sur l'ensemble des droites hyperboliques est transitive.

Définition. Définition du birapport. Formule du birapport.

Proposition. Les homographies conservent le birapport. Condition de cocyclicité et d'alignement en terme de birapport.

Théorème. On appelle groupe circulaire le groupe engendré par les homographies et la conjugaison complexe. C'est exactement l'ensemble des applications qui conservent les droites et les cercles de $\mathbb{P}^1(\mathbb{C})$.

9. **109 : Représentations des groupes de petit cardinal.**

Essentiellement comme la leçon : Représentations et caractères d'un groupe fini sur un $\mathbb{C}$ espace vectoriel.

10. 110 : Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications.

I. Caractères dans le cas général.

Définition. [Serre, 1967] Soit $\rho : G \to GL_(V)$ une représentation linéaire d'un groupe fini. On appelle caractère de la représentation, que l'on note $\chi_\rho : G \to \mathbb{C}$ ou χ l'application définie pour tout $g \in G$ par $\chi(g) = Tr(\rho(g))$.

Exemple. Pour la représentaion régulière et $g \neq e$ on a $\chi(g) = 0$.

Propriétés. Si n désigne le degré de la représentation :

(1) $\chi(e) = n$

(2) $\chi(s^{-1}) = \overline{\chi(s)}$

(3) Le caractère est constant le long des classes de conjugaison : $\chi(tst^{-1}) = \chi(s)$. On dit que le caractère est une **fonction centrale**.

(4) Le caractère de la somme directe est la somme des caractères.

Lemme de Schur. Soient $\rho_1 : G \to GL(V_1)$ et $\rho_2 : G \to GL(V_2)$ deux représentations irréductibles de G, et soit $f : V_1 \to V_2$ une application linéaire telle que pour tout $g \in G$, $\rho_2(g) \circ f = f \circ \rho_1(g)$, alors :

(1) Si ρ_1 et ρ_2 ne sont pas isomorphes, alors $f = 0$

(2) Si $V_1 = V_2$ et $\rho_1 = \rho_2$, f est une homothétie.

Conséquence. Soient φ et ψ deux fonctions de G à valeurs dans $\mathbb{C}$, on pose $\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\psi(g)}$. On a ainsi définit un **produit scalaire hermitien** qui vérifie les propriétés suivantes :

(1) Si χ est le caractère d'une représentation irréductible, alors $\langle \chi, \chi \rangle = 1$.

(2) Si χ et χ' sont deux caractères irréductibles non isomorphes, alors $\langle \chi, \chi' \rangle = 0$.

Corollaire. Soit $\rho : G \to V$ une représentation de caractère χ. Si $V = W_1 \oplus \cdots W_k$, est une décomposition en somme directe de représentations irréductibles, alors pour tout caractère irréductible χ' d'une représentation W, le nombre des W_i isomorphes à W est égal à $\langle \chi, \chi' \rangle$.

Corollaire. Deux représentations ayant le même caractère sont isomorphes.

Proposition. Toute représentation est isomorphe à une somme directe $V = \oplus m_i W_i$ où $m_i = \langle \chi, \chi_i \rangle$. Le caractère s'écrit $\chi = \sum_{i=1}^{k} m_i \chi_i$ où les χ_i sont des caractères irréductibles. En particulier $\langle \chi, \chi \rangle = \sum_{i=1}^{k} m_i^2$.

Corollaire. $\langle \chi, \chi \rangle$ est un entier strictement positif qui vaut 1 si et seulement si la représentation est irréductible.

Remarque. Les caractères irréductibles forment une base orthonormée de l'espace vectoriel des fonctions centrales sur G.

Théorème. Le nombre de représentations irréductibles de G est égal au nombre des classes de conjugaison de G. Soit $s \in G$, on note $c(s)$ le cardinal de la classe de conjugaison de s. On a :

(1) $\frac{1}{|G|}\sum_{i=1}^{k} \chi_i(s)\overline{\chi_i(s)} = c(s)$

(2) $\frac{1}{|G|}\sum_{i=1}^{k} \chi_i(s)\overline{\chi_i(g)} = 0$ si g n'est pas conjugué à s.

Conséquence importante. Pour la suite de la leçon, on travaillera sur des groupes abéliens, on aura donc $|G|$ caractères irréductibles de degré 1.

Définition. Soit G un groupe fini et c le nombre de classes de conjugaison de G. La table de caractère de G est le tableau $c \times c$ dont les coefficients sont les valeurs des caractères irréductibles sur les classes de conjugaison de G. En particulier les colonnes du tableau forment une famille orthogonale.

Exemple. Pour $\mathcal{S}_4$ on a :

	1	(1,2)	(1,2,3)	(1,2,3,4)	(1,2)(3,4)
Id	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_2	2	0	-1	0	2
χ_C	3	-1	0	1	-1
χ_3'	3	1	0	-1	-1

II. Transformée de Fourier discrète.

II.1. *Caractères des groupes abéliens fini.*

Proposition. [Peyré, 2004] On note $\hat{G}$, appelé dual de G, l'ensemble des caractères de dimension 1 de G. Si $G = \{1, g, g^2, \cdots, g^{n-1}\}$ est un groupe cyclique d'ordre n, et que $\omega = \exp(\frac{2i\pi}{n})$, alors les éléments de $\hat{G}$ sont de la forme :

$$\chi_j : h = g^k \mapsto (\omega^j)^k,$$

pour $j \in [\![0, n-1]\!]$. En particulier $G \cong \hat{G}$.

Remarque. Cet isomorphisme est non canonique, il dépend de la racine primitive ω choisie.

Structure des groupes abéliens finis. [Peyré, 2004] Soit G un groupe abélien fini. Il existe des entiers strictements positifs $n_1|n_2|\cdots|n_r$ tels que on ait l'isomorphisme :

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_r\mathbb{Z}$$

Grâce à ce théorème on démontre :

Théorème d'isomorphisme. Soit G un groupe fini commutatif. Alors $\hat{G}$ est isomorphe à G.

Proposition. Définition du bidual. Isomorphisme canonique entre G et $\hat{\hat{G}}$.

II.2. *Transformée de Fourier discrète.*

Définitions. [Peyré, 2004] Pour $f \in \mathbb{C}[G]$, et $\chi \in \hat{G}$, on définit le coefficient de Fourier de f, noté $c_\chi(f) = \langle f, \chi \rangle$, et on définit la transformée de Fourier de f, notée $\hat{f}$, par : $\hat{f}(\chi) = \sum\limits_{x \in G} f(x)\chi(x) = |G| \langle f, \bar{\chi} \rangle$

Formule d'inversion de Fourier. Pour $f \in \mathbb{C}[G]$, on a : $f(x) = \frac{1}{|G|} \sum\limits_{\chi \in \hat{G}} \bar{f}(\chi)\chi^{-1}$

Conséquence. La transformée de Fourier $\mathcal{F} : \mathbb{C}[G] \to \mathbb{C}[\hat{G}]$ est un isomorphisme d'espaces vectoriels.

Produit de convolution. Pour f_1 et f_2 dans $\mathbb{C}[G]$ on définit $f_1 \star f_2$ par : $(f_1 \star f_2)(g) = \sum\limits_{h \in G} f_1(h) f_2(h^{-1}g)$

Exemple. La convolution d'une fonction par un dirac réalise une translation de la fonction.

Proposition. La convolution fait de $\mathbb{C}[G]$ une algèbre. On a $f \hat{\star} g = \hat{f}\hat{g}$. La transformée de Fourier est donc un isomorphisme d'algèbres de $(\mathbb{C}[G], \star)$ sur $(\mathbb{C}[\hat{G}], \cdot)$

III. Applications.

III.1. *Traitement du signal.*

Contexte. On dispose pour un signal continue de $N \in \mathbb{N}^*$ valeurs régulièrement espacées rangées dans un vecteur $(f(n))_{n \in [\![0,N-1]\!]}$.

Proposition. Définition de la transformée de Fourier. Soit ω une racine primitive N-ième de l'unité. On définit $\hat{f} = \sum\limits_{n=0}^{N-1} f(n)\omega^{-nk}$.

Lien avec la transformée de Fourier discrète. Pour le groupe cyclique $\mathbb{Z}/N\mathbb{Z}$, on a $\chi_k(g) = \omega^{-kg}$.

Formule d'inversion. $f(n) = \frac{1}{N} \sum\limits_{k=0}^{N-1} \hat{f}(k)\omega^{nk}$.

Transformée de Fourier Rapide. On peut faire chuter le taux de calcul algorithmique de la transformée de Fourier discrète d'un $O(N^2)$ à $O(N\log(N))$.

III.2. *Multplications.*

Multiplications de polynômes

Multiplications de grands entiers

III.3. *Parallèle transformée de Fourier sur graphe.*

Expliquer brièvement ce qu'est la transformée de Fourier sur graphes pondérés non orientés.

Proposition. Équation de diffusion sur graphe. $x'(t) = -Lx(t)$.

Application. Enlever le bruit d'une image.

11. **120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.**

I. Structure et propriétés.

Définition. [Perrin, 1996] Les sous-groupes de $(\mathbb{Z},+)$ (tous distingués car $\mathbb{Z}$ abélien) sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$. On définit ainsi le sous-groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

Proposition. $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique. Pour tout diviser d de n il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d, $\mathbb{Z}/d\mathbb{Z}$.

Proposition. De même les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$. On peut donc donner à $\mathbb{Z}/n\mathbb{Z}$ une structure d'anneau.

Proposition. [Perrin, 1996] On a l'équivalence entre :

(1) s est premier avec n
(2) s est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z},+)$
(3) $s \in (\mathbb{Z}/n\mathbb{Z})^*$ groupe des éléments inversibles pour la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$
(4) $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si p est premier. On note $\mathbb{F}_p$ ce corps.

Définition. On note $\varphi(k) = |\{k \in [\![1,n]\!] | p.g.c.d(k,n) = 1\}|$. On appelle indicatrice d'Euler cette fonction.

Premiers calculs. Pour p premier, on a $\varphi(p) = p-1$ et $\varphi(p^{\alpha}) = p^{\alpha-1}(p-1)$.

Application. On a $Aut(\mathbb{Z}/n\mathbb{Z},+) \cong (\mathbb{Z}/n\mathbb{Z})^*$. En particulier c'est un groupe abélien de cardinal $\varphi(n)$.

Lemme Chinois. Si p et q sont premiers entre eux, on a l'isomorphisme $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. De fait pour m et n premiers entre eux : $\varphi(mn) = \varphi(m)\varphi(n)$.

Proposition. Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ décomposé en facteurs premiers.

(1) On a l'isomorphisme d'anneaux : $\mathbb{Z}/n\mathbb{Z} = \prod_{i=1} r\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.
(2) On a l'isomorphisme de groupes : $(\mathbb{Z}/n\mathbb{Z})^* = \prod_{i=1} r(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$
(3) On a la formule : $\varphi(n) = n\prod_{i=1}^{r}(1-\frac{1}{p_i})$.

II. Applications.

II.1. *Corps finis et carrés.*

Proposition. [Perrin, 1996] On admet que pour tout $p \in \mathcal{P}$ et tout $r \geq 1$, il existe un corps fini de cardinal $q = p^r$. C'est d'ailleurs un espace vectoriel de dimension r sur le corps $\mathbb{F}_p$.

Déterminons les carrés sur $\mathbb{F}_q$.

Proposition. Il y a $\frac{q+1}{2}$ carré dans $\mathbb{F}_q$. Lorsque $p \geq 3$, les carrés de $\mathbb{F}_q^*$ sont caractérisés par : $x \in \mathbb{F}_q^*$ si et seulement si $x^{\frac{q-1}{2}} = 1$.

Conséquences.

(1) [Beck et al., 2004]Le symbole de Legendre est un morphisme sur $\mathbb{F}_q^*$.

(2) [Perrin, 1996] L'équation $ax^2 + by^2 = 1$ avec a et b dans $\mathbb{F}_q^*$ a des solutions dans $\mathbb{F}_q$. Classification des formes quadratiques sur $\mathbb{F}_q$.

(3) -1 est un carré sur $\mathbb{F}_q$ si et seulement si $p = 2$ ou q est congru à 1 modulo 4.

Application. Théorème des deux carrés.

II.2. *Systèmes de congruences*

Dans cette partie on met en oeuvre le théorème d'isomorphisme chinois pour résoudre des systèmes congruentiels. [Gras and Gras, 2004]
Théorème. Soient $a_1, \cdots, a_n$ des élements étrangers deux à deux. Le système de congruence $x \equiv x_1[a_1], \cdots x \equiv x_n[a_n]$ admet une solution x'. L'ensemble des solutions est donné par $x' + \lambda a_1 \cdots a_n$ avec $\lambda \in A$.

Présentation de la méthode des idempotents.

Exemple. Résolution du système d'idempotents correspondant à la décomposition : $\mathbb{Z}/180\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Présentation de la méthode multi-adiques.

Exemple. Résolution de $x \equiv 1[4], x \equiv -1[9], x \equiv 3[5]$.

II.3. *Irréductibilité des polynômes*

Réduction. Soit $p \in \mathcal{P}$. Soit $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ avec a_n non divisible par p. On suppose que $\overline{P}$ est irréductible sur $(\mathbb{Z}/p\mathbb{Z})[X]$. Alors P est irréductible sur $\mathbb{Q}[X]$.

Application. $P(X) = X^3 + 462X^2 + 2433X - 67691$ et $p = 2$. On a $\overline{P}(X) = X^3 + X + 1$ est irréductible sur $\mathbb{F}_2$ donc P est irréductible sur $\mathbb{Q}[X]$.

Définition. des racines primitives de l'unité.

Définition. Définition des polynômes cyclotomiques.

Formule. $X^n - 1 = \prod\limits_{d|n} \phi_d(X)$

Exemples. $\phi_1(X) = X - 1$, $\phi_2(X) = X + 1$.

Proposition.

(1) $\phi_n(X) \in \mathbb{Z}[X]$.

(2) $\phi_n(X)$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

II.4. *Transformée de Fourier discrète*

Proposition. [Peyré, 2004] On note $\hat{G}$, appelé dual de G, l'ensemble des caractères de dimension 1 de G. Si $G = \{1, g, g^2, \cdots, g^{n-1}\}$ est un groupe cyclique d'ordre n, et que $\omega = \exp(\frac{2i\pi}{n})$, alors les éléments de $\hat{G}$ sont de la forme :

$$\chi_j : h = g^k \mapsto (\omega^j)^k,$$

pour $j \in [\![0, n-1]\!]$. En particulier $G \cong \hat{G}$.

Structure des groupes abéliens finis. [Peyré, 2004] Soit G un groupe abélien fini. Il existe des entiers strictements positifs $n_1 | n_2 | \cdots | n_r$ tels que on ait l'isomorphisme :

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_r\mathbb{Z}$$

Grâce à ce théorème on démontre :
Théorème d'isomorphisme. Soit G un groupe fini commutatif. Alors $\hat{G}$ est isomorphe à G.

12. **121 : Nombres premiers. Applications.**

I. Arithmétique dans l'anneau $\mathbb{Z}$.

I.1. *Rôle des nombres premiers*

Remarque importante. L'arithmétique sur $\mathbb{Z}$ peut être vue très tôt dans les études mathématiques, sa construction repose très fortement sur la relation d'ordre $\leq$ et la division euclidienne. On prend ici le parti d'interpréter les résultats connus sur $\mathbb{Z}$ comme des conséquences de résultats plus généraux sur la théorie des anneaux.

Proposition. [Gras and Gras, 2004] L'anneau $(Z, +, \cdot)$ est un anneau euclidien pour le stathme $|\cdot|$. A ce titre il est en particulier principal et factoriel.

Remarque. Il y a dans $\mathbb{Z}$, comme dans tout anneau commutatif intègre, trois sous-ensembles disjoints :

(1) Les inversibles ± 1
(2) Les irréductibles.
(3) Les éléments réductibles.

Définition. L'ensemble des éléments irréductibles de $\mathbb{Z}$ est l'ensemble des nombres premiers. On note $\mathcal{P}$ l'ensemble des nombres premiers positifs, que l'on choisit traditionnellement comme système exact de réprésentants.

En exprimant la factorialité de $\mathbb{Z}$, on obtient alors le théorème fondamental de l'arithmétique :
Théorème fondamental de l'arithmétique. Soit $n \in \mathbb{Z}$, alors, à l'ordre près des facteurs, et au signe près, on peut écrire n de manière unique comme un produit de nombres premiers :

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

où les $V_p(n)$ sont presques tous nuls.

Conséquence. Il existe une infinité de nombres premiers.

Conséquence de la factorialité :
Expression du p.g.c.d et du p.p.c.m. [Calais, 1998] Soit m et n deux entiers relatifs non nuls. Notons $\mu_p = \min(V_p(n), V_p(m))$ et $\nu_p = \max(V_p(n), V_p(m))$. Alors le p.g.c.d. et le p.p.c.m. positif de m et n sont donné par :

$$d = p.g.c.d(m, n) = \prod_{p \in \mathcal{P}} p^{\mu_p} \text{ et } l = p.p.c.m(m, n) = \prod_{p \in \mathcal{P}} p^{\nu_p}.$$

Proposition. $mn = \pm dl$.

Conséquences de la principalité :
Proposition. On a pour m et n non nuls : $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$ et $l\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$.

Relation de Bezout. Deux nombres m et n sont premiers entre eux si et seulement si il existe u et v tels que : $am + vn = 1$.

Remarque. La réciproque est vraie dans des anneaux non nécessairement factoriels, le sens direct découle de la principalité de $\mathbb{Z}$.

Conséquence. On peut déduire facilement du théorème de Bezout le théorème de Gauss et son corollaire : $p|bc \Rightarrow (p|b$ ou $p|c)$, mais ce sont des notions factorielles.

Conséquences du caractère euclidien :
Algorithme d'Euclide. Par division euclidienne successive, on peut déterminer des coefficients d'une relation de Bezout entre deux entiers relatifs.

Exemple. Exemple d'une descente d'Euclide.

I.2. *Anneau $\mathbb{Z}/n\mathbb{Z}$, indicatrice d'Euler.*

Proposition. Dans le cas général, Bezout montre que $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{k}|p.g.c.d(k,n) = 1\}$. On note $\varphi(k) = |\{k \in [\![1,n]\!]|p.g.c.d(k,n) = 1\}|$. On appelle indicatrice d'Euler cette fonction.

Application. [Gras and Gras, 2004] En pratique, l'algorithme d'Euclide donne l'inverse. On peut appliquer cette méthode pour résoudre des systèmes de congruences.

Proposition. On a pour m et n premiers entre eux : $\varphi(mn) = \varphi(m)\varphi(n)$.

Remarques. [Gras and Gras, 2004]

(1) Comme $\mathbb{Z}$ est factoriel, p est irréductible si et seulement si (p) est premier non nul.
(2) Comme $\mathbb{Z}$ est principal, I est premier si et seulement I est maximal.

Conséquence. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Proposition. Pour $p \in \mathcal{P}$, et $\alpha \in \mathbb{N}$, on a $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

II. Corps finis.

Proposition. Soit K un corps et $f : \mathbb{Z} \to K$ le morphisme d'anneaux défini par $f(n) = n.1 = 1 + \cdots 1$. Alors $\mathrm{Ker}(f)$ est un idéal de $\mathbb{Z}$ donc de la forme $p\mathbb{Z}$. Par propriété universelle du quotient, on a $\mathrm{Im}(f) \cong \mathbb{Z}/p\mathbb{Z}$. Comme K est intégre, ou bien $p = 0$ ou bien $p \in \mathcal{P}$. Ce nombre est appelé caractéristique de l'anneau.

Proposition. Si K est fini, la caractéristique de K est un nombre premier et le sous-corps premier de K est $\mathbb{Z}/p\mathbb{Z}$. K est un $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel, on a donc $|K| = p^n$ pour $n \in \mathbb{N}^*$.

Morphisme de Frobenius. Si $Car(K) = p$ alors $F : x \mapsto x^p$ est un automorphisme de corps. Si $K = \mathbb{F}_p$, ce morphisme est l'identité.

Existence. Il existe un corps à $q = p^n$ éléments, unique à isomorphisme près. C'est le corps de décomposition de polynôme $X^q - X$.

Proposition. $\mathbb{F}_q^*$ est un groupe cyclique de cardinal $q-1$.

Caractérisation des carrés sur les corps finis.

Théorème des deux carrés.

III. Application des nombres premiers à $\mathbb{Z}[X]$.

III.1. *Irréductibilité*

Proposition. [Perrin, 1996] $\mathbb{Z}[X]$ est factoriel.

Conséquence. Les éléments irréductibles de $\mathbb{Z}[X]$ sont les nombres premiers et les polynômes irréductibles de $\mathbb{Q}[X]$ primitifs (de contenu égal à 1).

Contre-exemple. $2X$ est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Z}$.

On voit apparaître la nécessité de savoir identifier les polynômes irréductibles de $\mathbb{Q}[X]$.
Critère d'Eisenstein. Soit $p \in \mathcal{P}$ et $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$. On suppose que :

(1) p ne divise pas a_n.

(2) p divise $a_0, \cdots a_{n-1}$.

(3) p^2 ne divise pas a_0.

Alors P est irréductible sur $\mathbb{Q}[X]$.

Applications. $X^{p-1} + \cdots + X + 1$ est irréductible sur $\mathbb{Z}[X]$.

Réduction. Soit $p \in \mathcal{P}$. Soit $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ avec a_n non divisible par p. On suppose que $\overline{P}$ est irréductible sur $(\mathbb{Z}/p\mathbb{Z})[X]$. Alors P est irréductible sur $\mathbb{Q}[X]$.

Application. $P(X) = X^3 + 462X^2 + 2433X - 67691$ et $p = 2$. On a $\overline{P}(X) = X^3 + X + 1$ est irréductible sur $\mathbb{F}_2$ donc P est irréductible sur $\mathbb{Q}[X]$.

III.2. *Polynômes cyclotomiques.*

Définition. des racines primitives de l'unité.

Définition. Définition des polynômes cyclotomiques.

Formule. $X^n - 1 = \prod_{d|n} \phi_d(X)$

Exemples. $\phi_1(X) = X - 1$, $\phi_2(X) = X + 1$.

Proposition.

(1) $\phi_n(X) \in \mathbb{Z}[X]$.

(2) $\phi_n(X)$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

13. **122 : Anneaux principaux. Exemples et applications.**

Définition. Définition d'un idéal principal.

Définition. Soit A un anneau intègre. On dit qu'il est principal lorsque tout idéal de A est principal.

Exemples et contre-exemples. $\mathbb{Z}$, $\mathbb{K}[X]$ sont principaux. $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{R}[X,Y]$ ne sont pas principaux.

Proposition. $A[X]$ est principal si et seulement si A est un corps.

Proposition. Un anneau principal est factoriel.

I. Arithmétique dans les anneaux principaux.

But. On peut faire de l'arithmétique sur des anneaux factoriels. Quelle est la valeur ajoutée de la principalité dans ce domaine ?

I.1. *Généralités et factorialité.*

Pour cette sous-partie, l'anneau A sera factoriel.

Définitions. [Gras and Gras, 2004]

(1) On dit que b divise a, noté $b|a$ lorsqu'il existe $c \in A$ tel que $a = bc$. On remarque par ailleurs que $b|a$ si et seulement si $(a) \subset (b)$.
(2) Un élément a non inversible est dit irréductible lorsque : $a = bc \Rightarrow b \in A^*$ ou $c \in A^*$.
(3) On dit que a et b sont étrangers lorsque $(a)+(b) = (1) = A$. (Existence d'une relation de Bezout).
(4) On dit que a et b sont premiers entre eux lorsque les seuls diviseurs communs de a et b sont les inversibles. Si a et b sont étrangers, alors ils sont premiers entre eux.

Exemples.

(1) Les irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.
(2) Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1. $2X$ est réductible dans $\mathbb{Z}[X]$.
(3) 3 est irréductible sur $\mathbb{Z}[i\sqrt{5}]$.

Contre-exemple. Dans $\mathbb{Z}[X]$, 2 et X sont premiers entre eux mais pas étrangers.

Théorème. Soient a et b deux éléments d'un anneau factoriel. Alors si l'idéal engendré par a et b est principal, tout générateur de cet idéal est un p.g.c.d. de a et b. En particulier si $(a,b) = (1) = A$ alors a et b sont premiers entre eux.

Réciproque fausse. $X+1$ et $X-1$ sont premiers entre eux dans $\mathbb{Z}[X]$, i.e un p.g.c.d. est égal à 1 cependant $(X-1, X+1) \neq \mathbb{Z}[X]$.

Proposition. Dans un anneau factoriel, p est irréductible si et seulement si (p) est un idéal premier non nul.

I.2. *L'apport de la principalité.*

Proposition. Soit A un anneau principal et I un idéal. Alors I est maximal si et seulement si I est premier non nul.

Proposition. Dans un anneau principal A qui n'est pas un corps. Un élément p est irréductible si et seulement si (p) est maximal.

Expression du p.g.c.d. et du p.p.c.m. Soient a et b dans A principal. Alors on peut écrire $(d) = (a) + (b)$ et $(m) = (a) \cap (b)$. Alors d est un p.g.c.d de a et b et m est un p.p.c.m. de a et b.

Proposition. Soit a et b et d un p.g.c.d. de a et b. Alors il existe u et v tels que $au + bv = d$

II. Anneaux euclidiens.

II.1. *Anneaux euclidiens.*

Définition. [Perrin, 1996] Définition d'un stathme. Définition d'un anneau euclidien.

Exemples.

(1) $\mathbb{K}[X]$ est euclidien pour pour stathme degré.

(2) $\mathbb{Z}$ est euclidien pour le stathme $|\cdot|$.

Proposition. Un anneau euclidien est principal.

Existe-t-il des anneaux euclidiens non principaux ?
Lemme. Si A est euclidien, alors il existe $x \in A \setminus A^*$ telle que la projection canonique sur $A/(x)$ restreinte à $A^* \cup \{0\}$ soit surjective.

Exemple. Si $A = \mathbb{Z}$ alors $x = 2$ ou $x = 3$ conviennent.

Existence d'anneaux euclidiens non principaux. L'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais pas euclidien.

Proposition. Dans un anneau euclidien, on dispose d'un algorithme d'Euclide pour déterminer des relations de Bezout entre deux éléments de l'anneau.

Exemple. Application de l'algorithme d'Euclide.

II.2. *Anneaux des séries formelles.*

Éléments inversibles. $f \in \mathbb{K}[[X]]$ est inversible si et seulement si $a_0 \neq 0$.

Proposition. Si a_0 est irréductible, alors $f \in A[[X]]$ est irréductible.

Proposition. $\mathbb{K}[[X]]$ est un anneau principal et ses idéaux sont les $(X^p)_{p\in\mathbb{N}}$.

Proposition. $\mathbb{K}[[X]]$ est euclidien pour la valuation.

II.3. *Anneau des entiers de Gauss.*

Définition. Définition de l'anneau intègre $\mathbb{Z}[i]$.

Proposition. L'anneau des entiers de Gauss est un anneau euclidien pour le stathme $N(z) = |z|^2$

Théorème des deux carrés.

Irréductibles de $\mathbb{Z}[i]$. Les irréductibles de $\mathbb{Z}[i]$ sont, aux élements inversibles près :

(1) Les entiers p premiers avec p congru à 3 modulo 4.
(2) Les entiers de Gauss dont la norme est un nombre premier.

III. Autres applications.

III.1. *Autours des systèmes de congruences*

Proposition. [Gras and Gras, 2004] Dans un anneau A, si deux élements a et b sont étrangers, alors on a : $(ab) = (a) + (b)$.

Théorème. Soient $a_1, \cdots, a_n$ des élements étrangers deux à deux. Alors on a l'isomorphisme canonique :

$$A/(a_1 \cdots a_n) \cong A/(a_1) \times A/(a_n).$$

Conséquence. Avec les hypothèses précédentes, le système de congruence $x \equiv x_1[a_1], \cdots x \equiv x_n[a_n]$ admet une solution x'. L'ensemble des solutions est donné par $x' + \lambda a_1 \cdots a_n$ avec $\lambda \in A$.

Présentation de la méthode des idempotents. [Gras and Gras, 2004]

Exemple. Résolution du système d'idempotents correspondant à la décomposition : $\mathbb{Z}/180\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Présentation de la méthode multi-adiques.

Exemple. Résolution de $x \equiv 1[4], x \equiv -1[9], x \equiv 3[5]$.

III.2. *Un peu d'algèbre linéaire.*

Application 1. [Beck et al., 2004] Démonstration du théorème de Dunford. Existence d'un polynôme $P \in \mathbb{K}[X]$ tel que $P \equiv \lambda_i[(X - \lambda_i)^{m_i}]$. Alors si $u = d + n$, on a $d = P(u) \in \mathbb{K}[u]$.

Application 2. Existence du polynôme minimal.

14. **123 : Corps finis. Applications.**

I. Corps finis.

I.1. *Existence et structure.*

Définition. [Perrin, 1996] On appelle sous-corps premier de $\mathbb{K}$ le plus petit sous-corps de $\mathbb{K}$.

Description du sous-corps premier. $\varphi : \mathbb{Z} \to \mathbb{K}$ l'homomorphisme d'anneaux défini par $\varphi(n) = 1 + \cdots + 1$ (n fois) a pour noyau un idéal premier $p\mathbb{Z}$ avec p premier ou nul.

Définition. L'entier p est appelé la caractéristique du corps.

Proposition. Un corps de caractéristique nulle est infini. Un corps fini a un nombre premier p pour caractéristique, et son sous-corps premier est $\mathbb{Z}/p\mathbb{Z}$, noté également $\mathbb{F}_p$. Enfin un tel corps est un $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel de dimension finie. Le cardinal d'un tel corps est une puissance de p.

Morphisme de Frobenius. Soit $\mathbb{K}$ un corps de caractéristique $p > 0$. L'application $F : \mathbb{K} \to \mathbb{K}$ définie par $F(x) = x^p$ est l'identité si $\mathbb{K} = \mathbb{F}_p$ et est un automorphisme si $\mathbb{K}$ a $\mathbb{F}_p$ pour sous-corps premier.

Existence de corps finis. Soit $q = p^r$ avec p premier et $r \geq 1$. Alors il existe un corps $\mathbb{K}$ à q éléments. C'est le corps (unique à isomorphisme près) de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

On a même mieux : **Théorème.** [Goblot, 1996]

(1) Dans la cloture algèbrique de $\mathbb{F}_p$ il existe un unique sous-corps de cardinal p^r, constitué des racines de $X^{p^r} - X$.
(2) Soit r et r' avec $r < r'$. Alors $\mathbb{F}_{p^{r'}}$ contient $\mathbb{F}_{p^r}$ et $\mathbb{F}_{p^{r'}}$ est l'unique extension de $\mathbb{F}_{p^r}$ de degré $r'-r$. De plus il existe des éléments primitifs de $\mathbb{F}_{p^{r'}}$ sur $\mathbb{F}_{p^r}$.

Proposition. Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique, isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$

Conséquence. $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/(p-1)\mathbb{Z})^*$

II. Polynômes irréductibles sur $\mathbb{F}_q$.

On veut déterminer un polynôme irréductible unitaire de degré $r \geq 1$ afin de construire $\mathbb{F}_{p^r}$. **Méthode générale.** [Gras and Gras, 2004] On trouve les polynômes irréductibles de degré 1 et 2. Une fois qu'on a trouvé tous les polynômes irréductibles de degré $j \leq E(d/2)$, on teste la divisibilité des polynômes de degré d par les polynômes qu'on a déterminés.

Proposition. [Gras and Gras, 2004] Soit P un polynôme irréductible unitaire de degré d. on pose $x = \pi(X)$ (image canonique de X dans $\mathbb{F}_p[X]/(P)$. Alors $(1, x, \cdots, x^{d-1})$ est une $\mathbb{F}_p$ base de $\mathbb{F}_{p^d}$.

Exemple. [Perrin, 1996]

(1) $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

(2) $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.

Remarque. Au delà de la construction de corps fini, il est utile de savoir déterminer l'irréductibilité des polynômes sur le corps $\mathbb{F}_p$ afin de déduire celle de certains éléments de $\mathbb{Z}[X]$.

Proposition. [FRANCINOU GIANELLA-Exercices d'algèbres pour l'agrégation.] Si on note $\mathcal{A}(n,q) = \{P \in \mathbb{F}_q[X] |$ irréductible, unitaire, de degré $n\}$ alors on a la formule :

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

Formule d'inversion de Moëbius.

Dénombrement des polynômes irréductibles. On note $I(n,q) = |\mathcal{A}(d,q)|$. Alors on a : $nI(n,q) = \sum_{d|n} \mu(\frac{n}{d}) q^d$ et $I(n,q) \sim \frac{q^n}{n}$.

II.1. *Polynômes cyclotomiques*

Définition. [Perrin, 1996] Définition des polynômes cyclotomiques.

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

Proposition. Les polynômes cyclotomiques sur le corps $\mathbb{F}_p$ s'obtient par réduction moludo p des coefficients des polynômes cyclotomiques sur $\mathbb{Q}$.

Théorème. Soit $n \in \mathbb{N}^*$. Les propriétés suivantes sont équivalentes :

(1) Il existe p premier avec n tel que le polynôme cyclotomique soit irréductible sur $\mathbb{F}_p$.

(2) $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique.

(3) $n = 1, 2, 4, q^\alpha$ ou $2q^\alpha$ avec q premier impair.

II.2. *Algorithmes de Bekerlamp*

Présentation de l'algorithme. [Beck et al., 2004]

Polynôme dérivé nul. $P' = 0$ si et seulement si $\exists R \in \mathbb{K}[X] | P = R^p$.

Proposition. Soit $\mathbb{K}$ un corps fini de caractéristique p. Considérons $P \in \mathbb{K}[X]$ et Q un facteur irréductible de P de multiplicité μ. Alors Q est un facteur irréductible de multiplicité $\mu - 1$ si p ne divise pas μ et de multiplicité μ dans le cas contraire.

Conséquences.

(1) p.g.c.d$(P, P') = 1$ ssi P est sans facteur carré.

(2) p.g.c.d$(P, P') = P$ ssi $P' = 0$ ssi $P = R^p$.

Factorisation des polynômes sur un corps finis.

III. Applications.

III.1. *Dénombrement, conséquences.*

Dénombrement. Cardinal de $GL_n(\mathbb{F}_q)$ de $SL_n(\mathbb{F}_q)$.

Critère de diagonalisabilité. [Gourdon, 1994b] Critère de diagonalisation sur le corps $\mathbb{F}_q$.

Application. [Caldero and Germoni, 2013] Cardinal des matrices diagonalisables inversible sur le corps $\mathbb{F}_q$.

Proposition. [Perrin, 1996]

(1) En caractéristique 2, $\mathbb{F}_q^2 = \mathbb{F}_q$.

(2) En caractéristique ≥ 3, on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $(\mathbb{F}_q^*)^2 = \frac{q-1}{2}$.

Lemme. [Perrin, 1996] L'équation $ax^2 + by^2 = 1$ avec a et b dans $\mathbb{F}_q^*$ a des solutions dans $\mathbb{F}_q$.

Classification des formes quadratiques sur $\mathbb{F}_q$.

III.2. *Caractérisation des carrés.*

Caractérisation des carrés. Pour $p > 2$, on a $x \in (\mathbb{F}_q^*)^2$ si et seulement si $x^{\frac{q-1}{2}} = 1$.

Application. Théorème des deux carrés.

Définition. [Caldero and Germoni, 2013] Définition du morphisme de Legendre. Remarque sur le fait qu'il est multiplicatif sur le corps $\mathbb{F}_q$ en caractéristique > 2.

Remarque. Si l'on dispose d'une factorisation d'un entier n en produits de facteurs premiers, on peut calculer son symbole de Legendre plus facilement.

Théorème de Frobenius Zoltarev [Beck et al., 2004]

Loi de réciprocité quadratique.

15. **124 : Anneaux des séries formelles. Applications.**

I. Anneaux des séries formelles.

Cadre : Dans toute la leçon, K désigne un corps commutatif.

I.1. *Définitions.*

Préliminaires. [Goblot, 1996] [?] On note $K^{\mathbb{N}}$ l'ensemble des suites à valeurs dans K. On définit l'addition et le produit de Cauchy sur $\mathbb{K}^{\mathbb{N}}$. On note $e_1 = (0, 1, 0, \cdots, 0, \cdots)$. Soit $f = (a_n)_{n\in\mathbb{N}}$. Formellement on a $f = \sum_{n\in\mathbb{N}} a_n e_1^n$. On pose alors $X = e_1$ (indéterminée) et on écrit alors :

$$f = \sum_{n\in\mathbb{N}} a_n X^n.$$

Définition. L'indéterminée ayant été notée X, l'algèbre $K^{\mathbb{N}}$ sera notée $K[[X]]$ et appelée algèbre des séries formelles à une indéterminée sur K.

Remarque : On a les inclusions strictes : $K \subset K[X] \subset K[[X]]$.

Exemple. Les sommes sont formelles, on ne se soucie par de la convergence. Pour autant les séries entières peuvent être vues comme des séries formelles. $\exp(X) = \sum_{n\in\mathbb{N}} \frac{X^n}{n!}$.

I.2. *Premières propriétés.*

Définition. Définition de la valuation d'une série formelle.

Propriétés. Propriétés de la valuation.

Conséquence. $K[[X]]$ est intègre.

Substitution d'une série formelle dans une autre. Soit $f \in K[[X]]$ de valuation plus grande que 1 et $g \in K[[X]]$ non nulle. On appelle composée de g par f la série formelle notée $g \circ f$ définie par :

$$g \circ f = \sum_{n\in\mathbb{N}} b_n f^n$$

Série formelle dérivée. Définition de la série formelle dérivée.

Propriétés.

(1) Dérivée du produit, de la composée, de l'inverse.
(2) En caractéristique nulle, les séries formelles de dérivée nulle sont les séries formelles constantes.
(3) En caractéristique nulle, il existe des primitives formelles définies à une constante près.

II. Étude de l'anneau des séries formelles.

II.1. *Éléments inversibles.*

16. **124 : Anneaux des séries formelles. Applications.**

I. Anneaux des séries formelles.

Cadre : Dans toute la leçon, K désigne un corps commutatif.

I.1. *Définitions.*

Préliminaires. [Goblot, 1996] [Calais, 1998] On note $K^{\mathbb{N}}$ l'ensemble des suites à valeurs dans K. On définit l'addition et le produit de Cauchy sur $\mathbb{K}^{\mathbb{N}}$. On note $e_1 = (0, 1, 0, \cdots, 0, \cdots)$. Soit $f = (a_n)_{n\in\mathbb{N}}$. Formellement on a $f = \sum_{n\in\mathbb{N}} a_n e_1^n$. On pose alors $X = e_1$ (indéterminée) et on écrit alors :

$$f = \sum_{n\in\mathbb{N}} a_n X^n.$$

Définition. L'indéterminée ayant été notée X, l'algèbre $K^{\mathbb{N}}$ sera notée $K[[X]]$ et appelée algèbre des séries formelles à une indéterminée sur K.

Remarque : On a les inclusions strictes : $K \subset K[X] \subset K[[X]]$.

Exemple. Les sommes sont formelles, on ne se soucie par de la convergence. Pour autant les séries entières peuvent être vues comme des séries formelles. $\exp(X) = \sum_{n\in\mathbb{N}} \frac{X^n}{n!}$.

I.2. *Premières propriétés.*

Définition. Définition de la valuation d'une série formelle.

Propriétés. Propriétés de la valuation.

Conséquence. $K[[X]]$ est intègre.

Substitution d'une série formelle dans une autre. Soit $f \in K[[X]]$ de valuation plus grande que 1 et $g \in K[[X]]$ non nulle. On appelle composée de g par f la série formelle notée $g \circ f$ définie par :

$$g \circ f = \sum_{n\in\mathbb{N}} b_n f^n$$

Série formelle dérivée. Définition de la série formelle dérivée.

Propriétés.

(1) Dérivée du produit, de la composée, de l'inverse.

(2) En caractéristique nulle, les séries formelles de dérivée nulle sont les séries formelles constantes.

(3) En caractéristique nulle, il existe des primitives formelles définies à une constante près.

II. Étude de l'anneau des séries formelles.

II.1. *Éléments inversibles.*

Exemple. [?] Par le calcul, on vérifie que $(1-X)\sum_{n\in\mathbb{N}} X^n = 1$. Autrement dit $(1-X)$ est inversible.

Proposition. f est inversible dans $K[[X]]$ si et seulement si sa valuation est nulle.

Conséquence. $K[[X]]$ est un anneau local, c'est à dire qu'il possède un unique idéal maximal : (X).

Principalité. $K[[X]]$ est un anneau principal.

Proposition. $K[[X]]$ est euclidien pour le stathme de valuation.

II.2. *Structure d'espace métrique.*

Définition. [Calais, 1998] Définition de l'application : $|f| = 2^{-\mathrm{val}(f)}$.

Propriétés. On a ainsi défini une norme et une distance.

Proposition. $(K[[X]], |\cdot|)$ est complet.

III. Applications.

III.1. *Lien avec les fractions rationnelles.*

Définition. [Calais, 1998] On note $\mathbb{K}_0(X)$ la sous algèbre de $\mathbb{K}(X)$ dont les éléments n'ont pas 0 pour pôle. En particulier les dénominateurs sont inversibles dans $\mathbb{K}[[X]]$. Pour $F = \frac{P}{Q} \in \mathbb{K}_0(X)$, on dit que $P * Q^{-1}$ est le développement en série formelle de F.

Exemple et contre-exemple.

(1) La fraction rationnelle $\frac{1}{1-X}$ admet $\sum\limits_{n\geq 0} X^n$ comme développement en série formelle.

(2) En revanche, $\exp(X) \in \mathbb{R}[[X]]$ n'est pas un élément de $\mathbb{R}_0(X)$.

Proposition. L'application qui injecte $\mathbb{K}_0(X)$ dans $\mathbb{K}[[X]]$ se comporte bien par rapport à la dérivation. La dérivation d'un développement en série formelle d'une fraction rationnelle est le développement en série formelle de la dérivation de la fraction rationnelle.

Application. Pour $a \neq 0$, on a le développement en série formelle : $\frac{1}{(a-X)^p} = \frac{1}{a^p}\sum\limits_{n\geq 0}\binom{p+n-1}{p-1}X^n$.

Cette relation trouve des applications dans le dénombrement.
Théorème. [X-ENS Algèbre 2] Partition d'un entier en parts fixés.

Exemple. [Calais, 1998] Calcul explicite du nombre de couples (p,q) tels que $2p+3q=n$.

III.2. *Autres exemples.*

Nombre de dérangements. [Goblot, 1996]

Nombres de Bell. [Pommelet, 1994]

Nombres d'arbres binaires. [Moisan et al., 1992]

17. **125 : Extensions de corps. Exemples et applications.**

I. Corps et extensions de corps.

Définition. [Perrin, 1996] Soient K et L des corps avec $K \subset L$. On dit que L est une extension de corps de K.

Exemples. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$.

Degré d'une extension. Si $K \subset L$, L est un K espace vectoriel. On note $[L : K]$ la dimension de L en tant que K espace vectoriel. On a deux cas :

(1) Si $[L : K] < \infty$ alors on dit que l'extension est (de degré) fini.

(2) Si $[L : K] = \infty$ alors l'extension est infinie.

Exemples. $[\mathbb{R} : \mathbb{Q}] = \infty$ tandis que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Théorème de la base télescopique. Soient $k \subset K \subset L$, $(e_i)_{i\in I}$ une base de K sur k et $(f_j)_{j\in J}$ une base de L sur K. Alors la famille $(e_i f_j)_{(i,j)\in I\times J}$ est un base de L sur k. On en déduit la formule de multiplicativité des degrés lorsque les deux extensions sont de degrés finis : $[L : k] = [L : K][K : k]$.

Application. On a : $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. On montre que $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(i)] = 2$ et donc $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.

Théorème. Soit $K \subset L$ une extension de corps et soit $\alpha \in L$. Notons $\varphi : K[T] \to L$ l'homomorphisme défini par $\varphi_{|K} = Id_K$ et $\varphi(T) = \alpha$. On a deux cas :

(1) Si φ est injectif, on dit que α est transcendant sur K.

(2) Sinon, on dit que α est algébrique sur K. Cela signifie qu'il existe un polynôme unitaire $P \in K[T]$, non nul, tel que $P(\alpha) = 0$ et qui engendre l'idéaln $Ker(\varphi)$. On appelle P le polynôme minimal de α sur K.

Exemples.

(1) e et π sont transcendants sur $\mathbb{Q}$.

(2) $\sqrt{2}$ et i sont algébriques sur $\mathbb{Q}$ de polynôme minimal $X^2 - 2$ et $X^2 + 1$.

Proposition. L'extension $K(\alpha)$ est finie ssi $K(\alpha) = K[\alpha]$ ssi α est algébrique sur K. Le degré de l'extension est égal au degré du polynôme minimal de α sur K.

Théorème. Soit $K \subset L$ une extension. Alors l'ensemble des éléments de L qui sont algébriques sur K est un sous-corps de L.

Définition. On appelle une extension algébrique une extension dans laquelle tout élément est algébrique.

Exemple. L'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est une extension algébrique, mais pas une extension de degré finie.

II. Constructions d'extensions de corps.

II.1. *Quelques critères d'irréductibilités.*

Remarque. [Perrin, 1996] Les parties suivantes nécessite de savoir démontrer qu'un polynôme à coefficients dans un corps est irréductible.

Critère 1. Polynôme sans racine dans le corps et de degré inférieur ou égal à 3.

Critère d'Eisenstein.

Application. Le polynôme $X^{p-1} + \cdots + X + 1$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

Critère 3. Réduction.

Applications. $X^p - X - 1$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

Théorème. $P \in k[X]$ est irréductible si et seulement si P n'a pas de racines dans toute extension K de k de degré inférieur ou égal à $\deg(P)/2$.

Applications. $X^4 + X^2 + 1$ est irréductible sur $\mathbb{F}^2$.

II.2. *Corps de rupture, décomposition, cloture algèbrique.*

Définition. [Perrin, 1996] Soit K un corps et $P \in K[X]$ un polynôme irréductible. Une extension de K si elle est monogène $K(\alpha)$ avec $P(\alpha) = 0$.

Théorème. Si P est irréductible, il existe un corps de rupture de P sur K, unique à isomorphisme près.

Exemple. $\mathbb{C}$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.

Remarque. [GOBLOT] Selon le choix de la racine, topologiquement parlant, les ensembles peuvent avoir des structures très différentes : $\mathbb{Q}(\sqrt[3]{2})$ est inclu et dense dans $\mathbb{R}$ tandis que $\mathbb{Q}(\sqrt[3]{2}j)$ est dense dans $\mathbb{C}$.

Définition. Définition d'un corps de décomposition.

Théorème. Existence et unicité du corps de décomposition à isomorphisme près.

Application. Démonstration du théorème de Cayley-Hamilton.

Application. Existence et unicité du corps fini de cardinal p^r.

Exemple. Si $P(X) = X^3 - 2$ alors $\mathbb{Q}(j, \sqrt[3]{2})$ est le corps de décomposition.

Définition. Définition d'une cloture algèbrique. Existence et unicité.

Théorème. [GOBLOT] Théorème de l'élément primitif.

III. Applications.

III.1. *Construction à la régle et au compas*

Proposition. [Perrin, 1996] Soit x un réel constructible à la régle et au compas. Alors x est algèbrique sur $\mathbb{Q}$ et le degré $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de 2.

Applications.

(1) Impossibilité de la construction de $\sqrt[3]{2}$. (Problème de l'autel de Délos).

(2) Impossibilité de la trisection de l'angle.

(3) Impossibilité de la quadrature du cercle.

