Pense-bête pour l'Agrégation

Raphaël Krikorian

M2 CYU 2021-22

1 Algèbre Linéaire

1.1 Espaces vectoriels

Exercice 1 Un cercle dans le plan peut-il être un sous-espace vectoriel de $\mathbb{R}^2$?

Exercice 2 Un espace vectoriel sur un corps infini (p.ex. $\mathbb{R}$ ou $\mathbb{C}$) n'est jamais union finie de sous-espaces vectoriels stricts. Une autre version qui utilise le théorème de Baire est : un espace de Banach n'est jamais union dénombrable de sous-espaces vectoriels fermés stricts.

Exercice 3 Soit E un K-espace vectoriel de dimension finie et $u \in End(E)$. Trouver une CNS sur u pour qu'il existe $v \in End(E)$ tel que $uv = 0$ et $u + v$ est inversible.

La théorie abstraite des e.v. peut avoir des conséquences inattendues.

Exercice 4 a) Soient $K \subset \mathbb{R}$ un $\mathbb{Q}$-espace vectoriel de dimension finie. Démontrer que si $a, b \in K$, $a/b \notin \mathbb{Q}$, il existe $\varphi : K \to \mathbb{R}$ additive ($\varphi(x+y) = \varphi(x) + \varphi(y)$) telle que $\varphi(a) = 1 = -\varphi(b)$.
b) Démontrer que si pour tout $(x_1, x_2, y_1, y_2) \in K$ on définit

$$\mu\Big([x_1, x_2] \times [y_1, y_2]\Big) = \varphi(x_2 - x_1)\varphi(y_2 - y_1)$$

alors, pour tous $x_{i,k}, y_{i,k}$, $i = 1, 2$, $k = 0, 1, \ldots, n$ dans K vérifiant

$$[x_{1,0}, x_{2,0}] \times [y_{1,0}, y_{2,0}] = \bigcup_{k=1}^{n} \Big([x_{1,k}, x_{2,k}] \times [y_{1,k}, y_{2,k}]\Big)$$

on a

$$\mu\Big([x_{1,0}, x_{2,0}] \times [y_{1,0}, y_{2,0}]\Big) = \sum_{k=1}^{n} \mu\Big([x_{1,k}, x_{2,k}] \times [y_{1,k}, y_{2,k}]\Big).$$

c) En déduire que s'il existe une partition d'un rectangle de côtés a, b en carrés alors $a/b \in \mathbb{Q}$.

d) Démontrer que s'il existe une partition d'un carré de côté 1 en carrés, alors ces carrés sont de côtés rationnels.

1.2 Théorie de la dimension

- Familles libres, liées. Rang. Bases.
- Toutes les bases ont le **même** nombre d'éléments : la **dimension**.
- On peut **compléter** une famille libre en une base.
- Algorithme du **pivot de Gauss**. Interprétation matricielle des opérations élémentaires.

1.2.1 Conséquences du pivot de Gauss

- $SL_n(K)$ est engendré par les transvections (matrices $I + \lambda E_{ij}$ où E_{ij} est la matrice dont tous les coefficients sont nuls sauf le coefficient i, j qui vaut 1) et $GL_n(K)$ par les transvections et les dilatations.
- Théorème de structure des **applications de rang** r. Si $A \in M_{n,m}(K)$ est de rang r, si et seulement si, il existe $Q \in GL_m(K)$, $P \in GL_n(K)$ inversibles, produits de matrices élémentaires, tq.

$$A = PJ_rQ, \qquad \text{où} \quad J_r = \begin{pmatrix} I_r & 0_{m-r} \\ 0_{n-r} & 0_{n-r,m-r} \end{pmatrix}$$

- **Décomposition** PLU : Toute matrice $A \in M_n(K)$ s'écrit sous la forme $A = PLU$ où P est une matrice de permutation, L est triangulaire inférieure avec des 1 sur la diagonale et U est triangulaire supérieure. Si tous les mineurs principaux de A sont non nuls on peut choisir $P = I$ et le décomposition LU est unique.

1.2.2 Dimension et rang

- $\dim(F + G) = \dim F + \dim G - \dim(F \cap G)$.
- Dimension et exemples de bases (bases échelonnées) de l'e.v. $\mathbb{R}_n[X]$ des polynômes de degrés $\leqslant n$.