18. **140 : Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.**

I. Corps des fractions rationnelles.

I.1. *Construction.*

Définition. [Goblot, 1996] Soit $A = \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\}$. Alors on définit la relation d'équivalence : $(P_1, Q_1) \sim (P_2, Q_2) \Leftrightarrow P_1Q_2 = Q_1P_2$. On appelle ensemble des fractions rationnelles, noté $\mathbb{K}(X)$ l'ensemble A quotienté par cette relation. On note $\frac{P}{Q}$ au lieu de $\overline{(P,Q)}$. On dit que $\frac{P}{Q}$ est irréductible lorsque $P \wedge Q = 1$.

Opérations. Définition de la somme et du produit de deux fractions rationnelles. Définition du degré. Ces notions ne dépendent pas du représentant choisi. Les deux opérations font de $\mathbb{K}(X)$ un corps.

Terminologie. Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$ une fraction rationnelle irréductible. On appelle racine de F un racine de P et un pôle de F une racine de Q.

I.2. *Décomposition en éléments simples.*

Proposition. Ces propositions amènent à la décomposition en éléments simples. [Goblot, 1996]

(1) Le $\mathbb{K}$ espace vectoriel $\mathbb{K}(X)$ est somme directe des sous-espaces $\mathbb{K}[X]$ et de $\mathbb{K}_{-}(X)$ les fractions rationnelles de degré strictement négatif. (Division euclidienne)

(2) Soient $B_1, \cdots B_k$ des polynômes premiers deux à deux entre eux. Le sous-espace vectoriel de $\mathbb{K}_{-}(X)$ des fractions rationnelles qui ont $\prod B_i$ en dénominateur. (Bezout)

(3) Sit P un polynôme irréductible unitaire. Le sous-espace vectoriel de $\mathbb{K}_{-}(X)$ des fractions rationnelles qui ont une puissance de P en dénominateur a pour base la famille $(\frac{X^i}{P^j})_{i<\deg(\mathrm{P}),j}$

Décomposition en éléments simples [Gourdon, 1994b] Soit $F \in \mathbb{K}(X)$ irréductible, avec $F = \frac{P}{Q}$. On a Q qui se décompose en produit de facteurs irréductibles $Q = \prod_{i=1}^{n} Q_i^{\alpha_i}$. Alors on peut écrire de manière unique :

$$F = S + \sum_{i=1}^{n} \sum_{j=1}^{\alpha_i} \frac{A_{i,j}}{Q_i^j},$$

avec $S \in \mathbb{K}[X]$.

Exemples.

(1) Sur $\mathbb{C}$, on a : $\frac{X+3}{(X-1)(X+2)} = \frac{4}{3}\frac{1}{X-1} - \frac{1}{3}\frac{1}{X+2}$.

(2) Sur $\mathbb{R}$, on a : $\frac{1}{X^4-1} = \frac{1}{4(X-1)} - \frac{1}{4(X+1)} - \frac{1}{2(X^2+1)}$.

Application. Calcul du déterminant de Cauchy.

II. Domaines d'applications.

II.1. *Calculs d'intégrales de fractions rationnelles*

Remarque. La décomposition en éléments simples permet de primitiver certaines fractions rationnelles.

Exemples. [Gourdon, 1994a]

Calcul de l'intégrale généralisée d'une fraction rationnelle de degré < -2. [Candelpergher, 2004]

Exemple. [Candelpergher, 2004]

Pour le calcul numérique, on peut utiliser : **Théorème de Rothstein-Trager.** [SAUX-PICART, Cours de calcul formel.]

II.2. *Lien avec les séries formelles.*

Définition. [Calais, 1998] On note $\mathbb{K}_0(X)$ la sous algèbre de $\mathbb{K}(X)$ dont les éléments n'ont pas 0 pour pôle. En particulier les dénominateurs sont inversibles dans $\mathbb{K}[[X]]$. Pour $F = \frac{P}{Q} \in \mathbb{K}_0(X)$, on dit que $P * Q^{-1}$ est le développement en série formelle de F.

Exemple et contre-exemple.

(1) La fraction rationnelle $\frac{1}{1-X}$ admet $\sum\limits_{n\geq 0} X^n$ comme développement en série formelle.

(2) En revanche, $\exp(X) \in \mathbb{R}[[X]]$ n'est pas un élément de $\mathbb{R}_0(X)$.

Proposition. L'application qui injecte $\mathbb{K}_0(X)$ dans $\mathbb{K}[[X]]$ se comporte bien par rapport à la dérivation. La dérivation d'un développement en série formelle d'une fraction rationnelle est le développement en série formelle de la dérivation de la fraction rationnelle.

Application. Pour $a \neq 0$, on a le développement en série formelle : $\frac{1}{(a-X)^p} = \frac{1}{a^p} \sum\limits_{n\geq 0} \binom{p+n-1}{p-1} X^n$.

Cette relation trouve des applications dans le dénombrement.
Théorème. [X-ENS Algèbre 2] Partition d'un entier en parts fixés.

Exemple. [Calais, 1998] Calcul explicite du nombre de couples (p, q) tels que $2p + 3q = n$.

19. **126 : Exemples d'équations diophantiennes.**

Définition. On appelle équation diophantienne toute équation de la forme $P(x_1, \cdots, x_n) = 0$, où P est un polynôme à coefficients entiers. On cherche des solutions entières.

I. Équations linéaires.

I.1. *Équation de Bezout*

Équation de Bezout. [COMBES, Algèbre et géométrie] On cherche à résoudre le système $AX = B$ avec A et B à coefficients entiers.

Premier cas. L'équation $ax = b$ admet une solution si et seulement si $a|b$.

Deuxième cas. L'équation $ax + by = c$ admet une solution dans $\mathbb{Z}^2$ si et seulement si le pgcd de a et b divise c.

Exemple. On veut résoudre l'équation $522x+2214y = 36$. On a p.g.c.d$(522, 2214) = 18|36$. L'équation équivaut à $29x+123y = 2$. On trouve que $29*17-123*4 = 1$, c'est-à-dire que 17 est l'inverse de 29 modulo 123. Enfin $29x \equiv 2[123]$ si et seulement si $x = 34 + 123k, k \in \mathbb{Z}$. D'où l'ensemble des solutions est $\{(34 + 123k, -8 - 29k)\}$.

Remarque. Pour le cas général, on se ramène à plusieurs équations du premier type en utilisant la **forme normale de Smith.**

I.2. *Théorème chinois.*

Dans cette partie on met en oeuvre le théorème d'isomorphisme chinois pour résoudre des systèmes congruentiels. [Gras and Gras, 2004]
Théorème. Soient $a_1, \cdots, a_n$ des élements étrangers deux à deux. Le système de congruence $x \equiv x_1[a_1], \cdots x \equiv x_n[a_n]$ admet une solution x'. L'ensemble des solutions est donné par $x' + \lambda a_1 \cdots a_n$ avec $\lambda \in Z$.

Présentation de la méthode des idempotents.

Exemple. Résolution du système d'idempotents correspondant à la décomposition : $\mathbb{Z}/180\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Remarque. Méthode utile si on a de nombreux calculs à faire avec les mêmes idéaux. Peu pratique autrement.

Présentation de la méthode multi-adiques.

Exemple. Résolution de $x \equiv 1[4], x \equiv -1[9], x \equiv 3[5]$.

Remarque. Méthode utilisable à la main.

Théorème. [X-ENS Algèbre 2] Partition d'un entier en parts fixés.

Exemple. [Calais, 1998] Calcul explicite du nombre de couples (p, q) tels que $2p + 3q = n$.

II. Entiers et carrés.

II.1. *Premiers résultats.*

Caractérisation des carrés. [Perrin, 1996] et introduction du symbole de Legendre.

Conséquence. Pour a et b dans $(\mathbb{Z}/p\mathbb{Z})^*$, l'équation $ax^2 + by^2 = 1$ admet toujours une solution dans $\mathbb{Z}/p\mathbb{Z}$. C'est par exemple utile pour classifier les formes quadratiques sur un corps fini.

Loi de réciprocité quadratique. [DUVERNEY] Soient p et q deux nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$.

Exemple. $\left(\frac{11}{83}\right) = 1$. Donc 11 est un carré modulo 3.

III. Sommes de carrés.

Entiers de Gauss. [Perrin, 1996]

Caractère euclidien des entiers de Gauss.

Inversibles des entiers de Gauss.

Théorème des deux carrés.

Exemple. [DUVERNEY-Théorie des nombres.] $585 = 24^2 + 3^2$.

Théorème des quatres carrés. [Gras and Gras, 2004]

IV. Autres équations.

Quelques équations de Fermat.
Premier résultat. [DUVERNEY] Les solutions de $x^2 + y^2 = z^2$ avec x, y et z premiers entre eux sont à permutations près $x = u^2 - v^2$, $y = 2uv$ et $z = u^2 + v^2$ avec u et v premiers entre eux de parités différentes.

Deuxième résultat. [DUVERNEY] L'équation $x^4+y^4 = z^2$ et $x^4+y^4 = z^4$ n'a pas de solution non triviale.

Troisième résultat. L'équation $x^3 + y^3 = z^3$ n'a pas de solution non triviale.

Équation de Mordell. $y^2 = x^3 - 1$ a pour unique solution $x = 1$ et $y = 0$.

20. 141 : Polynômes irréductibles à une indéterminée sur un corps commutatif.

I. Irréductibilité, et applications.

On travaille sur un anneau A qui est au minimum intègre, de sorte que $A[X]$ aussi.

I.1. *Définitions et exemples.*

Définition. [Perrin, 1996] Soit $P \in A[X] \setminus A[X]^*$ alors on dit que P est irréductible lorsque : $P = ST \Rightarrow S \in A[X]^*$ ou $T \in A[X]^*$.

Exemples.

(1) Pour tout $a \in A$, $X - a$ est irréductible.
(2) Sur un corps, un polynôme irréductible de degré plus grand que 2 n'a pas de racines. La réciproque est fausse : $(X^2+1)^2$ dans $\mathbb{R}[X]$.
(3) Les polynômes irréductibles de $\mathbb{C}[X]$ sont les $X - z$ et les polynômes irréductibles de $\mathbb{R}[X]$ sont les $X - a$ et les polynômes de degré 2 de discriminant strictement négatif.
(4) Le polynôme $2X$ est irréductible sur $\mathbb{Q}[X]$ mais pas sur $\mathbb{Z}[X]$. On va résoudre tout de suite ce dernier problème.

Définition. Si l'anneau A est factoriel ($A[X]$ est alors également factoriel), on appelle contenu d'un polynôme $P \in A[X]$ le *p.g.c.d* de ses coefficients.

Caractérisation des irréductible dans $A[X]$. Soit A factoriel et K son corps des fractions. Les irréductibles de $A[X]$ sont :

(1) Les constantes irréductibles de A.
(2) Les polynômes P de degré supérieur ou égal à 1, irréductibles sur $K[X]$, et primitifs.

I.2. *Critères classiques.*

On est maintenant ramené à l'étude des polynômes irréductibles sur un corps.

Critère 1. Un polynôme sans racine dans le corps et de degré inférieur ou égal à 3 est irréductible.

Critère d'Eisenstein. Soit A un anneau factoriel et K son corps de fractions. Soit $p \in A$ un élément irréductible et $P(X) = a_nX^n + \cdots + a_0 \in \mathcal{A}[X]$. On suppose que :

(1) p ne divise pas a_n.
(2) p divise $a_0, \cdots a_{n-1}$.
(3) p^2 ne divise pas a_0.

Alors P est irréductible sur $K[X]$.

Applications. $X^{p-1} + \cdots + X + 1$ est irréductible sur $\mathbb{Z}[X]$.

Réduction. Soit A un anneau factoriel et K son corps de fractions. Soit I un idéal premier de A et $B = A/I$ l'anneau intégre de corps de fractions L. Soit $P(X) = a_n X^n + \cdots + a_0 \in A[X]$. On suppose que $\overline{a_n} \neq 0$ dans B et que $\overline{P}$ est irréductible sur B ou L. Alors P est irréductible sur $K[X]$.

Applications.

(1) $P(X) = X^3 + 462X^2 + 2433X - 67691$ et $p = 2$. On a $\overline{P}(X) = X^3 + X + 1$ est irréductible sur $\mathbb{F}_2$ donc P est irréductible sur $\mathbb{Q}[X]$.

(2) $X^2 + Y^2 + 1$ est irréductible dans $\mathbb{R}[X, Y]$.

(3) $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$ donc par le critère, irréductible sur sur $\mathbb{Q}$.

Attention. Cette méthode donne une condition suffisante mais non nécessaire. $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais est réductible sur $\mathbb{F}_q$ pour tout $p \in \mathcal{P}$.

I.3. *Polynôme minimal en algèbre et en théorie des corps*

Définition. [Beck et al., 2004] Soit φ le morphisme de $\mathbb{K}$ algèbre $\varphi : \mathbb{K}[X] \to \mathcal{L}(\mathbb{K}^n)$ défini par $\varphi(P) = P(u)$. Son image est appelée **algèbre des polynômes en** u et est notée $\mathbb{K}[u]$. L'application φ est non injectif et son noyau est donc un idéal de $\mathbb{K}[X]$ (principal) non réduit à $\{0\}$, appelé **idéal des polynômes annulateurs**. Il est engendré par un unique polynôme unitaire, appelé **polynôme minimal** de u, noté $\mu_u(X)$.

Résultat de structure. On a l'isomorphisme $\frac{\mathbb{K}[X]}{(\mu_u(X))} \cong \mathbb{K}[u]$.

Corollaire. $\mathbb{K}[X]$ étant principal, $\mathbb{K}[u]$ est un corps si et seulement si $\mu_u(X)$ est irréductible.

Remarque. Un produits de polynômes distincts irréductibles et un produit de polynômes premiers deux à deux entre eux. Avec le lemme de noyaux on peut ainsi par exemple montrer qu'un endomorphisme dont le polynôme minimal est scindé à racines simples et diagonalisable.

Définition. [Perrin, 1996] Soit L une extension d'un corps K. Soit $\alpha \in L$. Soit $\varphi : K[T] \to L$ l'homomorphisme défini par $\varphi_{|K} = Id$ et $\varphi(X) = \alpha$. Si φ est non injectif, on dit que α est algébrique sur K. Notons $I = Ker(\varphi) = (P)$ avec P unitaire. Alors P est le polynôme minimal de α sur $\mathbb{K}$. Il est irréductible. L'extension $[K(\alpha) : K]$ est de même degré que P.

I.4. *Polynômes cyclotomiques.*

Définition. Définition de l'ensemble des racines n-ièmes de l'unité dans un corps K et des racines primitives n-ième de l'unité.

Définition. [Perrin, 1996] Définition du n-ième polynôme cyclotomique. Il est unitaire de degré $\varphi(n)$.

Proposition. $X^n - 1 = \prod_{d|n} \Phi_d(X)$. Cette formule permet le calcul de polynômes cyclotimiques par récurrence.

Exemples. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$ etc

Proposition. Les polynômes cyclotomiques sur $\mathbb{Q}$ sont à coeffients dans $\mathbb{Z}$.

Irréductibilité les polynômes cyclotomiques sur $\mathbb{Z}$.

Application. Soit ω une racine primitive n-ième de l'unité, on a alors $[Q(\omega) : \mathbb{Q}] = \varphi(n)$.

II. Extension de corps.

II.1. *Corps de rupture, décomposition, cloture algèbrique.*

Définition. [Perrin, 1996] Soit K un corps et $P \in K[X]$ un polynôme irréductible. Une extension de K si elle est monogène $K(\alpha)$ avec $P(\alpha) = 0$.

Théorème. Si P est irréductible, il existe un corps de rupture de P sur K, unique à isomorphisme près.

Exemple. $\mathbb{C}$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.

Remarque. [Goblot, 1996] Selon le choix de la racine, topologiquement parlant, les ensembles peuvent avoir des structures très différentes : $\mathbb{Q}(\sqrt[3]{2})$ est inclu et dense dans $\mathbb{R}$ tandis que $\mathbb{Q}(\sqrt[3]{2}j)$ est dense dans $\mathbb{C}$.

Définition. Définition d'un corps de décomposition.

Théorème. Existence et unicité du corps de décomposition à isomorphisme près.

Application. Une démonstration du théorème de Cayley-Hamilton sur un corps quelconque.

Application. Existence et unicité du corps fini de cardinal p^r.

Exemple. Si $P(X) = X^3 - 2$ alors $\mathbb{Q}(j, \sqrt[3]{2})$ est le corps de décomposition.

Définition. Définition d'une cloture algèbrique. Existence et unicité.

Critère 4. $P \in k[X]$ est irréductible si et seulement si P n'a pas de racines dans toute extension K de k de degré inférieur ou égal à $\deg(P)/2$.

Application. $X^4 + X^2 + 1$ est irréductible sur $\mathbb{F}^2$.

Critère 5. Soit $P \in k[X]$ un polynôme irréductible de degré n et K une extension de degré m avec $p.g.c.d(m, n) = 1$. Alors P est irréductible sur $K[X]$.

Application. $X^3 + X + 1$ est irréductible sur $\mathbb{Q}$ donc aussi sur $\mathbb{Q}(i)$.

III. Irréductibilité sur les corps finis.

III.1. *Dénombrement des polynômes irréductibles*

Proposition. [FRANCINOU GIANELLA-Exercices d'algèbres pour l'agrégation.] Si on note $\mathcal{A}(n,q) = \{P \in \mathbb{F}_q[X] |$ irréductible, unitaire, de degré $n\}$ alors on a la formule :

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

Formule d'inversion de Moëbius.

Dénombrement des polynômes irréductibles. On note $I(n,q) = |\mathcal{A}(d,q)|$. Alors on a : $nI(n,q) = \sum_{d|n} \mu(\frac{n}{d}) q^d$ et $I(n,q) \sim \frac{q^n}{n}$.

III.2. *Polynômes cyclotomiques, le retour*

Définition. Définition du n-ième polynôme cyclotomique sur le corps $\mathbb{F}_p$.

Proposition. Pour n premier à q, le n-ième polynôme cyclotomique est irréductible que $\mathbb{F}_q$ si et seulement si le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique et admet la classe de q modulo n pour générateur. [Goblot, 1996]

Remarque. [DEMAZURE] et [Beck et al., 2004] On a $X^{q^n} - X = \prod_{d|q^n} \Phi_d$. Et d'après la formule de dénombrement précédente, un polynôme irréductible unitaire de degré d divise $X^{q^n} - X$. Donc on peut déterminer tous les irréductibles de $\mathbb{F}_q[X]$ en factorisant les Φ_d et même mieux, seulement ceux pour lesquels le groupe $(\mathbb{Z}/d\mathbb{Z})^*$ est cyclique ($d = 1, 2, 4, p^\alpha$, ou $2p^\alpha$ avec p premier impair.) et tels que $\bar{q}$ soit un générateur de $(\mathbb{Z}/d\mathbb{Z})^*$. Une telle factorisation est donnée par des algorithmes comme celui de Bekerlamp.

21. 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

I. Racines, théorie des corps.

I.1. *Racines*

Définition. [Calais, 1998] Soit $P \in \mathbb{K}[X]$ un polynôme non constant. On dit que $\alpha \in \mathbb{K}$ est une racine de P lorsque $P(\alpha) = 0$.

Exemple.

(1) $X^2 + 1$ n'a pas de racines sur $\mathbb{R}$ mais a deux racines sur $\mathbb{C}$.

(2) $X^2 - 1$ a deux racines sur $\mathbb{R}$.

Proposition. Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Alors on a l'équivalence entre :

(1) $X - \alpha$ divise P.

(2) α est racine de P.

Proposition. Un polynôme $P \in \mathbb{K}[X]$ de degré n a au plus n racines distinctes sur $\mathbb{K}$.

Définition. Définition d'une racine simple, d'une racine multiple, de l'ordre de multiplicité.

Proposition. Si le corps est de caractéristique nulle, on a $\alpha \in \mathbb{K}$ racine de P d'ordre m si et seulement si $P(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.

Contre-exemple. $(X-1)^p$ admet 1 pour racine d'ordre p mais toutes les dérivées successives sont nulles sur $\mathbb{F}_p$.

Définition. On dit que P est scindé sur $\mathbb{K}$ s'il admet autant de racines sur K que son degré. Dans ce cas là on a : $P(X) = a_n \prod_{i=1}^{n} X - \alpha_i$.

Remarque. Ce résultat est à la base des **relations coefficients/racines**, on doit donc introduire des **extensions de corps sur lequel les polynômes sont scindés.**

I.2. *Obtention de racines par passage au surcorps.*

Proposition. Si P est irréductible sur $\mathbb{K}$, il n'a pas de racines sur $\mathbb{K}$.

Contre-exemple. La réciproque n'est vraie que pour degré de P plus petit que 3. Par exemple $(X^2+1)^2$ est sans racines sur $\mathbb{R}$ mais il est réductible.

Corps de rupture. Définition d'un corps de rupture.

Remarque. [Goblot, 1996] Selon le choix de la racine, topologiquement parlant, les ensembles peuvent avoir des structures très différentes : $\mathbb{Q}(\sqrt[3]{2})$ est inclu et dense dans $\mathbb{R}$ tandis que $\mathbb{Q}(\sqrt[3]{2}j)$ est dense dans $\mathbb{C}$.

Corps de décomposition. [Goblot, 1996] Définition d'un corps de décomposition. Unicité à isomorphisme près.

Exemple. $\mathbb{Q}(\sqrt[3]{2}, j)$ est le corps de décomposition de $X^3 + 2$.

Application. Démonstration du théorème de Cayley-Hamilton sur un corps quelconque.

Corps algébriquement clos. Un corps est dit algébriquement clos si tout polynôme non constant admet une racine sur ce corps. En particulier les polynômes sont scindés sur ce corps.

Exemples. $\mathbb{C}$ est algébriquement clos mais pas $\mathbb{R}$.

Cloture algébrique. Étant donné un corps $\mathbb{K}$, il existe un sur-corps algébriquement clos, algèbrique sur $\mathbb{K}$, unique à isomorphisme près.

Exemple. Construction d'une cloture algébrique de $\mathbb{F}_q$.

Proposition. [FRANCINOU GIANELLA-Exercices d'algèbres pour l'agrégation.] Si on note $\mathcal{A}(n, q) = \{P \in \mathbb{F}_q[X] |$ irréductible, unitaire, de degré $n\}$ alors on a la formule :

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

Dénombrement des polynômes irréductibles. On note $I(n, q) = |\mathcal{A}(d, q)|$. Alors on a : $nI(n, q) = \sum_{d|n} \mu(\frac{n}{d}) q^d$ et $I(n, q) \sim \frac{q^n}{n}$.

II. Coefficients/racines, polynômes symétriques.

II.1. *Relations coefficients racines.*

Polynômes symétriques élémentaires. [Goblot, 1996] Dans $\mathbb{Z}[T_1, \cdots, T_n, T]$ on considère le polynôme $\prod_{i=1}^n (T - T_i)$. Pour $k \in \{1, \cdots, n\}$, on définit le k-ième polynôme symétrique élémentaire, noté σ_k, par la relation :

$$\sigma_k(T_1, \cdots, T_n) = \sum_{1 \geq i_1 < \cdots < i_k \geq n} T_{i_1} \cdots T_{i_k}.$$

Exemple. On a $\sigma_n(T_1, \cdots, T_n) = T_1 \cdots T_n$ et $\sigma_1(T_1, \cdots, T_n) = T_1 + \cdots + T_n$.

Relations coefficients racines. Dans l'anneau $\mathbb{Z}[T_1, \cdots, T_n, T]$ on a les identités :

$$\prod_{i=1}^n (T - T_i) = \sum_{k=0}^n (-1)^k \sigma_k(T_1, \cdots, T_n) T^{n-k},$$

et pour tout $i \in \{1, \cdots, n\}$:

$$T_i^n - \sigma_1(T_1, \cdots, T_n) T_i^{n-1} + \cdots + (-1)^n \sigma_n(T_1, \cdots, T_n) = 0$$

Application. [ORAUX X-ENS Algèbre 1] et [SZPIRGLAS, Algèbre L3] Théorème de Kronecker.

II.2. *Polynômes symétriques.*

Action de $\mathcal{S}_n$ sur $\mathbb{K}[T_1, \cdots, T_n, T]$. [Goblot, 1996]

Définition. On dit qu'un polynôme est symétrique lorsqu'il est laissé fixe par l'action de $\mathcal{S}_n$.

Exemples. [Calais, 1998]

(1) Les sommes des puissances k-ièmes connues sous le nom de **polynômes de Newton** : $X_1^2 + X_2^2 + X_3^2$.
(2) Les polynômes de Wronski : $X_1^3+X_2^3+X_3^3+X_1^2X_2+X_1^2X_3+X_2^2X_1+X_2^2X_3+X_3^2X_1+X_3^2X_2+X_1X_2X_3$.
(3) Les polynômes symétriques élémentaires sont symétriques.
(4) Le discriminant : $D = \prod_{1 \leq i < j \leq n} (X_i - X_j)^2$.

Proposition. [Goblot, 1996] Les polynômes symétriques forment une sous-$\mathbb{K}$ algèbre de $\mathbb{K}[T_1, \cdots, T_n, T]$.

Théorème de structure des polynômes symétriques. Tout polynôme symétrique s'écrit comme un unique polynôme en les polynômes symétriques élémentaires.

Exemple. [Gourdon, 1994b] $X_1^3 + X_2^3 + X_3^3 = \sigma_1^3 - 3\sigma_2\sigma_2 + 2\sigma_3$.

Méthode pour trouver le polynôme. [Calais, 1998]

Exemple. Application au discriminant avec 3 indéterminées.

II.3. *Polynômes de Newton.*

Définition. [?] Définition des sommes de de Newton S_k.

Formules de Newton.

$$S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} - \cdots + (-1)^{k-1}\sigma_{k-1}S_1 + (-1)^k k\sigma_k = 0$$

Forme quadratique de Hankel [Caldero and Germoni, 2013]

Calcul des sommes de Newton de proche en proche.

III. Résultant.

Définition du résultant. [Calais, 1998]

Proposition fondamentale. Sur un corps algébriquement clos, le discriminant de deux polynômes non constants est nul si et seulement si ils ont au moins un racine commune. (Même conclusion sur un corps quelconque sur lequel les deux polynômes sont scindés...)

Expression du résultant en fonction des racines des polynômes.

Application. [SAUX-PICART, Cours de calcul formel] Théorème de Rothstein-Trager.

22. **150 : Exemples d'actions de groupes sur les espaces de matrices.**

De nombreux problèmes de classification en algèbre ou bilinéaire se ramènent à la détermination d'orbites pour l'action d'un groupe de matrice sur un ensemble de matrices. Les actions de groupes servent essentiellement à mieux comprendre le groupe ou l'ensemble. Ici c'est plutôt l'ensemble qui est ciblé.

I. Qu'est-ce qu'une action de groupe ?

[Ulmer, 2005]

Définition. Définition d'une action de groupe.

Définition. Définition de l'orbite d'un point et du sous-groupe du stabilisateur d'un point.

Proposition. Propriétés fondamentales :

(1) Être dans la même orbite est une relation d'équivalence.

(2) La fonction $f : G/G_x \to G \cdot x$ définie par $gG_x \mapsto gx$ est une bijection entre l'ensemble des classes du stabilisateur G_x dans G et l'orbite $G \cdot x$

Corollaire. On a : $|G \cdot x| = [G : G_x]$ et $|G| = |G_x||G \cdot x|$.

Application. Calcul du cardinal de $GL_n(\mathbb{F}_q) \cap \mathcal{D}$.

II. Actions par translations

II.1. *Action à gauche de $GL_n(\mathbb{K})$ sur $M_n(\mathbb{K})$*

Motivation. [Caldero and Germoni, 2013] On veut résoudre le système linéaire $AX = Y$. On se ramène au système $PAX = PY$ avec PA aussi simple que possible.

Définitions. [Beck et al., 2004]

(1) Définition des matrices de transvections.

(2) Définition des matrices de dilatations.

(3) Définition des matrices de transpositions et de permutations.

Proposition. L'action par translation à gauche agit sur les lignes de la matrice A. Plus précisément :

(1) Si $T = I_n + aE_{i,j}$, alors la i-ème ligne de TA est égale à $L_i + aL_j$.

(2) Si $D = I_n + (a-1)E_{i,i}$, alors la i-ème ligne de DA est égale à AL_i.

(3) Si $P_\tau = I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$ est une matrice de transposition, alors la i-ème et la j-ième ligne de $P_\tau A$ sont la j-ième et la i-ème ligne de A.

Proposition. [Caldero and Germoni, 2013] Soit $A \in M_{n,m}(\mathbb{K})$. Alors l'orbite de A contient une matrice sous forme échelonnée réduite. $\begin{pmatrix} 0 & 1 & * & * & * & * & * \\ 0 & 0 & 1 & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$

Théorème. Deux matrices A et B sont dans la même orbite si et seulement si elles ont même noyau.

Applications.

(1) Algorithme du pivot de Gauss.
(2) Résolutions de systèmes linéaires.
(3) Calcul de déterminant.

II.2. *Action à droite de $GL_n(\mathbb{K})$ sur $M_n(\mathbb{K})$*

Proposition. L'action par translation à droite agit sur les colonnes de la matrice A. Plus précisément :

(1) Si $T = I_n + aE_{i,j}$, alors la j-ème colonne de TA est égale à $C_j + aC_i$.
(2) Si $D = I_n + (a-1)E_{i,i}$, alors la i-ème colonne de DA est égale à AC_i.
(3) Si $P_\tau = I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$ est une matrice de transposition, alors la i-ème et la j-ième colonne de $P_\tau A$ sont la j-ième et la i-ème colonne de A.

Théorème. Deux matrices A et B sont dans la même orbite si et seulement si elles ont même image.

Application. Calcul du rang d'une matrice.

II.3. *Action de $O_n(\mathbb{R})$ sur $M_n(\mathbb{R})$.*

Décomposition polaire. [Mneimné and Testard, 1986]

Interprétation en terme d'action de groupe. Pour tout $A \in GL_n(\mathbb{R})$, l'orbite de A contient un unique élément dans $S_n^{++}(\mathbb{R})$.

On va maintenant combiner les deux premières actions étudiées.

III. Action de Steinitz

Définition de l'action de Steinitz. [Beck et al., 2004] C'est l'action de $GL_n(\mathbb{K}) \times GL_m(\mathbb{K})$ sur $M_{n,m}(\mathbb{K})$ définie par $(P,Q) \cdot M = PMQ^{-1}$. Deux actions dans la même orbites pour cette action son dites équivalentes.

Théorème. Soit $A \in M_{n,m}(\mathbb{K})$ de rang r. Alors A est équivalente à la matrice $J_r = \begin{pmatrix} I_r & 0_{r,m-r} \\ 0_{n-r,r} & 0_{n-r,m-r} \end{pmatrix}$

Corollaire. Deux matrices sont équivalentes si et seulement si elles ont même rang.

Applications.

(1) L'endomorphisme et l'endomorphisme adjoint ont même rang.
(2) Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, on en déduit la densité des matrices inversibles.
(3) Toute matrice de rang inférieur ou égal à r est limite d'une suite de matrices de rang exactement r.
(4) Deux matrices équivalentes dans un corps le sont également dans un surcorps.

IV. Action par conjugaison.

Définition. L'action ici étudiée est celle de $GL_n(\mathbb{K})$ sur $M_n(\mathbb{K})$ définie par : $G \cdot A = PAP^{-1}$. Des matrices dans la même orbite sont dites semblables.

On va se concentrer sur les corps $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ pour la classification des orbites.

IV.1. *Action de $GL_n(\mathbb{C})$ sur l'ensemble des matrices diagonalisables.*

Proposition. Deux matrices diagonalisables sont semblables si et seulement si elles ont même valeurs propres avec mêmes multiplicités, si et seulement si elles ont le même polynôme caractéristique.

Contre-exemple. En revanche des matrices ayant le même polynôme minimal ne sont pas en général dans la même orbite.

Caractérisation de la diagonalisation en terme d'action. Une matrice complexe est diagonalisable si et seulement si son orbite est fermée dans $M_n(\mathbb{C})$.

IV.2. *Action de $GL_n(\mathbb{C})$ sur l'ensemble des matrices nilpotentes.*

Proposition. [Beck et al., 2004] L'action de conjugaison laisse stable l'ensemble des matrices nilpotentes.

Caractérisation de la nilpotence en terme d'action. Une matrice complexe ou réelle est nilpotente si et seulement si la matrice nulle est dans l'adhérence de sa classe de conjugaison.

Définition. [Beck et al., 2004] Définition d'un bloc de Jordan élémentaire.

Proposition. Conditions équivalentes pour qu'un endomorphisme soit semblable à un tel bloc de Jordan.

Réduction de Jordan pour les endomorphismes nilpotents. Diagonalisation par blocs avec des blocs de Jordan élémentaire. Unicité du n-uplet de nilpotence : $(m_1, \cdots, m_n)$ qui contient le nombre de blocs de taille $(1, \cdots, n)$ dans la décomposition.

Conséquence. Deux endomorphismes nilpotents sont dans la même orbite si et seulement si ils ont le même n-uplet de nilpotence.

IV.3. *Action sur $M_n(\mathbb{K})$, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.*

Décomposition de Dunford.

Proposition. $\mathbb{K} = \mathbb{C}$. Soient $A = D + N$ et $A' = D' + N'$. Si A et A' sont semblables, alors D est semblable à D' et N à N'. Réciproquement si D et D' sont semblables et que sur chaque espace propre E_λ de dimension n_λ, l'endomorphisme induit par N et N' ont même n_λ-uplet de nilpotence, alors A et A' sont semblables.

Contre-exemple. Cas où les décompositions de Dunford sont semblables mais pas les matrices.

Application. Deux matrices complexes sont semblabes si et seulement si elles ont même polynômes caractéristique et que sur chaque espace propre, l'endomorphisme induit par N et N' sont semblables.

Lemme. Soit A et $A' \in M_n(\mathbb{R})$, alors A et A' semblables sur $\mathbb{C}$ si et seulement si elles sont semblables sur $\mathbb{R}$.

Proposition. L'orbite de A pour l'action de $GL_n(\mathbb{R})$ est exactement l'intersection de l'orbite de A pour l'action de $GL_n(\mathbb{C})$ intersectée avec $M_n(\mathbb{R})$.

V. Action par congruence sur $S_n(\mathbb{K})$.

Les corps sur lesquels ont travaille sont de caractéristique différentes de 2.

Définition. [Perrin, 1996] [Caldero and Germoni, 2013] On étudie l'action de $GL_n(\mathbb{K})$ sur $S_n(\mathbb{K})$ définie par $(P, S) = {}^tPSP$. Si deux matrices sont dans la même orbite pour cette action, on dit qu'elle sont congruentes.

Remarque. Deux matrices sont congruentes si elles représentent la même forme quadratique.

Classification sur $\mathbb{C}$

Application. Il y a $n + 1$ orbites pour l'action.

Classification sur $\mathbb{R}$

Réduction de Gauss. Exemple de l'obtention de la signature et d'une base orthogonale pour une forme quadratique réelle.

Remarque. L'orbite de I_n est l'ensemble des matrices symétriques définies positives. Le stabilisateur de I_n est l'ensemble des matrices orthogonales.

Application. Il y a $\frac{(n+1)(n+2)}{2}$ orbites pour cette action.

Application. Classification des coniques affines.

Classification sur $\mathbb{F}_q$

23. 151 : Dimension d'un espace vectoriel de dimension finie. Rang. Exemples et applications.

I. Premières propriétés et applications.

I.1. *Dimension finie.*

Définition. [Grifone, 1990] Définition d'une famille génératrice. Un espace vectoriel est dit de dimension finie lorsqu'il admet une famille génératrice de cardinal fini.

Exemples. $\mathbb{R}[X]$ est de dimension infinie. $\mathbb{K}^n$ est de dimension finie.

Définition. Définition d'une famille libre. Définition d'une base.

Existence de bases en dimension finie. Théorème de la base incomplète, ou de la base trop complète.

Application. [Beck et al., 2004] Si A est une partie dense de $\mathrm{M}_n(\mathbb{C})$, on peut trouver une base de $\mathrm{M}_n(\mathbb{C})$ constituée d'éléments de A. Par exemple des matrices diagonalisables ou des matrices inversibles.

Définition de la dimension. Toutes les bases ont même cardinal. Ce cardinal est appelé dimension de l'espace vectoriel.

Exemples. On a $\dim_{\mathbb{C}}(\mathbb{C}) = 1$ et $\dim_{\mathbb{R}}(\mathbb{C}) = 2$. $\dim(\mathbb{K}_n[X]) = n + 1$.

Proposition. [Beck et al., 2004] Un sous-espace vectoriel est de dimension finie.

Application. Une forme linéaire est soit nulle, soit surjective.

Proposition. Deux espaces vectoriels sont isomorphes si et seulement si ils ont même dimension.

Applications. L'espace des solutions d'un système différentielle linéaire est égal à la dimension de l'espace.

I.2. *Rang*

Définition. [Beck et al., 2004] Définition du rang d'une application linéaire entre deux espaces vectoriels. Du rang d'une famille de vecteurs et du rang d'une matrice.

Théorème. [Beck et al., 2004] Théorème du rang et formule du rang.

Application. Formule de Grassman. Caractérisation de la somme directe en terme de dimension.

Application. Caractérisation des isomorphismes.

Exemple. Polynôme interpolateur de Lagrange.

Exemple. Isomorphisme canonique entre le dual et le bidual.

I.3. *Rang et matrices équivalentes.*

Théorème. [Beck et al., 2004] Une matrice de rang r est équivalente à la matrice J_r.

Application. Une matrice et sa transposée ont même rang.

Application. Densité des matrices inversibles dans l'espace des matrices.

Caractérisation du rang d'une matrice. par les déterminants extraits.

Proposition. Le rang est indépendant du corps de base. Deux matrices équivalentes sur un sur-corps le sont aussi sur un sous-corps.

Application. Indépendance du polynôme minimal par rapport au corps de base.

Application. L'ensemble des matrices de rang inférieur ou égal à r est un fermé.

II. Domaines d'applications de ces théories

II.1. *Réduction des endomorphismes*

Proposition. Caractérisation géométrique de la diagonalisation en terme de dimension.

Exemple.

Remarques. [Gourdon, 1994b] On peut faire des preuves par récurrence sur la dimension de l'espace :

(1) diagonalisation simultanée
(2) trigonalisation simultanée
(3) orthodiagonalisation

II.2. *Dimension en théorie des corps.*

Définition. [Perrin, 1996] Définition d'une extension de corps. D'un élément algébrique.

Proposition. Si k est un sous-corps de K alors K est un espace vectoriel sur k. S'il est de dimension finie, on note $[K : k]$ sa dimension.

Théorème. Théorème de la base télescopique. Formule de multiplicativité des degrés.

Exemple. Le degré $[\mathbb{Q}(\sqrt[3]{2}, j)] = 3 * 2 = 6$.

Proposition. L'ensemble $\mathcal{A} = \{x \in K | x \text{algèbrique sur } k\}$ est un sous-corps de K.

Application. On a pas besoin de trouver un polynôme annulateur de $\sqrt[7]{5} + \sqrt[3]{7}\sqrt[5]{3}$ pour affirmer son algébricité.

Proposition. Soit x un réel constructible à la régle et au compas. Alors x est algèbrique sur $\mathbb{Q}$ et le degré $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de 2.

Applications.

(1) Impossibilité de la construction de $\sqrt[3]{2}$. (Problème de l'autel de Délos).

(2) Impossibilité de la trisection de l'angle.

(3) Impossibilité de la quadrature du cercle.

24. **152 : Déterminant. Exemples et applications.**

I. Définitions et calculs.

I.1. *Première propriétés.*

Proposition. [Gourdon, 1994b] Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$ espace vectoriel de dimension finie. Alors l'espace vectoriel des formes n linéaires alternées est un $\mathbb{K}$ espace vectoriel de dimension 1. Une base $\mathcal{B}$ étant fixée, il existe une unique forme n-linéaire alternée qui vaille 1 sur cette base. On l'appelle le déterminant. Cette application est appelée déterminant **dans la base** $\mathcal{B}$.

Expression. On a $det_{\mathcal{B}}(x_1, \cdots, x_n) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)}$.

Définition. Soit $M \in M_n(\mathbb{K})$. On appelle déterminant de M le déterminant dans la base canonique de $\mathbb{K}^n$ des vecteurs colonnes de M. La définition donnée par la formule ci-dessus s'étend naturellement aux matrices à coefficients dans un anneau $\mathbb{A}$.

Propositions. On a :

(1) $\det(A) = \det {}^t A$.

(2) $\det(AB) = \det(A)\det(B)$.

(3) $\det(A) \neq 0$ si et seulement si $A \in GL_n(\mathbb{K})$

Définition. Définition des cofacteurs de A et de la comatrice $\tilde{A}$.

Formule de la comatrice. On a $A^t\tilde{A} = \det(A)I_n$.

I.2. *Calcul de déterminant.*

Proposition.

(1) On ne change pas le déterminant en ajoutant à une colonne une combinaison linéaire des autres colonnes. Pareil pour les lignes.

(2) Le déterminant d'une matrice triangulaire supérieure est le produit des termes diagonaux.

Développement selon une ligne ou une colonne. Méthode d'utilisation rare. En pratique on fait apparaître le plus de zéros possibles avant de commencer : **Méthode du pivot de Gauss**.

Déterminant de Vandermonde. Valeur du déterminant de Vandermonde.

Applications. Il apparaît dans de **très nombreux problèmes** : polynômes d'interpolations de Lagrange, théorème de Burnside, Formes quadratiques de Hankel.

Déterminant circulant.

Applications. Ce déterminant est en relation avec des opérateurs de convolutions discrète et avec le traitement du signal discret sur des groupes cycliques ou des graphes circulaires.

On va maintenant étudier de nombreux domaines ou le déterminant intervient.

II. Systèmes linéaires, rang.

Solutions d'un système linéaire. [Beck et al., 2004] Formules de Cramer.

Caractérisation du rang par les déterminants extraits.

Application. Indépendance du rang par rapport au corps de base.

Applications.

(1) Deux matrices équivalentes sur un corps le sont aussi dans un sur-corps.
(2) Le polynôme minimal d'un endomorphisme est le même sur le corps de base ou un sur-corps.

III. Morphisme de groupe.

Proposition. [Perrin, 1996] L'application det est un homomorphisme multiplicatif de $GL(E)$ sur $\mathbb{K}^*$. Son noyau est appelé groupe spécial linéaire et est noté $SL_n(\mathbb{K})$. C'est donc un sous-groupe distingué de $GL_n(\mathbb{K})$.

Application. Par la propriété universelle du quotient appliqué au déterminant, on déduit le cardinal de $SL_n(\mathbb{F}_q)$.

Proposition. Sauf cas particuliers, $\mathcal{D}(GL_n(\mathbb{K})) = SL_n(\mathbb{K})$.

Théorème de Frobenius-Zoltarev

Proposition. Par propriété universelle du quotient, on montre que le déterminant d'une matrice de permutation est donnée par la signature de la permutation.

IV. Calcul différentiel. $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Proposition. [Mneimné and Testard, 1986] Le déterminant est polynomial en les coefficients de la matrice. C'est donc une application de classe $\mathcal{C}^\infty$ sur $M_n(\mathbb{K})$. On a la formule :

$$D_X \det \cdot H = \mathrm{Tr}({}^t\tilde{A}H).$$

Applications de la continuité. [Beck et al., 2004] [Mneimné and Testard, 1986]

(1) $GL_n(\mathbb{K})$ est un ouvert.
(2) L'ensemble des matrices de rang $\leq r$ est un fermé.
(3) $GL_n(\mathbb{R})$ n'est pas connexe.
(4) $SO_n(\mathbb{R})$ est un fermé.

Proposition. $SL_n(\mathbb{R})$ est une sous-variété de $M_n(\mathbb{R})$ de dimension n^2-1 et son espace tangent en I_n est l'espace des matrices de trace nulle. [Mneimné and Testard, 1986]

V. Polynôme caractéristique.

Définition. [Grifone, 1990] Définition du polynôme caractéristique.

Théorème de Cayley Hamilton.

Proposition. Sur le corps $\mathbb{R}$ ou $\mathbb{C}$ l'application $M \mapsto C_M(X)$ est continue.

Critère de diagonalisation. Sur $\mathbb{C}$, un endomorphisme u est diagonalisable si et seulement si sa classe de conjugaison est fermée.

VI. Théorème de Müntz.

Déterminant de Cauchy. [Gourdon, 1994b]

Déterminant de Gram.

Proposition. [Beck et al., 2004] Sur un espace préhilbertien réel, la distance d entre un vecteur $x \in H$ et un sous-espace vectoriel de dimension n, de base $(v_1, \cdots, v_n)$ s'exprime à l'aide du déterminant deGram :

$$d^2 = \frac{G(v_1, \cdots, v_n, x)}{G(v_1, \cdots, v_n)}.$$

Théorème de Müntz [Gourdon, 1994a]

VII. Volume, changement de variable.

Volume algébrique d'un parallélépipède. [Beck et al., 2004]

Déterminant et mesure de Lebesgue.

Exemples.

(1) Calcul de l'intégrale de Gauss par changement polaire.

(2) Volume d'un ellipsoïde.

Application. Ellisoïde de John-Loewner.

Inégalité d'Hadamard.

VIII. Résultant

Définition. [Beck et al., 2004] Définition du résultant.

Exemple. Le déterminant d'une matrice compagnon P est le résultant de P et 1

Proposition. Expression du résultant en fonction des racines des polynômes.

Proposition. Le résultant de P et Q est nul si et seulement si P et Q ne sont pas premiers entre eux.

25. **153 : Polynômes d'endomorphismes en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.**

I. L'algèbre des polynômes d'endomorphismes

I.1. *Propriétés.*

Définition. [Beck et al., 2004] Soit φ le morphisme de $\mathbb{K}$ algèbre $\varphi : \mathbb{K}[X] \to \mathcal{L}(\mathbb{K}^n)$ défini par $\varphi(P) = P(u)$. Son image est appelée **algèbre des polynômes en** u et est notée $\mathbb{K}[u]$. L'application φ est non injectif et son noyau est donc un idéal de $\mathbb{K}[X]$ (principal) non réduit à $\{0\}$, appelé **idéal des polynômes annulateurs**. Il est engendré par un unique polynôme unitaire, appelé **polynôme minimal** de u, noté $\mu_u(X)$.

Exemple. La matrice $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ a pour polynôme minimal $\mu(X) = (X - 2)(X - 1)$.

Résultat de structure. On a l'isomorphisme $\frac{\mathbb{K}[X]}{(\mu_u(X))} \cong \mathbb{K}[u]$.

Corollaire.

(1) $\mathbb{K}[X]$ étant principal, $\mathbb{K}[u]$ est un corps si et seulement si $(\mu_u(X))$ est irréductible.

(2) $\mathbb{K}[u]$ a même dimension que le degré de μ_u. Une base de $\mathbb{K}[u]$ est $(1, u, \cdots, u^{d-1})$.

Proposition. u est inversible si et seulement si $\mu_u(0) \neq 0$ et dans ce cas $u^{-1} \in \mathbb{K}[u]$.

Proposition. λ est valeur propre de u si et seulement si λ est racine du polynôme caractéristique $C_u(X)$.

Théorème. Théorème de Cayley Hamilton. Le polynôme caractéristique est annulateur pour u. Autrement dit le polynôme minimal divise le polynôme caractéristique.

Lemme des noyaux. [Beck et al., 2004]

Application. [Beck et al., 2004] Soit A une matrice telle que A^2 soit diagonalisable (par exemple une matrice antidiagonale), alors A est diagonalisable si et seulement si $\mathrm{Ker}(A) = \mathrm{Ker}(A^2)$.