– Si $f : E \to F$ est une application linéaire,

$$\dim E = \text{rang}(f) + \dim \ker f$$

(on a l'isomorphisme $\bar{f} : E/\ker f \to \text{Im} f$).
– Conséquence : si $\dim E = \dim F < \infty$ et $f \in \mathcal{L}(E, F)$ f est injective si et seulement si elle est surjective (donc bijective).

1.2.3 Trace

– **Trace**. Si $f : E \to E$ est un endomorphisme on peut définir sa trace dans une base $\mathcal{B} = (e_1, \ldots, e_n)$ de E de la façon suivante : si A est la matrice de f dans $\mathcal{B}$

$$\text{tr}(f) = \text{tr}_{\mathcal{B}}(f) = \text{tr}(A) = \sum_i A_{ii}.$$

Le résultat simple mais fondamental (et surprenant finalement) est que $\text{tr}_{\mathcal{B}}(f)$ **ne dépend pas de $\mathcal{B}$.**
– Si $A, B \in M_n(K)$,

$$\text{tr}(AB) = \text{tr}(BA), \qquad \text{et} \qquad \text{tr}({}^tA) = \text{tr}(A).$$

– **Projection** linéaire : $p \circ p = p$. De façon équivalente $E = \ker p \oplus \text{Im} p$ et $p_{|\text{Im}p} = id_{\text{Im}p}$. Pour un projecteur

$$\text{tr}(p) = \text{rang}(p).$$

Exercice 5 Toute application linéaire de rang r est somme de r applications linéaires de rang 1. Une application de rang 1 est un projecteur ($p^2 = p$) et est de la forme $p(x) = \varphi(x)v$ où $v \in E$, $\varphi \in E^*$ (E^* est le dual de E càd l'ensemble des formes linéaires $\varphi : E \to K$). Quand E est muni d'un produit scalaire $\varphi(x)$ est de la forme $\varphi(x) = \langle x, w \rangle$, $w \in E$).

Exercice 6 Soir $\varphi : M_n(K) \to K$ une forme linéaire. Montrer qu'il existe $A \in M_n(K)$ telle que

$$\forall\ M \in M_n(K), \quad \varphi(M) = \text{tr}(AM).$$

Exercice 7 Démontrer que pour tout polynôme $P \in \mathbb{R}_n[X]$, il existe un polynôme $Q \in \mathbb{R}_{n+1}[X]$ tel que

$$P(X) = Q(X + 1) - Q(X).$$

Exercice 8 Soient $p_1, \ldots, p_k$ des projecteurs (non nuls) dans $M_n(\mathbb{R})$. Démontrer que si $p_1 + \cdots + p_k = id$ alors pour tous $1 \leqslant i, j \leqslant n$ on a $p_i p_j = p_j p_i$. [Démontrer que $\mathbb{R}^n$ est la somme directe des $\mathrm{Im}(p_i)$ (on pensera à utiliser le fait que le rang d'un projecteur est égal à sa trace).]

1.3 Déterminants

1.3.1 Définitions et propriétés

- Formes n-linéaires alternées : sur K^n, elles sont toutes colinéaires (e.v. de dimension 1).
- Si $B = (e_1, \ldots, e_n)$ est une base il existe une forme n-linéaire alternée qui prend la valeur 1 au point $(e_1, \ldots, e_n)$. Cette Fn-LA est par définition le déterminant dans la base $B = (e_1, \ldots, e_n)$. Si A est la matrice dont les colonnes sont les composantes des vecteurs $(v_1, \ldots, v_n)$ dans la base $(e_1, \ldots, e_n)$ on a

$$\det{}_B(v_1, \ldots, v_n) := \det A = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

- Le déterminant est invariant par changement de base.
- Opérations sur les lignes et les colonnes. Développement par rapport aux lignes ou colonnes.
- $\det(AB) = \det A \times \det B$. Interprétation géométrique. On a aussi $\det({}^tA) = \det(A)$.
- **Vandermonde** (et ses preuves).