II. Réduction grâce aux polynômes d'endomorphismes.

II.1. *Diagonalisation, trigonalisation, nilpotence.*

Critères de diagonalisabilité. [Beck et al., 2004] On a l'équivalence :

(1) u est diagonalisable

(2) u admet un polynôme annulateur scindé à racines simples.

(3) $\mu_u(X)$ est scindé à racines simples.

(4) $C_u(X)$ est scindé sur $\mathbb{K}$, et pour toute valeur propre λ de u, la dimension de E_λ est égale à la multiplicité de λ dans $C_u(X)$.

Application. Si un endomorphisme u est diagonalisable et que E est un espace stable par u, alors l'endomorphisme induit par u sur E est aussi diagonalisable.

Exemples. [Beck et al., 2004]

(1) Les projecteurs vérifient $P^2 = P$, donc $X^2 - X = X(X-1)$ est annulateur. Donc ils sont diagonalisables.

(2) Les symétries vérifient $S^2 = I$, donc $(X-1)(X+1)$ est annulateur. Donc elles sont diagonalisables.

(3) En particulier la transposition est diagonalisable en tant qu'endomorphisme de $\mathcal{L}(\mathbb{K}^n)$

Application. Si $\mathbb{K} = \mathbb{F}_q$, alors u est diagonalisable si et seulement si $u^q - u = 0$

Application. [Caldero and Germoni, 2013] Soit $n \geq 1$. Alors le cardinal des matrices diagonalisables de $\mathrm{GL}_n(\mathbb{F}_q)$ est égal à :

$$\sum_{n_1+\cdots+n_{q-1}=n} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbb{F}_q)|\cdots|\mathrm{GL}_{n_{q-1}}(\mathbb{F}_q)|}.$$

Une caractérisation en terme d'action de groupe. [Caldero and Germoni, 2013] Sur le corps $\mathbb{C}$, une matrice A est diagonalisable si et seulement si $\{P^{-1}AP | P \in \mathrm{GL}_n(\mathbb{C})\}$ est fermé.

Critère de trigonalisation. [Beck et al., 2004] Les propositions suivantes sont équivalentes :

(1) u est trigonalisable

(2) Il existe un polynôme annulateur scindé.

(3) C_u est scindé.

(4) μ_u est scindé.

Corollaire 2. Sur un corps algébriquement clos, tout endomorphisme est trigonalisable.

Contre-exemple. $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ n'est pas trigonalisable sur $\mathbb{R}$.

Application 1. [Mneimné and Testard, 1986] Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ on a $\det(\exp(A)) = \exp(\mathrm{Tr}(A))$.

Application 2. L'ensemble des matrices trigonalisables est un fermé de $M_n(\mathbb{K})$.

Caractérisation de la nilpotence. Les propriétés suivantes sont équivalentes :

(1) u est nilpotent.

(2) $C_u(X) = X^n$

(3) Il existe $p \in \mathbb{N}$ tel que $\mu_u(X) = X^p$

Exemple. Sur $\mathbb{K} = \mathbb{C}$, l'endomorphisme $ad_A : M \mapsto AM - MA$ est nilpotent si et seulement si $\text{Spec}(A)$ est un singleton.

III. Décomposition de Dunford et applications.

III.1. *Décomposition de Dunford*

Décomposition de Dunford. [Beck et al., 2004]

Exemple. Si $A = D + N$ est la décomposition de Dunford de A alors la décomposition de Dunford de ad_A est $ad_A = ad_D + ad_N$.

III.2. *Exponentielle matricielle*

Remarque. La suite des sommes partielles définissant l'exponentielle d'une matrice étant à valeurs dans $\mathbb{K}[u]$, espace vectoriel fermé, l'exponentielle est un polynôme en u.

Proposition. Décomposition de Dunford de l'exponentielle d'une matrice.

Proposition. Si $\mathbb{K} = \mathbb{C}$ alors A est diagonalisable si et seulement si $\exp(A)$ est diagonalisable.

III.3. *Classification des matrices de $M_n(\mathbb{C})$ et $M_n(\mathbb{R})$.*

Proposition. $\mathbb{K} = \mathbb{C}$. Soient $A = D + N$ et $A' = D' + N'$. Si A et A' sont semblables, alors D est semblable à D' et N à N'. Réciproquement si D et D' sont semblables et que sur chaque espace propre E_λ de dimension n_λ, l'endomorphisme induit par N et N' ont même n_λ-uplet de nilpotence, alors A et A' sont semblables.

Contre-exemple. Cas où les décompositions de Dunford sont semblables mais pas les matrices.

Application. Deux matrices complexes sont semblabes si et seulement si elles ont même polynômes caractéristique et que sur chaque espace propre, l'endomorphisme induit par N et N' sont semblables.

Lemme. Soit A et $A' \in M_n(\mathbb{R})$, alors A et A' semblables sur $\mathbb{C}$ si et seulement si elles sont semblables sur $\mathbb{R}$.

Proposition. L'orbite de A pour l'action de $GL_n(\mathbb{R})$ est exactement l'intersection de l'orbite de A pour l'action de $GL_n(\mathbb{C})$ intersectée avec $M_n(\mathbb{R})$.

26. **154 : Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.**

I. Espaces stables

I.1. *Définitions*

Définition. [Beck et al., 2004] Définition d'un espace stable. Notation pour l'endomorphisme induit sur l'espace stable F par u : u_F. Et par l'endomorphisme induit sur E/F : $\overline{u}$.

Lecture matricielle.

(1) Si F est stable par u, il existe une base dans laquelle la matrice de u est de la forme $\begin{pmatrix} \mathrm{Mat}(u_F) & \star \\ 0 & \star \end{pmatrix}$.

(2) Réciproquement, si dans une certaine base, la matrice de u est de cette forme, l'endomorphisme admet un espace stable.

Applications.

(1) On a $C_u(X) = C_{u_F}(x)C_{\overline{u}}$. Donc C_u est irréductible si et seulement si u n'admet pas de sous-espaces vectoriels stables non triviaux.

(2) [Gourdon, 1994b] Soit u, v deux endomorphismes tels que $rg([u,v]) = 1$, alors c_u n'est pas irréductible.

I.2. *Recherche*

Proposition. [Beck et al., 2004] Soit u et v deux endomorphismes qui commutent. Alors $\mathrm{Im}(u)$ et $\mathrm{Ker}(u)$ sont stables par v.

Remarque. Cette proposition est fondamentale, elle s'applique en particulier à u et $\mathbb{K}[u]$

Applications.

(1) $P(X) = X - \lambda_i$ avec $\lambda_i \in \mathrm{Spec}(u)$. On obtient la stabilité de E_{λ_i}

(2) $P(X) = (X - \lambda_i)^{m_i}$ avec $m_i = \mathrm{mult}(\lambda_i, C_u)$. On obtient la stabilité de F_{λ_i}

Proposition. $F \subset E$ est stable par u si et seulement si $F^\perp \subset E^*$ est stable par ${}^t u$

II. Réduction des endomorphismes.

Remarque. [Beck et al., 2004] Réduire un endomorphisme, c'est décomposer E en somme directe de sous-espaces stable par u sur lequel u agit le plus simplement possible :

(1) Diagonalisation, espaces propres, homothétie.

(2) Dunford, espace caractéristiques, diagonalisable et nilpotente.

Théorème. Lemme des noyaux.

Application. $\mathbb{K} = \mathbb{C}$ Soit u un endomorphisme tel que u^2 soit diagonalisable. Alors u est diagonalisable si et seulement si $\mathrm{Ker}(u) = \mathrm{Ker}(u^2)$.

Critère de diagonalisation et de trigonalisation.

Exemples.

Décomposition de Dunford.

Application à l'exponentielle de matrice.

Proposition. Codiagonalisation et cotrigonalisation.

Exemple. Un groupe abélien fini de $GL_n(\mathbb{C})$ est codiagonalisable.

Proposition. Soit u un endomorphisme ayant n valeurs propres distintes et v tel que u et v commutent. Alors toute base de diagonalisation de u diagonalise v.

Application. Les solutions de $X^2 = \begin{pmatrix} 9 & 91 \\ 0 & 100 \end{pmatrix}$ sont $\left\{ P \begin{pmatrix} \pm 3 & 0 \\ 0 & \pm 10 \end{pmatrix} P^{-1} \right\}$, où $P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

III. Stabilité dans les espaces euclidiens et hermitiens

Proposition. [Gourdon, 1994b] Soit u un endomorphisme normal. Alors pour λ valeur propre de u, on a E_λ et $E_\lambda^\perp$ stables par u et u^*.

Application. Réduction des endomorphismes normaux.

Remarque. Théorème pour $SO_n(\mathbb{R})$

Application. Connexité par arcs de $SO_n(\mathbb{R})$.

Classification 1. Classification de $O_2(\mathbb{R})$ en fonction de la dimension de E_{-1}

Classification 2. Classification de $O_3(\mathbb{R})$ en fonction de la dimension de E_1

Exemple.

27. **155 : Endomorphismes diagonalisables en dimension finie.**

I. Diagonalisation

Définition. [Grifone, 1990] Définition d'un vecteur propre associé à une valeur propre pour un endomorphisme. Définition du spectre d'un endomorphisme.

Définition. Définition du sous-espace vectoriel E_λ appelé espace propre associé à la valeur propre λ.

Exemples.

(1) Une projection de $\mathbb{R}^3$ sur un plan a exactement deux espaces propres : le plan E_1 et la droite normale à ce plan E_0.

(2) Une rotation d'angle $\neq k\pi$ dans $\mathbb{R}^2$ n'a pas de valeur propre réelle. En revanche, elle a deux valeurs propres complexes. Le problème de la diagonalisation dépend du corps de base.

(3) Une homothétie de rapport k a pour seul espace propre $E_k = \mathbb{K}^n \backslash \{0\}$.

Définition. Définition du polynôme caractéristique de A, noté C_A. $C_A(X) = \det(XI_n - A)$. L'ensemble des racines de C_A sur $\mathbb{K}$ est exactement $\mathrm{Spec}_K(A)$.

Exemples. En reprenant les exemples précédents, on a $C_1(X) = X(X-1)^2$, $C_2(X) = X^2 - 2\cos(\theta)X + 1 = (X - \exp(i\theta))(X - \exp(-i\theta))$ et $C_3(X) = (X-k)^n$.

Définition de la diagonalisation. Un endomorphisme u est diagonalisable lorsqu'il existe une base de $\mathbb{K}^n$ formée de vecteurs propres de u.

Exemples. En reprenant l'exemple précédent, la projection est diagonalisable, la rotation n'est pas diagonalisable sur $\mathbb{R}$ mais est diagonalisable sur $\mathbb{C}$, l'homothétie est diagonale dans n'importe quelle base.

II. Critères de diagonalisation

II.1. *Critères géométriques*

Proposition. Si $\lambda_1, \cdots, \lambda_d$ sont des valeurs propres distinctes de u alors les espaces propres associés sont en somme directe.

Premiers critères de diagonalisation. On a l'équivalence entre :

(1) u est diagonalisable.

(2) $\mathbb{K}^n$ est la somme directe des espaces propres de u.

(3) La somme des dimensions des espaces propres de u est égale à n.

Corollaire. Si u admet n valeurs propres distinctes, alors il est diagonalisable.

Exemple. [Grifone, 1990] La matrice $\begin{pmatrix} 2 & 3 & 1 \\ 0 & 4 & 4 \\ 0 & 0 & 1 \end{pmatrix}$ a pour valeurs propres 2,4 et 1 donc est diagonalisable.

II.2. *L'apport des polynômes d'endomorphismes*

Théorème. Théorème de Cayley Hamilton. Le polynôme caractéristique est annulateur pour u.

Proposition. [Beck et al., 2004] Soit φ le morphisme de $\mathbb{K}$ algèbre $\varphi : \mathbb{K}[X] \to \mathcal{L}(\mathbb{K}^n)$ défini par $\varphi(P) = P(u)$. Son image est appelée algèbre des polynômes en u et est notée $\mathbb{K}[u]$. φ est non injectif et son noyau est donc un idéal de $\mathbb{K}[X]$ (principal) non réduit à $\{0\}$, appelé idéal des polynômes annulateurs. Il est engendré par un unique polynôme unitaire, appelé polynôme minimal de u, noté $\mu_u(X)$.

Exemple. La matrice $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ a pour polynôme minimal $\mu(X) = (X-2)(X-1)$.

Lemme des noyaux. [Beck et al., 2004]

Application. [Beck et al., 2004] Soit A une matrice telle que A^2 soit diagonalisable (par exemple une matrice antidiagonale), alors A est diagonalisable si et seulement si $\mathrm{Ker}(A) = \mathrm{Ker}(A^2)$.

Deuxième série de critères de diagonalisabilité. On a l'équivalence :

(1) u est diagonalisable

(2) u admet un polynôme annulateur scindé à racines simples.

(3) $\mu_u(X)$ est scindé à racines simples.

(4) $C_u(X)$ est scindé sur $\mathbb{K}$, et pour toute valeur propre λ de u, la dimension de E_λ est égale à la multiplicité de λ dans $C_u(X)$.

Application. Si un endomorphisme u est diagonalisable et que E est un espace stable par u, alors l'endomorphisme induit par u sur E est aussi diagonalisable.

Exemples. [Beck et al., 2004]

(1) Les projecteurs vérifient $P^2 = P$, donc $X^2 - X = X(X-1)$ est annulateur. Donc ils sont diagonalisables.

(2) Les symétries vérifient $S^2 = I$, donc $(X-1)(X+1)$ est annulateur. Donc elles sont diagonalisables.

(3) En particulier la transposition est diagonalisable en tant qu'endomorphisme de $\mathcal{L}(\mathbb{K}^n)$

Application. Si $\mathbb{K} = \mathbb{F}_q$, alors u est diagonalisable si et seulement si $u^q - u = 0$

Application. [Caldero and Germoni, 2013] Soit $n \geq 1$. Alors le cardinal des matrices diagonalisables de $\mathrm{GL}_n(\mathbb{F}_q)$ est égal à :

$$\sum_{n_1+\cdots+n_{q-1}=n} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbb{F}_q)| \cdots |\mathrm{GL}_{n_{q-1}}(\mathbb{F}_q)|}.$$

Une caractérisation en terme d'action de groupe. [Caldero and Germoni, 2013] Sur le corps $\mathbb{C}$, une matrice A est diagonalisable si et seulement si $\{P^{-1}AP | P \in \mathrm{GL}_n(\mathbb{C})\}$ est fermé.

II.3. *Autres exemples de diagonalisations.*

Propositon. Une famille d'endomorphismes diagonalisables qui commutent deux à deux sont codiagonalisables.

Application. Un sous-groupe abélien G de $\mathrm{GL}_n(\mathbb{C})$ est codiagonalisable.

Proposition. [Grifone, 1990] Un endomorphisme auto-adjoint d'un espace euclidien est orthodiagonalisable (matrice de passage orthogonale).

Application. Existence et unicité de la racine carrée d'une matrice symétrique définie positive. Décomposition polaire.

Proposition. Un endomorphisme auto-adjoint d'un espace hermitien est orthodiagonalisable (matrice de passage unitaire), ses valeurs propres sont réelles.

Proposition. Tout endomorphisme normal sur un espace hermitien est orthodiagonalisable. On en déduit la réduction des endomorphismes normaux sur le corps $\mathbb{R}$.

III. Applications.

Calcul des puissances d'une matrice. [Grifone, 1990]

Exemple. [Grifone, 1990]

Résolution d'un système de suite récurrente. [Grifone, 1990]

Remarque. Quand la matrice du système n'est pas diagonalisable, on fait intervenir d'autres réductions.

Théorème. Réduction de Dunford.

Application. [Beck et al., 2004] Sur le corps $\mathbb{C}$, $\exp(u)$ est diagonalisable si et seulement si u est diagonalisable.

Proposition. Sur le corps $\mathbb{C}$, les matrices diagonalisables sont denses dans $M_n(\mathbb{C})$.

Application. [Beck et al., 2004] L'application qui à une matrice associe sa partie diagonalisable dans la décomposition de Dunford n'est pas continue.

28. **156 : Exponentielle de matrices. Applications.**

On se place sur le corps $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I. Exponentielle matricielle

I.1. *Définition et propriétés fondamentales.*

Définition. [Mneimné and Testard, 1986] Pour $A \in M_n(\mathbb{K})$, l'exponentielle de A, notée $\exp(A)$ est définie comme la somme de la série normalement convergente $\sum_{k=0}^{+\infty} \frac{A^k}{k!}$.

Exemples.

(1) On a $\exp(0_n) = I_n$

(2) Si $A = \operatorname{diag}(\lambda_1, \cdots, \lambda_n)$ alors on a $\exp(A) = \operatorname{diag}(\mathrm{e}^{\lambda_1}, \cdots, \mathrm{e}^{\lambda_n})$.

(3) L'exponentielle d'une matrice triangulaire supérieure est triangulaire supérieure, avec les éléments diagonaux qui sont les exponentielles des éléments diagonaux.

Proposition. Pour tout $A \in M_n(\mathbb{K})$, $\exp(A) \in \mathbb{K}[A]$.

Remarque. Pour autant, exp n'est pas une application polynomiale.

Proposition. Si A et B commutent, on a $\exp(A+B) = \exp(A)\exp(B)$.

Conséquence. Pour tout $A \in M_n(\mathbb{K})$, $\exp(A) \in GL_n(\mathbb{K})$ et $\exp(A)^{-1} = \exp(-A)$.

Contre-exemple. Soit $A = \begin{pmatrix} 0 & 0 \\ \theta & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -\theta \\ 0 & 0 \end{pmatrix}$. Alors $\exp(A+B) = \mathrm{R}_\theta \neq \exp(A)\exp(B)$.

Non injectivité de l'exponentielle.

I.2. *Réduction de l'exponentielle matricielle.*

Proposition. Deux matrices semblables ont des exponentielles semblables. Pour tout $P \in GL_n(\mathbb{K})$, on a : $\exp(P^{-1}AP) = P^{-1}\exp(A)P$.

Application. On a $\det(\exp(A)) = \exp(\operatorname{Tr}(A))$.

Remarque. La propriété 'Si A et B commutent, on a $\exp(A+B) = \exp(A)\exp(B)$' indique que la décomposition de Dunford est particulièrement intéréssante dans le cas de l'exponentielle.

Proposition. [Beck et al., 2004] L'application exponentielle réalise un homéomorphisme entre l'ensemble des matrices nilpotentes et l'ensemble des matrices unipotentes.

Proposition. [Beck et al., 2004] Soit $A = D + N$ la décomposition de Dunford de A. Notons $N = I_n + N'$ avec N' nilpotente. Alors la décomposition de Dunford de $\exp(A)$ est :

$$\exp(A) = \exp(D) + \exp(D)N'.$$

Corollaire. $\mathbb{K} = \mathbb{C}$ A diagonalisable si et seulement si $\exp(A)$ est diagonalisable.

II. Image, régularité, inversion.

II.1. *Premiers résultats*

Proposition. L'application $\exp : M_n(\mathbb{C}) \to GL_n(\mathbb{C})$ est sujective.

Remarque. On a pas la surjectivité de $\exp : M_n(\mathbb{R}) \to GL_n(\mathbb{R})$. On a même pas la surjectivité de $\exp : M_n(\mathbb{R}) \to GL_n^+(\mathbb{R})$. Par exemple $\begin{pmatrix} -1 & 0 \\ 0 & -2 \end{pmatrix} \notin \exp(M_n(\mathbb{R}))$.

Différentielle de l'exponentielle. L'application exp est de classe $\mathcal{C}^\infty$ sur $M_n(\mathbb{R})$. Donner deux expressions de sa différentielle. [Rouvière, 1999]

Application. On appelle sous-groupes à un paramètre de $GL_n(\mathbb{K})$ l'image d'un morphisme continu du groupe additif $\mathbb{R}$ dans $GL_n(\mathbb{K})$. Alors pour tout sous-groupe à un paramètre, il existe un unique $X \in M_n(\mathbb{K})$ tel que $\varphi(t) = \exp(tX)$.

Corollaire. [Mneimné and Testard, 1986] D'après le théorème d'inversion locale, l'exponentielle réalise donc un difféomorphisme local entre un voisinage de 0 et un voisinage de I_n dans $GL_n(\mathbb{K})$.

Application. $GL_n(\mathbb{K})$ n'a pas de sous-groupes arbitrairement petits.

Proposition.

(1) L'exponentielle réalise un homéomorphisme de $H_n(\mathbb{C})$ sur $H_n^{++}(\mathbb{C})$.

(2) L'exponentielle réalise un homéomorphisme de $S_n(\mathbb{R})$ sur $S_n^{++}(\mathbb{R})$.

Application. De la décomposition polaire, on peut déduire : $GL_n(\mathbb{R}) \cong O_n(\mathbb{R}) \times \mathbb{R}^{\frac{n(n+1)}{2}}$ et $GL_n(\mathbb{C}) \cong U_n(\mathbb{C}) \times \mathbb{R}^{n^2}$.

II.2. *Logarithme. Algèbre de Lie.*

Définition. Si $A \in B(I_n, 1)$ on appelle logarithme de A, noté $\mathrm{Log}(A)$, la somme de la série normalement convergente : $\sum_{k=1}^{+\infty} (-1)^{n+1} \frac{(A-I_n)^k}{k}$.

Proposition. Pour tout $A \in B(I_n, 1)$, $\exp(\mathrm{Log}(A)) = A$ et pour tout $A \in B(0_n, \ln(2))$, $\mathrm{Log}(\exp(A)) = A$

Applications. On a :

(1) $\det[\exp(\frac{X}{n}) \exp(\frac{Y}{n})]^n = \exp(X+Y)$

(2) $\det[\exp(\frac{X}{n}) \exp(\frac{Y}{n}) \exp(-\frac{Y}{n})]^{n^2} = \exp(X+Y)$

On en déduit :

Proposition. Soit G un sous-groupe fermé de $GL_n(\mathbb{K})$. Soit $L_G = \{X \in M_n(\mathbb{K}) | \forall t \in \mathbb{R}, \exp(tX) \in G\}$. Alors L_G est un sous-expace vectoriel de $M_n(\mathbb{K})$ stable par $(X,Y) \mapsto XY - YX$. On l'appelle algèbre de Lie du groupe G.

Théorème de Cartan/Von Neumann [GONNORD et TOSEL, Calcul différentiel.] Un sous-groupe fermé de $GL_n(\mathbb{R})$ est une sous-variété de $M_n(\mathbb{R})$ de dimension égale à $\mathrm{L_G}$.

Proposition. L'espace vectoriel tangent à G en I_n est L_G.

Exemples.

(1) $SO_n(\mathbb{R})$ est une sous-variété de dimension $\frac{n(n-1)}{2}$.

(2) $SL_n(\mathbb{R})$ est une sous-variété de dimension n^2-1.

Donner aussi les espaces tangents en I_n.

III. Applications à l'étude des systèmes différentiels linéaires à coefficients constants.

Proposition. [Demailly, 2012] L'unique solution de $\frac{dY}{dt}(t) = AY(t)$ vérifiant $Y(t_0) = Y_0$ est donnée par : $Y(t) = \exp((t-t_0)A)Y_0$.

Remarque. En terme de résolvante : $R(t, t_0) = \exp((t-t_0)A)$.

Corollaire. Si $\forall t \in \mathbb{R}, \exp(tA) = \exp(tB)$ alors $A = B$

Proposition. L'unique solution de $\frac{dY}{dt}(t) = AY(t) + B(t)$ vérifiant $Y(t_0) = Y_0$ est donnée par : $Y(t) = \exp((t-t_0)A)Y_0 + \int_{t_0}^{t} \exp((t-u)A)B(u)\mathrm{d}u$.

Définition. Définition de la stabilité et de la stabilité asymptotique des solutions d'une équation différentielle.

Théorème de stabilité dans le cas linéaire à coefficients constants. Soient $\lambda_1, \cdots \lambda_m$ les valeurs propres complexes de la matrice A. Alors les solutions de $Y' = AY$ sont :

(1) asymptotiquement stables si et seulement si $\mathrm{Re}(\mathrm{Spec}(A)) \subset]-\infty, 0[$.

(2) stables si et seulement si pour tout $j \in [\![1, m]\!]$, ou bien $\mathrm{Re}(\lambda_j) < 0$ ou bien $\mathrm{Re}(\lambda_j) = 0$ et $\dim(E_{\lambda_j}) = \mathrm{Mult}(\lambda_j, C_A(X))$.

Exemple. Un exemple d'application du théorème.

Dessin en annexe pour la dimension 2

29. **157 : Endomorphismes trigonalisables. Endomorphismes nilpotents.**

I. Endomorphismes trigonalisables.

I.1. *Outils de bases.*

Définitions. [Grifone, 1990]

(1) Définition d'un espace propre.
(2) Définition du polynôme caractéristique.
(3) Définition du polynôme annulateur.

Théorème. Théorème de Cayley-Hamilton.

Théorème. Lemme des Noyaux.

I.2. *Trigonalisation.*

Définition. Un endomorphisme est trigonalisable lorsqu'il existe une base dans laquelle sa matrice est triangulaire. Une matrice est trigonalisable lorsqu'elle est semblable à une matrice triangulaire.

Critère de trigonalisation. [Beck et al., 2004] Les propositions suivantes sont équivalentes :

(1) u est trigonalisable
(2) Il existe un polynôme annulateur scindé.
(3) C_u est scindé.
(4) μ_u est scindé.

Corollaire 1. Si $F \subset E$ est un sous-espace vectoriel stable par u, alors l'endomorphisme induit par u sur F est trigonalisable.

Corollaire 2. Sur un corps algébriquement clos, tout endomorphisme est trigonalisable.

Contre-exemple. $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ n'est pas trigonalisable sur $\mathbb{R}$.

Application 1. [Mneimné and Testard, 1986] Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ on a $\det(\exp(A)) = \exp(\mathrm{Tr}(A))$.

Application 2. L'ensemble des matrices trigonalisables est un fermé de $M_n(\mathbb{K})$.

Trigonalisation simultanée. [Gourdon, 1994b] Si u et v commutent et sont trigonalisables alors u et v sont cotrigonalisables.

II. Endomorphismes nilpotents

Définition. [Beck et al., 2004] Définition d'un endomorphisme nilpotent.

Exemples.

(1) Si A est une matrice nilpotente, alors $M \mapsto AM$ est nilpotent.

(2) Sur $\mathbb{K}_n[X]$ la dérivation est nilpotente d'ordre n.

Structure de $\mathcal{N}$. L'ensemble des matrices nilpotentes est un cône.

Exemple en dimension 2. Équation et dessin du cône en dimension 2 dans l'espace des matrices de traces nulles de dimension 3.

Contre-exemple. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \notin \mathcal{N}$.

En revanche si on rajoute la commutativité on a :
Proposition. Soient u et v deux endomorphismes nilpotents qui commutent. Alors $u + v$ est nilpotent. Si f est un endomorphisme qui commute avec u alors $u \circ f$ est nilpotent.

Caractérisation de la nilpotence. Les propriétés suivantes sont équivalentes :

(1) u est nilpotent.

(2) $C_u(X) = X^n$

(3) Il existe $p \in \mathbb{N}$ tel que $\mu_u(X) = X^p$

(4) u est trigonalisable avec 0 pour seule valeur propre.

(5) L'endomorphisme nul est dans l'adhérence de la classe de conjugaison de u.

(6) En caractéristique nulle, $\forall k \in \mathbb{N}$, $\mathrm{Tr}(u^k) = 0$.

Exemple. Sur $\mathbb{K} = \mathbb{C}$, l'endomorphisme $ad_A : M \mapsto AM - MA$ est nilpotent si et seulement si $\mathrm{Spec}(A)$ est un singleton.

Contre-exemple. La matrice $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$ n'est pas nilpotente mais sa seule valeur propre réelle est 0.

Espace vectoriel engendré par $\mathcal{N}$. On a $\mathrm{Vect}(\mathcal{N}) = \mathrm{Ker}(\mathrm{Tr})$.

Application. Théorème de Burnside. [ORAUX X-ENS-Algèbre 2.]

III. Applications.

III.1. *Décomposition de Dunford*

Décomposition de Dunford.

Proposition. L'exponentielle réalise un homéomorphisme entre $\mathcal{N}$ et $\mathcal{U}$, l'ensemble des matrices unipotentes.

Exemples.

(1) Décomposition de Dunford de l'exponentielle d'une matrice.

(2) Si $A = D + N$ est la décomposition de Dunford de A alors la décomposition de Dunford de ad_A est $ad_A = ad_D + ad_N$.

Application. Si $\mathbb{K} = \mathbb{C}$ alors A est diagonalisable si et seulement si $\exp(A)$ est diagonalisable.

Remarque : Le fait que D et N commutent est particulièrement profitable dans l'étude théorique des systèmes différentielles linéaires à coefficients constants car alors $\exp(D+N) = \exp(D)\exp(N)$.

III.2. *Réduction de Jordan.*

Définition. Définition des blocs de Jordan élémentaires de taille n, noté J_n. Par exemple $J_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

Proposition. Les propositions suivantes sont équivalentes :

(1) Il existe une base dans laquelle la matrice de u est un bloc de Jordan de taille n.

(2) L'endomorphisme u est à la fois nilpotent et cyclique.

(3) u est un endomorphisme d'indice de nilpotence n.

(4) u est un endomorphisme de rang $n-1$.

Théorème. Réduction de Jordan pour les endomorphismes nilpotents.

Application. Classification des orbites de $\mathcal{N}$ sous l'action de $GL_n(\mathbb{K})$ par conjugaison. Deux endomorphismes nilpotents sont dans la même orbite lorsqu'ils ont le même nombre de blocs de Jordan de la même dimension.

Théorème. Réduction de Jordan pour les endomorphismes quelconques.

30. **158 : Matrices symétriques réelles, matrices hermitiennes.**

I. Lien avec l'étude des formes hermitiennes et quadratiques.

I.1. *Généralités.*

Définition. [Grifone, 1990] Soit E un $\mathbb{C}$ espace vectoriel. Soit $h : E \times E \to \mathbb{C}$. On dit que h est hermitienne lorsqu'elle est linéaire en la deuxième variable, antilinéaire en la deuxième variable, et vérfiant $\forall x, y \in E, h(x,y) = \overline{h(y,x)}$. Dans le cas d'un espace vectoriel réel, on considère plutôt les formes bilinéaires symétriques.

Proposition. Une base ayant été fixée, on peut définir la matrice d'une forme hermitienne $H = (h(e_i, e_j))_{i,j}$. On a la relation $H^* = H$. L'ensemble des matrices vérifiant cette relation est appelé ensemble des matrices hermitiennes. Pour les formes bilinéaires on a ${}^tM = M$ et on appelle l'ensemble de telles matrices matrices symétriques.

Remarque. Réciproquement, à une matrice hermitienne $H \in H_n(\mathbb{C})$ on peut associer une forme hermitienne définie par $(X,Y) \mapsto X^*HY$

Proposition. L'espace des matrices symétriques réelles est un sous-espace vectoriel de $M_n(\mathbb{R})$ de dimension $\frac{n(n+1)}{2}$. On a la décomposition en somme directe : $M_n(\mathbb{R}) = S_n(\mathbb{R}) \oplus A_n(\mathbb{R})$.

Contre-exemple. $i\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix} = \begin{pmatrix} i & -1 \\ 1 & i \end{pmatrix} \notin H_n$. Les matrices hermitiennes n'ont pas de structure d'espace vectoriel.

I.2. *Classification des formes hermitiennes et symétriques.*

Changement de base. On définit une action du groupe $GL_n(\mathbb{C})$ sur H_n définie par $(P,H) \mapsto PHP^*$. Deux éléments de $H_n(\mathbb{C})$ distincts sont dans la même orbite si et seulement si ils représentent la même forme hermitienne dans deux bases différentes.

Existence de base orthogonale. [Grifone, 1990]

Remarque. En pratique, on peut obtenir des bases orthogonales par réduction de Gauss.

Exemple. $q(x) = |x_1|^2 + 5|x_2|^2 + 3|x_3|^2 + 2i\overline{x_1}x_2 - 2i\overline{x_2}x_1 + i\overline{x_2}x_3 - i\overline{x_3}x_2 = |x_1 + 2ix_2|^2 + |x_2 + ix_3|^2 + 2|x_3|^2$

Théorème d'inertie de Sylvester. avec définition de la signature. Interprétation en terme d'orbites de l'action de groupe.

Exemple. La forme de l'exemple a pour signature $(3,0)$

Définition. Définition du groupe des matrices unitaires et des matrices orthogonales.

II. Espaces hermitiens et euclidiens.

Définition. On remarque que si h est une forme hermitienne, pour tout $x \in E$, on a $h(x,x) \in \mathbb{R}$. On dit que h est positive lorsque pour tout $x \in E$, $h(x,x) \geq 0$ et définie positive si de plus $h(x,x) = 0 \Leftrightarrow x = 0$.

Remarque. h est définie positive si et seulement si $sg(h) = (n, 0)$.

Définition. Un $\mathbb{C}$ espace vectoriel E de dimension finie muni d'une forme hermitienne définie positive est appelé un espace hermitien. Lorsqu'il s'agit d'un $\mathbb{R}$ espace vectoriel muni d'une forme bilinéaire symétrique définie positive, on parle d'espace euclidien.

Sur des espaces hermitiens, (resp. euclidiens), les matrices hermitiennes peuvent s'interpréter comme des matrices d'applications linéaires :
Définition. Un endomorphisme f d'un espace hermitien est dit auto-adjoint lorsque $f^* = f$, autrement dit si pour tout $x, y \in E$: $\langle f(x), y\rangle = \langle x, f(y)\rangle$. Dans une base orthonormée, si A désigne la matrice de f, A^* est la matrice de f^*. Ainsi dans toute base orthonormée, la matrice de f est hermitienne.

Remarque. Les valeurs propres d'un endomorphisme auto-adjoint sont réelles. De plus les endomorphismes auto-adjoints sont des endomorphismes normaux, c'est à dire qui commutent avec leur adjoint.

Théorème. [Grifone, 1990] Théorème de réduction des endomorphismes normaux.

Corollaire. Interprétation matricielle dans le cas des matrices hermitiennes et des matrices symétriques réelles.

Corollaire. Énoncé du théorème de réduction simultanée.

Application. Ellipsoïde de John-Loewner.

III. Applications.

III.1. *Décomposition polaire.*

Décomposition polaire. sur $GL_n(\mathbb{R})$ et $GL_n(\mathbb{C})$ [Mneimné and Testard, 1986]

Proposition. Homéomorphisme de l'exponentielle de $S_n(\mathbb{R})$ sur $S_n^{++}(\mathbb{R})$ et de H_n sur S_n^{++}.

Remarque. On a ainsi réalisé une sorte d'extension des coordonnées polaires complexes. On a pour $Z \in GL_n(\mathbb{C})$, $Z = U\exp(H) = Z\exp(i(-iH))$ avec $-iH$ antihermitienne.

III.2. *Classification des coniques*

Proposition. [Audin, 2012] Classification des coniques affines.

Proposition. [Audin, 2012] Classification des coniques euclidiennes.

III.3. *Calcul différentiel.*

Définition. [Rouvière, 1999] Définition de la matrice hessienne.

Lemme de Morse. [Rouvière, 1999]

Applications. Condition du deuxième ordre pour la recherche d'extrema. Forme des lignes de niveaux.

31. **159 : Formes linéaires et dualité en dimension finie. Exemples et applications.**

I. Formes linéaires et hyperplans.

I.1. *Formes linéaires.*

Définition. [Grifone, 1990] On appelle forme linéaire sur E une application linéaire de E sur $\mathbb{K}$. On appelle **dual** de E noté E^*, l'ensemble des formes linéaires sur E.

Proposition. Une forme linéaire est nulle ou surjective.

Écriture matricielle. Soit $l \in E^*$ une forme linéiare. Une base $B = (e_1, \cdots, e_n)$ de E ayant été fixée, $Mat_{B,(1)}(l)$ est une matrice ligne.

Exemples.
- La trace est une forme linéaire.
- Si $\langle \cdot, \cdot \rangle$ est un produit scalaire, alors $\langle x, \cdot \rangle \in E^*$.
- En particulier si $f : E \to \mathbb{R}$ est différentiable en x, alors $\mathrm{D}_x f = \langle \mathrm{Grad}_x f, \cdot \rangle$ est une forme linéaire.

I.2. *Hyperplans.*

Proposition. D'après le théorème du rang, une forme linéaire non nulle a un noyau de dimension $n-1$. On appelle le noyau d'une forme linéaire un hyperplan.

Transvections. [Perrin, 1996] Une transvection est une application linéaire bijective admettant un hyperplan de points fixes. Soit t une transvection d'hyperplan H. Alors il existe une forme linéaire f telle que $H = Ker(f)$ et $\omega \in H$ non nul tel que : $t(x) = x + f(x).\omega$.

II. Dualité

II.1. *Dual*

Définition. [Grifone, 1990] Définition de la base duale. Isomorphisme non canonique entre E et E^*.

Exemple. Exemple de la détermination d'une base duale.

Application. [ORAUX X-ENS ALGEBRE 1]

(1) L'application $f : M_n(\mathbb{K}) \to M_n(\mathbb{K})^*$ définie par $A \mapsto (X \mapsto Tr(AX)$ est un isomorphisme.

(2) Si $f \in M_n(\mathbb{K})^*$ et que $f(XY) = f(YX)$. Alors il existe $\lambda \in \mathbb{K}$ tel que $f = \lambda Tr(\cdot)$.

(3) Tout hyperplan de $M_n(\mathbb{K})$ rencontre $GL_n(\mathbb{K})$.

Définition. [Gourdon, 1994b] On appelle bidual de E, noté E^{**} le dual de E^*.

Proposition. L'application $\phi : E \to E^{**}$ définie par $x \mapsto (\phi_x : f \mapsto f(x))$ est un isomorphisme canonique.

Analogie. [Peyré, 2004] On observe le même phénomène lors de l'étude des représentations et des caractères. Un groupe G abélien fini et son dual $\hat{G}$ sont isomorphes (isomorphisme de groupes) de manière non canonique, mais G et son bidual son isomorphes de manière canonique. Par ailleurs remarquons que l'étude des caractères repose sur l'étude de l'image de la trace sur les éléments de l'image d'une représentation.

Base antéduale. Définition de la base antéduale.

II.2. *Orthogonalité au sens du dual.*

Définition. [Gourdon, 1994b] Définition de l'orthogonal d'un sous ensemble F de E : $F^\perp = \{\varphi \in E^* | \varphi(v) = 0 \forall v \in F\} \subset E^*$. C'est un sous-espace vectoriel. Définition de l'orthogonal d'un sous-ensemble A de E^* : $A^o = \{x \in E | \varphi(x) = 0 \forall \varphi \in A\} \subset E$. C'est un sous-espace vectoriel de E.

Proposition.

(1) On a $dim(E) = dim(F) + dim(F)^o$.
(2) Le double orthogonal laisse stable l'espace.

Remarque. Faux en dimension infinie. Contre-exemple.

Équations d'un sous-espace vectoriel en dimension finie.

Exemple. Exemple d'obtention de l'équation d'un sous espace vectoriel. [Grifone, 1990]

III. Applications.

III.1. *Calcul différentiel*

Théorème des extrémas liés. [Beck et al., 2004]

Applications.

(1) Orthodiagonalisation des matrices symétriques réelles.
(2) $SO_n(\mathbb{R})$ est l'ensemble des éléments de $SL_n(\mathbb{R})$ de norme minimale.

III.2. *Formes quadratiques.*

Dual et matrice de formes quadratiques. Les notions de rang et de noyau pour une forme bilinéaire symétrique sont définies comme le rang et le noyau de l'application linéaire : $\phi : E \to E^*$ définie par $y \mapsto (j_y : x \mapsto b(x, y)$.

Existence de bases orthogonales pour les formes quadratiques. (Preuve par récurrence sur la dimension utilisant l'orthogonalité au sens des formes linéaires.

Réduction de Gauss. Réduction d'une forme quadratique comme somme et différence de carrés de formes linéaires indépendantes.

Exemple d'une réduction de Gauss.

Formes quadratiques de Henkel. [Caldero and Germoni, 2013]

III.3. *Transposée, réduction.*

Définition. [Gourdon, 1994b] Soient E et F deux $\mathbb{K}$ espaces vectoriels. Soit $u \in \mathcal{L}(E, F)$. Pour tout $f \in F^*$, on a $f \circ u \in E^*$. L'application $F^* \to E^*$ définie par $f \mapsto f \circ u$ est appelée application transposée de u et est notée ${}^t u$.

Proposition.

(1) ${}^t(u \circ v) = {}^t v \circ {}^t u$.

(2) $Mat({}^t u) = {}^t(Mat(u))$.

Proposition. Soit F un sous-espace vectoriel de E et u un endomorphisme. Alors F est stable par u si et seulement si $F^\perp$ est stable par ${}^t u$

Corollaire. Si $x \in E^*$ est un vecteur propre de ${}^t u$ alors $(\mathbb{K}x)^o$ est un hyperplan de E stable par u.

Applications.

(1) On peut donc démontrer qu'un endomorphisme est diagonalisable si et seulement si sont polynôme caractéristique est scindé.

(2) Deux endomorphismes trigonalisables qui commutent son cotrigonalisables.

32. 160 : Endomorphismes remarquables d'un espace vectoriel euclidien (en dimension finie).

On se place sur un espace euclidien $(E, \langle \cdot, \cdot \rangle)$

I. Endomorphisme adjoint.

I.1. *Propriétés de l'adjoint.*

Définition. [Grifone, 1990] Définition de l'endomorphisme adjoint. Matrice de l'endomorphisme adjoint.

Proposition. on a :

(1) $f^{**} = f$
(2) $(\lambda f)^* = \lambda f^*$ et $(f+g)^* = f^* + g^*$
(3) $rgf^* = rgf$
(4) $(f \circ g)^* = g^* \circ f^*$

I.2. *Adjoints remarquables*

Définition. [Gourdon, 1994b] Un endomorphisme f est dit normal lorsque f et f^* commutent.

Exemples.

(1) Endomorphismes symétriques.
(2) Endomorphismes antisymétriques.
(3) Endomorphismes orthogonaux.

II. Réduction des endomorphismes normaux.

Proposition. [Gourdon, 1994b]

(1) Soit f un endomorphisme normal et F un sous-espace stable par f. Alors $F^\perp$ est stable par f^*.
(2) Soit E_λ un espace propre de f normal. Alors E_λ et $E_\lambda^\perp$ sont stables par f et f^*.

Théorème. Théorème de réduction des endomorphismes normaux.

Application. Réduction des endomorphismes antisymétriques.

Corollaire. En dimension impaire, un endomorphisme antisymétrique n'est jamais inversible.

III. Endomorsphismes orthogonaux.

Remarque. Structure de groupe de $\mathcal{O}(E)$.

Proposition. [Grifone, 1990] Soit $f \in \mathcal{O}(E)$. Les conditions suivantes sont équivalentes :

(1) $\langle f(x), f(y) \rangle = \langle x, y \rangle$

(2) $||f(x)|| = ||x||$

(3) Si $\mathcal{B}$ est une base orthonormée de E, $\text{Mat}_{\mathcal{B}}(f) \in O_n(\mathbb{R})$

Remarque. La matrice de passage d'une base orthonormée à une base orthonormée est orthogonale.

Proposition. Si f est orthogonal, son spectre est inclu dans $\{\pm 1\}$.

Contre-exemple. $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ a pour déterminant 1 mais n'est pas orthogonale.

Définition. Définition du groupe spécial orthogonal. C'est un sous-groupe distingué.

Proposition. Le groupe orthogonal et le groupe spécial orthogonal sont compacts.

Cas de la dimension 2. Structures de $\mathrm{SO}_2(\mathbb{R})$ et de $\mathrm{O}_2(\mathbb{R}) \setminus \mathrm{SO}_2(\mathbb{R})$.

Cas de la dimension 3. Structure de $\mathrm{O}_3(\mathbb{R})$.

Application. Un exemple.

Réduction des endomorphismes orthogonaux. Réduction en dimension quelconque.

Application. Connexité par arcs de $SO_n(\mathbb{R})$.

Génération. [Perrin, 1996] Le groupe orthogonal est engendré par les réflexions orthogonales. Le groupe spécial orthogonal est engendré par les retournements orthogonaux (symétries par rapport à un sous-espace de codimension 2).

Proposition. Le groupe spécial orthogonal SO_3 est simple.

IV. Endomorphismes symétriques.

Proposition. [Grifone, 1990] Somme directe des matrices symétriques et antisymétriques.

Proposition. Orthodiagonalisation des matrices symétriques réelles.

Contre-exemple. Faux sur $\mathbb{C}$.

Définition. Définition des matrices symétriques positives et définies positives.

Remarque. Lien entre les formes quadratiques et les matrices symétriques. Une matrice symétrique définie positive définit un produit scalaire.

Réduction simultanée.

Application. [ORAUX X-ENS] Ellipsoïde de John Loewner.

Proposition. Coorthogonalisation d'endomorphismes symétriques qui commutent.

Application. Existence et unicité de la racine carrée d'un endomorphisme symétrique positif.

Décomposition polaire. [Mneimné and Testard, 1986]

33. 170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Exemples et applications.

On se place sur un corps $\mathbb{K}$ de caractéristique différente de 2.

I. Formes bilinéaires symétriques et formes quadratiques

I.1. *Formes bilinéaires symétriques*

Définition. [Grifone, 1990] Définition d'une forme bilinéaire symétrique. Définition de la matrice d'une forme bilinéaire symétrique dans une base. La matrice est symétrique.

Exemple. La forme bilinéaire $b(x, y) = x_1y_1 - 2x_2y_2 + 6x_1y_2$ est symétrique et a pour matrice : $B = \begin{pmatrix} 1 & 3 \\ 3 & -2 \end{pmatrix}$

Expression matricielle. Si $X = \mathrm{Mat}(x)$, $Y = \mathrm{Mat}(y)$ et $B = \mathrm{Mat}(b)$ alors $b(x, y) = {}^tXBY$

Changement de base. Si $B = \mathrm{Mat}_{B_1}(b)$ et $B' = \mathrm{Mat}_{B_2}(b)$ alors en notant $P = P_{B_1}^{B_2}$, on a : $B' = {}^tPBP$. On dit que B et B' sont congruentes.

Définition. Définition du rang d'une forme bilinéaire comme le rang de sa matrice (indépendance par rapport à la base). Définition d'une forme bilinéaire non dégénérée.

Exemples. [Grifone, 1990]

(1) Un produit scalaire ou la forme de Lorentz sont non dégénérées.
(2) Un exemple d'une forme quadratique dégénérée.

Définition.

(1) Le rang de b est égal au rang de l'application $j : y \mapsto b(\cdot, y)$ qui va de E dans E^*.
(2) On appelle noyau de b l'ensemble $\{y \in E | b(x, y) = 0 \forall x \in E\}$. C'est aussi le noyau de la matrice de j.
(3) La forme b est non dégénérée si et seulement si j est injective, i.e si et seulement si $(\forall x \in E, b(x, y) = 0) \Rightarrow y = 0$.

Exemple. Exemple de calcul d'un noyau.

I.2. *Formes quadratiques*

Définition. Définition d'une forme quadratique réelle comme un polynôme homogène de degré 2.

Proposition. Il y a une correspondance bijective entre l'ensemble des formes bilinéaires symétriques et l'ensemble des formes quadratiques.

Exemple. Exemple d'un passage forme quadratique à forme bilinéaire.

Proposition.

(1) Définition du rang, noyau et noyau d'une forme quadratique comme celui de la forme polaire associée.
(2) Définition du discriminant d'une forme quadratique. Il n'est défini que à un carré du corps près.
(3) Définition d'une forme quadratique positive, définie.

I.3. *Isotropie*

Définition. Définition du cône isotrope d'une forme quadratique. $C(q) = \{x \in E | q(x) = 0\}$. On a $\text{Ker}(q) \subset C(q)$

Exemples. On peut être non dégénérée et avoir un cône isotrope non vide.
(1) $q(x) = x_1^2 + x_2^2$. $C = \{x_1 = \pm x_2\}$.
(2) $q(x) = x_1^2 + x_2^2 - x_3^2$. $C = \{x_3 = \pm\sqrt{x_1^2 + x_2^2}\}$

I.4. *Orthogonalité*

Définition. Définition de l'orthogonal d'une partie A : $A^\perp = \{x \in E | \forall a \in A, b(x, a) = 0\}$

Proposition.
(1) $A^\perp$ est un sous espace vectoriel de E.
(2) $E^\perp = \text{Ker}(q)$
(3) Si A est un sev, $\dim(E) = \dim(A) + \dim(A^\perp) - \dim(A \cap \text{Ker}(q)$.
(4) Si A est un sev, $A^{\perp\perp} = A + \text{Ker}(q)$.
(5) Si A est un sev, on a $E = A \oplus A^\perp$ si et seulement si A est non isotrope, i.e $A^\perp \cap A = \{0\}$.

II. Réduction des formes quadratiques, conséquences.

II.1. *Bases orthogonales, réductions des formes quadratiques.*

Remarque. [Perrin, 1996] Classifier les formes quadratiques c'est trouver l'ensemble des classes d'équivalences pour la relation d'équivalence $q_1 \sim q_2 \Leftrightarrow q_1$ congruente à q_2.

Proposition. [Perrin, 1996] Condition nécessaire de congruence :
(1) Égalité des rangs.
(2) Égalité des discriminants dans $\mathbb{K}/\mathbb{K}^{*2}$

Condition non suffisante. Considérer $x^2 + y^2$ et $-x^2 - y^2$. Même discriminant mais non congruentes.

Définition. Définition d'une base orthogonale et d'une base orthonormée pour une forme quadratique.

Théorème. [Perrin, 1996] Existence d'une base orthogonale pour une forme quadratique.

Proposition. Réduction de Gauss d'une forme quadratique.

Exemple. Exemple d'une réduction de Gauss. Et obtention d'une base orthogonale.

Classification des fomes quadratiques sur $\mathbb{C}$ (ou un corps algébriquement clos) Il y a $n+1$ classes d'équivalences de formes quadratiques sur $\mathbb{C}$. Chaque classe est entièrement déterminée par le rang.

Classification réelle. Théorème d'inertie de Sylvester. Introduction de la signature. Il y a $\frac{(n+1)(n+2)}{2}$ classes d'équivalences de formes quadratiques réelles. Chaque classe est entièrement déterminée par la signature.

Classification sur les corps finis. [Perrin, 1996] Soit $\mathbb{F}_q^{*2}$ un corps fini de caractéristique différente de 2. Soit $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_q^{*2}$. Alors il y a deux classes d'équivalences pour les formes quadratiques non dégénérées sur $\mathbb{F}_q$:

$$I_n \text{ et } \operatorname{diag}(1, \cdots, 1, \alpha).$$

Une forme quadratique est dans la même classe de congruence que l'identité si son discriminant est un carré dans $\mathbb{F}_q$ et dans l'autre si son discriminant n'est pas un carré. Il y a donc $2n+1$ classes d'équivalences de formes quadratiques sur $\mathbb{F}_q$.

Réduction simultanée dans le cas réel. Réduction d'une forme quadratique dans un espace qui possède une structure euclidienne.

Exemple. Obtention d'une base orthogonale à la fois pour q et pour $\langle \cdot, \cdot \rangle$.

Application. [ORAUX X-ENS] Ellipsoïde de John Loewner.

II.2. *Groupe orthogonal d'une forme quadratique.*

Définition. Définition de l'adjoint pour une forme quadratique non dégénérée.

Exemple. Exemple de l'obtention de l'adjoint d'une matrice A pour la forme quadratique $q(x) = x_1^2 - x_2^2$.

Définition. Définition du groupe orthogonal et du groupe spécial orthogonal.

Remarque. Si les formes quadratiques sont dans la même classe d'équivalence, les groupes orthogonaux sont isomorphes.

Proposition. Compacité du groupe orthogonal si et seulement si la forme quadratique est définie positive ou définie négative.

Proposition. Générateurs du groupe orthogonal.

Définition. [Perrin, 1996] Définition d'un plan hyperbolique.

Proposition. Si x est un vecteur isotrope, il existe un plan hyperbolique le contenant.

Définition. Définition d'un espace hyperbolique.

Proposition. Décomposition $E = \oplus_{i=1}^r P_i \oplus U$ avec P_i plan hyperbolique et U anisotrope.

Théorème de Witt. Soient F et F' deux sous-espaces de E, on a l'équivalence :

(1) Il existe $u \in O(q)$ tel que $u(F) = F'$

(2) Les formes $q_{|F}$ et $q_{|F'}$ sont équivalentes.

III. Applications.

III.1. *Classification des coniques*

Conique affines Il existe 8 coniques affines.

Coniques affines euclidiennes non dégénérées [Grifone, 1990] Il existe une infinité de coniques affines euclidiennes non dégénérées.

Exemples. Dessin.

III.2. *Calcul différentiel*

[Beck et al., 2004]

Proposition. Condition du deuxième ordre sur la matrice hessienne pour la recherche d'extrema.

Exemples et contre exemples.

Lemme de Morse en dimension 2. [Rouvière, 1999]

Application. Étude de la position du plan tangent par rapport à une surface.

34. **171 : Formes quadratiques réelles. Exemples et applications.**

I. Premières définitions et propriétés.

I.1. *Formes bilinéaires symétriques*

Définition. [Grifone, 1990] Définition d'une forme bilinéaire symétrique. Définition de la matrice d'une forme bilinéaire symétrique dans une base. La matrice est symétrique.

Exemple. La forme bilinéaire $b(x,y) = x_1y_1 - 2x_2y_2 + 6x_1y_2$ est symétrique et a pour matrice : $B = \begin{pmatrix} 1 & 3 \\ 3 & -2 \end{pmatrix}$

Expression matricielle. Si $X = \mathrm{Mat}(x)$, $Y = \mathrm{Mat}(y)$ et $B = \mathrm{Mat}(b)$ alors $b(x,y) = {}^tXBY$

Changement de base. Si $B = \mathrm{Mat}_{B_1}(b)$ et $B' = \mathrm{Mat}_{B_2}(b)$ alors en notant $P = P_{B_1}^{B_2}$, on a : $B' = {}^tPBP$. On dit que B et B' sont congruentes.

Définition. Définition du rang d'une forme quadratique comme le rang de sa matrice (indépendance par rapport à la base). Définition d'une forme quadratique non dégénérée.

Exemples. [Grifone, 1990]

(1) Un produit scalaire ou la forme de Lorentz sont non dégénérées.
(2) Un exemple d'une forme quadratique dégénérée.

Définition.

(1) Le rang de b est égal au rang de l'application $j : y \mapsto b(\cdot, y)$ qui va de E dans E^*.
(2) On appelle noyau de b l'ensemble $\{y \in E | b(x,y) = 0 \forall x \in E\}$. C'est aussi le noyau de la matrice de j.
(3) La forme b est non dégénérée si et seulement si j est injective, i.e si et seulement si $(\forall x \in E, b(x,y) = 0) \Rightarrow y = 0$.

Exemple. Exemple de calcul d'un noyau.

I.2. *Formes quadratiques*

Définition. Définition d'une forme quadratique réelle comme un polynôme homogène de degré 2.

Proposition. Il y a une correspondance bijective entre l'ensemble des formes bilinéaires symétriques et l'ensemble des formes quadratiques.

Exemple. Exemple d'un passage forme quadratique à forme bilinéaire.

Proposition.

(1) Définition du rang, noyau et noyau d'une forme quadratique comme celui de la forme polaire associée.
(2) Définition d'une forme quadratique positive, définie.

I.3. *Isotropie*

Définition. Définition du cône isotrope d'une forme quadratique. $C(q) = \{x \in E | q(x) = 0\}$. On a $\mathrm{Ker}(q) \subset C(q)$

Exemples. On peut être non dégénérée et avoir un cône isotrope non vide.

(1) $q(x) = x_1^2 + x_2^2$. $C = \{x_1 = \pm x_2\}$.
(2) $q(x) = x_1^2 + x_2^2 - x_3^2$. $C = \{x_3 = \pm\sqrt{x_1^2 + x_2^2}\}$

I.4. *Orthogonalité*

Définition. Définition de l'orthogonal d'une partie A : $A^\perp = \{x \in E | forall a \in A, b(x,a) = 0\}$

Proposition.

(1) $A^\perp$ est un sous espace vectoriel de E.
(2) $E^\perp = \mathrm{Ker}(q)$
(3) Si A est un sev, $\dim(E) = \dim(A) + \dim(A^\perp) - \dim(A \cap \mathrm{Ker}(q)$.
(4) Si A est un sev, $A^{\perp\perp} = A + \mathrm{Ker}(q)$.
(5) Si A est un sev, on a $E = A \oplus A^\perp$ si et seulement si A est non isotrope, i.e $A^\perp \cap A = \{0\}$.

II. Réduction des formes quadratiques

Définition. Définition d'une base orthogonale et d'une base orthonormée pour une forme quadratique.

Proposition. Réduction de Gauss d'une forme quadratique.

Exemple. Exemple d'une réduction de Gauss. Et obtention d'une base orthogonale.

Classification des fomes quadratiques sur $\mathbb{C}$

Classification réelle. Théorème d'inertie de Sylvester. Introduction de la signature.

Application. Il y a $\frac{(n+1)(n+2)}{2}$ classes d'équivalences de formes quadratiques réelles.

Réduction simultanée. Réduction d'une forme quadratique dans un espace qui possède une structure euclidienne.

Exemple. Obtention d'une base orthogonale à la fois pour q et pour $\langle \cdot, \cdot \rangle$.

Application. [ORAUX X-ENS] Ellipsoïde de John Loewner.

III. Groupe orthogonal.

Définition. Définition de l'adjoint pour une forme quadratique non dégénérée.

Exemple. Exemple de l'obtention de l'adjoint d'une matrice A pour la forme quadratique $q(x) = x_1^2 - x_2^2$.

Définition. Définition du groupe orthogonal et du groupe spécial orthogonal.

Proposition. Compacité du groupe orthogonal si et seulement si la forme quadratique est définie positive ou définie négative.

Proposition. Générateurs du groupe orthogonal.

IV. Applications.

IV.1. *Classification des coniques*

Conique affines [Audin, 2012]

Coniques affines euclidiennes [Grifone, 1990]

Exemples. Dessin.

IV.2. *Calcul différentiel*

[Beck et al., 2004]

Proposition. Condition du deuxième ordre sur la matrice hessienne pour la recherche d'extrema.

Exemples et contre exemples.

Lemme de Morse en dimension 2. [Rouvière, 1999]

Application. Étude de la position du plan tangent par rapport à une surface.

35. **183 : Utilisation des groupes en géométrie.**

I. Géométrie affine

I.1. *Groupe affine*

Cadre. [Audin, 2012] On note $\mathcal{E}$ un espace affine de dimension n, E l'espace vectoriel associé. On note $A(\mathcal{E})$ l'ensemble des applications affines de $\mathcal{E}$. C'est exactement l'ensemble des applications qui préservent les barycentres de $\mathcal{E}$.

Proposition. La seule transformation affine qui fixe $n+1$ points indépendants d'un espace affine de dimension n est l'identité.

Définition. Les bijections affines de $\mathcal{E}$ dans lui-même forment un groupe : le groupe affine $\mathcal{G}A(\mathcal{E})$.

Exemple.

(1) Une translation est une bijection affine.

(2) Une homothétie de centre O et de rapport λ (non nul) est une bijection affine.

Proposition. L'application $\mathcal{G}A(\mathcal{E}) \to GL(E)$ qui a une bijection affine associe sa partie linéaire est un homomorphisme surjectif de groupes, dont le noyau est le groupe des translations de $\mathcal{E}$.

I.2. *Coniques affines.*

Conique. [Audin, 2012] Soit f un polynôme à deux indéterminées de degré 2. On appelle conique affine l'ensemble des points vérifiants $f(M) = 0$.

Remarque. On ne distingue pas avec cette définition les coniques données par les équations $x^2 + y^2 + 1 = 0$ et $x^2 + 1 = 0$

Action du groupe linéaire sur les matrices symétriques. On définit une action de groupe de $GL_n(\mathbb{R})$ sur $S_n(\mathbb{R})$ par $(P, Q) \mapsto {}^tPSP$. Deux matrices S et S' sont dans la même orbite pour cette action sont dites équivalentes. Elles sont équivalentes si et seulement si elles représentent la même forme quadratiques dans deux bases différentes. Le théorème d'inertie de Sylvester affirme qu'un invariant totale pour cette action est la signature de la forme quadratique. Cette signature peut s'obtenir, par exemple, par réduction de Gauss.

Classification affine des coniques. A bijection affine prêt, il existe 8 coniques. Pour les classifier il faut effectuer un changement de base pour éliminer lorsque c'est possible le terme linéaire de f puis déterminer la signature de la forme quadratique.

(1) Signature $(2, 0)$: -Le cercle $x^2 + y^2 = 1$, -Le point : $x^2 + y^2 = 0$, -L'ensemble vide : $x^2 + y^2 = -1$

(2) Signature $(1, 1)$: -L'hyperbole $x^2 - y^2 = 1$, -Deux droites concourantes : $x^2 - y^2 = 0$.

(3) Signature $(1,0)$: -Deux droites parallèles $x^2 = 1$, Une droite : $x^2 = 0$, La parabole $x^2 + y = 0$, L'ensemble vide $x^2 = -1$.

II. Géométrie euclidienne.

Cadre. [Audin, 2012] On travaille désormais sur un espace affine euclidien.

Définition. On appelle isométrie affine toute application affine qui préserve la distance. On note $Isom(\mathcal{E})$ le groupe des isométries affines.

Exemples.

(1) Les translations sont des isométries.

(2) Les symétries orthogonales sont des isométries.

Proposition. L'application $Isom(\mathcal{E}) \to O(E)$ qui a une isométrie affine associe sa partie linéaire dans le groupe orthogonal est un homomorphisme surjectif de groupes, dont le noyau est le groupe des translations de $\mathcal{E}$.

Définition. On définit le sous-groupe des déplacements, noté $Isom^+(\mathcal{E})$ comme le noyau du déterminant.

Des résultats de structure sur $O_2(\mathbb{R})$ on déduit le théorème de structure suivant :

Proposition. Les isométries affines du plan affine euclidien sont :

(1) Si l'application linéaire est l'identité, on est face à une translation.

(2) Si l'application linéaire est une réflexion de droite D :
  - Ou bien l'isométrie a un point fixe A et on est face à une réflexion par rapport à la droite dirigée par D et passant par A.
  - Ou bien l'isométrie n'a pas de point fixe et on est face à une symétrie glissée. La composée commutative d'une translation de vecteur v dirigé par D et d'une réflexion de droite dirigée par D.

(3) Si l'application linéaire est une rotation (non triviale) alors on est face à une rotation de centre l'unique point fixe A et de même angle que la rotation.

II.1. *Coniques euclidiennes.*

Réduction des formes quadratiques. [Audin, 2012] Étant donnée une forme quadratique sur un espace euclidien, on peut trouver une base de diagonalisation de la forme quadratique, qui soit orthonormée pour le produit scalaire de l'espace.

Application. Ellipsoïde de John-Loewner.

Classification des coniques euclidiennes propres. On veut classifier les coniques euclidiennes propres non vides à isométrie affine près :

(1) $(2,0)$: $\frac{x^2}{a} + \frac{y^2}{b} = 1$ avec $0 < a \leq b$. Une infinité d'orbites d'ellipses.

(2) $(1,1)$: $\frac{x^2}{a} + \frac{y^2}{b} = 1$. Une infinité d'orbites d'hyperboles.

(3) $(1,0)$: $y^2 = 2px$. Une infinité d'orbites de paraboles.

II.2. *Sous-groupes de* $Isom(\mathcal{E}$.

Remarque. [Ulmer, 2005] Les éléments de U_n sont les sommets du polygône régulier à n côtés P_n.

Définition. Pour $n \geq 3$, le groupe diédral D_n est le groupe des isométries du plan affine qui laissent invariant P_n.

Proposition. Le groupe diédral est d'ordre $2n$ et il est engendré par la symétrie axiale $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et la rotation d'angle $\theta = \frac{2\pi}{n}$, $r = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$.

Proposition. Le groupe $\langle r \rangle$ est isomorphe à U_n et il est distingué dans D_n. On a les relations $r^n = e$, $s^2 = e$, et $srs = r^{-1}$

Application. Détermination des caractère irréductibles de degré 1 de D_n. $\chi(s)^2 = \chi(s^2) = \chi(e) = 1$ d'où $\chi(s) = \pm 1$ et $\chi(r) = \pm 1$.

Groupe dérivé. Le groupe dérivé de D_n est $\langle r^2 \rangle$. C'est $\langle r \rangle$ si et seulement si n est impair.

Définition. [Caldero and Germoni, 2013] Définition d'un solide platonicien.

Proposition.

(1) Le groupe d'isométries du tétraèdre est $\mathcal{S}_4$. Le groupe des déplacements du tétraèdre est $\mathcal{A}_4$.

(2) Le groupe des déplacements du cube est $\mathcal{S}_4$. Le groupe des isométries du cube est $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Application. [Serre, 1967] On en déduit un caractère irréductible de degré 3 de $\mathcal{S}_4$. Qui vaut $3, -1, 0, 1, -1$ (Identité, 2-cycle, 3-cycle, 4-cycle, 2 fois 2 cycle à supports disjoints).

III. Géométrie projective.

Définitions. [Perrin, 1996] Définition de la droite projective complexe. En dimension $n = 2$: Définition du groupe projectif complexe et réel. Du groupe spécial projectif complexe et réel.

Remarque. Dans le cas $n = 2$. Il y a un isomorphisme entre le groupe projectif complexe et le groupe spécial projectif complexe. Il y a un isomorphisme entre le groupe projectif réel dont un des représentant a un déterminant strictement positif et le groupe spécial projectif réel.

Proposition. [Caldero and Germoni, 2013] L'action du groupe projectif complexe sur la droite projective est trois fois simplement transitive.

Définition. Définition du birapport.

Proposition. [Audin, 2012] Expression calculatoire du birapport. Le birapport de 4 points est réel si et seulement si les 4 points sont cocycliques ou alignés.

Corollaire. Toute homographie de la droite projective complexe transforme un cercle/droite en un cercle/droite.

Proposition.

Théorème. [TOUT-EN-UN POUR LA LICENCE] [MÉRINDOL-Nombres et algèbre]
— $\mathbb{P}SL_2(\mathbb{R})$ agit transitivement sur le demi-plan de Poincarré.
— $\mathbb{P}SL_2(\mathbb{R})$ agit transitivement sur l'ensemble des droites hyperboliques.

36. **190 : Méthodes combinatoires, problèmes de dénombrement.**

I. Outils pour le dénombrement.

Remarque. Le principe de récurrence et les relations de récurrence linéaires sont très utiles pour compter des objets.

Exemple. Le cardinal de $\mathcal{S}_n$ est $n!$.

Cardinal d'un ensemble partitionné. Si $E = \bigcup_{i=1}^r E_i$ (union disjointe), alors $|E| = \sum_{i=1}^{r} |E_i|$.

Formule du crible. Dans ce cas d'une union non disjointe, on a la formule du crible, plus souvent utilisée dans le cas $r = 2$. Si $E = \bigcup_{i=1}^r E_i$ alors :

$$|E| = \sum_{i=1}^{r} |E_i| - \sum_{i<j} |E_i \cap E_j| + \sum_{i<j<k} |E_i \cap E_j \cap E_k| - \cdots (-1)^n \left| \bigcap_{i=1}^{n} E_i \right|.$$

Cardinal du produit cartésien. Le cardinal du produit cartésien d'ensembles finis est le produit des cardinaux des ensembles.

Application. Démonstration du théorème de Kronecker. Plus précisément, le cardinal des polynômes à coefficients dans $\mathbb{Z}$, de terme constant non nul, dont toutes les racines complexes sont de module inférieur ou égal à 1 est fini.

Bijection. Si deux ensembles sont en bijection, ils ont même cardinal.

Arrangement. Soit $1 \leq k \leq n$. Un k arrangement d'un ensemble fini de cardinal n est une application injective de $[\![1, k]\!]$ dans $[\![1, n]\!]$, on note le nombre d'arrangements A_n^k. On a $A_n^k = \frac{n!}{(n-k)!}$.

Exemple. Tirage ordonné de boules sans remise. Chance de gagner au tiercé.

Combinaison. Une k combinaison d'un ensemble à n élements est une partie de cet ensemble qui contient k éléments. On note $\binom{n}{k}$ le nombre de k combinaisons d'un ensemble à n éléments.

Exemple. Loi binomiale. Probabilité de gagner au loto.

II. Fonctions génératrices.

Définition. Soit $(a_n)_{n\in\mathbb{N}}$ une suite de réels ou de complexes. On appelle série génératrice de (a_n) la série formelle $\sum_{n\in\mathbb{N}} a_n X^n$. Pour les besoins de l'analyse, on appelle série génératrice exponentielle de (a_n) la série formelle : $\sum_{n\in\mathbb{N}} \frac{a_n}{n!} X^n$.

Remarque. En pratique, les a_n ont une signification combinatoire, et on ne peut pas les déterminer un par un. On peut par diverses méthodes (développements de fractions rationnelles, équations différentielles) déterminer la série génératrice de (a_n).

Nombre de dérangements d'un ensemble à n éléments. [X-ENS algèbre 1]

Calcul du cardinal d'un arbre binaire à n noeuds. [Moisan et al., 1992] [X-ENS algèbre 1]

Calcul du nombre de relations d'équivalences sur l'ensemble $\{1, \cdots, n\}$ [Pommelet, 1994]

Partitions d'un entiers en parts fixées. [X-ENS algèbre 2]

III. Indicatrice d'Euler et fonction de Moëbius.

III.1. *Indicatrice d'Euler.*

Définition. On note $\varphi(k) = |\{k \in [\![1, n]\!] | p.g.c.d(k, n) = 1\}|$. On appelle indicatrice d'Euler cette fonction.

Premiers calculs. Pour p premier, on a $\varphi(p) = p - 1$ et $\varphi(p^{\alpha)} = p^{\alpha-1}(p - 1)$.

Lemme Chinois. Si p et q sont premiers entre eux, on a l'isomorphisme $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. De fait pour m et n premiers entre eux : $\varphi(mn) = \varphi(m)\varphi(n)$.

Application. D'après le théorème fondamental de l'arithmétique, on peut ainsi calculer $\varphi(n)$ pour tout entier naturel $n \in \mathbb{N}$.

III.2. *Fonction de Moëbius.*

Proposition. [FRANCINOU GIANELLA-Exercices d'algèbres pour l'agrégation.] Si on note $\mathcal{A}(n, q) = \{P \in \mathbb{F}_q[X] |$ irréductible, unitaire, de degré $n\}$ alors on a la formule :

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

Formule d'inversion de Moëbius. Soit $f : \mathbb{N} \to \mathbb{R}$ et $g : \mathbb{N} \to \mathbb{R}$ défini par $g(n) = \sum\limits_{d|n} f(d)$. Alors on a la formule d'inversion :

$$f(n) = \sum_{d|n} \mu(n/d)g(d) = \sum_{d|n} d(n/d)\mu(d).$$

Dénombrement des polynômes irréductibles. On note $I(n, q) = |\mathcal{A}(d, q)|$. Alors on a : $nI(n, q) = \sum_{d|n} \mu(\frac{n}{d})q^d$ et $I(n, q) \sim \frac{q^n}{n}$.

IV. Dénombrement par la théorie des groupes.

IV.1. *Résultats utilisés.*

Remarque. Ces techniques utilisent principalement deux résultats, la propriété universelle du quotient, et la formule des classes.

Propriété universelle du quotient. [Ulmer, 2005] Soit G_1 et G_2 deux groupes. Soit $H \triangleleft G_1$ et $\varphi : G_1 \to G_2$ un morphisme de groupes. Alors les propriétés suivantes sont équivalentes :

(1) $H \subset \mathrm{Ker}(\varphi)$
(2) Le morphisme φ se factorise à travers G_1/H. Il existe un unique morphisme de groupes $\overline{\varphi} : G_1/H \to G_2$ tel que $\varphi = \overline{\varphi} \circ \pi$.

De plus $\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi)$ et $\mathrm{Ker}(\overline{\varphi}) = \mathrm{Ker}(\varphi)/H$.

Corollaire. Théorème d'isomorphisme. On a donc $\mathrm{Im}(\varphi) \cong G_1/\mathrm{Ker}(\varphi)$.

Exemple. Le cardinal de $\mathcal{A}_n$ est $\frac{n!}{2}$.

Proposition.

(1) La relation être dans la même orbite est une relation d'équivalence sur X.
(2) Le cardinal du stabilisateur est constant le long d'une orbite : $\mathrm{Stab}_G(g \cdot x) = g\mathrm{Stab}_G(x)g^{-1}$.
(3) $|G| = |\mathcal{O}_x||\mathrm{Stab}_G(x)|$.

Formule des classes. Soit $(x_1, \cdots, x_r)$ un système de représentant d'orbites alors on a : $|X| = \sum_{i=1}^{r} \frac{|G|}{\mathrm{Stab}_G(x_i)}$

Mentionnons également la formule de Burnside. **Formule de Burnside.**

Application. Classification des sous-groupes finis de $SO_3(\mathbb{R})$.

IV.2. *Problèmes de dénombrements sur les corps finis.*

Quelques cardinaux. [Perrin, 1996]

(1) Cardinal de $GL_n(\mathbb{F}_q)$ (Dénombrement des bases)
(2) Cardinal de $SL_n(\mathbb{F}_q)$ (Propriété universelle du quotient)

Proposition. (Formule des classes) [Caldero and Germoni, 2013] Soit $n \geq 1$. Alors le cardinal des matrices diagonalisables de $\mathrm{GL}_n(\mathbb{F}_q)$ est égal à :

$$\sum_{n_1+\cdots+n_{q-1}=n} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbb{F}_q)|\cdots|\mathrm{GL}_{n_{q-1}}(\mathbb{F}_q)|}.$$

Dénombrement des carrés dans $\mathbb{F}_q$. (Propriété universelle du quotient.) [Perrin, 1996]

Corollaire. [Perrin, 1996] L'équation $ax^2 + by^2 = 1$ avec a et b dans $\mathbb{F}_q^*$ a des solutions dans $\mathbb{F}_q$.

Conséquence. Classification des formes quadratiques sur $\mathbb{F}_q$.

37. **201 : Espaces de fonctions. Exemples et applications.**

I. Fonctions régulières

I.1. *L'espace des fonctions continues.*

On travaille sur $\mathcal{C}(K,\mathbb{R})$, où (K,d) est un espace métrique compact.

Proposition. [Hirsch and Lacombe, 1997]

(1) (K,d) est séparable.
(2) Une limite uniforme de fonctions continues est continue.
(3) $(\mathcal{C}(K,\mathbb{R}),||\cdot||)$ est un espace de Banach séparable.

Proposition. [Hirsch and Lacombe, 1997]

(1) Lemme de Dini 1
(2) Lemme de Dini 2

Théorème (de Weierstrass) dans le cas où $K=[a,b]$. [Hirsch and Lacombe, 1997]

Contre-exemples. Faux sur $\mathbb{R}$, car une limite uniforme de polynômes sur $\mathbb{R}$ est un polynôme.

Application. [Pommelet, 1994] Théorème des moments : Si pour tout $k\in\mathbb{N}$, $\int_a^b f(t)x^k\mathrm{d}t=0$, alors f est identiquement nulle. Et injectivité de la transformée de Laplace.

Application.

(1) On donne un exemple de fonction continue nulle part dérivable sur $[a,b]$. [Gourdon, 1994a]
(2) Par Weierstrass, ces fonctions sont denses dans $\mathcal{C}(K,\mathbb{R}),||\cdot||$.
(3) Par Baire, il existe un G_δ dense de telles fonctions.

Théorème (Müntz) Juste le critère pour que $\mathrm{Vect}(\{1,x^{\alpha_n}\})$ soit dense dans $\mathcal{C}(K,\mathbb{R}),||\cdot||$. [Gourdon, 1994a]

Proposition. Les fonctions escaliers sont denses dans $\mathcal{C}(K,\mathbb{R}),||\cdot||$. [Queffélec and Zuily, 2013]

Définition.

(1) Définition d'équicontinuité et d'uniforme équicontinuité.
(2) Heine équicontinue et Heine uniformément équicontinue.

Théorème d'Ascoli. [Hirsch and Lacombe, 1997]

Applications.

(1) Cauchy-Peano
(2) Montel.
(3) Compacité de l'opérateur $T:f\longmapsto(Tf:x\mapsto\int_a^b K(x,y)f(y)\mathrm{d}y)$.
(4) Riesz Fréchet Kolmogorov.

I.2. *Fonctions holomorphes.*

On travaille sur $\mathcal{H}(\Omega)$ où Ω est un ouvert de $\mathbb{C}$

Définition. [Queffélec and Zuily, 2013] topologie de la convergence uniforme sur tout compact.

Proposition. La convergence d'une suite de fonctions dans $\mathcal{H}(\Omega)$ est très forte. Elle implique l'holomorphie à la limite et la convergence de toutes les suites des dérivés.

Proposition. [Queffélec and Zuily, 2013] Définition d'une suite exhaustive de compact. Définition d'une distance pour métriser la topologie de $\mathcal{H}(\Omega)$.

Théorème de Montel.

Application. Il n'existe pas de norme sur $\mathcal{H}(\Omega)$ qui définisse la même topologie que la distance.

II. Espaces de fonctions mesurables

II.1. *Les espaces* $\mathbb{L}^p$

Définition. des espaces $\mathbb{L}^p$ et des normes associées.

Proposition. Hölder et Minkowski d'où l'on déduit que $\mathbb{L}^p$ est un espace vectoriel normé. [Brezis, 1983]

Application. Injections topologiques décroissante des $\mathbb{L}^p$ lorsque l'espace est de mesure finie.

Théorème. (Riesz-Fisher) [Brezis, 1983]

(1) $\mathbb{L}^p$ est un espace de Banach
(2) De toute suite convergeant dans $\mathbb{L}^p$ on peut extraire une sous-suite convergeant presque partout.

Théorème de Grothendieck. sur les sous-espaces vectoriels fermés de $\mathbb{L}^p$ [Rudin-Analyse fonctionnelle]

Proposition.

(1) Densité des fonctions continues à support compact. [Hirsch and Lacombe, 1997]
(2) Densité de $\mathbb{L}^1 \bigcap \mathbb{L}^\infty$ est dense dans $\mathbb{L}^p$. [Hirsch and Lacombe, 1997]
(3) Densité des fonctions infiniment dérivables à support compact dans $\mathbb{L}^p$. [Brezis, 1983] [Hirsch and Lacombe, 1997]

Applications.

(1) Inégalité de Hardy.
(2) Caractérisation des parties relativement compactes dans $\mathbb{L}^p$ (Fréchet-Kolmogorov, admis). [Hirsch and Lacombe, 1997]
(3) Prolongement de la transformée de Fourier en transformée de Fourier Plancherel.

II.2. *Le cas particulier de* $\mathbb{L}^2$

Théorème. Produit scalaire sur $\mathbb{L}^2$ qui en fait un espace de Hilbert.

Proposition. Caractérisation des parties denses de $\mathbb{L}^2$ par l'orthogonalité.

Théorème. Condition suffisante pour qu'une famille de polynômes orthogonaux forme une base hilbertienne de $\mathbb{L}^2$. [Beck et al., 2004]

Théorème de Lax-Milgram [Hirsch and Lacombe, 1997]

Remarque. Ce théorème permet de conclure à l'existence et l'unicité de solutions à des équations aux dérivées partielles élliptiques lorsque l'on travaille sur H^1 qui est un raffinement de $\mathbb{L}^2$.

Proposition.

(1) Base hilbertienne de $\mathbb{L}^2([0, 2\pi])$. [Beck et al., 2004]

(2) Convergence en norme $\mathbb{L}^2$ de la série de Fourier vers la fonction.

(3) Formule de Parseval.

Application. Calcul de sommes de séries. [Gourdon, 1994a]

Application. Inégalité Isopérimétrique.

38. **202 : Exemples de parties denses. Applications.**

I. Résultats théoriques.

Définition. Partie dense dans un espace métrique.

Définition. Espace séparable. [Hirsch and Lacombe, 1997]

Proposition. Une forme linéaire est continue ssi son noyau est fermé. [Pommelet, 1994]

Exemple. $\{f \in \mathcal{C}([0,1]) \mid f(0)=0\}$ est fermé dans $(\mathcal{C}([0,1]), ||\cdot||_\infty)$ et dense dans $(\mathcal{C}([0,1]), ||\cdot||_1)$ [Pommelet, 1994]

Proposition. Si deux fonctions continues coïncident sur un sous-ensemble dense, elles sont égales.

Prolongement. Prolongement des applications uniforméments continues. [Pommelet, 1994]

Théorème. Existence du complété d'un espace métrique.

II. Parties denses en dimension finies.

II.1. *Parties denses dans* $(\mathbb{R}, |\cdot|)$.

Proposition. $\mathbb{Q}$ est dense dans $\mathbb{R}$

Applications.

(1) Tout espace vectoriel normé de dimension finie sur $\mathbb{R}$ ou $\mathbb{C}$ est séparable.

(2) L'identité est le seul morphisme de corps sur $\mathbb{R}$.

(3) Détermination de solutions continues à certaines équations fonctionnelles. $f(x+y) = f(x) + f(y)$

Structure des sous-groupes de $\mathbb{R}$ Ils sont soit denses, soit de la forme $n\mathbb{Z}$. [Gourdon, 1994a]

Proposition $a\mathbb{Z} + b\mathbb{Z}$ est dense dans $\mathbb{R}$ ssi $\frac{a}{b}$ n'est pas rationnel. [Gourdon, 1994a]

Application. $sin(\mathbb{Z})$ est dense dans $[0,1]$.

II.2. *Parties denses dans* $M_n(\mathbb{K})$

Proposition. Les matrices de rang r sont denses dans l'ensemble des matrices de rang inférieur ou égal à r. En particulier, les matrices inversibles sont denses dans l'ensemble des matrices. [Gourdon-algèbre]

Applications.

(1) $C_{AB}(T) = C_{BA}(T)$ [ROMBALDI-Thèmes pour l'agrégation de mathématiques]

(2) différentielle du déterminant. [Gourdon, 1994a]

Proposition. Les matrices ayant n valeurs propres distinctes sont denses dans l'ensemble des matrices trigonalisables. En particulier elles sont denses dans les matrices complexes. [Gourdon, 1994a]

III. Parties denses en dimension infinie.

III.1. *Fonctions continues*

Théorème. Weierstrass [Hirsch and Lacombe, 1997] et Weierstrass trigonométrique.

Application. Théorème des moments.

Exemple d'une fonction continue nulle part dérivable. [Queffélec and Zuily, 2013]

Application de Weierstrass Les fonctions continues nulle part dérivables sont denses dans $(\mathcal{C}([0,1],\mathbb{R}), ||\cdot||)$.

Proposition. D'après Baire, elles forment même un G_δ dense. [Gourdon, 1994a]

Théorème. de Müntz.

Théorème. D'après Banach-Steinhaus, il existe un G_δ dense de fonctions continues $2\pi-$périodiques dont la série de Fourier diverge sur un ensemble contenant $\mathbb{Q}$. [Gourdon, 1994a]

Théorème. Ascoli (conséquence de la séparabilité d'un espace métrique compact).

III.2. *Parties denses dans $\mathbb{L}^p$.*

Proposition.

(1) Densité des fonctions étagées [Briane and Pages, 2000]
(2) Densité des fonctions continues à support compact. [Hirsch and Lacombe, 1997]

Proposition. Séparabilité des $\mathbb{L}^p$ pour $p \neq \infty$. [Brezis, 1983]

Proposition.

(1) Densité des fonctions infiniment dérivables à support compact. [Hirsch and Lacombe, 1997]
(2) Densité de $\mathbb{L}^1 \bigcap \mathbb{L}^2$ dans $\mathbb{L}^2$.

Applications.

(1) Riemann Lebesgue : Les coefficients de Fourier d'une fonction $\mathbb{L}^1$ tendent vers 0. [Gasquet and Witomski, 1990]
(2) Inégalité de Hardy. [Chambert-Loir, 1995]
(3) Prolongement de la transformée de Fourier en transformée de Fourier-Plancherel. [Gasquet and Witomski, 1990]

III.3. *Espaces de Hilberts.*

Proposition. Caractérisation de la densité par l'orthogonal. [Hirsch and Lacombe, 1997]

Proposition. Tout espace de Hilbert séparable admet une base de Hilbert dénombrable. [Hirsch and Lacombe, 1997]

Proposition. Condition suffisante pour qu'une famille de polynôme orthogonaux associée à un poids soit une base hilbertienne de $\mathbb{L}^2$. [Beck et al., 2004]

Définition. Définition de H^1 et H^1_0.

Remarque. Montrer comment on utilise ces espaces pour résoudre des EDPE.

39. **203 : Utilisation de la notion de compacité.**

I. Compacité : premières propriétés et applications.

La compacité est une propriété topologique qui permet de voir un ensemble infini comme un ensemble fini.

Propostion. [BONY-Cours d'Analyse]. Propriété de Borel-Lebesgue.

Proposition. Caractérisation de la compacité lorsque l'espace est métrique. (Bolzano-Weierstrass)

Proposition. Un espace métrique compact est séparable.

Proposition. Un espace métrique compact est complet.

Définition. D'un espace métrique précompact.

Proposition. Équivalence entre l'espace métrique est précompact et complet et l'espace topologique est compact.

Proposition. L'image continue d'un compact est compacte.

Applications.

(1) Ellipsoïde de John-Loewner.
(2) Simplicité de $\mathrm{SO}_3(R)$.

Proposition. Procédé d'extraction diagonale. [Hirsch and Lacombe, 1997]

Application. Théorème de Banach-Alaoglu (version Hilbert)

II. Compacité dans les espaces vectoriels normés.

Proposition. Une application continue d'un espace compact à valeurs dans $\mathbb{R}$ est bornée et atteint ses bornes.

Conséquence. En dimension finie, toutes les normes d'un espace vectoriel normé sont équivalentes. De plus les compacts d'un espace vectoriel normé sont exactement les fermés bornés.

Théorème. de Riesz. Un espace vectoriel normé est de dimension finie si et seulement si sa boule unité est relativement compacte.

Application. Un sous-espace vectoriel fermé de $\mathcal{C}^0$ qui est dans $\mathcal{C}^1$ est de dimension finie.

Définition. De la platitude. [RMS 119-4]

Proposition. Caractérisation des compacts dans les espaces de Banach. [RMS 119-4]

Application. Compacité du cube de Hilbert dans l^2. [RMS 119-4]

Application. Démonstration du sens le plus difficile dans le théorème d'Ascoli. [RMS 119-4]

III. Compacité et espace de fonctions continues.

Proposition. Théorème de Heine. Une application continue sur un compact est uniformément continue.

Application. Compacité de l'opérateur à noyau. $T : f \mapsto \left(x \mapsto \int_0^1 K(x,y)f(y)\mathrm{d}y\right)$.

Proposition. Heine équicontinue.

Théorème d'Ascoli.

IV. Applications du théorème d'Ascoli.

Proposition. Point fixe Brouwer. (admis)

Proposition. Théorème du point fixe de Schauder. [Rouvière, 1999]

Théorème. de Cauchy-Peano. [Demailly, 2012]

Définition. de la métrique sur $\mathcal{H}(\Omega)$. [Queffélec and Zuily, 2013]

Théorème de Montel

Application. Il n'existe pas de norme sur $\mathcal{H}(\Omega)$ qui définisse la même topologie que la distance définie plus haut.

Proposition. Continuité uniforme de l'opérateur de translation sur $\mathbb{L}^p(\mathbb{R})$. [Hirsch and Lacombe, 1997]

Théorème. de Fréchet Kolmogorov. [Hirsch and Lacombe, 1997]

Application. Compacité de l'opérateur à noyau défini sur $\mathbb{L}^2([0,1])$: $T : f \mapsto \left(x \mapsto \int_{\mathbb{R}} K(x,y)f(y)\mathrm{d}y\right)$.

40. **204 : Connexité. Exemples et applications.**

I. Première propriétés

I.1. *Connexité*

Définition. [Pommelet, 1994] Un espace topologique E est dit connexe s'il vérifie l'une des quatre propriétés (équivalentes) suivantes :

(1) Si E est réunion de deux ouverts disjoints, l'un de ces deux ouverts est vide.
(2) Si E est réunion de deux fermés disjoints, l'un de ces deux fermés est vide.
(3) Les seules parties ouvertes et fermées de E sont E et $\emptyset$.
(4) Toute fonction continue de E dans $\{0,1\}$ est constante.

Remarque. Une partie A de E est connexe si A est connexe pour la topologie induite.

Exemples.

(1) Une partie de R est connexe si et seulement si c'est un intervalle.
(2) $\mathbb{Q} \subset \mathbb{R}$ n'est pas connexe de $\mathbb{R}$. $\mathbb{Q} =]-\infty, \sqrt{2}[\cap\mathbb{Q} \bigcup]\sqrt{2}, +\infty[\cap\mathbb{Q}$.

Théorème. [Pommelet, 1994] Si E est connexe et si $\mathcal{R}$ est une relation d'équivalence ouverte sur E, alors E est la seule classe d'équivalence de $\mathcal{R}$.

Proposition. [Pommelet, 1994] L'adhérence d'une partie connexe est connexe.

Remarque. [Pommelet, 1994] C'est faux pour l'intérieur. Contre exemple : $\{(x,y) \in \mathbb{R}^2 | x > 0, y > 0\} \bigcup \{(0,0)\} \bigcup \{(x,y) \in \mathbb{R}^2 | x < 0, y < 0\}$.

Proposition. L'union de parties connexes ayant deux à deux une intersection non vide est connexe.

Remarque. C'est faux pour l'intersection. (Dessin de deux bananes...)

Théorème. L'image continue d'un connexe est connexe.

Applications.

(1) Les espaces $\mathbb{R}$ et $\mathbb{R}^2$ ne sont pas homéomorphes.
(2) Le théorème des valeurs intermédiaires.
(3) Une fonction continue d'un intervalle I à valeurs dans $\mathbb{R}$ est injective si et seulement si elle est strictement monotone.

Définition. Définition de la composante connexe contenant un point. Et des composantes connexes.

Exemple. Les composantes connexes de $\mathrm{GL}_n(\mathbb{R})$ sont $\mathrm{GL}_n(\mathbb{R})^+$ et $\mathrm{GL}_n(\mathbb{R})^-$.

Définition. Définition de la connexité par arcs.

Proposition. Si E est connexe par arcs, il est connexe. En particulier un convexe d'un evn est un connexe. Par exemple, une boule.

Contre-exemple. Notons Γ le graphe de $x \mapsto \sin(\frac{1}{x})$ sur $]0,1]$. Alors $\overline{\Gamma}$ est connexe mais pas connexe par arcs.

II. Passage du local au global.

Proposition. [Pommelet, 1994] Tout ouvert connexe d'un espace vectoriel normé est connexe par arcs. (Application des classes d'équivalence ouvertes).

Proposition. Toute application localement constante sur un espace connexe est constante.

Application. Unicité dans Cauchy-Lipschitz. Si deux solutions coïncident en un point, elles coïncident sur un petit intervalle ouvert, donc sur l'intervalle entier.

Théorème. [Amar and Matheron, 2004] Théorème des zéros isolés.

Exemple. L'identité est la seule fonction holomorphe qui vérifie $f(\frac{1}{n}) = \frac{1}{n}$.

Théorème. [Amar and Matheron, 2004] Théorème du prolongement analytique.

Exemples. [Amar and Matheron, 2004]

(1) Prolongement méromorphe de la fonction Γ d'Euler.
(2) Formule des compléments.

III. Autres exemples et applications.

Théorème. Théorème d'Hadamard Lévy par la méthode des chemins.

Proposition. [Gourdon, 1994a] Soit (E, d) un espace métrique compact et (u_n) une suite de E telle que $\lim d(u_{n+1}, u_n) = 0$. Alors l'ensemble des valeurs d'adhérences de u_n est connexe.

Proposition. Si la différentielle d'une application est nulle sur un ouvert connexe, alors l'application est constante.

Théorème. [Amar and Matheron, 2004] Théorème de Hurwitz. Soit Ω un ouvert connexe de $\mathbb{C}$ et soit f_n une suite de fonctions holomorphes injectives convergeant dans $\mathcal{H}(\Omega)$ vers une fonction f. Alors ou bien f est injective, ou bien f est constante.

III.1. *Groupes topologiques*

[Mneimné and Testard, 1986]

Proposition. Si G est un groupe topologique connexe, alors tout sous groupe ouvert H est égal à G.

Application. L'application exponentielle de $M_n(\mathbb{C})$ sur $GL_n(\mathbb{C})$ est surjective.

Proposition.

(1) $GL_n(\mathbb{C})$ est connexe par arcs.

(2) $SL_n(\mathbb{C})$ est connexe par arcs. $SL_n(\mathbb{R})$ aussi.

(3) $O_n(\mathbb{R})$ a exactement deux composantes connexes.

(4) $SO_n(\mathbb{R})$ est connexe par arcs.

Application. Le groupe $SO_3(\mathbb{R})$ est simple.

41. **205 : Espaces complets. Exemples et applications.**

I. Espaces métriques complets.

Définition. [Pommelet, 1994] d'une suite de Cauchy.

Proposition. [Pommelet, 1994] Une suite convergente est de Cauchy.

Définition. [Pommelet, 1994] Un espace dans lequel toute suite de Cauchy converge est un espace complet.

Remarque. La complétude est un outil essentiel qui permet de montrer qu'une suite converge sans pour autant connaître la limite.

Exemple.

(1) $\mathbb{Q}$ n'est pas complet.

(2) $\mathbb{R}$ est complet.

(3) Une conséquence : le théorème de Banach Alaoglu.

(4) $(\mathcal{C}^0([0,1]), ||\cdot||_2)$ n'est pas complet.

(5) $(\mathcal{C}^0([0,1]), ||\cdot||_\infty)$ est complet. La complétude dépend de la distance.

(6) Une conséquence : le théorème d'Ascoli.

Théorème. [Rouvière, 1999] Théorème du point fixe de Picard. Corollaire sur la vitesse de convergence.

Théorème. [Demailly, 2012] Théorème de Cauchy-Lipschitz.

Proposition. [Hirsch and Lacombe, 1997] E est compact si et seulement si (E,d) est précompact et complet.

Application. [RMS 119-4] Caractérisation des compacts dans les Banachs.

Exemple. [RMS 119-4] Le cube de Hilbert est compact.

Théorème. [Pommelet, 1994] Prolongement d'une application uniformément continue sur une partie dense.

Exemples.

(1) Prolongement de la transformée de Fourier en transformée de Fourier Plancherel par densité de $\mathbb{L}^1 \cap \mathbb{L}^2$.

(2) [Chambert-Loir, 1995] Inégalité de Hardy par densité de $\mathcal{C}_c^\infty$ dans $\mathbb{L}^p$.

Proposition. Complété d'un espace métrique.

Exemple. $\mathbb{H}_0^1([0,1])$ est un complété de $\mathcal{C}_c^\infty$ muni de la norme de $\mathbb{H}_0^1([0,1])$.

Exemple. [Queffélec and Zuily, 2013] Sur l'espace des fonctions holomorphes sur un ouvert de $\mathbb{C}$ on peut définir la topologie de la convergence uniforme sur tout compact. Cette topologie est métrisable, et $\mathcal{H}(\Omega)$ est complet pour cette métrique.