1.3.2 Déterminant et exponentielle

- Si $A \in M_n(K)$,

$$\det(\exp A)) = \exp(\mathrm{tr}(A)).$$

  Rappels :

$$\exp(A) = \sum_{k=0}^{\infty} \frac{A^k}{k!}.$$

  Si A et B commutent (mais sinon, c'est faux) on a $\exp(A + B) = \exp(A)\exp(B)$.
- On a

$$\det(I + H) = 1 + \mathrm{tr}(H) + O^2(H).$$

1.3.3 Déterminant et inversion des matrices

- Mineurs d'une matrice : on appelle mineur $\Delta_{ij}(A)$ d'une matrice $A \in M_n(K)$ le déterminant de la matrice $(n-1) \times (n-1)$ où on a éliminé la ligne i et la colonne j de A.
- Si $Co(A)$ est la comatrice de A càd la matrice dont le coefficient i, j est $(-1)^{i+j} \times \Delta_{ij}(A)$ on a

$$^tCo(A) \times A = \det(A) \times I_n.$$

  Permet en principe (mais rarement en pratique) le calcul de A^{-1} si A est inversible. Connaître la formule de A^{-1} au moins pour $n = 2$.

Exercice 9 On considère la matrice $n \times n$ de Jacobi : z sur la diagonale et des 1 sur la sur et sous-diagonale. On note déterminant $\Delta_n(z)$ de cette matrice.

1) Démontrer que $\Delta_{n+1}(z) = z\Delta_n(z) - \Delta_{n-1}(z)$.

2) Déterminer les z pour lesquels $\Delta_n(z) = 0$. [Voir que $\Delta_n(z)$ est un polynôme de degré n. Puis calculer en utilisant 1) $\Delta_n(e^{i\theta})$].

Exercice 10 Déterminant de Cauchy. Calculer

$$\det\left(\frac{1}{a_i + b_j}\right)_{1 \leqslant i,j \leqslant n}.$$

1.4 Réduction des endomorphismes

On ne considère que des applications linéaires (resp. matrices) $f : E \to E$ où E est un $K - ev$ de dim finie n (resp. $A \in M_n(K)$).

1.4.1 Matrices équivalentes, matrices semblables

- Deux matrices A, B (ou endomorphismes) sont équivalentes s'il existe $P, Q \in GL_n(\mathbb{R})$ tq

$$A = PBQ^{-1}.$$

  Notion qui intervient quand on fait des changements de bases. Intervient aussi dans la forme normale des matrices de rang r.
- Deux matrices A, B (ou endomorphismes) sont semblables (on dit aussi conjuguées) s'il existe $P \in GL_n(\mathbb{R})$ tq

$$B = PAP^{-1}.$$

– Invariance de la trace et du déterminant par conjugaison :

$$\mathrm{tr}(PAP^{-1}) = \mathrm{tr}(A), \qquad \det(PAP^{-1}) = \det A.$$

– Notion de conjugaison très utile pour itérer (prendre des puissances) de matrices :

$$(PAP^{-1})^N = PA^NP^{-1}, \qquad \exp(PAP^{-1}) = P\exp(A)P^{-1}.$$

– Remarque sur la conjugaison : Soient $h : X \to Y$ une bijection entre deux ensembles X et Y et $f : X \to X$. La bijection h transporte l'action de f sur X en une action de $h \circ f \circ h^{-1}$ sur Y (faire un dessin). Un ensemble $A \subset X$ invariant par f est transporté par h en $h(A) \subset Y$ invariant par $h \circ f \circ h^{-1}$.

1.4.2 Valeur propres, vecteurs propres

Le vecteur $u \in K^n \backslash \{0\}$ est vecteur propre de la matrice (ou de l'endomorphisme) $A \in M(n, K)$ ssi il existe $\lambda \in K$ tq $Au = \lambda u$.

$$\exists\, u \in K^n\backslash\{0\}, \quad Au = \lambda u, \qquad \Longleftrightarrow \qquad \chi_A(\lambda) := \det(A - \lambda I) = 0.$$

– Si $K = \mathbb{R}$ et $A \in M_n(\mathbb{R})$ admet $\lambda \in \mathbb{C}$ pour valeur propre, il existe $F \subset \mathbb{R}^n$ sev de dimension 1 ou 2 qui est A-invariant :

$$\dim F \in \{1, 2\} \quad \text{et} \quad AF \subset F.$$

F est de dimension 1 si $\lambda \in \mathbb{R}$, 2 si $\lambda \in \mathbb{C}\backslash\mathbb{R}$.