II. Espaces de Banach

Définition. Un espace vectoriel normé complet pour sa norme est appelé un espace de Banach.

Exemples.

(1) Un espace vectoriel normé de dimension finie sur $\mathbb{R}$ ou $\mathbb{C}$ est complet.

(2) Si E est un evn et F un Banach, alors l'espace vectoriel des applications linéaires continues muni de la norme d'opérateur est un espace de Banach.

II.1. *Théorème de Baire et applications.*

Proposition. [Gourdon, 1994a] Dans un espace de Banach, toute intersection dénombrable d'ouverts denses est dense.

Application. [Gourdon, 1994a] Un espace vectoriel à base dénombrable n'est pas complet. Il n'existe pas de norme sur l'espace vectoriel des polynômes qui rende cet espace complet.

Théorème. Théorème de Banach Steinhaus.

Applications.

(1) Sur le G_δ dense de fonctions continues 2π périodiques différentes de leurs séries de Fourier.

(2) Une suite faiblement convergente dans un Hilbert est bornée.

Théorème. [RUDIN] Théorème de l'application ouverte.

Corollaire. [RUDIN] Théorème de Banach.

Application. [RUDIN] L'application qui à $f \in \mathbb{L}^1(\mathbb{R})$ associe ses coefficients de Fourier dans $\mathrm{c}_0(\mathbb{R})$ est une application linéaire injective mais pas surjective.

Théorème. Théorème du graphe fermé.

Application.

(1) Les sous espaces vectoriels fermé de $\mathcal{C}^0([0,1])$ inclu dans $\mathcal{C}^1([0,1])$ sont de dimension finie.

II.2. *Autres propriétés et exemples.*

Proposition. Un espace vectoriel normé est un Banach si et seulement si toute série absolument convergente est convergente.

Théorème. Théorème de Riesz-Fischer [Brezis, 1983] Ajouter l'extraction d'une sous-suite qui converge presque partout.

Application. [RUDIN] Théorème de Grothendieck.

II.3. *Espaces préhilbertiens et hilbertiens.*

Théorème. de projection dans un préhilbertien sur un convexe complet. Caractérisation en terme d'angle obtus.

Application. Polynôme de degré fixé de meilleure approximation en norme 2. [Beck et al., 2004]

Application. Critère de densité pour un sev dans un espace de Hilbert.

Théorème. Théorème de représentation de Riesz. [Hirsch and Lacombe, 1997]

Application. Banach Alaoglu version Hilbert. [Hirsch and Lacombe, 1997]

Théorème. de Lax-Milgram. [Hirsch and Lacombe, 1997]

Application. Résolution d'EDPE [Brezis, 1983]

42. **206 : Théorèmes de point fixe. Exemples et applications.**

I. Théorème de point fixe de Picard et répercussions

Énoncé. [Rouvière, 1999] Théorème du point fixe de Picard dans un espace métrique complet X pour une application F contractante. Convergence de la suite des itérations et vitesse de convergence géométrique.

Contre-exemples.

(1) Contre-exemple lorsque l'espace n'est pas complet : $X =]0,1[$ et $F(x) = \frac{x}{2}$.
(2) Contre-exemple lorsque X n'est pas stable par F.
(3) Contre-exemple lorsque la fonction n'est pas contractante.

Remarque. Il s'agit d'une condition nécessaire mais non suffisante d'existence et d'unicité du point fixe.

Corollaire. Cas où seule une itérée de la fonction est contractante.

Application 1. Théorème de Cauchy linéaire et de [Demailly, 2012] Cauchy Lipschitz.

Application 2. Théorème de l'application ouverte.

Application 3. Théorème des fonctions implicites.

Exemple. Exemple d'application.

II. Théorèmes de points fixes compacts

Énoncé. [Rouvière, 1999] Énoncé du théorème de point fixe dans un espace métrique compact X pour une fonction F vérifiant : $\forall x, y \in X, x \neq y$, on a $\mathrm{d}(F(x), F(y)) < \mathrm{d}(x, y)$. Existence et unicité. Convergence de la suite des itérations.

Remarque. La vitesse de convergence peut être extrêmement lente pour ce théorème. Par exemple on peut étudier la fonction $x \mapsto x - x^r$ sur $[0,1]$ et montrer que la suite des itérés converge vers 0 à une vitesse de l'ordre de $\frac{1}{n^{\frac{1}{r-1}}}$.

Application. Étude de la suite sinus itéré.

Énoncé. Énoncé du théorème de point fixe dans un espace métrique compact étoilé X pour une fonction F vérifiant : $\forall x, y \in X, x \neq y$, on a $\mathrm{d}(F(x), F(y)) \leq \mathrm{d}(x, y)$.Existence.

Contre-exemple.

(1) Sans l'hypothèse étoilé. Une rotation d'angle non trivial sur une couronne n'a pas de point fixe.
(2) Évidemment pas d'unicité, par exemple l'identité sur n'importe quel compact.

III. Point fixe de Brouwer

Énoncé. Théorème de point de Brouwer.

Remarque. En dimension 1 le théorème est une conséquence du théorème des valeurs intermédiaires. On en déduit que la sphère et un segment ne sont pas homéomorphes.

Contre-exemple en dimension infinie. On considère l'application continue f de l^2 définie par $f(u)_n = u_{n-1}$ si $n \geq 1$ et $f(u)_0 = \sqrt{1-||u||^2}$. C'est une application qui envoie la boule unité dans elle même. Mais elle n'admet pas de point fixe.

Théorème de Schauder. [Rouvière, 1999] Soit X une partie convexe fermée (non vide) d'un espace vectoriel normé et F une application continue de X dans X telle que $\overline{F(X)}$ soit compacte. Alors F admet au moins un point fixe dans X.

A l'aide du théorème d'Ascoli, on peut alors démontrer le :

Application. [Demailly, 2012] Théorème de Cauchy Peaono.

IV. Autres aspects des points fixes

Dépendance du point fixe par rapport au paramètre. [Rouvière, 1999]

Application. Régularité des solutions d'une équation différentielle par rapport au paramètre. Hadamard par la méthode des chemins.

IV.1. *Objets qui sont des points fixes*

Remarque. Pour une application linéaire, les vecteurs propres associés à la valeur propre 1 sont des point fixes.

Exemple. La transformée de Fourier d'une gaussienne est une gaussienne.

Exemple. La transformée de Fourier du peigne de dirac est un peigne de dirac.

43. **207 : Prolongements de fonctions. Exemples et applications.**

I. Prolongement et continuité

Définition. du prolongement par continuité.

Exemples.

(1) $x \mapsto \frac{\sin(x)}{x}$ prolongé par 1 en $x = 0$ sur $\mathbb{R}_+$.

(2) $x \mapsto \exp(-\frac{1}{x^2})$ prolongé par 0 en $x = 0$.

Théorème de Hahn-Banach. Plutôt le corollaire utile. [Brezis, 1983]

Remarque. Sur le fait que dans un Hilbert, cette propriété se retrouve grâce à Riesz.

Application. Un sous-espace vectoriel $F \subset E$ est dense si et seulement si toute forme linéaire nulle sur F est nulle sur E. [Pommelet, 1994]

Théorème. [Pommelet, 1994] Prolongement d'une application uniformément continue définie sur une partie dense.

Remarque. Particulièrement utile dans le cas des applications linéaires continues, qui sont toutes uniformément continues.

Applications.

(1) Unicité du complété dans un espace métrique à isométrie près. [Pommelet, 1994]

(2) Inégalité de Hardy dans les espaces $\mathbb{L}^p$.

Application. Prolongement de la transformée de Fourier en transformée de Fourier plancherel.

Théorème. de Tietze-Urysohn. Soit $A \subset E$ un fermé, et $f : A \to \mathbb{R}$ continue et bornée, alors f admet un prolongement continu de E dans $\mathbb{R}$ avec les mêmes bornes. [Gourdon, 1994a]

Application. [Queffélec and Zuily, 2013] E est un compact ssi toute fonction fonctinue de E dans $\mathbb{R}$ est bornée.

II. Autres prolongements réguliers

II.1. *Prolongement de classe supérieure*

Théorème. de prolongement $\mathcal{C}^1$. Remarque sur le fait qu'on puisse l'itérer.

Exemple. $x \mapsto \exp(-\frac{1}{x^2})$ prolongée à tout ordre par 0 en $x = 0$ est $\mathcal{C}^\infty$.

Théorème. de Borel. [Rouvière, 1999]

Application. Toute fonction $\mathcal{C}^\infty$ sur $[a, b]$ peut être prolongé en une fonction $\mathcal{C}^\infty$ sur $\mathbb{R}$. [Rouvière, 1999]

II.2. *Prolongement des solutions d'EDO*

Théorème. Principe de sortie de tout compact. [Queffélec and Zuily, 2013]

Application. [Queffélec and Zuily, 2013] Si f est continue et bornée, alors les solutions de $x' = f(t, x)$ sont globales.

Exemple. $f(x) = \frac{x^2}{1+x^2}$, $f(x) = Arctan(x)$.

Application. Intervient dans la démonstration du théorème d'Hadamard par la méthode des chemins.

III. Prolongement et analycité.

Théorème. Principe de réflexion de Schwarz. [RUDIN]

Théorème des zéros isolés. [Amar and Matheron, 2004]

Théorème. Prolongement analytique. [Amar and Matheron, 2004]

Applications.

(1) Prolongement de la fonction Γ d'Euler à $\mathbb{C} \setminus \mathbb{Z}_-$. [Beck et al., 2004] [Queffélec and Zuily, 2013]

(2) Formule des compléments. [Amar and Matheron, 2004]

(3) Une fonction analytique sur un intervalle $I \subset \mathbb{R}$ se prolonge en une fonction holomorphe sur un ouvert de $\mathbb{C}$ contenant I. [Beck et al., 2004]

Définition. d'un point régulier et d'un point singulier sur le bord du disque de convergence d'une série entière.

Proposition. Si aucun point du cercle de convergence n'est singulier, on peut prolonger la somme de la série entière.

44. 208 : Espaces vectoriels normés. Applications linéaires continues. Exemples.

I. Première propriétés.

On admet les définitions d'un e.v sur $\mathbb{R}$ ou $\mathbb{C}$, d'une norme et d'un e.v.n $(E, ||\cdot||_E)$.

Exemples 1.
— $\mathbb{C}^n$ muni de la norme 2 est un e.v.n.
— $(l^p(\mathbb{N}), ||\cdot||_p)$ est un e.v.n.

Définition 2. Définition de normes équivalentes. Deux normes équivalentes sur E définissent la même topologie sur E.

Proposition 3. Si $\dim(E) < +\infty$, toutes les normes sur E sont équivalentes.

Théorème 3. Théorème de Riesz.

Définition 4. Définition de $\mathcal{L}_c(E, F)$, l'e.v des applications linéaires continues.

Théorème 5. [Brezis, 1983] Caractérisation de la continuité de $L \in \mathcal{L}_(E, F)$. L continue ssi L continue en 0 ssi $||Lx|| \leq M||x||$ ssi f est uniformément continue.

Corollaire 5. En dimension finie, $\mathcal{L}_c(E, F) = \mathcal{L}(E, F)$

Définition 6. Définition de la norme triple.

Théorème 7. $(\mathcal{L}_c(E, F), |||\cdot|||)$ est un evn.

Exemple 7. Continuité et norme de l'opérateur de décallage vers la gauche sur $l^1(\mathbb{N})$.

Définition 8. Définition d'être séparable pour E e.v.n. [Hirsch and Lacombe, 1997]

Exemple 8. Tout e.v.n de dimension finie est séparable car isomorphe à $\mathbb{R}^n$ ou $\mathbb{C}^n$ qui contient $\mathbb{Q}^n$ ou $(\mathbb{Q} + i\mathbb{Q})^n$ [Hirsch and Lacombe, 1997]

Théorème 9. Banach-Alaoglu pour des e.v.n.s séparables. [Hirsch and Lacombe, 1997]

II. Premier raffinement : espaces de Banachs.

Définition 10. E est un Banach s'il est complet pour sa norme.

Exemple 10. $\mathbb{R}^n$ et $\mathbb{C}^n$ sont des Banachs pour n'importe quelle norme.

Proposition 11. Si F est un Banach, alors $(\mathcal{L}_c(E, F), |||\cdot|||)$ est un Banach.

Exemple 12. Introduction des espaces $\mathcal{L}^p([0, 1])$. On quotiente par la relation d'égalité presque partout pour avoir une norme, et alors, les espaces

$L^p([0,1])$ et $L^\infty([0,1])$ sont des espaces de Banach pour leur norme. [Briane and Pages, 2000]

Exemple 13. $\mathcal{C}^p([0,1])$ muni de $||f|| = \sum_{i=0}^{p} ||f^{(i)}||_\infty$ est un espace de Banach pour tout p.

Contre-exemple 14. En dimension infinie, la complétude dépend de la norme choisie. Montrer une suite de fonctions continues sur $[0,1]$, affines par morceaux, qui converge pour la norme $\mathbb{L}^1$ vers $\mathbb{1}_{[0,1/2]}$ qui n'est pas continue.

Proposition. A est compact ssi (A,d) complet précompacte.

Définition. Définition d'une partie $\varepsilon-$plate. [RMS 119-4]

Proposition. Caractérisation des parties relativement compactes dans un Banach. [RMS 119-4]

Théorème 15. Théorème de Hahn-Banach analytique. [Gourdon, 1994a]

Application 15. Prolongement de forme linéaire continue avec la même norme. Un sous-espace vectoriel $F \subset E$ est dense ssi toute forme linéaire continue qui s'annule sur F s'annule sur E. [Pommelet, 1994]

Théorème 16. Théorème de Baire. [Gourdon, 1994a]

Application 16. Si E est un espace vectoriel normé admettant une base dénombrable, alors E n'est pas un Banach. [Gourdon, 1994a]

Exemple. Aucune norme ne rend $\mathbb{R}[X]$ complet !

Théorème 17. Théorème de Banach-Steinhaus [Gourdon, 1994a]

Application 17. Dans un Hilbert, une suite faiblement convergente est bornée. [Hirsch and Lacombe, 1997]

Application 18. Existence d'un G_δ dense de fonctions continues 2π périodiques différentes de leur série de Fourier. [Gourdon, 1994a] [Rudin et al., 1975]

Théorème 19. Théorème de l'application ouverte. [Brezis, 1983]

Application 19. Continuité de L^{-1} lorsque L est continue et inversible. [Brezis, 1983]

Exemple. Par l'absurde l'application qui à une fonction de $\mathbb{L}^1$ associe la suite de ses coefficients de Fourier est injective mais pas surjective (Utiliser le noyau de Dirichlet).

Théorème 20. Théorème du graphe fermé. [Gourdon, 1994a]

Application 20. Grothendieck. Les sous-espaces vectoriels fermés de $L^p([0,1])$ inclu dans L^∞ sont de dimension finie. [RUDIN-Analyse fonctionnelle.]

Application 20. Les sous-espaces vectoriels fermés de $\mathcal{C}^0([0,1])$ inclu dans $\mathcal{C}^1$ sont de dimension finie.

III. Encore plus riche : les espaces de Hilbert.

Définition 22. Définition d'un espace de Hilbert. [Hirsch and Lacombe, 1997]

Exemple 23. $l^2(\mathbb{N})$, $\mathbb{L}^{\nvDash}$.

Théorème 24. Représentation de Riesz. [Hirsch and Lacombe, 1997]

Application. On retrouve le théorème de Hahn-Banach analytique. [Beck et al., 2004]

Application 25. Définition de l'adjoint. [Hirsch and Lacombe, 1997] [Beck et al., 2004]

Exemple 26. Sur $l^2(\mathbb{N})$, l'adjoint du décallage vers la gauche est le décallage vers la droite.

Application 26. Banach-Alaoglu version Hilbert. [Hirsch and Lacombe, 1997]

Définition. d'une base hilbertienne. [Beck et al., 2004]

Proposition. Bessel-Parseval. [Hirsch and Lacombe, 1997]

Application. Obtention d'un calcul de somme par Parseval et les séries de Fourier. Inégalité isopérimétrique. [Queffélec and Zuily, 2013] [Beck et al., 2004] [Gourdon, 1994a]

45. **209 : Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications.**

I. Approximation par des polynômes.

I.1. *Approximations de fonctions continues.*

Théorème. Théorème de Weierstrass sur un segment.

Contre-exemple. Le théorème est faux sur $\mathbb{R}$. Une limite uniforme de polynôme est un polynôme.

Application. Théorème des moments.

Application. [Pommelet, 1994] Injectivité de la transformée de Laplace.

Application.

(1) [Gourdon, 1994a] On donne une fonction continue nulle part dérivable.
(2) Les fonctions continues nulle part dérivable sont denses dans l'espace des fonctions continues.

I.2. *Approximation locale de fonctions régulières*

Proposition. [Gourdon, 1994a] Taylor avec reste intégral.

Application. [Gourdon, 1994a] Inégalité de Kolmogorov.

Remarque. La formule de Taylor Young permet d'obtenir des développements limités.

Exemple. Un ou deux développements limités.

I.3. *Polynômes orthogonaux*

Proposition. [Beck et al., 2004] Polynôme de degré fixé approchant au mieux une fonction continue sur un segment en norme 2. Expression de celui-ci lorqu'on dispose d'une base hilbertienne de polynômes.

Définition. [Beck et al., 2004] d'une fonction de poids.

Définition. du Hilbert $\mathbb{L}^2(I, \rho)$ associé à une fonction de poids.

Théorème. [Beck et al., 2004] Condition suffisante pour avoir la densité des polynômes orthononaux dans $\mathbb{L}^2(I, \rho)$.

Exemples. Polynômes de l'Hermite et de Laguerre.

Proposition.

(1) Formule de récurrence d'ordre deux pour obtenir les polynômes orthogonaux.
(2) Nombre de zéros des polynômes.

I.4. *Interpolation de Lagrange.*

Définition. [Demailly, 2012] Définition du polynôme d'interpolation de Lagrange. Expression de ce polynôme sur la base des (l_i).

Proposition. [Demailly, 2012] Majoration de l'erreur d'interpolation pour une fonction régulière.

Définition. Des polynômes de Tchebychev et des points d'interpolation de Tchebychev.

Définition. Définition de l'opérateur d'interpolation de Lagrange.

Proposition. Equivalent de la norme de l'opérateur d'interpolation de Lagrange.

Conséquence. D'après Banach Steinhaus, il existe un G_δ dense de fonctions continues dont le polynôme d'interpolation diverge.

II. Approximation par des polynômes trigonométriques

II.1. *Séries de Fourier*

Propriété. Convergence en moyenne quadratique pour les fonctions $\mathbb{L}^2$. Formule de Parseval.

Applications.

(1) Calcul de sommes.
(2) Inégalité de Poincarré-Wirtinger, inégalité isopérimétrique.

Théorème. Théorème de convergence normale.

Application. [Moisan et al., 1992] Équation de la chaleur sur $[0, \pi]$.

Théorème. Théorème de Féjer.

Application. Les polynômes trigonométriques sont denses dans l'ensemble des fonctions continues sur un segment.

II.2. *Convergence ponctuelle.*

Théorème. Théorème de Dirichlet pour les fonctions de classe $\mathcal{C}^1$ par morceaux.

Proposition. Il existe un G_δ dense de fonctions continues 2π périodiques différentes de leur série de Fourier.

46. 213 : Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.

On fixe un corps $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On admet les définitions de produit scalaire, espace préhilbertiens, espace de Hilbert, et l'inégalité de Cauchy-Schwarz.

I. Espaces de Hilbert

Exemples. [Beck et al., 2004]

(1) $\mathbb{R}^n$ muni du produit scalaire $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$,

(2) $\mathbb{C}^n$ muni du produit scalaire $\langle x, y\rangle = \sum_{i=1}^{n} x_i \overline{y_i}$,

(3) $\mathbb{L}^2_{2\pi}(\mathbb{R}, \mathbb{C})$ muni du produit scalaire $\langle f, g\rangle = \frac{1}{2\pi}\int_0^{2\pi} f(t)\overline{g(t)}\mathrm{d}t$,

(4) $l^2(\mathbb{N})$ muni du produit scalaire $\langle x, y\rangle = \sum_{i=1}^{+\infty} x_i y_i$.

Proposition Égalité du parallélogramme. Caractérisation des normes issues d'un produit scalaire par l'égalité du parallélogramme. [Hirsch and Lacombe, 1997] Dessin en annexe

Cette égalité permet de démontrer le fondamental...
Théorème de projection sur un convexe fermé et sa caractérisation en terme de produit scalaire. 1-Lipschitzité de la projection. [Hirsch and Lacombe, 1997] Dessin en annexe [Beck et al., 2004]

Applications.

(1) Définition de l'espérance conditionnelle d'une variable aléatoire dans $\mathbb{L}^2$, [Beck et al., 2004]

(2) Projection sur $\mathbb{R}_n[X]$ dans le préhilbertien $(\mathcal{C}([0,1]), ||\cdot||_2$ [Beck et al., 2004]

Corollaire. Définition de l'opérateur de projection lorsqu'on projette sur un sev fermé. [Hirsch and Lacombe, 1997]
Corollaire. Théorème du supplémentaire orthogonal, caractérisation de la densité un sev par son noyau.

Le théorème de projection sur un convexe fermé permet de démontrer le fameux...
Théorème de représentation de Riesz

Applications du théorème de Riesz.

(1) Définition, (anti)linéarité et continuité de l'adjoint d'un opérateur,

(2) Définition intrinsèque du gradient d'une application différentiable à valeurs dans $\mathbb{R}$,

(3) On retrouve le théorème de Hahn-Banach analytique. [Beck et al., 2004]

Définition. de la convergence faible. [Hirsch and Lacombe, 1997]

Propriétés [Hirsch and Lacombe, 1997]

(1) Une suite faiblement convergente est bornée (Application de Banach-Steinhaus)

(2) Equivalence : (convergence faible + convergence de la suite des normes) $\Leftrightarrow$ convergence forte

Théorème de Banach Alaoglu version Hilbert [Hirsch and Lacombe, 1997]

II. Bases Hilbertiennes

Définition d'une base hilbertienne. [Beck et al., 2004]

Remarque. sur le fait qu'une base algébrique ne peut être dénombrable [Gourdon, 1994a]

Exemples.

(1) La famille des δ_k dans $l^2(\mathbb{N})$, [Hirsch and Lacombe, 1997]

(2) La famille des $x \mapsto \mathrm{e}^{inx}$ sur $\mathbb{L}^2([0, 2\pi])$, [Hirsch and Lacombe, 1997]

(3) Un espace de Hilbert séparable admet une base hilbertienne dénombrable. [Beck et al., 2004] (Tout espace de Hilbert admet une base hilbertienne, mais ça fait appel à Zorn...)

Proposition. Expression de la projection sur un sev lorsqu'on dispose d'une base orthonormée. Inégalité de Bessel. [Hirsch and Lacombe, 1997] [Beck et al., 2004]

Théorème de Bessel-Perseval. Caractérisation du fait qu'une famille orthonormée de H soit une base hilbertienne. [Hirsch and Lacombe, 1997] [Beck et al., 2004]

Conséquence. Un espace de Hilbert de dimension infinie séparable est isométrique à $l^2(\mathbb{N})$.

Orthonormalisation de Gram-Schmidt.

Application. Démonstration du théorème de Grothendieck.

III. Un grands domaine d'application

III.1. *Équations aux dérivées partielles*

Définition. Définition des Hilberts $H^1(]0,1[)$ et $H^1_0(]0,1[)$ avec leur produit scalaire.

Proposition.

(1) Existence d'un représentant continu pour H^1. Caractérisation des éléments de H^1_0.

(2) Inégalité de Poincarré Wirtinger. Nouveau produit scalaire sur H^1_0 équivalent au précédent.

Une première équation. [Brezis, 1983]

Théorème de Lax-Milgram

Application. [Brezis, 1983] Soit $f \in \mathbb{L}^2(]0,1[)$, $\alpha \in \mathbb{L}^\infty$ et $\beta \in \mathcal{C}^1([0,1])$ telles que : $0 < \alpha_{min} \leq \alpha(x)$ pour presque tout x et $\beta' \leq 2$. Alors il existe une unique fonction dans H_0^1 telle que

$$-(\alpha u')' + \beta u' + u = f$$

dans $\mathcal{D}'(0,1)$.

47. 214 : Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.

I. Théorème d'inversion locale.

I.1. *Résultats théoriques.*

Définition. d'un $\mathcal{C}^k$ difféomorphisme entre deux ouverts. [Rouvière, 1999]

Théorème d'inversion locale [Rouvière, 1999] Dessin en annexe.

Exemples.

(1) Changement de coordonnées polaires.
(2) $f(x,y) = (x^2 - y^2, 2xy)$ est un difféomorphisme au voisinage de tout point de $\mathbb{R}^2 \setminus \{0\}$.

Proposition. Théorème d'inversion locale holomorphe. [Beck et al., 2004]

Théorème. d'inversion globale. [Rouvière, 1999]

Théorème. d'inversion globale holomorphe. [Beck et al., 2004]

I.2. *Applications*

Théorème. d'Hadamard-Lévy dans le cas $\mathcal{C}^2$.

Application. Une application $\mathcal{C}^1$, $k > 0$ dilatante de $\mathbb{R}^n$ dans $\mathbb{R}^n$ est un $\mathcal{C}^1$ difféo global de $\mathbb{R}^n$. [Rouvière, 1999]

Application. Existence d'une racine k-ième d'une matrice proche de l'identité. [Beck et al., 2004]

Définition. Immersion et Submersion. [Rouvière, 1999]

Proposition.

(1) Une immersion est à difféomorphisme près une injection canonique.
(2) Une submersion est à difféomorphisme près une projection canonique.
(3) Théorème du rang constant. [Rouvière, 1999]

Proposition. L'exponentielle matricielle est un $\mathcal{C}^1$ difféo entre un voisinage de 0 dans $\mathcal{M}_n(\mathbb{K})$ et un voisinage de Id dans $\mathcal{GL}_n(\mathbb{K})$. [Mneimné and Testard, 1986]

Proposition. Lemme de Morse en dimension 2.

Applications.

(1) On retrouve un critère suffisant de minimalité. [Beck et al., 2004]
(2) Application à une courbe et une surface. [Rouvière, 1999]

II. Théorème des fonctions implicites

II.1. *Énoncés*

Théorème des fonctions implicites et dessin. [Rouvière, 1999]

Exemple. du cercle.

Corollaire. Obtention des dérivées de la fonction implicite. [Rouvière, 1999]

Application. Exemple $x^2 + y^2 + 1 = 0$ [Rouvière, 1999]

II.2. *Applications.*

Théorème des extrémas liés. [Gourdon, 1994a] [Beck et al., 2004]

Contre-exemple. Où les formes ne sont pas linéairement indépendantes. [Beck et al., 2004]

Application. Diagonalisation des endomorphismes symétriques. [Beck et al., 2004]

Applications.

(1) Dépendance $\mathcal{C}^\infty$ des racines d'un polynômes par rapport au polynôme. [Beck et al., 2004]
(2) L'ensemble des polynômes scindés à racines simples est un ouvert de $\mathbb{R}_n[X]$. [Beck et al., 2004]

III. Application importante : les sous-variétés.

Définition d'une sous-variété.

Proposition. Théorème des sous-variétés.

Exemples.

(1) La sphère $\mathbb{S}^n$.
(2) Le tore

Théorème. Théorème de Cartan Von-Neumann

Application. Le groupe orthogonal et $SL_n(\mathbb{R})$

48. 215 : Applications différentiables sur un ouvert de $\mathbb{R}^n$. Exemples et applications.

I. Applications différentiables.

Définition. [Lafontaine, 2012]

(1) Définition d'une application différentiable en un point. Unicité de la différentielle.

(2) Définition d'une application différentiable sur un ouvert. Définition d'une application continûment dérivable sur un ouvert.

Remarque. Indépendance de la notion de différentiabilité par rapport à la norme en dimension finie.

Proposition.

(1) Différentiable $\Longrightarrow$ Continue

(2) Chain rule

Définition.

(1) Définition des dérivées directionnelles.

(2) Différentiable $\Rightarrow$ existence de dérivées directionnelles selon toute direction.

Contre-exemple. Une fonction admettant des dérivées directionnelles selon toutes les directions mais pas continue.

Proposition. Une fonction positivement homogène d'ordre 1 admet des dérivées dans toutes les directions en 0. Elle est différentiable en 0 si et seulement si elle est linéaire.

Exemples.

(1) Une application linéaire est sa propre différentielle.

(2) Différentielle de la norme

(3) Différentielle de $M \mapsto M^{-1}$ sur $\mathrm{GL}_n(\mathbb{R})$.

(4) Différentielle du déterminant.

Théorème. [Rouvière, 1999] Inégalité des accroissements finis.

Applications.

(1) Si la différentielle est nulle sur un ouvert connexe, alors f est constante sur l'ouvert.

(2) Une fonction est de classe $\mathcal{C}^1$ si et seulement si f elle admet des dérivées partielles continues.

Proposition. [Rouvière, 1999] Différentielle de la limite.

Application. [Rouvière, 1999] Différentielle de l'exponentielle.

II. Inversion locale, fonction implicite.

II.1. *Inversion locale*

Définition. d'un $\mathcal{C}^k$ difféomorphisme entre deux ouverts. [Rouvière, 1999]

Théorème d'inversion locale [Rouvière, 1999] Dessin en annexe.

Exemples.

(1) Changement de coordonnées polaires.
(2) $f(x, y) = (x^2 - y^2, 2xy)$ est un difféomorphisme au voisinage de tout point de $\mathbb{R}^2 \setminus \{0\}$.

Théorème. d'inversion globale. [Rouvière, 1999]

Théorème. [Queffélec and Zuily, 2013] d'Hadamard-Lévy dans le cas $\mathcal{C}^2$ par la méthode des chemins.

Application. Existence d'une racine k-ième d'une matrice proche de l'identité. [Beck et al., 2004]

Proposition. L'exponentielle matricielle est un $\mathcal{C}^1$ difféo entre un voisinage de 0 dans $\mathcal{M}_n(\mathbb{K})$ et un voisinage de Id dans $\mathcal{GL}_n(\mathbb{K})$. [Mneimné and Testard, 1986]

II.2. *Théorème des fonctions implicites*

Théorème des fonctions implicites et dessin. [Rouvière, 1999]

Exemple. du cercle.

Corollaire. Obtention des dérivées de la fonction implicite. [Rouvière, 1999]

Application. Exemple $x^2 + y^2 + 1 = 0$ [Rouvière, 1999]

Applications.

(1) Dépendance $\mathcal{C}^\infty$ des racines d'un polynômes par rapport au polynôme. [Beck et al., 2004]
(2) L'ensemble des polynômes scindés à racines simples est un ouvert de $\mathbb{R}_n[X]$. [Beck et al., 2004]

III. Différentielle d'ordre 2, applications aux extrema.

III.1. *Différentielle d'ordre 2.*

Définition. Définition d'une application deux fois différentiable et de la matrice hessienne.

Proposition. Formule de Taylor reste intégral.

Proposition. Lemme de Morse en dimension 2.

Application. Application à une courbe et une surface. [Rouvière, 1999]

III.2. *Recherche d'extrema*

Proposition. [Beck et al., 2004] Conditions d'ordre 1 et 2.

Exemples. [Beck et al., 2004] Exemples et contre exemples pour cette proposition.

Théorème des extrémas liés. [Gourdon, 1994a] [Beck et al., 2004]

Contre-exemple. Où les formes ne sont pas linéairement indépendantes. [Beck et al., 2004]

Application. Diagonalisation des endomorphismes symétriques. [Beck et al., 2004]

49. **217 : Sous-variétés de $\mathbb{R}^n$. Exemples.**

I. Sous-variétés. Définitions et exemples.

I.1. *Qu'est-ce qu'une sous-variété ?*

Définition. [Rouvière, 1999] Soit $V \subset \mathbb{R}^n$ un sous-ensemble de $\mathbb{R}^n$, $a \in V$ et $d \in \mathbb{N}$ un entier naturel. On dit que V est lisse en a de dimension d s'il existe un difféomorphisme F de classe $\mathcal{C}^1$ d'un voisinage ouvert U de a dans $\mathbb{R}^n$ sur le voisinage ouvert $F(U)$ de 0 dans $\mathbb{R}^n$ qui transforme V en un sous-espace vectoriel de dimension d, c'est-à-dire : $F(V \bigcap U) = (\mathbb{R}^d \times \{0\}) \bigcap F(U)$.

Définition. [Rouvière, 1999] On dit que V est une sous-variété de dimension d si V est lisse en dimension d en chacun de ces points.

Remarque. Les notions lisse et sous-variété sont invariants par difféomorphisme.

Exemple. $F : (x, y) \mapsto (x, y - x^2)$ est un $\mathcal{C}^1$ difféomorphisme qui envoie la parabole d'équation $y = x^2$ sur la droite d'équation $y = 0$. La parabole est donc une sous-variété de dimension 1 de $\mathbb{R}^2$.

Remarque. [Rouvière, 1999] On appelle courbe lisse, resp. surface lisse, resp. hypersurface lisse une sous-variété de dimension 1, resp.2, resp. $n - 1$ de $\mathbb{R}^n$.

Exemples. [Rouvière, 1999]

(1) Une ellipse est une courbe lisse.
(2) Soit $C = \{x^2 + y^2 - z^2 = 0\}$ le cône en dimension 2. Alors $C \setminus \{0\}$ est une surface lisse de $\mathbb{R}^3$.

Théorème des sous-variétés [Lafontaine, 2012] Soit $V \subset \mathbb{R}^n$. Les propriétés suivantes sont équivalentes :

(1) V est une sous-variété de $\mathbb{R}^n$
(2) Pour tout $a \in V$, il existe un ouvert U de $\mathbb{R}^n$ contenant a et une submersion $g : U \to \mathbb{R}^{n-d}$ telle que $U \bigcap V = g^{-1}(\{0\})$. (Définition implicite)
(3) Pour tout $a \in V$, il existe un ouvert U de $\mathbb{R}^n$ contenant a, $\Omega\mathbb{R}^d$ ouvert contenant 0, et $h : \Omega \to \mathbb{R}^n$ une immersion qui est aussi un homéomorphisme de Ω sur $U \bigcap V$. (Définition paramétrique)
(4) Pour tout $a \in V$, il existe un ouvert U de $\mathbb{R}^n$ contenant a, un ouvert W de $\mathbb{R}^d$ contenant $(a_1, \cdots, a_d)$ et un $\mathcal{C}^1$ difféomorphisme g de W dans $\mathbb{R}^{n-d}$, tels que, après permutation éventuelle des coordonnées, $U \bigcap V$ soit le graphe de g. (Définition par graphe).

Exemple. [Lafontaine, 2012]

(1) La définition implicite permet de montrer que $\mathbb{S}^{n-1} = \{(x_1, \cdots, x_n) | \sum_{i=1}^n x_i^2 = 1\}$ est une sous-variété de dimension $n - 1$ de $\mathbb{R}^n$.
(2) Le tore $T = \{(x_1, \cdots, x_{2n}) \in \mathbb{R}^{2n} | (x_1^2 + x_2^2 - 1, \cdots, x_{2n-1}^2 + x_{2n}^2 - 1) = (0, \cdots, 0)\}$ est une sous-variété de $\mathbb{R}^{2n}$ de dimension n.

(3) Le graphe d'une fonction régulière, par exemple $(x, \sin(x))$ est une sous-variété de dimension 1 de $\mathbb{R}^2$.

I.2. *Quelques objets qui ne sont pas des sous-variétés.*

Contre-exemples.

(1) Le graphe d'une fonction non régulière. Par exemple $(x, |x|)$ n'est pas une sous-variété.

(2) Le cône de révolution n'est pas une sous-variété. Aucun voisinage connexe du sommet ne reste connexe privé de ce point.

(3) Une courbe avec un point double. $x^2 - y^2 = 0$.

(4) (t^2, t^3) n'est pas une sous-variété. (vecteur tangent à l'origine...)

II. Espace tangent à une sous-variété.

Définition. On dit qu'un vecteur v est tangent en un point a de $A \in \mathbb{R}^d$ s'il existe une application différentiable $\varphi :]-\varepsilon, \varepsilon[\to \mathbb{R}^d$ telle que $\varphi(]-\varepsilon, \varepsilon[) \subset A$, $\varphi(0) = a$ et $\varphi'(0) = v$.

Proposition. Les vecteurs tangents en un point à une sous-variété de dimension d de $\mathbb{R}^n$ forment un espace vectoriel de dimension d.

Proposition. Caractérisation de l'espace tangent selon les définitions du théorème des sous-variétés.

— Pour (2) définition implicite, $T_aV = \mathrm{Ker}(D_a g) + a$
— Pour (3) définition paramétrique, $T_aV = (Im)(D_0 h) + a$
— Pour (4) définition par graphe, T_aV est le graphe de $a + D_{(a_1, \cdots, a_d)} g$

Exemples. [Lafontaine, 2012]

(1) Le graphe d'une fonction régulière. $\Gamma = \{y = f(x)\}$ alors $T_{x_0}\Gamma = \{(x_0, f(x_0)) + h(1, f'(x_0))\}$.

(2) Définition implicite d'une surface dans $\mathbb{R}^3$. $S = g^{-1}(0)$. $T_{(a,b,c)}S$ a pour équation :

$$(x-a)\partial_1 g(a,b,c) + (y-b)\partial_2 g(a,b,c) + (z-c)\partial_3 g(a,b,c) = 0$$

(3) Définition paramétrique d'une surface S de $\mathbb{R}^3$. $h : (u,v) \mapsto (h_1(u,v), h_2(u,v), h_3(u,v))$ avec $h(0,0) = (a,b,c)$:

$$(a,b,c) + \partial_1 h(0,0)u + \partial_2 h(0,0)v.$$

(4) Plan tangent à $\mathbb{S}^{n-1}$ en un point a. C'est le plan passant par a dont un vecteur orthogonal est $(x_1, \cdots, x_n)$.

II.1. *Position du plan tangent.*

Lemme de Morse. [Rouvière, 1999]

Application. Détermination de la position du plan tangent en fonction de la signature de la hessienne.

II.2. *Extrema liés*

Théorème. Théorème des extrema liés pour une fonction réelle définie sur une sous-variété.

Interprétation. Dans le cas de la définition implicite d'une sous-variété, $V = g^{-1}(\{0\})$ cela signifie que $\bigcap \mathrm{Ker}(D_m g_i) \subset D_m f$ ou encore que le gradient de f en m est orthogonal à $T_m V$

Exemple. [Rouvière, 1999] On peut trouver les extrema de la norme euclidienne sur l'ellipse d'équation $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$. On trouve $(\pm a, 0)$ et $(0, \pm b)$.

Exemple. La fonction $x \mapsto \langle Ax, x\rangle$ avec $A \in \mathcal{S}_n(\mathbb{R})$ admet un extremum sur $\mathbb{S}^{n-1}$ compact. Le théorème nous dit que cet extremum est atteint pour un vecteur propre de la matrice A. [Beck et al., 2004]

III. Sous-variétés et matrices

Proposition. [Rouvière, 1999] Les matrices de rang fixé r forment une sous-variété de $\mathcal{M}_n(\mathbb{R})$ de dimension $n^2-(n-r)^2$.

Proposition. Tout ouvert d'une sous-variété de dimension n est une sous-variété de dimension n.

Corollaire. $\mathcal{GL}_n(\mathbb{R})$ est une sous-variété de dimension n^2.

Définition. [GONNORD TOSEL, Calcul différentiel] Définition de l'algèbre de Lie d'un sous-groupe fermé de $\mathcal{GL}_n(\mathbb{R})$.

Théorème. [GONNORD TOSEL, Calcul différentiel] Théorème de Cartan-Von Neumann.

Corollaire. $\mathrm{SL}_n(\mathbb{R})$, $\mathrm{SO_n}(\mathbb{R})$, et $\mathrm{O}_n(\mathbb{R})$ sont des sous-variétés de dimensions respectives n^2-1, $\frac{n(n-1)}{2}$.

Proposition. L'espace vectoriel tangent à G en I_n est l'algèbre de Lie.

Exemples. Les espaces vectoriels tangents à $\mathrm{SL}_n(\mathbb{R})$, $\mathrm{SO_n}(\mathbb{R})$, et $\mathrm{O}_n(\mathbb{R})$ sont respectivement $\mathrm{Trace}^{-1}(0)$ et $\mathcal{A}_n(\mathbb{R})$.

50. **218 : Applications des formules de Taylor**

I. Les formules de Taylor.

Proposition. [Gourdon, 1994a] Formule de Taylor avec reste intégral.

Proposition. [Gourdon, 1994a] Formule de Taylor Lagrange.

Application. Pour tout $x \in \mathbb{R}_+$, on a : $x - \frac{x^3}{6} \leq \sin(x) \leq x - \frac{x^3}{6} + \frac{x^5}{120}$.

Contre-exemple. Le paramétrage du cercle $F(t) = (\cos(t), \sin(t))$. Alors $0 = F(2\pi) - F(0) \neq 2\pi F(c)$ pour tout c.

Proposition. Formule de Taylor-Young.

Application. Si f est n fois dérivable en 0 alors f admet un développement limité au voisinage de 0.

Proposition. [Rouvière, 1999] Formule de Taylor en dimension supérieure.

II. Applications

II.1. *Fonctions DSE*

Remarque. Une fonction de classe $\mathcal{C}^\infty$ au voisinage d'un point n'est pas nécessairement DSE au voisinage de ce point.

Proposition. Lemme de Borel.

Application. Soit f une fonction $\mathcal{C}^\infty$ telle que $f^{(0)}(0) = n!$. Alors la série de Taylor de la fonction a un rayon de convergence nul...

Remarque. En outre, même si la série de Taylor d'une fonction en un point à un rayon de convergence non nul, rien ne garantit que la fonction soit égale à sa série de Taylor. $x \mapsto \exp(1\frac{1}{x^2})$.

Proposition. [Combes, 1982] Pour qu'une fonction $\mathcal{C}^\infty$ soit DSE au voisinage d'un point, il faut et il suffit que le reste intégral ou le reste de Taylor Lagrange tende vers 0 lorsque n tend vers $+\infty$.

Théorème. [Combes, 1982] de Bernstein et de Valiron.

Application. Tout fonction $\mathcal{C}^\infty$ impaire est DSE au voisinage de 0. Par exemple tan est DSE en 0 sur $]-\frac{\pi}{2}, \frac{\pi}{2}[$

II.2. *Recherche d'extrema*

Proposition. [Beck et al., 2004] Condition nécessaire du premier ordre.

Contre-exemple. $x \mapsto x^3$

Proposition. Dans le cas convexe la réciproque est également vraie.

Proposition. [Beck et al., 2004] Conditions du second ordre.

Contre-exemple. [Beck et al., 2004]

II.3. *Géométrie.*

Étude affine locale d'une courbe plane. [Rouvière, 1999]

Lemme de Morse en dimension 2

Application. Etude de la position de la surface par rapport à son plan tangent.

II.4. *Analyse numérique.*

Proposition. Méthode de Newton.

Proposition. Majoration de l'erreur pour les méthodes d'approximation de calcul d'intégrales. [CIARLET] ou [DEMAILLY]

II.5. *Autres*

Théorème central limite.

Proposition. Lemme de division d'Hadamard.

Application. La valeur principale de $\frac{1}{x}$ est une distribution tempérée.

51. **219 : Extremums : Existence, caractéristation, recherche. Exemples et applications.**

I. Définitions et existence.

I.1. *définitions.*

Définition. d'un maxiumum (resp. minimum) local, global, strict d'une fonction f en un point a. [Rouvière, 1999]

Exemples.

(1) d'une fonction admettant un minimum local non strict. $(x, y) \mapsto |x|$.

(2) d'une fonction admettant un minimum global strict. Une norme.

I.2. *Existence.*

Théorème. Une fonction continue sur un compact est bornée et atteint ses bornes. [Testard, 2010]

Application. Existence de l'éllipsoïde de John-Loewner [ORAUX X-ENS ALBG3]

Application. Équivalence des normes en dimension finie. [Testard, 2010]

Définition. D'une fonction coercive. [Testard, 2010]

Proposition. Une fonction coercive est minorée et atteint sa borne inférieure. [Testard, 2010]

Application. Théorème de d'Alembert. [Testard, 2010]

Théorème. de projection sur un convexe fermé. [Beck et al., 2004]

Application. [Testard, 2010] Théorème de Motzkin. Si $U \subset \mathbb{R}^n$ est un fermé. Alors on a :

U est convexe $\Leftrightarrow \forall x \in U^c, y \in U \mapsto ||y - x||$ atteint son minimum en un unique point de U.

Application. Méthode des moindres carrés. [Rouvière, 1999]

II. Caractéristation des extremums.

Proposition. Caractéristation du projeté sur un convexe fermé par l'angle obtus. [Beck et al., 2004]

II.1. *Conditions du premier ordre*

Théorème. Définition d'un point critique. Si une application différentiable admet un extremum local en ce point, alors sa différentielle est nulle en ce point. [Rouvière, 1999] [Beck et al., 2004]

Contre-exemple. $x \mapsto x^3$.

Application. Théorème de Rolle et théorème des accroissements finis. [Testard, 2010]

II.2. *Conditions d'ordre 2*

Théorème. [Rouvière, 1999]

(1) Si f admet un minimum local en a et est deux fois différentiable, alors $D_a f = 0$ et $D_a^2 f$ est positive.

(2) Si f est deux fois différentiable et que $D_a f = 0$ et $D_a^2 f$ est définie positive, alors f admet un minimum local strict en a.

Contre-exemple. $(x, y) \mapsto x^2 + y^4$ a une hessienne positive en $(0, 0)$, mais pas définie positive. Pourtant $(0, 0)$ est un minimum strict. Condition suffisante mais pas nécessaire.

Exemples. [Rouvière, 1999] $(x, y) \mapsto x^2 - y^2 + \frac{y^4}{4}$ admet trois points critiques admet trois points critiques. Deux sont des minima locaux stricts.

II.3. *Problème sous contrainte.*

Théorème. des extrémas liés. [Rouvière, 1999]

Remarque. Interprétation géométrique. [Beck et al., 2004]

Contre-exemple. Dans le cas où les Dg ne sont pas indépendants. [Beck et al., 2004]

Application. Diagonalisation des endomorphismes symétriques. [Beck et al., 2004]

Application. Inégalité arithmético-géométrique. [Rouvière, 1999]

Application. Inégalité d'Hadamard. [Rouvière, 1999]

III. Autres outils, recherche d'extrema

III.1. *Fonctions convexes.*

Proposition. Pour une fonction convexe, les conditions nécessaires de minimalité sont aussi des conditions suffisantes. [Beck et al., 2004]

Exemple. L'exponentielle est convexe. Sa dérivée n'est jamais nulle. Donc elle n'admet pas de maximum.

Proposition. Si f est une fonction strictement convexe qui admet un minimum local, alors il est unique. [Beck et al., 2004]

Proposition. Si f est convexe et admet un minimum local, alors il est global. [Rouvière, 1999]

Exemple. Points de Fermat. [Beck et al., 2004]

Application. La convexité permet d'obtenir l'unicité de l'éllipsoïde de John Loewner.

Théorème. Principe du maximum pour les fonctions holomorphes. [Testard, 2010]

Application. Lemme de Schwarz. [Testard, 2010]

Proposition. Inégalité Isopérimétrique. [Queffélec and Zuily, 2013]

III.2. *Exemples d'algorithmes.*

[Beck et al., 2004]

Proposition. Décente du gradient. Convergence lente.

Proposition. Méthode de Newton. Convergence quadratique.

52. **221 : Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications. Exemples et applications.**

I. Cadre du problème, premières propriétés

Remarque. [Gourdon, 1994a] Une équation différentielle sur $\mathbb{K}^n$ d'ordre p peut se ramener à une équation différentielle d'ordre 1. On étudie donc l'équation :

$$y'(t) = A(t)y(t) + b(t),$$

Avec A et b à coefficients continus.