1.4.3 Polynôme caractéristique, polynôme minimal

– $\chi_A \in K[X]$ **polynôme caractéristique** de A.
– **Cayley-Hamilton** : $\chi_A(A) = 0$.
– Ne pas confondre avec le **polynôme minimal** de A qui est le polynôme normalisé (i.e. le coefficient du monôme de plus haut degré vaut qui engendre l'idéal principal annulateur de A :

$$(\mu_A(X)K[X]) = \{P(X) \in K[X], \quad P(A) = 0.\}$$

– On a toujours $\mu_A \mid \chi_A$. Plus précisément : si

$$\chi_A(X) = (-1)^n \prod_{i=1}^{r} (X - \lambda_i)^{c_i}$$

on a

$$\mu_A(X) = \prod_{i=1}^{r} (X - \lambda_i)^{m_i}, \qquad \text{avec} \quad 1 \leqslant m_i \leqslant c_i.$$

Exercice 11 Soient $A \in M_n(\mathbb{R})$, $\lambda = t + is \in \mathbb{C}$ $(t, s \in \mathbb{R},\ s \neq 0)$, $v, w \in \mathbb{R}^n$ tq

$$A(v + iw) = (t + is)(v + iw).$$

Mq (1) $F = \mathbb{R}v \oplus \mathbb{R}w$; (2) $AF \subset F$; (3) la restriction de A à F est semblable à une matrice de similitude

$$A\,|F = P \begin{pmatrix} t & -s \\ s & t \end{pmatrix} P^{-1}, \qquad P \in GL(F).$$

Exercice 12 (Matrices compagnons.) On considère une matrice telle que $A : e_1 \to e_2 \to \cdots \to e_{n-1} \to e_n \to a_{n-1}e_1 + \cdots + a_0 e_n$. Démontrer qu'on a

$$(-1)^n \chi_A(X) = X^n - a_1 X^{n-1} + \cdots - a_n = \mu_A(X).$$

1.4.4 Trigonalisation

Trigonaliser $A \in M_n(K)$ c'est écrire

$A = PTP^{-1}$, $\quad P \in GL_n(K)$, $\quad T$ triangulaire supérieure (ou inférieure).

- Si $K = \mathbb{C}$, toute matrice $A \in M_n(\mathbb{C})$ est trigonalisable.
- Si $A, B \in M_n(\mathbb{C})$ commutent i.e. $AB = BA$ alors elles sont trigonalisables dans une même base :

  $AB = BA \implies \exists P \in GL_n(\mathbb{R})$, $\quad PAP^{-1}$ et PBP^{-1} sont triangulaires supérieures.

1.4.5 Diagonalisation

- Une matrice est par définition diagonalisable sur K si elle est semblable à une matrice diagonale (la conjugaison étant dans K).
- Une matrice n'est pas toujours diagonalisable. Le prototype d'une matrice non diagonalisable est une matrice *nilpotente* càd une matrice N pour laquelle il existe $p \in \mathbb{N}^*$ vérifiant $N^p = 0$, $N^{p-1} \neq 0$.
- Une matrice réelle peut ne pas être diagonalisable sur $\mathbb{R}$ car toutes ses vp peuvent ne pas être réelle.
- Une matrice complexe n'est pas nécessairement diagonalisable, mais l'ensemble des matrices de $M_n(\mathbb{R})$ ou $M_n(\mathbb{C})$ qui sont diagonalisables sur $\mathbb{C}$ est dense.
- Des matrices diagonalisables qui commutent entre eux deux à deux peuvent être diagonalisées simultanément.

– Un critère **très utile** de diagonalisation est le suivant : **Si une matrice est annulée par un polynôme scindé à racines simples elle est diagonalisable**.
– En conséquence : l'ensemble des matrices diagonalisables est dense dans $M(n, \mathbb{C})$.