Théorème. Théorème de Cauchy-Lipschitz linéaire.

Contre-exemple. [Demailly, 2012] $y' = 3|y|^{\frac{2}{3}}$ avec $y(0) = 0$ admet une infinité de solutions sur $\mathbb{R}$, par exemple $y(t) = 0$ et $y(t) = t^3$.

Le théorème de Cauchy-Lipschitz linéaire permet de déduire le résultat de structure suivant :

Proposition. [Gourdon, 1994a]

(1) L'ensemble des solutions de l'équation différentielle linéaire homogène est un sous-espace vectoriel de dimension n de $\mathcal{C}^1(I, \mathbb{K}^n)$.

(2) L'ensemble des solutions de l'équation est donc un espace affine de dimension n

Définition. [Gourdon, 1994a] Définition du Wronskien de n solutions noté W.

Théorème. [Gourdon, 1994a]

(1) Pour tout $t \in I$, on a : $W(t) = W(a)\exp\left(\int\limits_a^t \mathrm{Tr}(A(s))\mathrm{d}s\right)$. Ainsi le Wronskien est soit identiquement nul, soit jamais nul.

(2) Un ensemble de n solutions de l'équation forment une base de solutions si et seulement si leur Wronskien est non nul en un point.

Exemple. Wronskien de sinus et cosinus pour l'équation $y'' = y$.

Théorème. [Gourdon, 1994a] Théorème d'entrelacement de Sturm

II. Résolution explicite de l'équation.

Définition. [Gourdon, 1994a] Définition de la résolvante pour le système linéaire homogène.

Propriétés. [Gourdon, 1994a] Propriétés essentielles de la résolvante. Inversibilité, Chasles etc

Proposition. Expression de la solution grâce à la résolvante.

II.1. *Cas des coefficients constants.*

Proposition. Expression de la résolvante en terme d'exponentielle matricielle. Expression de la solution du système homogène.

Application. [Pommelet, 1994] Si A et B commutent, alors $\exp(A+B) = \exp(A)\exp(B)$.

Exemple. [Gourdon, 1994a] Résolution de $x' = x + z, y' = -y - z, z' = 2y + z$.

Proposition. [Gourdon, 1994a] Cas particulier des équations linéaires d'ordre p.

Proposition. [?] Méthode de variation des constantes.

Applications.

(1) [Gourdon, 1994a] $y' + y = \sin(t)$.

(2) $y'' + 2y' + y = t\exp(t)$

II.2. *Coefficients non constants*

Remarque. La méthode de la variation de la constante reste efficace.

Exemples.

Proposition. Développement asymptotique d'une solution de l'équation de Bessel.

III. Applications.

Théorème. Résolution de l'équation de la chaleur par séparation des variables.

III.1. *Etude de la stabilité d'équation différentielle autonome.*

Définition. Définition d'un point d'équilibre pour une équation autonome de la forme $y' = f(y(t))$. Définition d'un point d'équilibre stable et asymptotiquement stable.

Théorème. [Demailly, 2012] Théorème de stabilité dans le cas des coefficients constants.

Théorème. Condition nécessaire et suffisante d'asymptotique stabilité en regardant le système linéarisé.

Contre-exemple. pour montrer qu'on ne peut pas conclure à la stabilité du système comme pour le cas linéaire.

Annexe [Demailly, 2012] Quelques portraits de phases en dimension 2.

53. **222 : Exemples d'équations aux dérivées partielles linéaires.**

I. Quelques équations simples

I.1. *Équations de bases*

I.2. *Équations de transport*

[Claire David, Pierre Gosselet-Équations aux dérivées partielles]

Proposition. Équation générale. $\partial_t f(t,x) + c\partial_x f(x,t) = 0$. Expliquer ce qu'est la caractéristique.

Équation 1. $\partial_t f(t,x) + c\partial_x f(x,t) = 0$ et $f(0,x) = f_0(x)$. Cas d'une célérité constante et d'un domaine non borné.

Équation 2. $\partial_t f(t,x) + x\partial_x f(x,t) = 0$ et $f(0,x) = f_0(x)$. Cas d'une célérité qui varie dans l'espace.

II. L'apport de Fourier.

II.1. *Méthode de séparation des variables.*

Équation 1. [Moisan et al., 1992] Équation de la chaleur sur un segment. $\partial_t f(x,t) = \partial^2_{xx} f(x,t)$ avec conditions nulles aux bords. [Moisan et al., 1992]

Équation 2. Une version simpliste de Schrödinger : $\mathrm{i}\partial_t f(x,t) = -\partial^2_{xx} f(x,t)$ avec conditions nulles aux bords.

Remarque. On constate l'effet régularisant de l'équation de la chaleur. A l'inverse on n'a pas d'amélioration de la régularité avec Schrödinger.

Équation 3. Équation des cordes. $\partial^2_t t f(x,t) = \partial^2_{xx} f(x,t)$

II.2. *Utilisation de la transformée de Fourier.*

Équation 1. [Claire David, Pierre Gosselet-Équations aux dérivées partielles] Équation de la chaleur sur une barre infinie par la transformée de Fourier en x.

Équation 2. Équation des ondes en dimension 1 sur $\mathbb{R}$.

III. Espaces de Sobolev, équations aux dérivées partielles élliptiques

Définition. Définition des Hilberts $H^1(\Omega)$, $H^2(\Omega)$ et $H^1_0(\Omega)$ avec leur produit scalaire.

Proposition.

(1) Cas où $\Omega =]0,1[$. Existence d'un représentant continu pour H^1. Caractérisation des éléments de H^1_0.
(2) Inégalité de Poincarré. Nouveau produit scalaire sur H^1_0.

Théorème de Lax-Milgram

Équation 1. [Brezis, 1983] Soit $f \in \mathbb{L}^2(]0,1[)$, alors l'équation $-u'' + u = f$ et $u(0) = u(1) = 0$ (Condition de Dirichlet) admet une unique solution faible, i.e $u \in H_0^1$. Si $f \in \mathcal{C}^1([0,1])$, alors u est solution forte de classe $\mathcal{C}^2$.

Équation 2. [Brezis, 1983] Soit $f \in \mathbb{L}^2(]0,1[)$, $\alpha \in \mathbb{L}^\infty$ et $\beta \in \mathcal{C}^1([0,1])$ telles que : $0 < \alpha_{min} \leq \alpha(x)$ pour presque tout x et $\beta' \leq 2$. Alors il existe une unique fonction dans H_0^1 telle que

$$-(\alpha u')' + \beta u' + u = f$$

dans $\mathcal{D}'(0,1)$.

Équation 3. [Brezis, 1983] Soit $f \in \mathbb{L}^2(]0,1[)$, alors l'équation $-u'' + u = f$ et $u'(0) = u'(1) = 0$ (Condition de Neumann homogène) admet une unique solution $u \in H^2$. Si $f \in \mathcal{C}^1([0,1])$ alors $u \in \mathcal{C}^2([0,1])$.

Équation 4. [Brezis, 1983] Soit $f \in \mathbb{L}^2(]0,1[)$, alors l'équation $-u'' + u = f$ et $u'(0) = u(1) = 0$ (Conditions mixtes).

54. **224 : Exemples de développements asymptotiques de suites et de fonctions.**

I. Comportement asymptotiques de suites et de séries.

Théorème. [Gourdon, 1994a] Théorème sur les sommes partielles et les restes d'une série à terme général positif.

Remarque. On voit l'intérêt d'utiliser des équivalents télescopiques du terme général de la série.

Exemple. $n^n \sim n^n - (n-1)^{n-1}$ donc $\sum_{k=1}^n k^k \sim n^n$.

Exemple. [Gourdon, 1994a] $\frac{1}{n} \sim \ln(1+\frac{1}{n})$ donc on peut déduire que la somme partielle de la série harmonique H_n est équivalente à $\ln(n)$. On peut ensuite montrer que $U_n = H_n - \ln(n)$ converge vers un réel γ. On utilise ensuite que $\frac{1}{n^2} \sim \frac{1}{n} - \frac{1}{n+1}$ et on montre que $H_n = \ln(n) + \gamma + \frac{1}{2n} + o(\frac{1}{n})$

I.1. *Points fixes de suites récurrentes*

Théorème. [Rouvière, 1999] Théorème du point fixe de Picard. Vitesse de convergence.

Théorème. Théorème du point fixe compact. Vitesse de convergence.

Proposition. La vitesse de convergence du point fixe compact peut être extrêment lente. Pour la fonction $f : x \mapsto x - x^r$ on a $U_n \sim \frac{C}{n^{\frac{1}{r-1}}}$.

Exemple. [ORAUX X-ENS] Exemple du sinus itéré. $u_n = \sqrt{\frac{3}{n}} - \frac{3\sqrt{3}}{10}\frac{\ln(n)}{n\sqrt{n}} + o(\frac{\ln(n)}{n\sqrt{n}})$.

Exemple. [ORAUX X-ENS] Exemple d'un cas divergeant. $u_{n+1} = \exp(-u_n) + u_n$. On a $u_n = \ln(n) + \frac{1}{2}\frac{\ln(n)}{n} + o(\frac{\ln(n)}{n})$.

Théorème. Formule d'Euler Mac-Laurin

Application. Application à la série harmonique.

Application. Application à la fonction Γ.

II. Développements asymptotiques en probabilité

Application. [Barbe and Ledoux, 2012] Le max d'une suite de variables aléatoires indépendantes suivants une loi exponentielle tend vers l'infini à une vitesse $\ln(n)$

Définition. [CADRE-VIAL] Définition de la vitesse de convergence d'un estimateur.

Exemples. [CADRE-VIAL]

(1) Pour l'estimation de la probabilité de tomber sur pile θ dans le jeu de pile ou face, $\overline{X_n}$ est un estimateur asymptotiquement normal de θ.

(2) Dans le modèle $\left(\mathbb{R}^n, \{\mathcal{U}([\theta, \theta+1])^{\otimes n}\}_{\theta\in[0,1]}\right)$, $\min_{i=1\cdots n} X_i$ est un estimateur de vitesse n.

Exemple. [? ? ? ? ? ?] Une fonction utile dans les inégalité de déviations. La fonction Erf.

III. Développements asymptotiques de fonctions

III.1. *Développements limités*

Formule de Taylor-Young

Exemples. Exemples de développements limités

III.2. *Intégrale à paramètre*

Proposition. [Gourdon, 1994a] Méthode de Laplace.

Application. Formule de Stirling.

Théorème. Comportement des intégrales et des restes des intégrales par comparaison.

Exemple. [Gourdon, 1994a] Cas où $x\frac{g'(x)}{g(x)} \to \mu \neq -1$

Exemple. Développement asymptotique d'une solution de l'équation de Bessel.

III.3. *Développements de fonctions implicites*

Exemple. [Rouvière, 1999]

55. **226 : Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.**

I. Généralités.

Définition. Définition de la convergence d'une suite vers un réel l. Définition d'une suite divergente.

Exemple. Convergence de la suite géométrique pour $|q| < 1$, divergence pour $|q| > 1$.

Proposition. Caractérisation de la convergence par les suites de Cauchy.

Applications. [Combes, 1982]

(1) La série $\sum \frac{1}{n}$ diverge car la suite de ses sommes partielles n'est pas de Cauchy.

(2) Soit $\theta \in \mathbb{R}$ et $k \in]0,1[$. On pose $u_0 = 1$ et $u_{n+1} = u_n + k^n \cos(n\theta)$. Alors la série de terme général u_n converge.

Proposition. Toute suite réelle croissante majorée ou décroissante minorée converge.

Exemple. Études de suites récurrentes.

Proposition. Définition de suites adjacentes.

Exemple. [Combes, 1982] $u_n = \sum\limits_{p=0}^{n} \frac{1}{p!}$ et $v_n = u_n + \frac{1}{nn!}$ sont adjacentes et tendent vers e.

Proposition. Théorème des gendarmes.

Exemple. $u_n = \frac{\sin(n)}{n}$ tend vers 0.

Théorème. Théorème d'Abel. Cas particulier des séries alternées.

Exemples. $(\sum\limits_{p=1}^{n} \frac{(-1)^p}{\sqrt{p}})_n$, et $(\sum\limits_{p=1}^{n} \frac{e^{ip}}{p})_n$.

Proposition. Moyenne de Césaro. Cas général avec une suite de coefficients positifs dont la série diverge.

I.1. *Valeurs d'adhérences*

Définition. Définition d'une valeur d'adhérence. L'ensemble de valeurs d'adhérence d'une suite peut s'écrire $\bigcap\limits_{n \in \mathbb{N}^*} \overline{\{u_p, p \geq n\}}$, c'est un fermé.

Exemple. Le segment $[-1, 1]$ est l'ensemble des valeurs d'adhérences de $\sin(n)$.

Proposition. [Gourdon, 1994a] Soit (E, d) un espace métrique compact et (u_n) une suite de E telle que $\lim d(u_{n+1}, u_n) = 0$. Alors l'ensemble des valeurs d'adhérences de u_n est connexe.

Définition. Définition de la limite supérieure et inférieure, interprétation en tant que valeur d'adhérence.

Application. Formule d'Hadamard pour le rayon de convergence d'une série entière.

Proposition. La suite converge si et seulement si sa limite supérieure est égal à sa limite inférieure.

Application. [Barbe and Ledoux, 2012] Le max d'une suite de variables aléatoires indépendantes suivants une loi exponentielle tend vers l'infini à une vitesse $\ln(n)$

Définition. Suites équivalentes.

Exemple. Formule de Stirling.

II. Suites définies par récurrence

Proposition. Suite récurrente linéaire. Solutions.

Exemple. Suite de Fibonacci.

Exemple. Ruine du joueur.

Proposition. Cas $U_{n+1} = f(U_n)$. Si la suite converge, c'est vers un point fixe.

Théorème. Point fixe de Picard. Vitesse de convergence des itérées.

Application. Théorème de Cauchy Lipschitz.

Théorème. Théorème du point fixe compact. Vitesse de convergence possiblement très lente.

Exemple. Sinus itéré. Exponentielle itérée.

Proposition. Méthode de Newton. [Rouvière, 1999]

Définition. [ORAUX X ENS ANALYSE 2] Suite équirépartie.

Proposition. Critère de Weyl.

56. **226 : Suites vectorielles et réelles définies par une relation de récurrence. Exemples et applications.**

I. Généralités.

Soit (X,d) un espace métrique. Et $f : \Omega \subset X \longrightarrow X$. On suppose que $f(\Omega) \subset \Omega$. On pose $u_0 \in \Omega$ et $u_{n+1} = f(u_n)$.

Proposition 1. Si f est continue sur Ω, et que $U_n \to a \in \Omega$ alors $f(a) = a$.

I.1. *Le cas des suites réelles.*

Proposition 4 (monotonie). Si f est croissante, u_n est monotone. La monotonie est donnée par le signe de $f(x)-x$ où par le signe de $u_1 - u_0$. Si f est décroissante, les sous-suites d'indices paires et impaires sont monotones de monotonie opposées. [Gourdon, 1994a]

Exemple 4. $u_{n+1} = \frac{1}{2-\sqrt{u_n}}$. Le choix de u_0 détermine la monotonie et la limite de la suite. [Madère]

Définition 5. Définition d'un point fixe α de période p de f, et de l'orbite de α. [X-ENSA1]

Exemple 5. Suite possédant un point fixe de période 2

Théorème 6 (récurrence homographique. $u_{n+1} = \frac{au_n+b}{cu_n+d}$. Disjonction des cas. 3 cas possible selon la valeur de Δ. [Gourdon, 1994a]

Exemple 6. Illustration des 3 cas possibles. [Madère]

Proposition 7 (Chaos du cas non monotone) Itération de la fonction tente. Apparition du cantor. [Rouvière, 1999]

Proposition 8. Soit $f : [0,1] \to [0,1]$ continue. Alors (u_n) converge si et seulement si $|u_{n+1} - u_n| \to 0$. [X-ENS A1]

I.2. *Le cas vectoriel*

.

Définition 8 (suite récurrente linéaire d'ordre p).

Remarque 9. On peut vectorialiser pour que $u_{n+1} = f(u_n, u_{n-1}, \cdots, u_{n-p})$ rentre dans le cas de la leçon.

Proposition 10. Résultat de structure pour les suites récurrentes linéaires d'ordre p. (Espace vectoriel) [Gourdon, 1994a]

Exemple 10. Suite géométrique. Suite arithmético-géométrique.

Exemple 10. Suite de Fibonacci. $u_0 = u_1 = 1$ et $u_{n+2} = u_n + u_{n-1}$

Exemple. Suite récurrente d'ordre 1 avec second membre. Variation de la constante.

Exemple. Suite récurrente d'ordre 2 avec second membre, recherche d'une solution particulière et structure d'espace affine.

Exemple 11. (Ruine du joueur) DVP1 Un joueur avec un certain capital a de départ joue compulsivement à pile ou face avec une pièce (probabilité de gagner p) à hauteur de 1 euro par partie jusqu'à être ruiné ou gagner $a+b$. La probabilité de ruine et l'espérance du temps de jeu vérifient des relations de récurrence linéaires. [Grimmett and Stirzaker, 2001]

II. Points fixes de la suite et vitesse de convergence.

Théorème 12 (Point fixe de Picard). Énoncé du théorème (f contractante) + existence et unicité de la limite de (u_n) + estimation de la vitesse de convergence. [Rouvière, 1999]

Application 13. Démonstration du théorème de Cauchy-Lipshitz par itération. [Demailly, 2012]

Exemple 14. Sur $\mathbb{R}^n$, $x_0 \in \mathbb{R}^n$ et $x_{k+1} = Ax_k$. Alors (x_k) converge ssi $\rho(A) < 1$. [Ciarlet, 1988]

Application 14 (Résolution de systèmes linéaires). Résolution d'un système linéaire, caractérisation de la convergence de la méthode [Ciarlet, 1988]

Exemple 14 (Méthode de Jacobi). [Ciarlet, 1988]

Définition 15. Point fixe attractif. Point fixe répulsif.

Proposition 16. Cas où $f :]a,b[\to \mathbb{R}$ de classe $\mathcal{C}^\infty$ admet un point fixe a. Si $|f'(a)| < 1$ alors a point fixe attractif. Si $|f'(a)| > 1$ alors a point répulsif. [Rouvière, 1999]

Remarque 1. On ne peut pas conclure si $|f'(a)| = 1$. Exemple de $\sin(x)$ et $\operatorname{sh}(x)$ [Demailly, 2012]

Proposition 17. Soit $f : \Omega \subset \mathbb{R}^n \longrightarrow \mathbb{R}^n$ de classe $\mathcal{C}^1$ et a un point fixe de f. Il y a équivalence entre a est un point fixe attractif et $\rho(D_a f) < 1$. [Demailly, 2012]

Exemple 17. $f(x,y) = (-x + (3/2)y + 5/4, -(1/2)x + y^2 + 3/4)$ [Demailly, 2012]

Remarque 17. On ne peut pas conclure pour $\rho(D_a f) > 1$. $f(x,y) = (x/2, 2y)$. [Demailly, 2012]

Proposition 19. Point fixe super attractif. Vitesse de convergence. Méthode de Newton. [Rouvière, 1999]

Exemple 19. Méthode de Newton-Raphson. [Demailly, 2012]

Exemple 20. Approximation de l'inverse. [Rouvière, 1999]

Proposition 20. Point fixe à convergence lente.

Théorème. Théorème du point fixe compact.

Exemple 20. DVP2 Sinus itéré. + cas général. [Rouvière, 1999] [Chambert-Loir, 1995]

Exemple 20. Un autre exemple. $u_{n+1} = u_n + \exp(-u_n)$. [X-ENS A1]

57. **228 : Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.**

On admet les notions suivantes : continuité, continuité séquentielle, dérivabilité, opérations préservant la continuité et la dérivabilité, fonctions de classe $\mathcal{C}^k$.

I. Premiers exemples et applications.

I.1. *Exemples.*

Exemple 1. Les fonctions polynomiales sont $\mathcal{C}^\infty$.

Proposition. Si la restriction de f à un ouvert est continue, alors f est continue. En revanche...

Contre-exemple 2. L'indicatrice de $\mathbb{Q}$ est discontinue en tout point de $\mathbb{R}$ tandis que l'indicatrice de $\mathbb{Q}$ restreinte à $\mathbb{Q}$ ou à $\mathbb{R} \setminus \mathbb{Q}$ est continue.

Application 3. sur la continuité séquentielle. La limite d'une suite définie par récurrence est un point fixe de l'application f qui sert à la construire. [Rombaldi, 2004]

Application 4. Si f et g sont continues et coïncident sur un sous-ensemble dense, alors $f = g$. [Rombaldi, 2004]

Exemple. Solutions continues de $f(x+y) = f(x) + f(y)$. Ce sont les fonctions linéaires. [Rombaldi, 2004]

Exemple. Prolongement par continuité de $x \sin(1/x)$.

Exemple. La fonction $x^2 \sin(1/x)$ prolongée par 0 en $x = 0$ est dérivable, mais pas de classe $\mathcal{C}^1$.

Théorème. de Rolle. [Gourdon, 1994a]

Applications.

(1) Un polynôme simplement scindé a ses polynômes dérivés simplement scindés.
(2) Un polynôme ayant deux coefficients consécutifs nuls n'est pas simplement scindé.

Théorème des accroissements finis et égalité des accroissements finis.

II. Continuité et topologie

II.1. *Continuité et connexité*

Théorème des valeurs intermédiaires L'image d'un intervalle par une fonction continue est un intervalle. [Rombaldi, 2004]

Contre-exemple. La fonction $\mathbb{1}_{]0,1/2[} + 2\,\mathbb{1}_{[1/2,1[}$ est continue sur $[0,1] \setminus \{1/2\}$ mais ne vérifie pas le théorème des valeurs intermédiaires. [Rombaldi, 2004]

Contre-exemple. $\cos(1/x)$ prolongé par 1 vérifie le théorème des valeurs intermédiaires, mais n'est pas continue en 0.

Théorème. Soit f définie sur I à valeurs réelles vérifiant la propriété des valeurs intermédiaires alors f est continue si et seulement si, pour tout $y \in \mathbb{R}$, l'ensemble $f^{-1}(\{y\})$ est fermé dans I.

II.2. *Relations entre continuité et dérivabilité.*

Moralement une fonction continue n'est pas dérivable et une fonction dérivée est continue.

Contre-exemple. Fonction continue mais nulle part dérivable sur $[-1,1]$. [Gourdon, 1994a]

Application. Théorème de Weierstrass + le contre exemple précédent : L'ensemble des fonctions continues nulle part dérivable est dense dans l'ensemble des fonctions continues.

Théorème de Darboux Une fonction dérivée vérifie le théorème des valeurs intermédiaires. [Rombaldi, 2004]

Théorème. De plus, l'ensemble des points de continuité d'une dérivée est un G_δ dense. [Gourdon, 1994a]

II.3. *Continuité et compacité*

Théorème. Une fonction continue sur un compact est bornée et atteint ses bornes. [Rombaldi, 2004] page 50.

Théorèmes (Heine). [Hirsch and Lacombe, 1997]

(1) Une fonction continue sur un compact est uniformément continue.
(2) Une suite de fonctions équicontinues sur un compact est uniformément équicontinue.

Théorème (Weierstrass). Les polynômes sont denses dans l'ensemble des fonctions continue sur un segment muni de la norme uniforme. [Pommelet, 1994]

Application. Théorème des moments, et injectivité de la transformée de Laplace d'une fonction continue. [Pommelet, 1994]

Proposition. L'e.v. $(\mathcal{C}^0(K), ||\cdot||_\infty)$ est un espace de Banach. En particulier une limite uniforme de fonctions continues est continue.

Théorème (Ascoli). Caractérisation des parties relativement compactes des fonctions continues sur un compact muni de la norme uniforme.

Applications. Théorème de Montel, théorème d'Arzela Peano. Démonstration de la compacité des opérateurs à noyaux.

III. Liens avec des espaces de fonctions.

III.1. *Fonctions monotones.*

Théorème. Si f est une fonction croissante sur un intervalle, elle admet une limite à gauche et à droite en chaque point. [Rombaldi, 2004]

Théorème. L'ensemble des points de discontinuités d'une fonction monotone sur un intervalle est au plus dénombrable. [Rombaldi, 2004]

Proposition. Soit f monotone définie sur I. Alors f est continue ssi $f(I)$ est un intervalle. [Rombaldi, 2004]

Proposition.

(1) Le signe de la dérivée d'une fonction dérivable détermine la monotonie de la fonction.

(2) Soit f dérivable sur I. Si f admet extremum local en $a \in I$, alors $f'(a) = 0$.

[Rombaldi, 2004]

Exemple (L'escalier du diable). Fonction continue strictemement monotone dérivable pp et de dérivée nulle pp. Ref à trouver.

III.2. *Fonctions convexes.*

Proposition. Soit f une fonction continue définie sur I un intervalle. La fonction f est convexe si et seulement si $f(\frac{x+y}{2}) \leq \frac{1}{2}f(x) + \frac{1}{2}f(y)$.

Proposition. Une fonction convexe définie sur un intervalle ouvert est continue sur l'intervalle. [Rombaldi, 2004]

Contre-exemple. x^2 sur $]0, +\infty]$ et 1 en 0. Fonction convexe non continue.

Proposition. [Rombaldi, 2004]

(1) Si f convexe sur I vérifie $f'(a) = 0$, alors f admet un minimum global en a.

(2) Si f convexe admet un minimum local, alors ce minimum est global.

Proposition. Caractérisation de la convexité en fonction de la croissance de la dérivée dans le cas dérivable, et la positivité de la dérivée seconde dans le cas deux fois dérivable. [Rombaldi, 2004]

Proposition. Une fonction convexe et dérivable de I dans $\mathbb{R}$ est continûment dérivable.

III.3. *Fonctions périodiques*

Proposition. Une fonction continue périodique est bornée, atteint ses bornes, et est uniformément continue. [Rombaldi, 2004]

Théorème. Il existe un G_δ dense de fonctions continues2π-périodiques $\mathcal{F}$ tel que pour tout $f \in \mathcal{F}$ la série de Fourier de f diverge sur un G_δ dense de $\mathbb{R}$. [Gourdon, 1994a] [RUDIN]

Théorème. de convergence normale de Dirichlet. [Gourdon, 1994a]

58. 229 : Fonctions monotones. Fonctions convexes. Exemples.

I. Fonctions monotones.

Proposition. Soit $f : I \to \mathbb{R}$ de classe $\mathcal{C}^1$. Alors f est monotone si et seulement si f' est de signe constant.

Contre-exemple. L'escalier du diable construit sur l'ensemble triadique de Cantor est une fonction continue car affine par morceaux, presque partout dérivable, de dérivée nulle, mais croissante et telle que $f(0) = 0$ et $f(1) = 1$.

Proposition. Soit $f : I \to \mathbb{R}$ continue. Alors f est injective si et seulement si f est strictement monotone.

Proposition. Le nombre de points de discontinuités d'une fonction monotone est au plus dénombrable.

Théorème de Dini. Soit (f_n) une suite de fonctions croissantes et continues définies sur $[a, b]$ à valeurs dans $\mathbb{R}$. Alors si les (f_n) convergent simplement vers f continue, la convergence est en fait uniforme.

Théorème de Helly. Soit (f_n) une suite de fonctions croissantes de I dans $\mathbb{R}$ telle que pour tout $x \in I$, $(f_n(x))$ soit bornée. Alors il existe une sous-suite (f_{n_k}) qui converge simplement vers f croissante.

Définition. [Barbe and Ledoux, 2012] Définition de la fonction de répartition d'une variable aléatoire. Une fonction de répartition est cadlag. Une fonction cadlag avec les bonnes limites est une fonction de répartition.

Exemple. [Barbe and Ledoux, 2012] Variable aléatoire exponentielle. Vitesse de convergence logarithmique du max de variables aléatoires exponentielles indépendantes.

Proposition. [Barbe and Ledoux, 2012] Caractérisation de la convergence en loi par la convergence simple de la suite des fonctions de répartitions.

Exemple. [Barbe and Ledoux, 2012] En fait ce max, $M_n - \ln(n)$ tend vers une variable aléatoire Z vérifiant $F_Z(t) = \exp(-\exp(-t))$

II. Fonctions convexes

II.1. *Définitions.*

Définition. d'un ensemble convexe. [Beck et al., 2004]

Définition. D'une fonction convexe (resp. strictement convexe) définie sur un convexe. Lien avec l'épigraphe. [Beck et al., 2004]

Proposition. Caractéristation par la position de la courbe au dessus de sa tangente dans le cas réel.

Exemples.

(1) Une fonction affine est à la fois convexe et concave.
(2) $x \mapsto ||x||$ est convexe mais pas strictement convexe. [Beck et al., 2004]
(3) Pour $u \in \mathcal{S}_n^{++}$, $x \mapsto \langle u(x), x\rangle$ est strictement convexe. [Beck et al., 2004]
(4) Le sup d'une famille de fonctions convexes majorées par une même fonction est convexe. Démonstration par l'épigraphe.

Théorème. Pentes croissantes dans le cas réel. [Beck et al., 2004]

II.2. *Régularité, caractérisations.*

Théorème.

(1) Si f est convexe définie sur $I \subset \mathbb{R}$, alors f est continue sur l'intérieur de I. [Beck et al., 2004]
(2) On a le même résultat en dimension finie. [Gourdon, 1994a]

Contre-exemple. En dimension infinie, on a pas forcément la continuité. Dans $(\mathcal{C}([0,1]), ||\cdot||_1)$ l'application $||\cdot||_\infty$ est convexe mais pas continue. Regarder la suite $x \mapsto n\,\mathbb{1}_{[0,\frac{1}{n}]}$ et considérer deux termes consécutif dont la différence en $||\cdot||_\infty$ est plus grande que 1, mais dont l'intégrale de la différence tend vers 0.

Théorème. [Beck et al., 2004] Caractérisation pour une fonction différentiable f sur un ouvert U de la convexité. Sont équivalents :

(1) f convexe.
(2) L'application ∇f est monotone : $\forall x, y \in U, \langle \nabla f(y) - \nabla f(x), y - x\rangle \geq 0$
(3) Le graphe de f est au dessus de ses tangentes : $\forall x, y \in U, f(y) \geq f(x) + \langle \nabla f(x), y - x\rangle$

Si en plus f est deux fois différentiables on a aussi la caractéristation suivante : $\forall x, h \in U, \langle H_x f \cdot h, h\rangle \geq 0$.

Exemple. Soit $A \in \mathcal{S}_n$, on a : $x \mapsto \langle Ax, x\rangle$ est (strictement) convexe $\Leftrightarrow A$ est (définie) positive. [Beck et al., 2004]

III. Utilisations de la convexité.

III.1. *Extrema de fonctions convexes.*

Proposition. Les conditions nécessaires du premier et deuxième ordre pour un extremum sont aussi suffisantes pour une fonction convexe.

Proposition. Ellipsoïde de John-Loewner.

III.2. *Obtention d'inégalités.*

Applications. [Beck et al., 2004]

(1) Démonstration du théorème de représentation de Riesz.
(2) Théorème du supplémentaire orthogonal. Critère de densité.
(3) Définition de l'espérance conditonnelle dans $\mathbb{L}^2$.

Propositions. Inégalités pratiques. []

(1) $\exp(x) \geq x + 1$
(2) $\ln(x) \leq x - 1$
(3) Inégalité arithmético-géométrique.
(4) Young [Briane and Pages, 2000]

Proposition. Inégalité de Hoeffding.

Proposition. Inégalités de Hölder et Minkowski.

Conséquence. Les espaces $\mathcal{L}^p$ sont des espaces vectoriels normés. [Briane and Pages, 2000]

59. **230 : Séries de nombres réels ou complexes. Comportement des restes et des sommes partielles des séries numériques. Exemples.**

I. Généralités

[Combes, 1982] [Gourdon, 1994a]

Définition. Définition d'une série de terme général u_n. Définition de la suite des sommes partielles. Définition de la suite des restes. Définition d'une série convergente. Définition de la somme.

Exemple. La série géométrique converge pour $|q| < 1$, sa somme est $\frac{1}{1-q}$.

Proposition. Caractérisation de la convergence d'une série grâce au critère de Cauchy.

Contre-exemple. La série harmonique n'est pas de Cauchy donc elle diverge.

Application. Définition d'une série absolument convergente. Si la série converge absolument, alors elle converge. C'est pourquoi il est important de bien étudier le cas des séries à terme général positif. Définition d'une série semi-convergente.

Exemple. $\sum_{n\geq 1} \frac{(-1)^n}{n}$ est semi-convergente.

Remarque. On peut caractériser la complétude d'un espace vectoriel normé grâce aux séries numériques. $(E, ||\cdot||)$ est complet si et seulement si toute série absolument convergente est convergente.

Exemple (série telescopique). Si on dispose d'une suite (v_n) telle que $u_n = v_n - v_{n-1}$ alors la nature de $\sum_{n\geq 0} u_n$ est la même que celle de (v_n).

(1) $\sum \frac{1}{n(n+1)} = 1$

(2) $\sum \ln(\frac{n+1}{n}) = +\infty$

II. Séries remarquables

II.1. *Séries à termes positifs.*

Proposition. Si la série est à terme général positif, la suite des sommes partielles est croissante. Donc ou bien la série converge, ou bien elle diverge et vaut $+\infty$.

Théorème. Comportement des séries à terme général positif par comparaison (équivalent, petit o, grand O). Comparaison des restes dans le cas convergeant, des sommes partielles dans le cas divergent.

Remarque. Ce théorème montre qu'il est souvent utile de trouver des équivalents télescopique du termé général pour connaître le comportement de la série.

Exemple. Série harmonique : $\sum_{k=1}^{n} \frac{1}{k} = \ln(n) + \gamma + \frac{1}{2n} + o(\frac{1}{2n})$

Application. Étude de la vitesse de convergence du sinus itéré et de l'exponentielle itérée.

Exemple. Pour $\beta > 0$, $\frac{1}{n^\beta} - \frac{1}{(n+1)^\beta} \sim \frac{\beta}{n^{1+\beta}}$. On en déduit que pour $\alpha > 1$, la série de Riemann converge.

Théorème. Comparaison série intégrale.

Exemple. Application à la série $\sum \frac{1}{n \ln(n)^\alpha}$

II.2. *Séries alternées et Abel*

Théorème. Définition d'une série alternée. Convergence. Majoration du reste.

Théorème d'Abel.

Exemple. Séries trigonométriques.

Définition. Définition du produit de Cauchy de deux séries. Absolue convergence.

Théorème. Abel angulaire et théorème taubérien faible.

Application. Théorème de Mertens. Cas où l'une des deux séries est seulement semi-convergente.

Contre-exemple. Le produit de Cauchy de deux séries de terme général $\frac{(-1)^n}{\sqrt{n}}$ diverge.

III. Ordre de sommation, interversion des sommations.

Exemple. Dans le cas des séries alternées, l'ordre de sommation importe. On peut construire des séries divergentes ou convergeant vers un réel arbitraire à partir de la série harmonique alternée.

Théorème. Les séries commutativement convergentes sont les séries absolument convergentes.

Définition. Définition d'une série double.

Contre-exemples. Deux séries doubles non absolument convergentes dans lequel on ne peut pas choisir l'ordre de sommation.

Exemple. $\sum \frac{1}{(m+n)^\alpha}$ converge pour $\alpha > 2$.

III.1. *Coefficients de Fourier*

Définition. Définition des coefficients de Fourier.

Formule de Parseval.

Exemples. Deux exemples de calculs de sommes.

60. **234 :Espaces $\mathbb{L}^p$, $1 \leq p \leq +\infty$.**

I. Construction et propriétés des espaces $\mathbb{L}^p$.

I.1. *Construction*

Définition. des espaces $\mathcal{L}^p$. Cas particulier de $l^p(\mathbb{N})$. [Briane and Pages, 2000]

Proposition. L'espace $\mathcal{L}^p$ est un espace vectoriel. [Briane and Pages, 2000]

Proposition. En mesure finie, inclusion décroissante des $\mathcal{L}^p$ en fonction de p, et inclusion croissante des $l^p(\mathbb{N})$ [Briane and Pages, 2000]

Contre-exemple. Aucune inclusion en mesure infinie. $\frac{\mathbb{1}_{]0,1]}}{\sqrt{\cdot}} \in \mathcal{L}^1 \setminus \mathcal{L}^2$ et $\frac{1}{(\sqrt{(\cdot)}^2+1)} \in \mathcal{L}^2 \setminus \mathcal{L}^1$

Proposition. [Briane and Pages, 2000]

(1) Définition des normes $||\cdot||_p$ (qui n'en sont pas encore)
(2) Inégalité de Hölder.
(3) Cas d'égalité.

Théorème. [Briane and Pages, 2000]

(1) Inégalité triangulaire (de Minkowski)
(2) $\mathcal{L}^p$ est un espace vectoriel semi-normé.

Définition. de $\mathbb{L}^p$ par passage au quotient de $\mathcal{L}^p$ par la relation d'équivalence $\{||\cdot||_p = 0\}$. L'espace $\mathbb{L}^p$ est ainsi un espace vectoriel normé.

Remarque. Si le seul ensemble mesurable étant de mesure nulle est l'ensemble vide, l'espace $\mathcal{L}^p$ et $\mathbb{L}^p$ coïncident. C'est le cas pour $l^p(\mathbb{N})$.

I.2. *Propriétés*

Proposition. L'inégalité de Hölder permet de conclure qu'en mesure finie, l'inclusion décroissante des $\mathbb{L}^p$ est topologique. (Les injections sont continues).

Théorème de Riez-Fisher. [Brezis, 1983]

(1) $\mathbb{L}^p$ est un espace de Banach.
(2) De toute suite convergente dans $\mathbb{L}^p$ on peut extraire une sous-suite qui converge presque partout.

Contre-exemple. [Briane and Pages, 2000] En mesure infinie, la convergence $\mathbb{L}^p$ n'implique pas la convergence presque partout. Contre-exemple. De même la convergence presque partout n'implique pas la convergence $\mathbb{L}^p$. Contre-exemple. Cependant on a le

Théorème de convergence dominée $\mathbb{L}^p$. [Briane and Pages, 2000]

Propriété. Cas particulier de $\mathbb{L}^2$. Structure d'espace de Hilbert.

II. Propriétés des $\mathbb{L}^p$.

II.1. *Analyse fonctionnelle sur les $\mathbb{L}^p$.*

Application de la structure de Banach, de la structure de Hilbert de $\mathbb{L}^2$, et des inclusions topologiques en masse finie. Le théorème de Grothendieck. [RUDIN-Analyse fonctionnelle.]

Proposition. Séparabilité des $\mathbb{L}^p$ pour $p \neq \infty$. [Brezis, 1983]

Proposition. Dual de $\mathbb{L}^p$. [Brezis, 1983]

Remarque. Le dual de $\mathbb{L}^\infty$ est strictement plus grand que $\mathbb{L}^1$ [Brezis, 1983]

Théorème.

(1) Densité des fonctions étagées intégrables dans $\mathbb{L}^p$, $p \neq \infty$. [Briane and Pages, 2000]

(2) Densité des fonctions étagées dans $\mathbb{L}^\infty$

(3) Densité des fonctions continues à support compact dans $\mathbb{L}^p$. [Briane and Pages, 2000]

Application.

(1) Inégalité de Hardy.

II.2. *Convolution et applications*

Définition. de la convolution pour des exposants conjugués. [Hirsch and Lacombe, 1997]

Proposition. Le produit de convolution est dans $\mathbb{L}^\infty$, nulle à l'infini, uniformément continue.

Proposition. Inégalité de Young. [Hirsch and Lacombe, 1997]

Définition Approximation de l'unité. [Briane and Pages, 2000]

Exemple. [Briane and Pages, 2000]

Proposition. Régularisation par convolution.

Application. Densité de $\mathcal{C}_c^\infty$ dans $\mathbb{L}^p$.

Application. Théorème de convergence de Féjer. Le noyau de Féjer est régularisant. [Queffélec and Zuily, 2013]

III. Un domaine d'application : la transformée de Fourier.

Définition de la transformée de Fourier sur $\mathbb{L}^1$

Exemple. Calcul de la transformée de Fourier d'une indicatrice.

Application de la densité. Théorème de Riemann-Lebesgue. On prend des fonctions $\mathcal{C}^1$ pour faire l'intégration par parties.

Proposition. Injectivité de la transformée de Fourier sur l'espace des continues de limite nulle à l'infini.

Proposition. Densité de $\mathbb{L}^1 \bigcap \mathbb{L}^2$ dans $\mathbb{L}^2$.

Définition. de la transformée de Fourier-Plancherel

Exemple. Calcul de l'intégrale du sinus cardinal sur $\mathbb{R}_+$.

61. **235 : Problèmes d'interversions de limites et d'intégrales.**

I. Préliminaires.

Contre-exemple. $f_n(x) = \frac{1}{n}\mathbb{1}_{[0,n]}$ converge (uniformément) vers la fonction nulle. Mais on ne peut pas intervertir limite et intégrale.

II. Suites et séries de fonctions.

Théorème. Interversion limite intégrale possible lorsqu'on a convergence uniforme sur un segment. [Gourdon, 1994a]

Exemple. Application à la permutation d'une série de fonctions qui converge uniformément sur un segment. On obtient la formule :

$$\int_0^1 x^{-x}\mathrm{d}x = \sum_{n=1}^{+\infty} n^{-n}.$$

[Candelpergher, 2004]

Contre-exemple. Le théorème donne une condition suffisante mais non nécessaire. On considère $x \mapsto x^n$ sur $[0,1]$. Ou bien $\int_0^{\frac{\pi}{2}} \sin^n(t)\mathrm{d}t$. La théorie de la mesure réduit les hypothèses. [Madère, 1997]

Théorème (Beppo-Levi) [Candelpergher, 2004]

Applications.

(1) Soit f une fonction mesurable positive alors on a : $\det_{n\to+\infty} \int (f\wedge n)(x)\mathrm{d}\mu(x) = \int f(x)\mathrm{d}\mu(x)$.

(2) Expression de la fonction Γ en terme de limite. Application à son prolongement holomorphe sur $\mathbb{C}\setminus\mathbb{Z}$ [Queffélec and Zuily, 2013]

Théorème (de convergence dominée $\mathbb{L}^p$). [Candelpergher, 2004]

Applications.

(1)
$$\det_{n\to+\infty} \int_{\mathbb{R}_+} \frac{\exp(-nx^3)}{1+x^2}\mathrm{d}x = 0.$$
[Candelpergher, 2004]

(2) DVP : Formule des compléments. [Amar and Matheron, 2004]

(3)
$$\det_{n\to+\infty} \int_0^{\sqrt{n}} \left(1-\frac{x^2}{n}\right)^n \mathrm{d}x = \int_0^{+\infty} \exp(-x^2)\mathrm{d}x.$$
On déduit l'intégrale de Gauss. [Moisan et al., 1992]

Théorème sur l'interversion $\sum\int$ pour une série de fonctions. [Candelpergher, 2004]

Exemple. $\int_0^{+\infty} \frac{x\exp(-x)}{1+\exp(-x)}\mathrm{d}x = \sum\limits_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n^2}$.

Contre-exemple. Une fois de plus les conditions sont suffisantes mais pas nécessaires.
$\int_0^{+\infty} \sum\limits_{n=0}^{+\infty} (-1)^n\exp(-(n+1)x)\mathrm{d}x = \sum\limits_{n=0}^{+\infty} \int_0^{+\infty} (-1)^n\exp(-(n+1)x)\mathrm{d}x = \ln(2)$. Cependant on a : $\int_0^{+\infty} \sum\limits_{n=0}^{+\infty} \exp(-(n+1)x)\mathrm{d}x = +\infty$.

III. Intégrales à paramètre

Remarque. Continuité et dérivabilité sont des notions locales définies comme des limites.

Théorème continuité et dérivabilité d'une intégrale à paramètre. [Briane and Pages, 2000]

Applications

(1) Transformée de Fourier de la dérivée [Briane and Pages, 2000]

(2) Convolution et dérivation [Briane and Pages, 2000]

(3) Calcul de l'intégrale de Gauss par étude d'une intégrale à paramètre

(4) Continuité de la transformée de Laplace en 0 et application à l'intégrale du sinus cardinal. DVP : 3 méthodes de calcul de $\int_0^{+\infty} \frac{\sin(t)}{t}\mathrm{d}t$.

62. 236 : Illustrer par des exemples quelques méthodes d'intégration des fonctions d'une ou plusieurs variables réelles.

On fait le choix de prendre le titre de la leçon au pied de la lettre. On ne donnera aucun résultat théorique. Les principaux résultats utilisés ici sont : l'intégration par parties, le changement de variable (à une ou plusieurs variables), le théorème de Fubini-Tonelli et Fubini, les théorèmes de régularité d'une intégrale à paramètre, le théorème des résidus, le théorème de convergence dominée.

I. Premiers calculs

Proposition. (Intégrale de Wallis). [Gourdon, 1994a] On pose $I_n = \int\limits_0^{\frac{\pi}{2}} \sin^n(x)\mathrm{d}x$.

(1) $I_0 = \frac{\pi}{2}$ et $I_1 = 1$,

(2) Une intégration par parties donne $I_n = \frac{n-1}{n} I_{n-2}$ pour tout $n \geq 2$.

(3) Pour tout $p \in \mathbb{N}$, $I_{2p} = \frac{(2p-1)(2p-3)\cdots 1}{2p(2p-2)\cdots 2}\frac{\pi}{2}$, et $I_{2p+1} = \frac{2p(2p-2)\cdots 2}{(2p+1)(2p-1)\cdots 2}$,

(4) I_n est équivalent à $\sqrt{\frac{\pi}{2n}}$ en $+\infty$.

Proposition. [Candelpergher, 2004] Le théorème des résidus permet de montrer que $\int\limits_{-\infty}^{+\infty} \frac{1}{1+x^4}\mathrm{d}x = \frac{\pi\sqrt{2}}{4}$.

On considère l'intégrale de la fonction $f : z \mapsto \frac{1}{1+z^4}$ (holomorphe sur $\mathbb{C}$ privé des racines 4ème de -1) sur un demi cercle C_R représenté par un joli dessin. Par le théorème des résidus, pour $R > 1$, cette intégralle vaut $2i\pi\left(\mathrm{Res}(f, \exp(i\frac{\pi}{4})) + \mathrm{Res}(f, \exp(i\frac{3\pi}{4}))\right)$. L'intégrale sur les deux segments tend vers l'intégrale recherchée par convergence dominée, et l'intégrale sur le demi cercle tend vers 0. D'où le résultat.

II. L'intégrale de la gaussienne

Proposition. On a $\int\limits_0^{+\infty} \exp(-t^2)\mathrm{d}t = \frac{\sqrt{\pi}}{2}$.

Première méthode (coordonnées polaires). [Candelpergher, 2004] On a :

$$\left(\int_{\mathbb{R}} \exp(-t^2)\mathrm{d}t\right)^2 = \int_{\mathbb{R}^2} \exp(-x^2-y^2)\mathrm{d}x\mathrm{d}y = \int_{]0,+\infty[\times]-\pi,\pi[} \exp(-r^2)r\mathrm{d}r\mathrm{d}\theta = \frac{1}{2}2\pi = \pi.$$

D'où le résultat par parité de l'intégrande.

Deuxième méthode (intégrale à paramètre). [Gourdon, 1994a] Pour $x \in \mathbb{R}_+$, on pose $g(x) = \int_0^1 \frac{\exp(-(t^2+1)x^2)}{t^2+1}\mathrm{d}t$. D'après le théorème de dérivabilité, on a :
$g'(x) = -2x\exp(-x^2)\int_0^1 \exp(-(tx)^2)\mathrm{d}t$. Donc par changement de variable $u = tx$, on a $g'(x) = -2\exp(-x^2)\int\limits_0^x \exp(-u^2)\mathrm{d}u$. D'où en posant $f(x) = \int\limits_0^x \exp(-u^2)\mathrm{d}u$, et en primitivant à vue, $g(x) - g(0) = -(f^2(x) - f^2(0))$, soit $g(x) = \frac{\pi}{4} - f^2(x)$. Pour finir, $\det_{x\to 0} g(x) = 0$, d'où le résultat.