1.4.6 Réduction des endomorphismes

– Le résultat précédent est une conséquence du
Théorème de décomposition des noyaux : Soient $P_1, \ldots, P_r$ des polynômes premiers entre eux deux à deux
  – On a $\ker((P_1 \cdots P_r)(f)) = \bigoplus_{i=1}^{r} \ker P_i(f) \quad (*)$;
  – La projection $p_i : \ker((P_1 \cdots P_r)(f)) \to \ker P_i(f)$ relativement à la décomposition $(*)$ est la restriction à $\ker((P_1 \cdots P_r)(f))$ d'un polynôme en f.
  – (En particulier chaque sev $\ker(P_i(f))$ est f-invariant.)
– Quand on l'applique à $\mu_A(X) = \prod_{i=1}^{r}(X - \lambda_i)^{m_i}$ où $A \in M_n(\mathbb{C})$ on en déduit le
Théorème de **Dunford-Schwartz**

$$\begin{cases} A = S + N, \qquad S \text{ diagonalisable}, \quad N \text{ nilpotente}, \quad NS = SN \\ S \text{ et } N \text{ sont des polynômes en } A. \end{cases}$$

– En fait, le théorème de décomposition des noyaux démontre que l'on peut conjuguer A à une matrice diagonale par blocs qui contient r blocs de taille m_i, $1 \leqslant i \leqslant r$ et ces blocs sont de la forme $\lambda_i Id_{m_i} + N_i$ où N_i est nilpotente d'orde m_i.
– Il est possible de réduire par conjugaisons les blocs $\lambda_i I_{m_i} + N_i$ pour obtenir une **forme normale de Jordan**.
– Lien avec les suites définies par **récurrence linéaire** et les équations différentielles linéaires : *cf.* Exercice 14

Exercice 13 Soit $A \in M_n(\mathbb{C})$ telle que $A^3 = I$. Est-elle diagonalisable ?

Exercice 14
1) Soit $(u_k)_{k\in\mathbb{N}}$ une suite vérifiant

$$\forall\ k, \quad u_k = a_1 u_{k-1} + \cdots + a_n u_{k-n}.$$

Mq si on note $U_k = {}^t(u_{k-n}, \ldots u_{k-1})$ on a

$$U_{k+1} = ({}^tA)U_k$$

où A est la matrice de l'exercice 12.

2) Si on note

$$P(X) = X^n - a_1 X^{n-1} - \cdots - a_n = \prod_{i=1}^{r} (X - \lambda_i)^{m_i}$$

la suite (u_k) de la question 1) est de la forme

$$u_k = \sum_{i=1}^{r} \lambda_i^k p_i(k)$$

où les $p_i(k)$ sont des polynômes de degré $\leqslant m_i - 1$ en k.

3) Soit $u : \mathbb{R} \to \mathbb{R}$ solution de l'EDO linéaire à coefficients constants $u^{(n)}(t) - a_1 u^{(n-1}(t) - \cdots - a_n u(t) = 0$. Montrer que $u(t)$ est de la forme

$$u(t) = \sum_{i=1}^{r} e^{\lambda_i t} p_i(t)$$

où les p_i sont des polynômes de degré $\leqslant m_i - 1$.

1.5 Facteurs invariants, espaces cycliques

1.6 Matrices symétriques, matrices hermitiennes

1.6.1 Adjoint

- Adjoint d'un endomorphisme pour un produit scalaire :

  $$\forall\ u, v \in \mathbb{R}^n, \qquad \langle u, f(v) \rangle = \langle {}^t f(u), v \rangle.$$

  Si le produit scalaire est le produit scalaire standard sur $\mathbb{R}^n$ ($\langle u, v \rangle = {}^t uv$) et qu'on identifie f à une matrice A alors ${}^t f$ s'identifie à la transposée ${}^t A$ de A.
- Par définition une matrice $A \in M_n(\mathbb{R})$ est symétrique si ${}^t A = A$ (pour le produit scalaire standard sur $\mathbb{R}^n$). L'ensemble des matrices symétriques est un sev de $M_n(\mathbb{R})$.
- ${}^t(AB) = {}^t B {}^t A$.
- Toute matrice se décompose de façon unique en somme d'une matrice symétrique et d'une matrice antisymétrique.

1.6.2 Théorème spectral ($K = \mathbb{R}$)

- **Théorème spectral : Toute matrice symétrique est diagonalisable en base orthonormale.**
- **Théorème spectral (forme générale)** : Toute endomorphisme symétrique pour un produit scalaire est diagonalisable en base orthonormale (pour ce produit scalaire).
- Une matrice symétrique est dite **positive** (resp. définie positive) si pour tout $X \in \mathbb{R}^n \backslash \{0\}$, le *réel* ${}^tXAX$ est $\geqslant 0$ (resp. > 0).
- Une matrice symétrique définie positive définit un produit scalaire sur $\mathbb{R}^n$ et réciproquement un produit scalaire sur $\mathbb{R}^n$ définit une matrice définie positive :
$$\langle u, v \rangle_A = \langle u, Av \rangle.$$

1.6.3 Formes quadtratiques ($K = \mathbb{R}$)

- Plus généralement, il y a une correspondance biunivoque entre les matrices symétriques et les formes quadratiques :
$$\begin{array}{ccc} q \text{ forme quadratique} & \longleftrightarrow & A \text{ matrice symétrique} \\ q(u) & = & {}^tuAu. \end{array}$$
- Si $q_A(u) = {}^tuAu$ est une forme quadratique et $P \in GL_n(\mathbb{R})$ la forme quadratique $\tilde{q}(u) = q_A(Pu)$ est de la forme
$$\tilde{q}(u) = q_A(Pu) = q_{\tilde{A}}(u), \qquad \text{avec} \quad \tilde{A} = {}^tPAP.$$
- Une conséquence du théorème spectral dans sa version générale est la **réduction simultanée** des formes quadratiques : Soit A un matrice définie positive et B une matrice symétrique. Alors, il existe un matrice $P \in GL(n, \mathbb{R})$ telle que
$${}^tPAP = I \qquad \text{et} \qquad {}^tPBP = \text{matrice diagonale.}$$
- Comparer le théorème spectral avec le **Théorème de Gram-Schmidt**. Si q est un produit scalaire (donc de la forme q_A avec A définie positive), il existe une matrice triangulaire supérieure T telle $(Te_1, \ldots, Te_n)$ soit orthonormale et donc telle que $u \mapsto q_A(Tu)$ soit le produit scalaire usuel. Conséquence
$${}^tTAT = I, \qquad T \text{ TS.}$$
- Une matrice est définie positive si et seulement si tous ses mineurs (resp. mineurs principaux) sont définis positifs.

1.6.4 Isométries

- **Isométries** C'est le groupe des automorphismes linéaires qui préservent un produit scalaire. On note $O(n,\mathbb{R})$ le *groupe* des matrices (vues comme transformations linéaires) qui préservent le produit scalaire euclidien sur $\mathbb{R}^n$

$$A \in O(n,\mathbb{R}) \iff \forall\, u \in \mathbb{R}^n, \quad \langle Au, Au\rangle = \langle u, u\rangle \qquad \iff \qquad {}^tAA = I.$$

- Deux exemples importants : les symétries orthogonales et les rotations.
- Symétries : $\sigma : \mathbb{R}^n \to \mathbb{R}^n$, $\sigma^2 = I$. On a (par exemple parce que $(X-1)(X+1)$ annule σ)

$$\mathbb{R}^n = \ker(\sigma - id) \oplus^{\perp} \ker(\sigma + id).$$

  Les symétries orthogonales engendrent $O(n,\mathbb{R})$.
- **Groupe des rotations :** $SO(n,\mathbb{R}) = O(n,\mathbb{R}) \cap \{A,\ \det A = 1\}$.
- **Forme normale des rotations :** Une rotation s'écrit dans une base orthonormale comme une matrice par blocs dont les blocs sont soit de taille 1 et réduit à 1, soit de taille 2 et de la forme $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ où θ dépend du bloc (matrice de rotation du plan).
- **Matrices de Gram.**
- Distance euclidienne d'un point à un hyperplan ou un sev.
- Polynômes orthogonaux.

Exercice 15 Une matrice de rotation dans $\mathbb{R}^{2n+1}$ admet une droite invariante.