Troisième méthode (en utilisant l'intégrale de Wallis). Pour $n \in \mathbb{N}^*$, par concavité du logarithme, on montre que :

$$\int\limits_0^{\sqrt{n}} \left(1 - \frac{t^2}{n}\right)^n \mathrm{d}t \leq \int\limits_0^{\sqrt{n}} \exp(-t^2)\mathrm{d}t \leq \int\limits_0^{\sqrt{n}} \left(1 + \frac{t^2}{n}\right)^{-n} \mathrm{d}t.$$

Alors par changements de variables $t = \sqrt{n}\cos(u)$ et $t = \sqrt{n}\mathrm{cotan}(u)$, on a :

$$\int\limits_0^{\frac{\pi}{2}} \sin^{2n+1}(u)\mathrm{d}u \leq \int\limits_0^{\sqrt{n}} \exp(-t^2)\mathrm{d}t \leq \int\limits_0^{\frac{\pi}{2}} \sin^{2n-2}(u)\mathrm{d}u.$$

En utilisant les équivalents de l'intégrale de Wallis on a le résultat.

L'intégrale de la gaussienne permet de calculer :
Proposition (Intégrale de Fresnel). [Candelpergher, 2004] L'intégrale $I = \int\limits_0^{+\infty} \exp(it^2)\mathrm{d}t$ est bien définie et vaut $\exp(i\frac{\pi}{4})\frac{\sqrt{\pi}}{2}$.

On pose $z = \exp(-i\frac{\pi}{4})t$, on a $I = \int\limits_{\mathbb{R}_+(1,-1)} \exp(-z^2)\mathrm{d}z$. On considère l'intégrale de cette fonction sur un compact K_R défini par un joli dessin. Par holomorphie, cette intégrale est nulle. On considère chacun des morceaux à la limite sur R. L'un est nul, l'autre est l'intégral de Gauss. D'où le résultat.

III. Un exemple riche : le calcul de l'intégral sur $\mathbb{R}_+$ du sinus cardinal.

Proposition.

(1) $\int\limits_0^{+\infty} \frac{\sin(t)}{t}\mathrm{d}t$ est bien définie, car l'intégrande est prolongeable par continuité en 0 par la valeur 0, et admet une limite en $+\infty$ par intégration par parties.

(2) En revanche, $t \mapsto \frac{\sin(t)}{t}$ n'est pas une fonction intégrable sur $\mathbb{R}_+$. L'intégrale considérée est impropre.

(3) $\int\limits_0^{+\infty} \frac{\sin(t)}{t}\mathrm{d}t = \frac{\pi}{2}$.

Première méthode (Fubini). [Candelpergher, 2004] On étudie f : $\mathcal{D} =]0, A[\times\mathbb{R}_+^* \to \mathbb{R}$, définie par $f(x, y) = \exp(-xy)\sin(x)$. Fubini-Tonelli montre que f est intégrable sur $\mathcal{D} =]0, A[\times\mathbb{R}_+^*$. Fubini montre alors que $\int\limits_{\mathcal{D}} f(x, y)\mathrm{d}x\mathrm{d}y = \int\limits_0^A \frac{\sin(x)}{x}\mathrm{d}x$. Or $\int\limits_0^A f(x, y)\mathrm{d}x = \frac{1-\exp(-yA)\cos(A)-y\exp(-yA)\sin(A)}{1+y^2}$. Le théorème de convergence dominée permet de conclure.

Deuxième méthode (Formule des résidus). [Candelpergher, 2004] Par convergence dominée : $\int\limits_0^{+\infty} \frac{\sin(t)}{t}\mathrm{d}t = \det_{\varepsilon\to0,\, R\to+\infty} \frac{1}{2i}\left(\int\limits_{-R}^{-\varepsilon} \frac{\exp(it)}{t}\mathrm{d}t + \int\limits_{\varepsilon}^{R} \frac{\exp(it)}{t}\mathrm{d}t\right)$.
Étude de la fonction $z \mapsto \frac{\exp(iz)}{z} \in \mathcal{H}(\mathbb{C} \setminus \{0\})$ sur $K_{\varepsilon,R}$ défini par un joli dessin. La fonction est holomorphe donc l'intégrale est nulle. On regarde chacune des contributions. L'intégrale sur le grand cercle est nulle à la limite, celle sur le petit tend vers $-i\pi$ par convergence dominée, et on a le résultat.

Troisième méthode (Continuité de la transormée de laplace en 0). [Pommelet, 1994] Pour $x > 0$, on pose $L(x) = \int\limits_0^{+\infty} \exp(-xt)\frac{\sin(t)}{t}\mathrm{d}t$.
On montre que $\det_{x\to0} L(x) = \int\limits_0^{+\infty} \frac{\sin(t)}{t}\mathrm{d}t$ par intégration par parties puis Cesaro continu. On montre que L est de classe $\mathcal{C}^1$ sur $\mathbb{R}_+^*$ par théorème sur les intégrales à paramètre. Par une double intégration par parties, on montre que L' est la dérivée de $-\mathrm{Arctan}$. On détermine la constante d'intégration par convergence dominée.

Quatrième méthode (Transformée de Fourier Plancherel). Le sinus cardinal est la transformée de Fourier de l'indicatrice d'un segment. Ces deux fonctions étant $\mathbb{L}^2$, elles ont même norme $\mathbb{L}^2$. Le calcul de norme, qui repose sur une formule de trigonométrie et une intégration par parties, donne le résultat.

IV. Un peu de fonction Gamma

Définition. de la fonction γ sur $\{z \in \mathbb{C}|\mathcal{R}](z) > 0\}$. [Candelpergher, 2004]

Proposition. Prolongement holomorphe de Γ à $\mathbb{Z}_-$ à l'aide d'un calcul d'intégral.

Proposition. Pour tout $\alpha \in]0, 1[$, $I_\alpha = \int\limits_0^{+\infty} \frac{1}{t^\alpha(1+t)} = \frac{\pi}{\sin(\pi\alpha)}$.

Il faut considérer l'intégrale de la fonction $f : z \mapsto \frac{1}{z^\alpha(1+z)} \in \mathcal{H}(\mathbb{C} \setminus \{-1\})$ sur $K_{\varepsilon,R}$ défini par un joli dessin.

Proposition (formule des compléments). $\Gamma(\alpha)\Gamma(1-\alpha) = \frac{\pi}{\sin(\pi\alpha)}$.

63. **239 : Fonction définies par une intégrale dépendant d'un paramètre. Exemples et applications.**

I. Régularité des intégrales à paramètre.

I.1. *Intégrales à paramètre réel.*

Continuité des intégrales à paramètre. [Queffélec and Zuily, 2013]

Dérivabilité des intégrales à paramètre. [Queffélec and Zuily, 2013]

Application 1. [Moisan et al., 1992] Unicité de l'équation de la chaleur sur un segment.

Application 2. [Pommelet, 1994] La transformée de Laplace du sinus cardinal : $L(x) = \int_0^{+\infty} \exp(-tx)\frac{\sin(t)}{t}\mathrm{d}t$ est continue sur $[0,+\infty[$ et de classe $\mathcal{C}^1$ sur $]0,+\infty[$. On en déduit le calcul de l'intégrale $\int_0^{+\infty} \frac{\sin(t)}{t}\mathrm{d}t$.

Application 3. [Gasquet and Witomski, 1990] Calcul de la transformée de Fourier de la gaussienne.

Lemme de division d'Hadamard. [Gourdon, 1994a] [Beck et al., 2004] Factorisation d'une fonction de classe $\mathcal{C}^1$ s'annulant en 0 par la fonction monôme $x \mapsto x$. On en déduit par exemple que la valeur principale de $\frac{1}{x}$ est une distribution tempérée.

Remarque. En itérant le théorème on obtient des théorèmes du type caractère $\mathcal{C}^p$ des intégrales à paramètre.

I.2. *Intégrales à paramètre complexe.*

Holomorphie sous le signe intégrale. [Queffélec and Zuily, 2013]

Remarque. Ce théorème illustre la puissance de la formule de Cauchy : on a seulement besoin d'un contrôle sur la fonction et pas sur sa dérivée. A ce titre, quand on est confronté à une intégrale à paramètre réel, on peut passer en variable complexe pour démontrer plus facilement l'holomorphie, et conclure par un argument de prolongement analytique.

Exemple 1. [Beck et al., 2004] Une deuxième méthode de calcul de l'intégrale de la gaussienne.

Exemple 2. [Queffélec and Zuily, 2013] La fonction Γ est définie et holomorphe sur $\{z \in \mathbb{C} | \mathrm{Re}(z) > 0\}$. On en déduit que la fonction Γ est $\mathcal{C}^\infty$ sur $\mathbb{R}_+^*$.

Prolongement méromorphe de la fonction Γ [Beck et al., 2004]

Formule des compléments. [Amar and Matheron, 2004]

II. Produit de convolution.

Remarque. La convolée de deux fonctions est un cas particulier d'intégrale à paramètre particulièrement exploitée en analyse.

Définition. [Beck et al., 2004] Fonction convolée de deux fonctions.

Exemples de classes de fonctions convolables.

(1) Convolution $\mathbb{L}^1 \times \mathbb{L}^1$ à valeurs dans $\mathbb{L}^1$.

(2) Convolution $\mathbb{L}^p \times \mathbb{L}^{p'}$ à valeurs dans $\mathbb{L}^\infty$, uniformément continue.

(3) Convolution $\mathbb{L}^1 \times \mathbb{L}^p$ à valeurs dans $\mathbb{L}^p$.

Convolution et régularisation. Transfert de la dérivée sur la fonction régulière avec de bonnes hypothèses.

Définition. Définition d'une approximation de l'unité.

Exemple. Exemple d'une approximation de l'unité.

Proposition. Régularisation par convolution.

Application. Densité des fonctions $\mathcal{C}_c^\infty$ dans $\mathbb{L}^p$

III. Transformée de Fourier.

Définition. [Gasquet and Witomski, 1990] Définition sur $\mathbb{L}^1$ de $\mathcal{F}$ et $\overline{\mathcal{F}}$.

Exemple. Transformée de Fourier d'une indicatrice.

Théorème de Riemann Lebesgue.

Formulaire. Propriété de $\mathcal{F}$ par rapport à la dérivation, la translation, la convolution.

Autres exemples. Transformée de Fourier de Cauchy.

Inversion de Fourier.

Application. Transformée de Fourier inverse de la transformée de Fourier de Cauchy.

Fourier Plancherel.

Application. Deuxième méthode de calcul de l'intégral du sinus cardinal.

Remarque. L'échange entre décroissance à l'infini et régularité motive l'introduction de l'espace de Schwartz.

Transformée de Fourier sur l'espace de Schartz.

Application. Formule sommatoire de Poisson et Shannon.

Application. Résolution de l'équation de la chaleur.

64. 240 : Produit de convolution, transformation de Fourier. Applications.

I. Convolution et régularisation.

I.1. *Deux exemples de fonctions convolables*

Définition. On dit que deux fonctions sont convolables lorsque $f \star g$ est bien définie.

Définition. [Beck et al., 2004] Convolution $\mathbb{L}^1 \times \mathbb{L}^1 \to \mathbb{L}^1$.

Proposition. [Beck et al., 2004] Cette opération fait de $\mathbb{L}^1$ une algèbre normée. Cette algèbre n'admet pas d'élément unité.

Définition. [Beck et al., 2004] Convolution $\mathbb{L}^p \times \mathbb{L}^q$. Cette convolution est à valeurs dans les fonctions bornées uniformément continues.

I.2. *Régularisation.*

Proposition. [Beck et al., 2004] Quelques exemples du comportement de la convolution vis à vis de la dérivation.

Application. On pose $G_t(x))\exp(-\frac{x^2}{2t})$. Solution de l'équation de la chaleur. Alors pour f continue bornée, $F(x,t) = (f \star G_t)$ est encore solution.

Définition. [BRIANE-PAGES]
(1) Définition d'une approximation de l'unité. (On pourrait même parler de dirac approché)
(2) Définition d'une suite régularisante.

Exemple. [BRIANA] Exemple d'une approximation de l'unité.

Proposition. Convergence de la convolution d'une fonction avec une approximation de l'unité.

Applications.
(1) Densité des fonctions $\mathcal{C}^\infty$ dans $\mathbb{L}^p$.
(2) Riemann Lebesgue pour les coefficients de Fourier.

Un exemple célèbre de régularisation par convolution : Le noyau de Féjer.

Théorème de Féjer.

II. Transformée de Fourier.

II.1. *Transformée de Fourier* $\mathbb{L}^1$

Définition. [Gasquet and Witomski, 1990] de la transformée de Fourier $\mathcal{F}$ et de $\overline{\mathcal{F}}$ dans $\mathbb{L}^1$.

Exemples. [Gasquet and Witomski, 1990]

(1) Transformée de Fourier d'une indicatrice.

(2) Transformée de Fourier de $x \mapsto \exp(-a|x|)$.

(3) Transformée de Fourier d'une gaussienne.

Théorème. [Gasquet and Witomski, 1990] Théorème de Riemann-Lebesgue.

Proposition. [Gasquet and Witomski, 1990] Propriétés de la transformée de Fourier vis à vis de la dérivation, de la translation, et de la convolution.

Théorème. [Gasquet and Witomski, 1990] Théorème d'inversion de Fourier.

Théorème. Transformée de Fourier Plancherel.

Application. Calcul de l'intégrale du sinus cardinal.

II.2. *Espace de Schwartz* $\mathcal{S}(\mathbb{R})$

Définition. [Gasquet and Witomski, 1990] On dit que $f : \mathbb{R} \longrightarrow \mathbb{C}$ est à décroissance rapide lorsque pour tout $p \in \mathbb{N}$ on a :

$$\det_{|x| \to +\infty} |x^p f(x)| = 0.$$

Proposition. [Gasquet and Witomski, 1990]

(1) Soit f une fonction de $\mathbb{L}^1(\mathbb{R})$ à décroissance rapide. Alors $\hat{f}$ est indéfiniment dérivable.

(2) Réciproquement, soit $f \in \mathcal{C}^\infty(\mathbb{R})$. Si pour tout $f \in \mathbb{N}$, $f^{(k)}$ est dans $\mathbb{L}^1(\mathbb{R})$ alors $\hat{f}$ est à décroissance rapide.

Moralité. La transformée de Fourier échange décroissance à l'infini et régularité. On va définir un espace de fonctions qui sont à la fois très régulières et très décroissantes à l'infini, ce sera commode pour généraliser la transformée de Fourier.

Définition. [Gasquet and Witomski, 1990] $\mathcal{S}(\mathbb{R})$ est le sous-ensemble des fonctions $f \in \mathcal{C}_c^\infty(\mathbb{R})$ tel que pour tout $(\alpha, \beta) \in \mathbb{N}^2$:

$$\det_{|x| \to +\infty} |x^\alpha f^{(\beta)}(x)| = 0.$$

Exemple. Pour $z \in \mathbb{C}$ tel que $\mathrm{Re}(z) > 0$, $\varphi(x) = \exp(-zx^2)$ est dans $\mathcal{S}(\mathbb{R})$.

Propriétés. [Gasquet and Witomski, 1990]

(1) $\mathcal{S}(\mathbb{R})$ est stable par multiplication par un polynôme.

(2) $\mathcal{S}(\mathbb{R})$ est stable par dérivation.

(3) $\mathcal{S}(\mathbb{R}) \subset \mathbb{L}^p(\mathbb{R})$.

Proposition. L'espace $\mathcal{S}(\mathbb{R})$ est stable par transformation de Fourier : $f \in \mathcal{S}(\mathbb{R}) \Rightarrow \hat{f} \in \mathcal{S}(\mathbb{R})$.

Propriétés. [Gasquet and Witomski, 1990]

(1) Pour tout $(\alpha, \beta) \in \mathbb{N}^2$ on pose $p_{\alpha,\beta} = \sup\{|x^\alpha f^{(\beta)}(x)|\}$. C'est une famille de semi-normes sur $\mathcal{S}(\mathbb{R})$ qui fait de $\mathcal{S}(\mathbb{R})$ un espace métrisable complet.

(2) Pour cette topologie, la dérivation et la transformation de Fourier sont des opérations continues.

Théorème. [Gasquet and Witomski, 1990] La transformation de Fourier $\mathcal{F}$ est une application linéaire bijective et bicontinue de $\mathcal{S}(\mathbb{R})$ sur $\mathcal{S}(\mathbb{R})$. L'application inverse est $\overline{\mathcal{F}}$.

Remarque. L'espace de Schwartz permet de définir les distributions tempérées $\mathcal{S}'(\mathbb{R})$ comme le dual de $\mathcal{S}(\mathbb{R})$, et la transformée de Fourier de tels distributions.

Exemples.

(1) Transformée de Fourier du dirac.

(2) Transformée de Fourier de la valeur principale de $\frac{1}{x}$ et de H.

III. Quelques domaines d'applications.

III.1. *Probabilités*

Définition. [Ouvrard, 2004] de la fonction caractéristique d'une variable aléatoire.

Proposition. La fonction caractéristique caractérise la loi.

Théorème. Théorème central limite.

III.2. *Traitement du signal.*

Théorème. [Gourdon, 1994a] Formule sommatoire de Poisson.

Application. Théorème de Shannon.

III.3. *Résolution d'équations aux dérivées partielles*

Exemple. [BONY] Équation de la chaleur sur une barre infinie.

65. **241 : Suites et séries de fonctions. Exemples et contre-exemples.**

On admet les définitions de convergence simple et uniforme.

I. Théorèmes et exemples généraux.

I.1. *Régularité*

Proposition. Une limite uniforme de fonctions continues est continue. [Moisan et al., 1992]

Exemple. Pour tout $n \in \mathbb{N}^*$, on pose $f_n = \left(1 - \frac{\cdot}{n}\right)^n \mathbb{1}_{[0,n]} \in \mathcal{C}^0(\mathbb{R}_+)$. On a alors convergence uniforme sur $\mathbb{R}_+$ de $(f_n)_{n\in\mathbb{N}}$ vers l'application $\exp(-\cdot) \in \mathcal{C}^0(\mathbb{R}_+)$. [Madère, 1997]

Contre-exemple. Pour tout $n \in \mathbb{N}^*$, pour tout $x \in [0,1]$, on pose $f_n(x) = x^n$. La suite $(f_n)_{n\in\mathbb{N}}$ est continue et converge simplement vers $\mathbb{1}_{\{1\}}$ qui n'est pas continue. La convergence n'est ici pas uniforme. [Combes, 1982]

Proposition. Sur le caractère $\mathcal{C}^1$ d'une limite de fonctions $\mathcal{C}^1$. [Moisan et al., 1992]

Contre-exemple.

(1) Pour tout $n \in \mathbb{N}^*$, pour tout $x \in \mathbb{R}$, on pose $f_n(x) = \sqrt{x^2 + \frac{1}{n^2}}$. Alors la suite $(f_n)_{n\in\mathbb{N}}$ est de classe $\mathcal{C}^\infty(\mathbb{R})$ et converge uniformément vers $|\cdot|$, fonction qui n'est pas dérivable en 0. [Hauchecorne, 1988]

(2) Pour tout $n \in \mathbb{N}^*$, pour tout $x \in \mathbb{R}$, on pose $f_n(x) = \frac{sin(n^2x)}{n}$. Alors la suite $(f_n)_{n\in\mathbb{N}}$ est de classe $\mathcal{C}^\infty(\mathbb{R})$ et converge uniformément vers la fonction nulle, mais pour tout $n \in \mathbb{N}^*$, $f_n'(0) = n$ qui tend vers l'infini lorsque n tend vers $+\infty$. [Pommelet, 1994] [Madère, 1997]

Théorème. sur la convergence des suites de fonctions holomorphes.

Exemple. Convergence d'une suite de fonction holomorphes.

Remarque. En appliquant ses résultats à la suite des sommes partielles, on peut les étendre aux séries de fonctions.

Applications.

(1) Équation de la chaleur sur un segment. [Queffélec and Zuily, 2013] [Moisan et al., 1992]

(2) Holomorphie de la fonction ζ sur le demi-plan

I.2. *Autres résultats.*

Proposition. La convergence uniforme sur un segment permet d'intervertir limite et intégral. [Combes, 1982]

Contre-exemple. $\frac{1}{n}\mathbb{1}_{[0,n]}$ converge uniformément vers 0 sur $\mathbb{R}$ mais pas en norme $\mathbb{L}^1$

Remarque. Il s'agit seulement de conditions suffisantes. x^n sur $[0,1]$ ne converge pas uniformément vers 0, mais converge vers 0 en norme $\mathbb{L}^1$. La théorie de la mesure (théorème de Beppo-Lévi et de convergence dominée) répondent à ces questions. [Combes, 1982]

Proposition. Dini lorsque $(f_n(x))_n$ est décroissante. [Combes, 1982]

Application. Convergence uniforme de $P_0 = 0$ et $P_{n+1} = P_n(x) + \frac{1}{2}(x - (P_n(x))^2)$ vers $\sqrt{x}$ sur $[0,1]$.

Théorème. Weierstrass.

Exemple. L'exponentielle.

Application. Théorème des moments. [Pommelet, 1994]

Contre-exemple. Une limite unforme de polynômes sur $\mathbb{R}$ est un polynôme. [Pommelet, 1994]

Théorème. de Borel. [Rouvière, 1999]

II. Séries entières.

II.1. *Propriétés.*

Définition. d'une série entière. [Gourdon, 1994a]

Proposition (Lemme d'Abel). [Gourdon, 1994a]

Définition. du rayon de convergence et de la somme d'une série entière. [Gourdon, 1994a]

Proposition. (Régle de d'Alembert). [Gourdon, 1994a]

Exemples. Trois séries entières dont le rayon peut être déterminé par d'Alembert. On exhibe aussi le fait que le rayon peut être nul, infini, ou réel.

Proposition. Citer comme un résultat théorique la formule d'Hadamard pour le rayon de convergence. [Gourdon, 1994a]

Applications.

(1) $a_n = \exp(\cos(n))$ rayon de convergence $\frac{1}{\mathrm{e}}$.

(2) Une série entière et la série dérivée terme à terme ont même rayon de convergence.

Remarque. Sur le cercle de convergence, la série peut diverger ou converger ponctuellement.

Exemples. $a_n = \frac{1}{n}$ on a convergence au bord, sauf en $z = 1$.

II.2. *Régularité de la somme.*

Proposition. Continuité de la somme d'une série entière sur le disque ouvert de convergence.

Proposition. [Pommelet, 1994]

(1) Les séries entières $\sum_{n=0}^{+\infty} a_n z^n$ et $\sum_{n=0}^{+\infty} (n+1)a_{n+1}z^n$ ont même rayon de convergence.

(2) La somme d'une série entière réelle est infiniment dérivable sur son intervalle ouvert de convergence. Expression de la dérivée et unicité des coefficients.

(3) La somme d'une série entière complexe est holomorphe sur le disque ouvert de convergence.

Exemples. $\frac{1}{(1-x)^2}$ s'obtient par dérivation de $\frac{1}{1-x}$

II.3. *Quelques applications.*

Proposition. (Applications en combinatoire) Calcul du nombre de relations d'équivalences sur l'ensemble $\{1, \cdots, n\}$ par l'introduction de séries génératrices. [Pommelet, 1994]

Proposition. (équation différentielle du premier ordre) [Moisan et al., 1992]

Proposition. Série génératrice des moments. [Ouvrard-1].

III. Séries de Fourier.

Définition des coefficients de Fourier et de la série de Fourier. (si elle converge).

Contre-exemple.

(1) Une fonction continue dont la série de Fourier diverge. [Hauchecorne, 1988]

(2) Existence d'un G_δ dense de fonctions continues 2π périodique dont les séries de Fourier divergent sur un G_δ contenant $\mathbb{Q}$. [Gourdon, 1994a] [Rudin-Analyse fonctionnelle.]

Théorème. de convergence de Dirichlet dans le cas $\mathcal{C}^1_{pm}$. [Gourdon, 1994a]

Théorème. de convergence normale de Dirichlet. [Gourdon, 1994a]

Théorème. Définition du noyau de Féjer et théorème de convergence de Féjer. [Combes, 1982]

Proposition. Parseval. [Gourdon, 1994a]

Exemples.

(1) de calculs de somme grâce à Fourier. (dessins en annexe) [Gourdon, 1994a]

(2) Inégalité isopérimétrique [Queffélec and Zuily, 2013]

(3) Formule sommatoire de Poisson et application. [Gourdon, 1994a] [Gasquet and Witomski, 1990]

66. **243 : Convergence des séries entières, propriétés de la somme. Exemples et applications.**

I. Définition et premières propriétés.

I.1. *Domaine et détermination du domaine de définition.*

Définition. d'une série entière. [Gourdon, 1994a]

Proposition (Lemme d'Abel). [Gourdon, 1994a]

Définition. du rayon de convergence et de la somme d'une série entière. [Gourdon, 1994a]

Proposition. Détermination du rayon par comparaison. Si les suites sont équivalentes, les rayons sont les mêmes, si les suites sont ordonnées, les rayons sont ordonnés dans le sens contraire. [Beck et al., 2004]

Proposition. (Régle de d'Alembert). [Gourdon, 1994a]

Exemples. Trois séries entières dont le rayon peut être déterminé par d'Alembert. On exhibe aussi le fait que le rayon peut être nul, infini, ou réel.

Proposition (Règle de Cauchy). [Gourdon, 1994a]

Remarque. La règle de Cauchy s'applique quand celle de d'Alembert s'applique.

Proposition. Citer comme un résultat théorique la formule d'Hadamard pour le rayon de convergence. [Gourdon, 1994a]

Applications.

(1) $a_n = \exp(\cos(n))$ rayon de convergence $\frac{1}{e}$.
(2) Une série entière et la série dérivée terme à terme ont même rayon de convergence.

Remarque. Sur le cercle de convergence, la série peut diverger ou converger ponctuellement.

Exemples. $a_n = \frac{1}{n}$ on a convergence au bord, sauf en $z = 1$.

I.2. *Opérations sur les séries entières, régularité de la somme.*

Proposition. Somme et produit de Cauchy de deux séries entières. Propriétés du rayon. [Gourdon, 1994a]

Proposition. Continuité de la somme d'une série entière sur le disque ouvert de convergence.

Proposition. [Pommelet, 1994]

(1) Les séries entières $\sum_{n=0}^{+\infty} a_n z^n$ et $\sum_{n=0}^{+\infty} (n+1)a_{n+1}z^n$ ont même rayon de convergence.

(2) La somme d'une série entière réelle est infiniment dérivable sur son intervalle ouvert de convergence. Expression de la dérivée et unicité des coefficients.

(3) La somme d'une série entière complexe est holomorphe sur le disque ouvert de convergence.

Exemples. $\frac{1}{(1-x)^2}$ s'obtient par dérivation de $\frac{1}{1-x}$

Proposition. Intégration de séries entières.

Application. $\ln(1+x)$ et $\mathrm{Arctan}(x)$

Théorèmes Abel angulaire, taubérien faible, taubérien fort.

II. Applications des séries entières.

II.1. *fonctions développables en séries entières*

Définition. d'une fonction développable en série entière et d'une fonction analytique.

Proposition. [Pommelet, 1994] Si une fonction est DSE alors elle est analytique sur son disque ouvert de convergence. En particulier les points d'analycité d'une fonction analytique forment un ensemble ouvert.

Proposition.

(1) Il y a au moins un point singulier sur le cercle de convergence. [Queffélec and Zuily, 2013]

(2) Il existe des cas où tous les points sont singuliers (séries lacunaires). [Queffélec and Zuily, 2013]

Proposition. [Beck et al., 2004]

(1) Principe des zéros isolés

(2) Principe du prolongement analytique

Applications.

(1) Formule de trigonométries complexes.

(2) Formule des compléments.

(3) Prolongement analytique de Γ (On utilise aussi un développement en série entière et une interversion $\sum \int$).

Proposition. Liouville.

Application. Un polynôme complexe est scindé.

Application. (en probabilités) Définition de la fonction génératrice d'une variable aléatoire + quelques propriétés. [Ouvrard 1].

Proposition. (Applications en combinatoire)

(1) Calcul du nombre de relations d'équivalences sur l'ensemble $\{1, \cdots, n\}$ par l'introduction de séries génératrices. [Pommelet, 1994]

(2) Calcul du cardinal d'un arbre binaire à n noeuds. [Moisan et al., 1992] [X-ENS algèbre 1]

(3) Nombre de dérangements d'un ensemble à n éléments. [X-ENS algèbre 1]

Proposition. (équation différentielle du premier ordre) [Moisan et al., 1992]

Proposition. (équation différentielle du second ordre) [Moisan et al., 1992]

67. 244 : Fonctions développables en série entière, fonctions analytiques. Exemples.

I. Définitions et propriétés.

I.1. *Les série entières.*

Définition. d'une série entière réelle et complexe. [Queffélec and Zuily, 2013]

Définition. du rayon de convergence. [Queffélec and Zuily, 2013]

Proposition (Lemme d'Abel). [Queffélec and Zuily, 2013]

Proposition. Opérations compatibles avec les séries entières. [Gourdon, 1994a] [Combes, 1982]

Proposition. [Pommelet, 1994]

(1) Les séries entières $\sum_{n=0}^{+\infty} a_n z^n$ et $\sum_{n=0}^{+\infty} (n+1)a_{n+1}z^n$ ont même rayon de convergence.
(2) La somme d'une série entière réelle est infiniment dérivable sur son intervalle ouvert de convergence.
(3) La somme d'une série entière complexe est holomorphe sur le disque ouvert de convergence.

I.2. *Fonctions développables en série entière et analytiques.*

Définitions. [Pommelet, 1994]

(1) d'une fonction développable en série entière.
(2) d'une fonction analytique sur $\mathbb{R}$ et $\mathbb{C}$.

Remarque. [Beck et al., 2004] Une fonction analytique réelle est la restriction d'une fonction analytique complexe.

Proposition. Opérations compatibles avec le caractère développable en série entières.

Exemples. $\exp(x)$, $\frac{1}{1-x}$, $\ln(1-x)$.

II. Relations entre classes de fonctions.

II.1. *Fonctions développables en série entière et analycité*

Proposition. [Pommelet, 1994]

(1) Si une fonction est DSE alors elle est analytique sur son disque ouvert de convergence. En particulier les points d'analycité d'une fonction analytique forment un ensemble ouvert.

(2) Une fonction analytique réelle est de classe $\mathcal{C}^\infty$, une fonction analytique complexe est holomorphe.

Proposition. [Beck et al., 2004]

(1) Principe des zéros isolés

(2) Principe du prolongement analytique

Applications.

(1) Formule de trigonométries complexes.

(2) Formule des compléments.

(3) Prolongement analytique de Γ

II.2. *Analycité réelle vs* $\mathcal{C}^\infty$

Contre-exemple. Le caractère $\mathcal{C}^\infty$ n'implique pas l'analycité réelle. Par exemple $x \mapsto \exp(-\frac{1}{x^2})$ prolongée par 0 en $x = 0$ est $\mathcal{C}^\infty$ mais pas analytique. [Beck et al., 2004]

Proposition. Soit f $\mathcal{C}^\infty$ sur I. Alors f analytique sur I ssi son reste intégral de Taylor tend simplement vers 0. [Gourdon, 1994a]

Voilà une condition suffisante pour que l'implication fonctionne :

Proposition (Bernstein et Valiron). [Combes, 1982]

(1) Soit f $\mathcal{C}^\infty$ sur I. Si toutes les dérivées successives de f sur I sont positives, alors f est analytique sur I.

(2) Soit f $\mathcal{C}^\infty$ sur I. Si toutes les dérivées successives d'ordre paires de f sur I sont positives, alors f est analytique sur I.

Proposition. [Beck et al., 2004]

(1) On peut prescrire arbitrairement les valeurs successives des dérivées d'une fonction $\mathcal{C}^\infty(\mathbb{R})$ en un point. [Beck et al., 2004]

(2) On montrera que les dérivées d'une fonction analytique réelle vérifient une majoration rigide. [Pommelet, 1994]

Remarque. Les fonctions $\mathcal{C}^\infty$ peuvent être à support compact. Pas les fonctions analytiques réelles d'après le principe des zéros isolés. [Beck et al., 2004]

II.3. *Analycité complexe et holomorphie.*

Définition. d'une fonction holomorphe sur un ouvert. [Beck et al., 2004]

Proposition. Formule intégrale de Cauchy. [Beck et al., 2004]

Théorème. Si f est holomorphe sur un ouvert, alors elle est analytique sur cet ouvert. [Beck et al., 2004]

III. Applications.

Voir la partie applications de la leçon séries entières.

68. **245 : Fonctions holomorphes sur un ouvert de $\mathbb{C}$. Exemples et applications.**

I. Définitions et premiers exemples.

Définition. [Amar and Matheron, 2004] d'une fonction holomorphe.

Proposition. Conditions de Cauchy-Riemann [Beck et al., 2004] (rajouter la condition polaire $\frac{\partial f}{\partial \theta}(r,\theta) = ir\frac{\partial f}{\partial r}(r,\theta)$.

Contre-exemple. Fonction vérifiant les conditions de Cauchy-Riemann en $(0,0)$ mais n'étant pas différentiable, et qui en plus n'est pas holomorphe.

Définition. D'une fonction analytique.

Proposition. Les fonctions analytiques sont holomorphes.

I.1. *Exponentielle complexe*

Définition. de l'exponentielle complexe. L'exponentielle complexe est holomorphe sur $\mathbb{C}$ et est sa propre dérivée.

Proposition. L'exponentielle complexe réalise un homomorphisme surjectif de $(\mathbb{C},+)$ sur $(\mathbb{C},\times)$, homomorphisme de noyau $2i\pi\mathbb{Z}$.

Définition. Du sinus et du cosinus complexe.

I.2. *Logarithme complexe*

Définition. Définition de la détermination principale du logarithme complexe sur $\mathbb{C}\setminus\mathbb{R}_-$. $\mathrm{Log}(z) = \ln(|z|) + i\mathrm{Arg}(z)$.

Proposition. Le logarithme complexe est holomorphe sur $\mathbb{C}\setminus\mathbb{R}_-$. Sa dérivée est la fonction inverse.

Définition. Détermination principale de la racine k-ème.

II. Propriétés fondamentales des fonctions holomorphes.

II.1. *Formule de Cauchy.*

Théorème. [Beck et al., 2004] Formule de Cauchy. [Beck et al., 2004] (Attention le chemin doit être pris $\mathcal{C}^1$ par morceaux.

Conséquence. [Amar and Matheron, 2004] Toute fonction holomorphe est infiniment $\mathbb{C}$ dérivable. Formule de Cauchy généralisée.

Proposition. Formule de la moyenne.

Théorème. Si f est une fonction holomorphe sur un disque ouvert $\mathrm{D}(z_0, R)$, on a :

$$f(z) = \sum_{n=0}^{+\infty} \frac{f^{(n)}(z_0)}{n!}(z - z_0)^n.$$

Corollaire. Si f est holomorphe sur un ouvert, alors elle est analytique sur cet ouvert.

Corollaire. Toute fonction holomorphe sur un disque admet des primitives holomorphes.

II.2. *Intégrale à paramètre holomorphe*

Théorème. Holomorphie d'une intégrale à paramètre.

Exemple. Défintion et holomorphie de la fonction Γ.

Exemple. Calcul de la transformée de Fourier d'une gaussienne. [Beck et al., 2004]

II.3. *Zéros de fonctions holomorphes.*

Théorème. du prolongement analytique.

Exemples.

(1) Il existe une unique fonction holomorphe sur $\mathbb{C}$ vérifiant $f(\frac{1}{n}) = \frac{1}{n}$ pour tout $n \in \mathbb{N}*$. [Beck et al., 2004]

(2) Démonstration de la formule des compléments.

Proposition. Principe des zéros isolés sur un connexe.

Théorème. Théorème de Liouville.

Application. Tout polynôme on constant à coefficients complexes admet au moins une racine complexe.

Théorème. Principe du maximum.

Application. Soit Ω un ouvert connexe de $\mathbb{C}$ qui contient le disque unité fermé. Soit f une fonction holomorphe sur Ω telle que $f(0) = 1$ et $|f(z)| \geq 2$ sur le cercle unité. Alors f s'annule sur le disque unité.

Application. Lemme de Schwarz.

II.4. *Suite de fonctions holomorphes.*

Définition. de la topologie métrique sur $\mathcal{H}(\Omega)$.

Théorème. de convergence de Weierstrass.

Théorème. Théorème de Montel.

Application. Il n'existe pas de norme sur $\mathcal{H}(\Omega)$ qui définisse la même topologie que la métrique définie plus haut.

III. Résidus, applications.

Définition. D'une fonction méromorphe. Du résidus d'une fonction méromorphe en un complexe.

Proposition. Série de fonctions méromorphes.

Exemple. [Beck et al., 2004] La série qui intervient dans le prolongement de la fonction Γ est méromorphe. La fonction Γ admet un unique prolongement méromorphe à $\mathbb{C} \setminus \mathbb{Z}_-$

Théorème. Théorème des résidus.

Applications. Calculs d'intégrales :

(1) Calcul de l'intégrale sur $\mathbb{R}$ de certaines fractions rationnelles.
(2) Calcul de l'intégrale sur $\mathbb{R}_+$ du sinus cardinal.
(3) Formule des compléments

Théorème de Rouché. [Beck et al., 2004]

Application. [Beck et al., 2004]

69. **246 : Séries de Fourier. Exemples et applications.**

I. Théories des séries de Fourier

Définition. [Beck et al., 2004] Pour $f \in \mathbb{L}^1([0, 2\pi])$, et pour tout $n \in \mathbb{Z}$ on définit $c_n(f) = \frac{1}{2\pi} \int_0^{2\pi} f(x) exp(-inx) \mathrm{d}x$ le n-ième coefficient de Fourier de f. On définit la somme partielle de la série de Fourier d'ordre N, par $S_N(f) = \sum_{|n| \leq N} c_n(f) e_n$.

I.1. *Série de Fourier dans* $\mathbb{L}^2([0, 2\pi])$

Proposition. [Beck et al., 2004] La famille de fonctions $(e_n = x \mapsto \exp(inx))_{n \in \mathbb{Z}}$ est une base hilbertienne de $\mathbb{L}^2([0, 2\pi])$.

Interprétation hilbertienne. [Beck et al., 2004] Sur l'espace $\mathbb{L}^2([0, 2\pi])$ on a donc $c_n(f) = \langle f, e_n \rangle$ et $S_N(f) = P_{V_N}(f)$ c'est à dire la projection orthogonale sur $V_N = \mathrm{Vect}(e_n, |n| \leq N)$.

Proposition. [Beck et al., 2004] (Parseval)

(1) Pour $f \in \mathbb{L}^2([0, 2\pi])$, on a $\det_{N \to +\infty} ||S_n(f) - f||_2 = 0$

(2) L'application $f \mapsto (c_n(f))_n$ est une isométrie bijective de $\mathbb{L}^2([0, 2\pi])$ sur $l^2(\mathbb{Z})$, on a donc l'égalité de Parseval :

$$||f||_2 = \sum_{-\infty}^{+\infty} |c_n(f)|^2$$

Application. [Gourdon, 1994a] au calcul de sommes.

I.2. *Série de Fourier sur* $\mathbb{L}^1([0, 2\pi])$

Définition. [Beck et al., 2004] Définition du produit de convolution sur $\mathbb{L}^1([0, 2\pi])$ et de l'algèbre $(\mathbb{L}^2([0, 2\pi]), +, \star, || \cdot ||_1)$

Proposition. [Beck et al., 2004] (Riemann Lebesgue). Pour tout $f \in \mathbb{L}^1([0, 2\pi])$, la suite $(c_n(f))_n$ tend vers 0 en $\pm\infty$. On note cet espace de suites $c_0(\mathbb{Z})$.

Théorème. L'application qui à $f \in \mathbb{L}^1([0, 2\pi])$ associe la suite de ses coefficients de Fourier est un morphisme d'algèbre continu, injectif, de norme 1, de $(\mathbb{L}^2([0, 2\pi]), +, \star, || \cdot ||_1)$ dans mais PAS SUR $(c_0(\mathbb{Z}), +, \cdot, || \cdot ||_\infty)$.

I.3. *Le bon et le mauvais noyau*

Définition. [Beck et al., 2004]

(1) Définition de la suite des noyaux de Dirichlet $D_N = \sum_{|n|\leq N} e_n$.
$D_N(x) = \frac{\sin(\frac{2N+1}{2}x)}{\sin(\frac{x}{2})}$.

(2) Définition de la suite des noayux de Féjer $K_N = \frac{1}{N}\sum_{n=0}^{N-1} D_n$.
$K_N(x) = \frac{1}{N}\left(\frac{\sin(\frac{Nx}{2})}{\sin(\frac{x}{2})}\right)^2$.

Remarque. Le gros défaut du noyau de Dirichlet est qu'il n'est pas de signe constant.

Proposition. [Beck et al., 2004]

(1) Pour $f \in \mathbb{L}^1([0,2\pi])$ on définit la suite de ses sommes de Cesaro : $\sigma_N(f) = \frac{1}{N}\sum_{n=0}^{N-1} S_n(f)$. On a $\sigma_N(f) = f \star K_N$.

(2) On a $S_N(f) = f \star D_N$.

Théorème. [Beck et al., 2004] de Féjer.

(1) Si f est continue, $\sigma_N(f)$ converge uniformément vers f.

(2) Si f est dans $\mathbb{L}^1([0,2\pi])$ ou $\mathbb{L}^2([0,2\pi])$, $\sigma_N(f)$ converge vers f pour $||\cdot||_1$ ou $||\cdot||_2$.

Conséquences. [Beck et al., 2004]

(1) Densité des polynômes trigonométriques dans l'espace des fonctions continues sur $[0,2\pi]$.

(2) Injectivité de l'application qui à f dans $\mathbb{L}^1([0,2\pi])$ associe la suite de ses coefficients de Fourier.

I.4. *Un problème délicat : la convergence ponctuelle.*

Théorème. [Gourdon, 1994a] [RUDIN] Il existe $G \subset \mathcal{C}^0_{2\pi}$ un G_δ dense tel que, pour tout $f \in G$, $S_N(f)$ diverge sur $G(f)$ un G_δ dense de $\mathbb{R}$.

Théorème de Dirichlet. [Beck et al., 2004] Si $f \in \mathbb{L}^1([0,2\pi])$ admet en un point à la fois une limite à droite et à gauche et si :

$$h \mapsto \frac{1}{h}(f(x_0+h) + f(x_0-h) - f(x_0^+) - f(x_0^-)]$$

est bornée au voisinage de 0, alors on a :

$$S_N(f)(x_0) \to \frac{1}{2}(f(x_0^+) + f(x_0^-))$$

Remarque. Une fonction $\mathcal{C}^1$ par morceaux vérifie ses hypothèses.

Exemple. [Beck et al., 2004] Pour $a \in]0,\pi[$, on a l'égalité : $\frac{\pi-a}{2} = \sum_{n=1}^{+\infty} \frac{\sin(na)}{n}$

Théorème. Théorème de convergence normale de Dirichlet pour une fonction continue et de classe $\mathcal{C}^1$ par morceaux.

II. Applications des séries de Fourier

Une inégalité importante. Inégalité de Poincarré Wirtinger.

Application 1. Définition d'un produit scalaire sur $H_0^1([0,1])$ qui donne une norme équivalente à la norme $||\cdot||_{H^1([0,1])}$.

Application 2. Inégalité isopérimétrique.

Résolution de l'équation de la chaleur sur un segment. [Moisan et al., 1992] [Candelpergher, 2004]

Résolution de l'équation des ondes sur un segment. [Moisan et al., 1992]

Formule sommatoire de Poisson.

Application. Une règle d'échantillonnage de Shanon.

70. **247 : Exemples de problèmes d'interversions de limites.**

I. Préliminaires.

Contre-exemple 1. Pour tout $n \in \mathbb{N}^*$, pour tout $x \in \mathbb{R}^*$, on pose $f_n(x) = \frac{x}{x+n}$. On a :

$$0 = \det_{x\to+\infty} \det_{n\to+\infty} f_n(x) \neq \det_{n\to+\infty} \det_{x\to+\infty} f_n(x) = 1.$$

Contre-exemple 2. Pour tout $n \in \mathbb{N}^*$, on pose $f_n = \frac{1}{n} \mathbb{1}_{[0,n]}$. On a la convergence uniforme de (f_n) vers la fonction nulle, cependant :

$$1 = \det_{n\to+\infty} \int_{\mathbb{R}} f_n(x)\mathrm{d}x \neq \int_{\mathbb{R}} \det_{n\to+\infty} f_n(x)\mathrm{d}x = 0.$$

L'interversion des limites nécessite des hypothèses précises. Sinon on se retrouve face à des calculs dont les résultats sont incohérents, ou des suites d'objets réguliers dont la régularité est perdue à la limite.

II. Régularité des suites et des séries de fonctions.

Remarque 3. La continuité et la dérivabilité sont des notions locales définies comme des limites, ce qui correspond parfaitement au cadre de la leçon.

II.1. *Continuité.*

Théorème 4. Soient X un espace métrique, E un espace métrique, et $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions continues de $A \subset X$ dans E telle que $(f_n)_{n\in\mathbb{N}}$ **converge uniformément** vers f. Alors f est continue sur A.

Exemple 4. Pour tout $n \in \mathbb{N}^*$, on pose $f_n = \left(1 - \frac{\cdot}{n}\right)^n \mathbb{1}_{[0,n]} \in \mathcal{C}^0(\mathbb{R}_+)$. On a alors convergence uniforme sur $\mathbb{R}_+$ de $(f_n)_{n\in\mathbb{N}}$ vers l'application $\exp(-\cdot) \in \mathcal{C}^0(\mathbb{R}_+)$.

Contre-exemple 4. Pour tout $n \in \mathbb{N}^*$, pour tout $x \in [0,1]$, on pose $f_n(x) = x^n$. La suite $(f_n)_{n\in\mathbb{N}}$ est continue et converge simplement vers $\mathbb{1}_{\{1\}}$ qui n'est pas continue. La convergence n'est ici pas uniforme.

Théorème 5. (Double limite) Soient X un espace topologique, E un espace métrique complet, et $(f_n)_{n\in\mathbb{N}}$ une suite d'applications de $A \subset X$ dans E. Soit $a \in \overline{A}$, on suppose que :

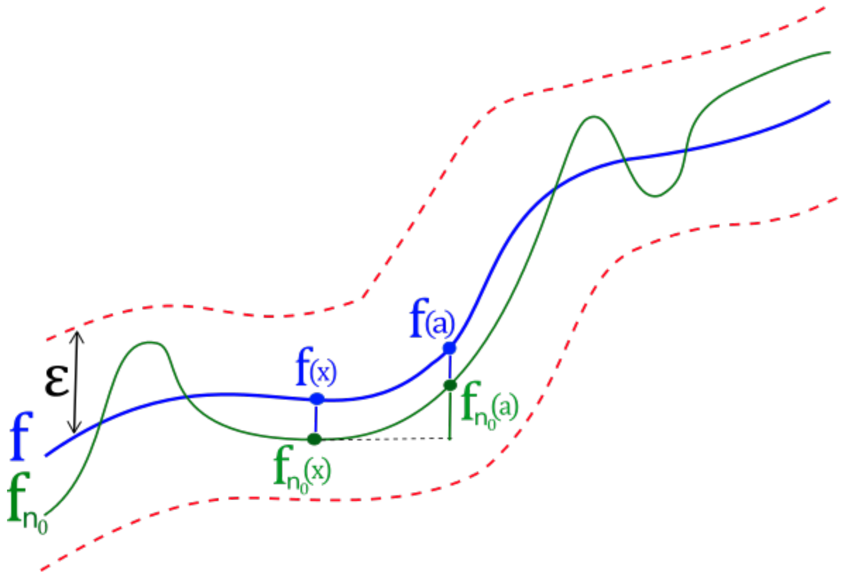
— la suite $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers f,

— pour tout $n \in \mathbb{N}$, $\det_{x\to a} f_n(x) = l_n$.