Exercice 16 Quelle est l'image d'un cercle (resp. sphère) par une application linéaire de $\mathbb{R}^2$ (resp. $\mathbb{R}^3$) ?

Exercice 17 Démontrer que la matrice $((i+j+1)^{-1})_{1\leqslant i,j\leqslant n}$ est définie positive. [Introduire un produit scalaire dans un espace de fonctions.]

Exercice 18 Toute matrice de $A \in GL(n,\mathbb{R})$ s'écrit sous la forme $A = SU$ où S est symétrique et $U \in SO(n,\mathbb{R})$. En déduire que $GL(n,\mathbb{R})^+$ est connexe.

Exercice 19 Démontrer que le groupe $SO(n,\mathbb{R})$, $n \geqslant 3$ est simple.

Exercice 20 (Inégalités de Hadamard) Soit $A \in M_n(\mathbb{R})$. On note $C_1, \ldots, C_n$ les colonnes de A et $\|\cdot\|_2$ la norme euclidienne dans $\mathbb{R}^n$. Démontrer que

$$|\det(A)| \leqslant \prod_{i=1}^{n} \|C_i\|_2.$$

2 Analyse réelle

2.1 $\mathbb{R}$, Topologie de $\mathbb{R}$

2.1.1 Définition de $\mathbb{R}$ et propriétés

- Le corps $(\mathbb{Q}, +, \times)$, $\mathbb{Q} = \{p/q,\ (p,q) \in \mathbb{Z} \times \mathbb{Z}^*\}$ est totalement ordonné et dénombrable. On peut le munir d'une topologie en décrétant qu'un ouvert non vide de $\mathbb{Q}$ est un ensemble contenant un intervalle ouvert $]r, s[$, $r < s$, $r, s \in \mathbb{Q}$. Le corps $\mathbb{Q}$ ne permet pas de résoudre $x^2 = 2$ (Euclide). D'autre part il n'est pas complet : une *suite de Cauchy* dans $\mathbb{Q}$ ne converge pas nécessairement.
- Suite de Cauchy dans $\mathbb{Q}$: $(u_n)_{n\in\mathbb{N}}$ telle que pour tout $\epsilon \in \mathbb{Q}_+^*$ il existe $N \in \mathbb{N}$ tel que pour tout $n, m \in [N, \infty[\cap\mathbb{N}$, $|u_n - u_m| \leqslant \epsilon$.
- Le corps $\mathbb{R}$ est le **complété de** $\mathbb{Q}$: Si $(\mathcal{C}, +, \times)$ est l'anneau de toutes les suites de Cauchy à valeurs dans $\mathbb{Q}$ et $\mathcal{N}$ est l'idéal des suites à valeurs dans $\mathbb{Q}$ convergeant vers 0 (pour tout $\epsilon \in \mathbb{Q}_+^*$, $\exists N \in \mathbb{N}$, $\forall\ n \geqslant N$, $|u_n| \leqslant \epsilon$), l'anneau quotient $\mathcal{C}/\mathcal{N}$ est par définition $(\mathbb{R}, +, \times)$. On peut voir que c'est un corps. On peut définir une relation d'ordre total sur $\mathbb{R}$: si $x = (u_n)_n \mod \mathcal{N}$, $y = (v_n)_n \mod \mathcal{N}$ on a $x < y$ si à partir d'un certain rang $u_n < v_n - \epsilon$ pour un certain $\epsilon > 0$. On peut munir $\mathbb{R}$ d'une topologie en décrétant qu'un ouvert non vide de $\mathbb{R}$ est un ensemble U tel que pour tout $x \in U$ il existe un intervalle ouvert $]r, s[$, $r < s$, $r, s \in \mathbb{R}$ tel que $x \in]r, s[\subset U$. Muni de cette topologie, $\mathbb{R}$ est complet : toute suite de Cauchy converge. Il existe une injection naturelle de $\mathbb{Q}$ dans $\mathbb{R}$ ("$\mathbb{R}$ contient $\mathbb{Q}$").