Alors $(l_n)_{n\in\mathbb{N}}$ converge et on a :

$$\det_{x\to a,\, x\in A} \det_{n\to+\infty} f_n(x) = \det_{n\to+\infty} \det_{x\to a,\, x\in A} f_n(x) = \det_{n\to+\infty} l_n.$$

FIGURE 1. La preuve de ce théorème repose sur ce dessin.



Exemple 5. Soit E un espace de Banach, et $u \in \mathcal{L}_c(E)$. Alors on a :

$$\det_{n\to+\infty}\left(\mathrm{Id}+\frac{u}{n}\right)^n = \exp(u).$$

Contre-exemple 5. Pour tout $n \in \mathbb{N}^*$, pour tout $x \in \mathbb{R}_+^*$, on pose $f_n(x) = \mathrm{Arctan}\left(\frac{x}{n}\right)$. Alors la suite $(f_n)_{n\in\mathbb{N}}$ converge simplement mais pas uniformément vers la fonction nulle. On constate que pour tout $x > 0$, $\det_{n\to+\infty} f_n(x) = \frac{\pi}{2}$ mais on a :

$$0 = \det_{x\to+\infty}\det_{n\to+\infty} f_n(x) \neq \det_{n\to+\infty}\det_{x\to+\infty} f_n(x) = \frac{\pi}{2}.$$

Contre-exemple 5. Pour tout $n \in \mathbb{N}^*$, pour tout $x \in \mathbb{R}_+$, on pose $f_n(x) = \frac{2nx}{1+n^2x^2}$. Alors la suite $(f_n)_{n\in\mathbb{N}}$ converge simplement vers la fonction nulle, mais pas uniformément, cependant on a :

$$\det_{n\to+\infty}\det_{x\to 0} f_n(x) = \det_{x\to 0}\det_{n\to+\infty} f_n(x) = 0.$$

La continuité uniforme est une hypothèse suffisante mais pas nécessaire.

II.2. *Dérivabilité.*

Théorème 6. Soit $I \subset \mathbb{R}$ un intervalle, F un espace de Banach et $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions de classe $\mathcal{C}^1(I, F)$. On suppose que :
— il existe $x_0 \in I$ tel que $(f_n(x_0))_{n\in\mathbb{N}}$ converge,
— la suite $(f'_n)_{n\in\mathbb{N}}$ converge uniformément vers g.
Alors il existe $f \in \mathcal{C}^1(I, F)$ telle que $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers f et telle que $f' = g$.

Application 6. Soit $f \in \mathcal{C}^0(I, \mathbb{R})$. Alors, sans faire appel à l'intégration, on peut montre que f admet une primitive, en l'approchant uniformément par des fonctions affines par morceaux.

Contre-exemple 6. Pour tout $n \in \mathbb{N}^*$, pour tout $x \in \mathbb{R}$, on pose $f_n(x) = \sqrt{x^2 + \frac{1}{n^2}}$. Alors la suite $(f_n)_{n\in\mathbb{N}}$ est de classe $\mathcal{C}^\infty(\mathbb{R})$ et converge uniformément vers $|\cdot|$, fonction qui n'est pas dérivable en 0.

Contre-exemple 6. Pour tout $n \in \mathbb{N}^*$, pour tout $x \in \mathbb{R}$, on pose $f_n(x) = \frac{sin(n^2x)}{n}$. Alors la suite $(f_n)_{n\in\mathbb{N}}$ est de classe $\mathcal{C}^\infty(\mathbb{R})$ et converge uniformément vers la fonction nulle, mais pour tout $n \in \mathbb{N}^*$, $f_n'(0) = n$ qui tend vers l'infini lorsque n tend vers $+\infty$.
Ces deux contre-exemples montrent que la seule convergence simple d'une fonction, même très régulière, ne suffit pas à conclure sur la dérivabilité de sa limite.

Théorème 7. Soit E, F deux espaces de Banach et $U \subseteq E$ un ouvert. Soit $(f_n)_{n\geq 0}$ une suite d'applications différentiables sur U. On suppose qu'il existe une application $f : U \to F$ et L une application de U dans $\mathcal{L}_c(E, F)$ telles que :
— $(f_n)_{n\geq 0}$ converge simplement vers f sur U,
— $\mathrm{D}f_n$ converge uniformément vers L sur U.
Alors f est différentiable sur U et on a :

$$\mathrm{D}f = \mathrm{det}_{n\to+\infty} \mathrm{D}f_n.$$

En outre, si pour tout $n \geq 0$, $f_n \in \mathcal{C}^1(U, F)$, alors $f \in \mathcal{C}^1(U, F)$.

Application 7. L'exponentielle est de classe $\mathcal{C}^1$ sur $\mathcal{M}_n(\mathbb{C})$ et pour tout M, $H \in \mathcal{M}_n(\mathbb{C})$, on a :

$$\mathrm{D}_M\mathrm{exp}.H = \sum_{p=1}^{+\infty} \frac{1}{p!} \left(M^{p-1}H + M^{p-2}HM + \cdots MHM^{p-2} + HM^{p-1}\right).$$

Théorème 8. Soient $\Omega \subset \mathbb{C}$ un ouvert et $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions holomorphes sur Ω. Si $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers f sur tout compact de Ω, c'est-à-dire converge vers f pour la topologie de $\mathcal{H}(\Omega)$, alors $f \in \mathcal{H}(\Omega)$ et pour tout $p \in \mathbb{N}$, $f_n^{(p)}$ converge vers $f^{(p)}$ pour la topologie de $\mathcal{H}(\Omega)$.

Exemple 8. Soit $\Omega = \mathbb{C} - \mathbb{R}_-$. Pour tout $n \in \mathbb{N}^*$, et tout $z \in \Omega$, on pose $f_n(z) = z^{\frac{1}{n}}$. Alors la suite $(f_n)_{n\in\mathbb{N}}$ converge vers la fonction constante égale à 1 pour la topologie de $\mathcal{H}(\Omega)$.

II.3. *séries de fonctions*

Remarque 9. Les théorèmes de régularité pour les limites de suites de fonctions sont applicables pour les sommes de séries de fonctions en utilisant les théorèmes précédents sur la suite des sommes partielles.

Application 9. La fonction $\zeta : z \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^z}$ est holomorphe sur $\{z \in \mathbb{C} \,|\, \mathrm{Re}(z) > 1\}$.

Application 9. (Équation de la chaleur sur un segment) Soit $f \in \mathcal{C}^1([0,\pi],\mathbb{R})$ telle que $f(0) = f(\pi) = 0$. Notons K_f l'ensemble des éléments $(x,t) \mapsto u(x,t)$ de $\mathcal{C}^0([0,\pi] \times \mathbb{R}_+)$ tels que :

(1) — $\partial_x u$ et $\partial_t u$ existent et sont continues sur $[0,\pi] \times \mathbb{R}_+^*$,
— $\partial^2_{x^2} u$ existe et est continue sur $[0,\pi] \times \mathbb{R}_+^*$,
— $\forall t \in \mathbb{R}_+$, $u(0,t) = u(\pi,t) = 0$,
— $\forall (x,t) \in [0,\pi] \times \mathbb{R}_+^*$, $\partial^2_{x^2} u(x,t) = \partial_t u(x,t)$. (C)

(2) $\forall x \in [0,\pi]$, $u(x,0) = f(x)$

Alors K_f est un singleton.

Proposition 10. Soit $\sum_{n=0}^{+\infty} a_n z^n$ une série entière de rayon de convergence $R \in \mathbb{R}_+^*$. Alors on a :

— $t \in]-R,R[\longmapsto \sum_{n=0}^{+\infty} a_n t^n$ est de classe $\mathcal{C}^\infty$,
— $z \longmapsto \sum_{n=0}^{+\infty} a_n z^n$ est holomorphe sur $\mathcal{D}(0,R)$.

Théorème 11. (Abel angulaire) Soit $\sum_{n=0}^{+\infty} a_n z^n$ une série entière de rayon de convergence supérieur ou égal à 1 et de somme notée f. Soit $\theta_0 \in [0;\frac{\pi}{2}[$, et posons alors :

$$\Delta_{\theta_0} = \left\{z \in \mathbb{C} \,|\, \exists \theta \in [-\theta_0,\theta_0], \exists \rho \in \mathbb{R}_+^* |z| < 1, z = 1 - \rho \exp(i\theta)\right\}.$$

Alors si $\sum_{n=0}^{+\infty} a_n$ converge, alors $\det_{z\to 1,\, z \in \Delta_{\theta_0}} f(z) = \sum_{n=0}^{+\infty} a_n$.

Application 11. On a $\ln(2) = \sum_{n=0}^{+\infty} \frac{(-1)^{n-1}}{n}$.

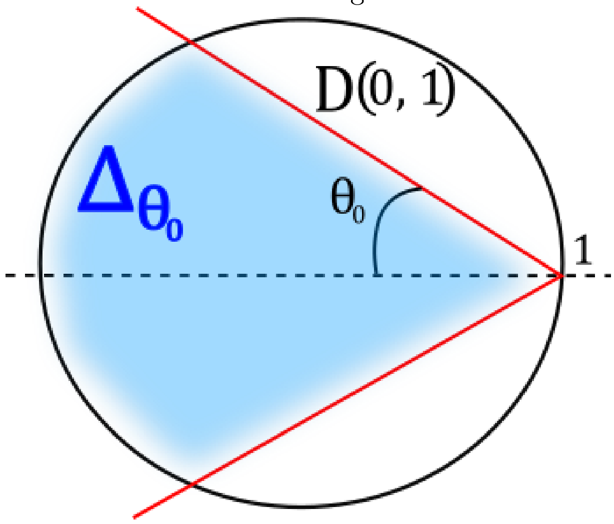
Théorème 11. (Taubérien faible) Soit $\sum_{n\geq 0} a_n z^n$ une série entière de rayon de convergence supérieur ou égal à 1. On note f sa somme sur $\mathrm{D}(0,1)$. On suppose qu'il existe $S \in \mathbb{C}$ tel que $\det_{x\to 1^-} f(x) = S$ et que $\det_{n\to+\infty} na_n = 0$.
Alors $\sum_{n\geq 0} a_n$ converge et $S = \sum_{n=0}^{+\infty} a_n$.

III. Fonction de deux variables.

Théorème 13. Soient X et Y deux espaces topologiques, E un espace métrique complet, $A \subset X$, $B \subset Y$, et $(a,b) \in \overline{A} \times \overline{B}$. Soit $f : A \times B \to E$. On suppose qu'il existe $g : A \to E$ et $h : B \to E$ telles que :

— $f(\cdot,y)$ converge uniformément vers g sur A lorsque y tend vers b,

FIGURE 2. Domaine angulaire considéré.



— $f(x, \cdot)$ converge simplement vers h sur B lorsque x tend vers a.

Alors f possède une limite en (a, b), g possède une limite en a, h possède une limite en b. De plus on a :

$$\det_{(x,y)\to(a,b)} f(x, y) = \det_{x\to a} g(x) = \det_{y\to b} h(x).$$

Application 13. Soit $\varphi : \mathbb{R}^2 \to \mathbb{R}$, continue. On pose $f : \mathbb{R}^2 \to \mathbb{R}$, définie pour tout $(x, y) \in \mathbb{R}^2$ par $f(x, y) = \int\limits_0^y \varphi(x, t)\mathrm{d}t$. Alors f est continue sur $\mathbb{R}^2$.

Contre-exemple 13. On définit $f : \mathbb{R}^2 - \{(0, 0)\} \to \mathbb{R}$ par $f(x, y) = \frac{xy}{x^2+y^2}$. On a bien $\det_{x\to0} \det_{y\to0} f(x, y) = \det_{y\to0} \det_{x\to0} f(x, y) = 0$, cependant f n'a pas de limite en (0,0) car $\frac{1}{2} = f(x, x) = f(x, -x) = -\frac{1}{2}$.

Théorème 14. (Schwarz) Soit $U \subset \mathbb{R}^2$ un ouvert et soit $a \in U$. Soit $f : U \to \mathbb{R}^2$ deux fois différentiable en a alors on a :

$$\partial^2_{xy} f(a) = \partial^2_{yx} f(a).$$

Application 14. Soit $f : \mathbb{R}^2 \to \mathbb{R}$ définie par $f(x, y) = \frac{(x^2-y^2)xy}{x^2+y^2}$ si $(x, y) \neq (0, 0)$ et $f(0, 0) = 0$. Alors on a :

$$\partial^2_{yx} f(0, 0) = -1 \neq 1 = \partial^2_{x,y} f(0, 0),$$

donc f n'est pas deux fois différentiable en $(0, 0)$.

IV. Limite et intégration

Remarque. On se place sur $(X, \mathcal{A}, \mu)$ un espace mesuré. On va se concentrer sur des intégrales à domaines non bornées pour mieux correspondre au cadre de la leçon.

IV.1. *Interversion limite intégrale*

Théorème 16 (convergence dominée) Soit $(f_n)_{n\in\mathbb{N}}$ une suite de $\mathbb{L}^p(\mu)$ vérifiant :
- La suite $(f_n)_{n\in\mathbb{N}}$ converge vers f μ-presque partout,
- Il existe $g \in \mathbb{L}^p(\mu)$ positive telle que $\forall n \in \mathbb{N}$, $|f_n| \leq g$, μ-presque partout.

Alors la suite $(f_n)_{n\in\mathbb{N}}$ converge vers f dans $\mathbb{L}^p(\mu)$ et on a alors :

$$\det_{n\to+\infty} \int f_n(x)\mathrm{d}\mu(x) = \int f(x)\mathrm{d}\mu(x).$$

Application 16. On a la formule suivante :

$$\det_{n\to+\infty} \int_{\mathbb{R}_+} \frac{\exp(-nx^3)}{1+x^2}\mathrm{d}x = 0.$$

Application 16. On a la formule suivante :

$$\det_{n\to+\infty} \int_0^{\sqrt{n}} \left(1 - \frac{x^2}{n}\right)^n \mathrm{d}x = \int_0^{+\infty} \exp(-x^2)\mathrm{d}x.$$

On déduit de cette formule que la valeur de l'intégrale de Gauss est $\frac{\sqrt{\pi}}{2}$.

Théorème 17. (Beppo Levi) Soit $(f_n)_{n\in\mathbb{N}}$ une suite croissante de fonctions mesurables positives. Alors $\det_{n\to+\infty} f_n$ est mesurable positive et on a :

$$\det_{n\to+\infty} \int f_n(x)\mathrm{d}\mu(x) = \int \det_{n\to+\infty} f_n(x)\mathrm{d}\mu(x).$$

Application 17. Soit f une fonction mesurable positive alors on a :

$$\det_{n\to+\infty} \int (f \wedge n)(x)\mathrm{d}\mu(x) = \int f(x)\mathrm{d}\mu(x).$$

Proposition 18. (Continuité de la transformée de Laplace en 0) Soit $f \in \mathcal{C}^0(\mathbb{R}_+, \mathbb{R})$ telle que $\int_0^{+\infty} f(t)\mathrm{d}t$ converge. Alors on a :

$$\det_{x\to 0^+} \int_0^{+\infty} f(t)\exp(-xt)\mathrm{d}t = \int_0^{+\infty} f(t)\mathrm{d}t.$$

Application 18. Cette proposition nous permet de calculer :

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

IV.2. *Interversion des sommations.*

Théorème 19. (Fubini et Fubini-Tonelli) Soient $(X, \mathcal{A}, \mu)$ et $(Y, \mathcal{B}, \nu)$ deux espaces mesurés avec μ et ν mesures σ-finies. Alors on a les deux théorèmes suivants :

(1) (Fubini-Tonelli) Soit $f : X \times Y \to \overline{\mathbb{R}}_+$ mesurable. Alors on a :

$$\int\int_{X\times Y} f(x,y)\mathrm{d}(\mu\otimes\nu)(x,y) = \int_X \left(\int_Y f(x,y)\mathrm{d}\nu(y) \right) \mathrm{d}\mu(x) = \int_Y \left(\int_X f(x,y)\mathrm{d}\mu(x) \right) \mathrm{d}\nu(y).$$

(2) (Fubini) Soit $f \in \mathbb{L}^1(X \times Y, \mu \otimes \nu)$. Alors on a :
- Les applications $x \mapsto \int\limits_Y f(x,y)\mathrm{d}\nu(y)$ et $y \mapsto \int\limits_X f(x,y)\mathrm{d}\mu(x)$ sont mesurables,
- On peut intervertir l'ordre de sommation :

$$\int\int_{X\times Y} f(x,y)\mathrm{d}(\mu\otimes\nu)(x,y) = \int_X \left(\int_Y f(x,y)\mathrm{d}\nu(y) \right) \mathrm{d}\mu(x) = \int_Y \left(\int_X f(x,y)\mathrm{d}\mu(x) \right) \mathrm{d}\nu(y).$$

Application 19. Le théorème de Fubini-Tonelli nous donne une deuxième méthode pour calculer l'intégralle de Gauss.

Application 19. On a les relations suivantes :

$$\int_0^{+\infty} \frac{x\exp(-x)}{1+\exp(-x)}\mathrm{d}x = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n^2}.$$

$$\sum_{p\geq 2}\sum_{q\geq 2} \frac{(-1)^p}{q^p} = \sum_{q\geq 2}\sum_{p\geq 2} \frac{(-1)^p}{q^p} = \frac{1}{2}.$$

Application 19. Soit X une variable aléatoire positive définie sur un espace de probabilité $(\Omega, \mathcal{F}, \mathbb{P})$, alors on a :

$$\mathbb{E}[X] = \int_0^{+\infty} \mathbb{P}(X \geq t)\mathrm{d}t.$$

Contre-exemple 19. Pour tout $(n,p) \in \mathbb{N}^2$, on définit $u_{n,p}$ par : $u_{n,p} = 0$ si $n > p$, $u_{n,p} = 1$ si $n = p$ et $u_{n,p} = \frac{-1}{2^{p-n}}$ si $n < p$. Alors on a :

$$0 = \sum_{n\geq 0}\sum_{p\geq 0} u_{n,p} \neq \sum_{p\geq 0}\sum_{q\geq 0} u_{n,p} = 2.$$

Contre-exemple 19. On a l'égalité suivante :

$$\int_0^{+\infty} \sum_{n=0}^{+\infty} (-1)^n \exp(-(n+1)x)\mathrm{d}x = \sum_{n=0}^{+\infty} \int_0^{+\infty} (-1)^n \exp(-(n+1)x)\mathrm{d}x = \ln(2).$$

Cependant on a :

$$\int_0^{+\infty} \sum_{n=0}^{+\infty} \exp(-(n+1)x)\mathrm{d}x = +\infty.$$

Ce contre-exemple montre que les conditions d'interversions exigées par Fubini sont seulement suffisantes.

Proposition 20. (Produit de Cauchy) Soit $\sum\limits_{n=0}^{+\infty} a_n$ et $\sum\limits_{n=0}^{+\infty} b_n$ deux séries absolument convergentes dans $\mathbb{C}$. Pour tout $n \in \mathbb{N}$, on pose $c_n = \sum\limits_{n=0}^{+\infty} a_k b_{n-k}$. Alors la série $\sum\limits_{n=0}^{+\infty} c_n$ est absolument convergente dans $\mathbb{C}$, et de plus on a la relation suivante :

$$\sum_{n=0}^{+\infty} c_n = \left(\sum_{n=0}^{+\infty} a_n\right)\left(\sum_{n=0}^{+\infty} b_n\right).$$

Application 20. Soient x et y dans $\mathbb{C}$. Alors on a :

$$\sum_{n=0}^{+\infty} \frac{(x+y)^n}{n!} = \left(\sum_{n=0}^{+\infty} \frac{x^n}{n!}\right)\left(\sum_{n=0}^{+\infty} \frac{y^n}{n!}\right),$$

d'où $\exp(x+y) = \exp(x) + \exp(y)$.

Contre-exemple 20. La série $\sum\limits_{n=1}^{+\infty} \frac{(-1)^n}{\sqrt{n}}$ converge, mais la série $\sum\limits_{n=1}^{+\infty}\sum\limits_{k=1}^{+\infty} \frac{(-1)^n}{\sqrt{k(n-k)}}$ ne converge pas.

71. **253 : Utilisation de la notion de convexité en analyse.**

I. Espaces convexes, fonctions convexes

I.1. *Définitions.*

Définition. d'un ensemble convexe. [Beck et al., 2004]

Proposition. Les convexes de $\mathbb{R}$ sont les intervalles.

Proposition.

(1) Les demi-espaces sont convexes [Beck et al., 2004]
(2) Une dilatation d'un convexe est un convexe.
(3) La somme de Minkowski de deux convexes est un convexe.
(4) Une intersection de convexes est un convexe. [Beck et al., 2004]

Définition. D'une fonction convexe (resp. strictement convexe) définie sur un convexe. Lien avec l'épigraphe. [Beck et al., 2004]

Proposition. Caractéristation par la position de la courbe au dessus de sa tangente dans le cas réel.

Exemples.

(1) Une fonction affine est à la fois convexe et concave.
(2) $x \mapsto ||x||$ est convexe mais pas strictement convexe. [Beck et al., 2004]
(3) Pour $u \in \mathcal{S}_n^{++}$, $x \mapsto \langle u(x), x\rangle$ est strictement convexe. [Beck et al., 2004]
(4) Le sup d'une famille de fonctions convexes majorées par une même fonction est convexe. Démonstration par l'épigraphe.

Théorème. Pentes croissantes dans le cas réel. [Beck et al., 2004]

I.2. *Régularité, caractérisations.*

Théorème.

(1) Si f est convexe définie sur $I \subset \mathbb{R}$, alors f est continue sur l'intérieur de I. [Beck et al., 2004]
(2) On a le même résultat en dimension finie. [Gourdon, 1994a]

Contre-exemple. En dimension infinie, on a pas forcément la continuité. Dans $(\mathcal{C}([0,1]), ||\cdot||_1)$ l'application $||\cdot||_\infty$ est convexe mais pas continue. Regarder la suite $x \mapsto n\,\mathbb{1}_{[0,\frac{1}{n}]}$ et considérer deux termes consécutif dont la différence en $||\cdot||_\infty$ est plus grande que 1, mais dont l'intégrale de la différence tend vers 0.

Théorème. [Beck et al., 2004] Caractérisation pour une fonction différentiable f sur un ouvert U de la convexité. Sont équivalents :

(1) f convexe.

(2) L'application ∇f est monotone : $\forall x, y \in U, \langle \nabla f(y) - \nabla f(x), y - x\rangle \geq 0$

(3) Le graphe de f est au dessus de ses tangentes : $\forall x, y \in U, f(y) \geq f(x) + \langle \nabla f(x), y - x\rangle$

Si en plus f est deux fois différentiables on a aussi la caractéristation suivante : $\forall x, h \in U, \langle H_x f \cdot h, h\rangle \geq 0$.

Exemple. Soit $A \in \mathcal{S}_n$, on a : $x \mapsto \langle Ax, x\rangle$ est (strictement) convexe $\Leftrightarrow A$ est (définie) positive. [Beck et al., 2004]

II. Utilisations de la convexité.

II.1. *Obtention d'inégalités.*

Théorème. de projection sur un convexe fermé. [Beck et al., 2004]

Applications. [Beck et al., 2004]

(1) Démonstration du théorème de représentation de Riesz.

(2) Théorème du supplémentaire orthogonal. Critère de densité.

(3) Définition de l'espérance conditonnelle dans $\mathbb{L}^2$.

Propositions. Inégalités pratiques. []

(1) $\exp(x) \geq x + 1$

(2) $\ln(x) \leq x - 1$

(3) Inégalité arithmético-géométrique.

(4) Young [Briane and Pages, 2000]

Proposition. Inégalité de Hoeffding.

Proposition. Inégalités de Hölder et Minkowski.

Conséquence. Les espaces $\mathcal{L}^p$ sont des espaces vectoriels normés. [Briane and Pages, 2000]

72. **254 : Espaces de Schwartz $\mathcal{S}(\mathbb{R}^d)$ et distributions tempérées. Dérivation et transformée de Fourier dans $\mathcal{S}(\mathbb{R}^d)$ et $\mathcal{S}'(\mathbb{R}^d)$.**

I. Espace de Schwartz $\mathcal{S}(\mathbb{R}^d)$

Définition. [Gasquet and Witomski, 1990] On dit que $f : \mathbb{R} \longrightarrow \mathbb{C}$ est à décroissance rapide lorsque pour tout $p \in \mathbb{N}$ on a :

$$\det_{|x| \to +\infty} |x^p f(x)| = 0.$$

Proposition. [Gasquet and Witomski, 1990]

(1) Soit f une fonction de $\mathbb{L}^1(\mathbb{R})$ à décroissance rapide. Alors $\hat{f}$ est indéfiniment dérivable.

(2) Réciproquement, soit $f \in \mathcal{C}^\infty(\mathbb{R})$. Si pour tout $f \in \mathbb{N}$, $f^{(k)}$ est dans $\mathbb{L}^1(\mathbb{R})$ alors $\hat{f}$ est à décroissance rapide.

Moralité. La transformée de Fourier échange décroissance à l'infini et régularité. On va définir un espace de fonctions qui sont à la fois très régulières et très décroissantes à l'infini, ce sera commode pour généraliser la transformée de Fourier.

Définition. [Gasquet and Witomski, 1990] $\mathcal{S}(\mathbb{R})$ est le sous-ensemble des fonctions $f \in \mathcal{C}_c^\infty(\mathbb{R})$ tel que pour tout $(\alpha, \beta) \in \mathbb{N}^2$:

$$\det_{|x| \to +\infty} |x^\alpha f^{(\beta)}(x)| = 0.$$

Exemple. Pour $z \in \mathbb{C}$ tel que $\mathrm{Re}(z) > 0$, $\varphi(x) = \exp(-zx^2)$ est dans $\mathcal{S}(\mathbb{R})$.

Propriétés. [Gasquet and Witomski, 1990]

(1) $\mathcal{S}(\mathbb{R})$ est stable par multiplication par un polynôme.

(2) $\mathcal{S}(\mathbb{R})$ est stable par dérivation.

(3) $\mathcal{S}(\mathbb{R}) \subset \mathbb{L}^p(\mathbb{R})$.

Proposition. L'espace $\mathcal{S}(\mathbb{R})$ est stable par transformation de Fourier : $f \in \mathcal{S}(\mathbb{R}) \Rightarrow \hat{f} \in \mathcal{S}(\mathbb{R})$.

Propriétés. [Gasquet and Witomski, 1990]

(1) Pour tout $(\alpha, \beta) \in \mathbb{N}^2$ on pose $p_{\alpha,\beta} = \sup\{|x^\alpha f^{(\beta)}(x)|\}$. C'est une famille de semi-normes sur $\mathcal{S}(\mathbb{R})$ qui fait de $\mathcal{S}(\mathbb{R})$ un espace métrisable complet.

(2) Pour cette topologie, la dérivation et la transformation de Fourier sont des opérations continues.

Théorème. [Gasquet and Witomski, 1990] La transformation de Fourier $\mathcal{F}$ est une application linéaire bijective et bicontinue de $\mathcal{S}(\mathbb{R})$ sur $\mathcal{S}(\mathbb{R})$. L'application inverse est $\overline{\mathcal{F}}$.

II. Distributions tempérées

Définition. On dit que T est une distribution tempérée, i.e $T \in \mathcal{S}'(\mathbb{R})$ lorsque T est une forme linéaire continue sur $\mathcal{S}(\mathbb{R})$, autrement dit s'il existe $p \in \mathbb{N}$ et $c > 0$ tels que pour tout $\varphi \in \mathcal{S}(\mathbb{R})$:

$$|\langle T, \varphi \rangle| \leq c \sum_{|\alpha|<p, |\beta|<p} p_{\alpha,\beta}(\varphi).$$

Exemples. Le dirac en 0 est une distribution tempérée. Le peigne de dirac est une distribution tempérée.

Proposition. [Gasquet and Witomski, 1990] Soit $(T_n)_{n\in\mathbb{N}}$ une suite de $\mathcal{S}'(\mathbb{R})$. On dit que (T_n) tend vers 0 dans $\mathcal{S}'(\mathbb{R})$ lorsque pour tout $\varphi \in \mathcal{S}(\mathbb{R})$:

$$\det{}_{n\to+\infty} \langle T_n, \varphi \rangle = 0.$$

Exemple. $T_n = n1_{[-1/2n, 1/2n]}$ converge vers δ_0 dans $\mathcal{S}'(\mathbb{R})$.

Proposition. Soit $T \in \mathcal{S}'(\mathbb{R})$, alors :

(1) Pour tout $k \in \mathbb{N}$, $x^k T \in \mathcal{S}'(\mathbb{R})$.

(2) Pour tout $k \in \mathbb{N}$, $T^{(k)} \in \mathcal{S}'(\mathbb{R})$.

(3) Les applications $T \mapsto x^k T$ et $T \mapsto T^{(k)}$ sont continues de $\mathcal{S}'(\mathbb{R})$ dans $\mathcal{S}'(\mathbb{R})$.

Exemples.

(1) Les fonctions de $\mathbb{L}^p(\mathbb{R})$ sont des distributions tempérées. Les fonctions à croissance lente sont des distributions tempérées.

(2) $x \mapsto \ln(|x|)$ est une distribution tempérée.

(3) H est une distribution tempérée.

(4) La valeur principale de $\frac{1}{x}$, notée $Vp(\frac{1}{x})$ est une distribition tempérée car $Vp(\frac{1}{x}) = (\ln(|x|))'$. Parler aussi de $\mathrm{Pf}(\frac{1}{\mathrm{x}^2})$.

Définition. Espace des multiplicateurs de $\mathcal{S}(\mathbb{R})$, noté $\mathcal{O}_M(\mathbb{R})$. [BONY-Cours d'analyse.]. C'est l'ensemble des fonctions f de $\mathcal{C}^\infty(\mathbb{R})$ tel que pour tout $\alpha \in \mathbb{N}$, il existe $C_\alpha > 0$ et $N_\alpha \in \mathbb{N}$ tel que :

$$|f^{(\alpha)}(x)| \leq C_\alpha (1 + |x|)^{N_\alpha}.$$

Pour tout $f \in \mathcal{O}_M(\mathbb{R})$ et tout $\varphi \in \mathcal{S}(\mathbb{R})$, on a alors $f\varphi \in \mathcal{S}(\mathbb{R})$. Et alors pour tout $T \in \mathcal{S}'(\mathbb{R})$, on peut définir fT par la relation :

$$\langle fT, \varphi \rangle = \langle T, f\varphi \rangle .$$

Exemple. On a $x\mathrm{Vp}(\frac{1}{x}) = 1$ dans $\mathcal{S}'(\mathbb{R})$.

II.1. *Transformée de Fourier dans $\mathcal{S}'(\mathbb{R})$*

Définition. Soit $T \in \mathcal{S}'(\mathbb{R})$. On appelle transformée de Fourier de T la distribution tempérée notée $\hat{T}$ ou $\mathcal{F}(T)$ définie pour tout $\varphi \in \mathcal{S}(\mathbb{R})$ par :

$$\left\langle \hat{T}, \varphi \right\rangle = \langle T, \hat{\varphi} \rangle .$$

Proposition. La transformée de Fourier que l'on vient de définir prolonge la transformée de Fourier sur $\mathbb{L}^1$ et $\mathbb{L}^2$.

Proposition. La transformée de Fourier est une application linéaire bijective et bicontinue de $\mathcal{S}'(\mathbb{R})$ sur $\mathcal{S}'(\mathbb{R})$.

Proposition. Propriétés sur la dérivation et la multiplication par un monôme.

Exemples.

(1) Transformée de Fourier de δ : $\overline{\delta} = 1$.

(2) Transformée de Fourier d'un monôme. $\overline{t^k} = \frac{(-1)^k}{(2i\pi)^k}\delta^{(k)}$.

Proposition. Transformée de Fourier de la valeur principale de $\frac{1}{x}$ et de H.

Proposition. Transformée de Fourier du peigne de dirac : $\overline{\Delta} = \Delta$. Formule sommatoire de Poisson.

Application. Une règle d'échantillonnage de Shanon pour un signal à spectre borné.

Proposition. Résolution de l'équation de la chaleur. [BONY]

73. **261 : Fonction caractéristique et transformée de Laplace d'une variable aléatoire. Exemples et applications.**

I. Définition et premières propriétés.

Définition. de la transformée de Laplace d'une variable aléatoire réelle $L_X(t) = \mathbb{E}[X]$ainsi que du domaine où celle-ci est bien définie $\mathcal{D}_X$. [Foata et al., 2012]

Exemples. [Foata et al., 2012] $L_X(t)$ est toujours définie en 0. On a $L_X(0) = 1$. Cependant on peut avoir de nombreuses formes pour $\mathcal{D}_X$.

(1) Si $X \sim \mathcal{C}(1)$, alors $\mathcal{D}_X = \{0\}$.

(2) Si X est bornée, alors $\mathcal{D}_X = \mathbb{R}$ et L_X est continue.

(3) Si X est positive, alors L_X est continue et bornée sur $]-\infty, 0]$.

Proposition. [Foata et al., 2012] Propriétés élémentaires de L_X. En particulier $\mathcal{D}_X$ est un intervalle.

Exemples. [Foata et al., 2012]

(1) $X \sim b(p)$, $L_X(t) = 1 - p + p\,\mathrm{e}^t$, $\mathcal{D}_X = \mathbb{R}$.

(2) $X \sim \mathcal{E}(\lambda)$, $L_X(t) = \frac{\lambda}{\lambda - t}$, $\mathcal{D}_X =]-\infty, \lambda[$.

(3) Autres exemples si besoin

Cas particulier. Fonction génératrice des moments factoriels. (Référence au programme de prépa). [Foata et al., 2012]

Définition. de la fonction caractéristique $\varphi_X(t)$. Expression pour une variable discrète et une variable à densité. [Foata et al., 2012]

Remarque. [Foata et al., 2012]

(1) La fonction caractéristique présente l'avantage d'être définie partout.

(2) La fonction caractéristique présente l'inconvénient de faire intervenir l'analyse complexe, plus difficile.

(3) La fonction caractéristique est la transformée de Fourier de la variable aléatoire.

Exemples. [Foata et al., 2012]

(1) $X \sim \mathcal{P}(\lambda)$, $\varphi_X(t) = \mathrm{e}^{\mathrm{e}^{it} - 1}$.

(2) $X \sim \mathcal{N}(0, 1)$, $\varphi_X(t) = \mathrm{e}^{-\frac{t^2}{2}}$.

(3) $X \sim \mathcal{C}(1)$, $\varphi_X(t) = \mathrm{e}^{-|t|}$. En particulier ici elle est bien définie.

Théorème. La fonction caractéristique et la transformée de Laplace caractérisent la loi d'une variable aléatoire. [Ouvrard, 2004] [Foata et al., 2012]

I.1. *Lien avec l'indépendance*

Proposition.

Proposition. [Ouvrard, 2004] Si X et Y sont deux variables aléatoires réelles alors on a l'équivalence entre :

(1) $\varphi_{(X,Y)}(s,t) = \varphi_X(s)\varphi_Y(t)$

(2) X et Y sont indépendantes.

Proposition. Rappel sur le fait que la loi de la somme de deux variables aléatoires est la convolution des deux lois.

Corollaire. Soient X et Y deux variables aléatoires réelles indépendantes. Alors $\varphi_{X+Y}(t) = \varphi_X(t)\varphi_Y(t)$. [Ouvrard, 2004]

Remarque. On retrouve le fait que la transformée de Fourier échange produit et produit de convolution. Ces propriétés sont aussi vraies pour la transformée de Laplace.

Contre-exemple Si on prend deux variables aléatoires suivant une loi de Cauchy de paramètre 1, non indépendantes, la fonction caractéristique de leur somme est égale au produit de leurs fonctions caractéristiques. Ce n'est pas une équivalence. [Foata et al., 2012]

Applications. Calcul de nouvelles fonctions caractéristiques. Donner l'exemple de la loi binomiale. De la loi Gamma. D'une somme de lois normales.

Application. Inégalité de Hoeffding. [Ouvrard, 2004]

Application. Grands ensembles de vecteurs presque orthogonaux. [RMS]

II. Lien avec les moments

Proposition. Si X admet une transformée de Laplace définie sur un intervalle ouvert autour de 0, alors X admet des moments à tout ordre, L_X admet une développement en série entière faisant intervenir les moments de X, et $L_x^{(0)}(0) = \mathbb{E}[X^k]$. [Foata et al., 2012]

Application. Si X suit une loi normale centrée réduit, $L_X(t) = \mathrm{e}^{-\frac{t^2}{2}} = \sum_{i=0}^{+\infty} \frac{(-t)^{2i}}{2^i i!} t^i$, d'où l'on déduit les moments de la loi.

Remarque. Cas particulier de la fonction génératrice des moments factoriels. Pourquoi dit-on qu'elle génère les moments ? [Foata et al., 2012]

Proposition. Rapports entre fonction caractéristique et moments. Sens direct et réciproque. [Ouvrard, 2004]

III. Notion de convergence en loi.

Définition. De la convergence en loi d'une suite de variables aléatoires réelles $(X_n)_{n\in\mathbb{N}}$ vers X, en terme de convergence simple de la suite des fonctions de répartition aux points de continuité de F_X. [Foata et al., 2012]

Théorème de Lévy. [Foata et al., 2012]

La fonction caractéristique et ses propriétés permettent de démontrer le très important...

Théorème. de la limite centrale. Et sa réciproque. [Foata et al., 2012]

Application. Détermination d'un intervalle de confiance.

74. **262 : Modes de convergence d'une suite de variables aléatoires. Exemples et applications.**

I. Convergence presque sûre et convergence en probabilités

I.1. *Convergence presque sûre*

Définition. [Barbe and Ledoux, 2012] Définition de la convergence presque sûre.

Proposition. [Barbe and Ledoux, 2012] Critère de Cauchy pour la convergence presque sûre.

Remarque. Il y a unicité de la limite presque sûre. [Ouvrard, 2004]

Exemple. Soit (X_i) une suite de variables aléatoire iid suivant une loi de bernouilli. Alors la suite $U_n = \sum_{i=1}^{n} 2^{-i} X_i$ vérifie le critère de Cauchy. Elle converge presque sûrement vers $\sum_{i=1}^{+\infty} 2^{-i} X_i$.

Proposition. Si f est continue sur $\mathbb{R}$ et que X_n tend vers X presque sûrement, alors $f(X_n)$ tend presque sûrement vers $f(X)$.

Proposition. [Ouvrard, 2004] Borel Cantelli.

Corollaire. [Barbe and Ledoux, 2012] Borel Cantelli pour la convergence presque sûre.

Contre-exemple. [Ouvrard, 2004] On pose $X_n = 1_{]0,\frac{1}{n}}$. X_n tend presque sûrement vers 0 mais $\sum\limits_{i=1}^{+\infty} \mathbb{P}(|X_n| > \varepsilon) = +\infty$.

Exemple. [Barbe and Ledoux, 2012] Soit (X_i) une suite de variables aléatoire iid suivant une loi exponentielle de paramètre 1. On pose $M_n = \frac{\max(X_i, i \leq n)}{\ln(n)}$ Alors M_n tend vers 1 presque sûrement.

I.2. *Convergence en probabilités*

Définition. Définition de la convergence en probabilité.

Exemple. Soit X_i des variables aléatoires réelles non corrélées, telles que $\mathbb{E}[X_i] = 0$ et $\mathrm{Var}(X_i) = \sigma^2$. Alors la suite des moyennes empiriques des X_i tend vers 0 en probabilité. (Tchebychev).

Proposition. [Ouvrard, 2004] La convergence presque sûre implique la convergence en probabilités, vers la même limite. En particulier la limite en probabilités est unique.

Contre-exemple. [Ouvrard, 2004] On considère (X_n) suite de variables aléatoires indépendantes avec X_n de loi $\mathrm{b}(\frac{1}{n})$. Alors X_n tend vers 0 en probabilités mais pas presque sûrement.

Proposition. [Ouvrard, 2004] Inégalité de Hoeffding.

Théorème. [Barbe and Ledoux, 2012] Soient X_n une suite de variables aléatoires et X une va. Alors X_n converge en probabilité vers X si et seulement si de toute suite extraite $X_{\varphi_1(n)}$ on peut réextraire une sous-suite $X_{\varphi_1 \circ \varphi_2(n)}$ qui converge presque sûrement vers X.

I.3. *Lois des grands nombres.*

Théorème. [Barbe and Ledoux, 2012] Loi faible des grands nombres.

Application. Presque tout nombre de $[0,1]$ admet en moyenne autant de 0 que de 1 dans son développement dyadique.

Théorème. Loi forte des grands nombres.

Corollaire. En statistiques paramètriques, la moyenne empirique est un estimateur fortement consistant de l'espérance.

II. Convergence en norme $\mathbb{L}^p$

Définition. Définition de la convergence $\mathbb{L}^p$.

Proposition. La convergence $\mathbb{L}^p$ implique la convergence en probabilités.

Contres-exemples.

(1) On pose $X_n(\omega) = \omega^{-\alpha} 1_{]0,\frac{1}{n}]}(\omega)$. La suite converge en probabilités, mais n'est pas dans $\mathbb{L}^p$ dès lors que $\alpha \geq \frac{1}{p}$.

(2) On prend X_n variable aléatoire de loi $(1 - n^{-p})\delta_0 + n^{-p}\delta_n$. On a X_n qui converge presque sûrement vers 0, mais $\mathbb{E}[|X_n|^p] = 1$.

Définition. Uniforme intégrabilité.

Exemples. Quelques critères qui donnent l'uniforme intégrabilité.

Théorème. Théorème de Vitali.

III. Convergence en loi

Définition. de la convergence en loi.

Remarque. C'est la convergence la plus faible. Elle est conséquence de toutes les autres.

Exemples et contre exemples. [Barbe and Ledoux, 2012]

Proposition. La convergence en loi vers une constante implique la convergence en probabilités.

Application. [Ouvrard, 2004] Théorème de Poisson.

III.1. *Théorème central limite.*

Application à la recherche d'un intervalle de confiance asymptotique.

I. *

Références

[Amar and Matheron, 2004] Amar, E. and Matheron, E. (2004). *Analyse complexe*, volume 517. Cassini.

[Audin, 2012] Audin, M. (2012). *Géométrie (L3M1)*. EDP sciences.

[Avez, 1983] Avez, A. (1983). *Calcul différentiel*. Masson.

[Barbe and Ledoux, 2012] Barbe, P. and Ledoux, M. (2012). *Probabilité (L3M1)*. EDP Sciences.

[Beck et al., 2004] Beck, V., Malick, J., and Peyré, G. (2004). *Objectif agrégation*. H&K.

[Brezis, 1983] Brezis, H. (1983). *Analyse fonctionnelle*.

[Briane and Pages, 2000] Briane, M. and Pages, G. (2000). *Théorie de l'intégration : licence de mathématiques ; cours et exercices*. Vuibert.

[Calais, 1998] Calais, J. (1998). Elenment de theorie des anneaux, anneaux commutative.

[Caldero and Germoni, 2013] Caldero, P. and Germoni, J. (2013). *Histoires hédonistes de groupes et de géométries*. Calvage & Mounet.

[Candelpergher, 2004] Candelpergher, B. (2004). *Calcul intégral*. Cassini.

[Chambert-Loir, 1995] Chambert-Loir, A. (1995). *Exercices de Mathématiques pour l'agrégation.. Analyse 1*.

[Ciarlet, 1988] Ciarlet, P. G. (1988). *Introduction à l'analyse numérique matricielle et à l'optimisation*.

[Combes, 1982] Combes, J. (1982). *Suites et séries*. Presses universitaires de France.

[Demailly, 2012] Demailly, J.-P. (2012). *Analyse numérique et équations différentielles*. EDP sciences.

[Foata et al., 2012] Foata, D., Fuchs, A., and Franchi, J. (2012). *Calcul des probabilités-3e édition : Cours, exercices et problèmes corrigés*. Dunod.

[Gapaillard, 1997] Gapaillard, J. (1997). *Intégration pour la licence : cours avec exercices corrigés*. Masson.

[Gasquet and Witomski, 1990] Gasquet, C. and Witomski, P. (1990). *Analyse de Fourier et applications*. Masson.

[Goblot, 1996] Goblot, R. (1996). *Algèbre commutative : cours et exercices résolus*. Masson.

[Gourdon, 1994a] Gourdon, X. (1994a). *Les maths en tête*.

[Gourdon, 1994b] Gourdon, X. (1994b). *Les maths en tête : mathématiques pour M'. Algèbre*.

[Gras and Gras, 2004] Gras, G. and Gras, M.-N. (2004). *Algèbre fondamentale : arithmétique : niveau L3 et M1*. Elllipses.

[Grifone, 1990] Grifone, J. (1990). *Algebre linéaire*. Cépadues-Éditions.

[Grimmett and Stirzaker, 2001] Grimmett, G. and Stirzaker, D. (2001). *Probability and random processes*. Oxford university press.

[Hauchecorne, 1988] Hauchecorne, B. (1988). *Les contre-exemples en mathématiques*. Ellipses Paris.

[Hirsch and Lacombe, 1997] Hirsch, F. and Lacombe, G. (1997). *Eléments d'analyse fonctionnelle : cours et exercices*. Masson.

[Lafontaine, 2012] Lafontaine, J. (2012). *Introduction aux variétés différentielles*. EDP sciences.

[Madère, 1997] Madère, K. (1997). *Préparation à l'oral de l'agrégation : LeÃ§ons d'analyse*. Ellipses.

[Mneimné and Testard, 1986] Mneimné, R. and Testard, F. (1986). Introduction à la théorie des groupes de lie classiques.

[Moisan et al., 1992] Moisan, J., Vernotte, A., and Tosel, N. (1992). Suites et séries de fonctions.

[Ouvrard, 2004] Ouvrard, J.-Y. (2004). *Probabilités, 2 Tome, Licence-CAPES et Master-Agrégation*. VUIBERT.

[Perrin, 1996] Perrin, D. (1996). *Cours d'algèbre*.

[Peyré, 2004] Peyré, G. (2004). *L'algèbre discrète de la transformée de Fourier*. Ellipses.

[Pommelet, 1994] Pommelet, A. (1994). *Analyse pour l'agrégation*. Ellipses.

[Queffélec and Zuily, 2013] Queffélec, H. and Zuily, C. (2013). *Analyse pour l'agrégation-4e éd*. Dunod.

[Rombaldi, 2004] Rombaldi, J.-E. (2004). *Éléments d'analyse réelle : CAPES et agrégation interne de mathématiques*. EDP sciences.

[Rouvière, 1999] Rouvière, F. (1999). *Petit guide de calcul différentiel : à l'usage de la licence et de l'agrégation*. Cassini.

[Rudin et al., 1975] Rudin, W., Dhombres, N., Hoffman, F., Hoffman, F., and Hoffman, F. (1975). *Analyse réelle et complexe*. Masson.

[Serre, 1967] Serre, J.-P. (1967). Representations lineaires des groupes finis.

[Testard, 2010] Testard, F. (2010). *Analyse mathématiques : La maîtrise de l'implicite Préparation à l'oral de l'agrégation : LeÃ§ons d'analyse*. Calvage et Mounet.

[Ulmer, 2005] Ulmer, F. (2005). ThÃ©orie des groupes.