2.1.2 $\mathbb{R}$ est archimédien

- Le corps ordonné $\mathbb{R}$ (comme $\mathbb{Q}$) est **achimédien** : si $0 < x < y$ il existe un unique entier $n \in \mathbb{N}$ tel que $nx \leqslant y < (n+1)x$.
- **Classification des sous-groupes additifs fermés de $\mathbb{R}$.** Cette dernière propriété permet de démontrer qu'un **sous-groupe fermé** de $(\mathbb{R}, +)$ est soit de la forme $a\mathbb{Z}$, $a \in \mathbb{R}$, soit égal à $\mathbb{R}$.

2.1.3 inf, sup, valeur d'adhérence, lim inf, lim sup *etc.*

- Si A est un sous-ensemble non vide de $\mathbb{R}$ on dit que $M \in \mathbb{R}$ est un majorant de A si $\forall\ x \in A$, $x \leqslant M$. Si l'ensemble des majorants de A est non vide, il admet un plus petit élément (un min) que l'on appelle $\sup A$. (Définition analogue pour $\inf A$).

– Un ensemble borné $A \subset \mathbb{R}$ (i.e. $A \subset [-M, M]$) non vide admet toujours un inf et un sup.
– $\sup A = s$ est équivalent aux deux propriétés suivantes : (1) $\forall a \in A,\ a \leqslant s$; (2) $\forall\ \epsilon > 0,\ [s - \epsilon, s] \cap A \neq \varnothing$.
– Une suite monotone admet une limite (qui peut être finie ou égale à $\pm\infty$). Si par exemple la suite est croissante majorée, cette limite est finie.
– Si $(u_n)_n$ est une suite de réels (disons bornée) la suite

$$\overline{u}_n = \sup\{u_p,\ p \geqslant n\}$$

est décroissante et admet donc une limite

$$\limsup_n u_n = \lim_n \overline{u}_n = \lim_n \sup\{u_p,\ p \geqslant n\}.$$

On a

$$\limsup(-u_n) = -\liminf u_n.$$

Si on autorise $\pm\infty$, une suite admet toujours une lim sup et une lim inf.
– Caractérisation de lim sup. On a $\limsup u_n = \alpha$ si et seulement si pour tout $\alpha' > \alpha$
  – Il n'y a qu'un nombre fini de termes de la suite à droite de α'
  – et : il y a une infinité de termes à gauche de α'.
– Une suite $(u_n)_n$ converge si et seulement si

$$\limsup_n u_n = \liminf_n u_n \quad (\in \mathbb{R})$$

et sa limite est ce nombre.
– Soit $(u_n)_n$ une suite bornée. On dit que $a \in \mathbb{R}$ est une **valeur d'adhérence** (point de la suite (u_n) s'il existe une sous-suite u_{n_k} qui converge vers a. Si A est l'ensemble des valeurs d'adhérence :

$$A = \bigcap_{n \geqslant 0} \overline{\{u_k, k \geqslant n\}}.$$

C'est un fermé et on a

$$\limsup_n u_n = \max A, \qquad \liminf_n u_n = \min A.$$

2.1.4 Représentation a-adique

– Une représentation commode des réels sont les **développement décimaux ou dyadiques** (triadiques, etc.) :

$$x = \sum_{n=-N}^{\infty} a_n \times 10^{-n}, \qquad a_n \in \{0, 1, 2, \ldots, 9\}$$

$$x = \sum_{n=-N}^{\infty} a_n \times 2^{-n}, \qquad a_n \in \{0,1\}.$$

La représentation existe toujours mais n'est pas unique si x est un nombre décimal $10^{-n}m$, $m \in \mathbb{Z}$) (resp. un nombre dyadique $2^{-n}m$, $m \in \mathbb{Z}$) : $0,999999\cdots = 1$. Dans les autres cas elle est unique.

2.1.5 Topologie

- Les **compacts de** $\mathbb{R}$ sont les fermés bornés. Un compact admet toujours un max et un min.
- Les **connexes de** $\mathbb{R}$ sont les convexes de $\mathbb{R}$, i.e. les intervalles (fermés ou pas).
- Si U est un ouvert de $\mathbb{R}$, il a un nombre dénombrable de composantes connexes.

2.1.6 Suites et séries

- Suites équivalentes. Sommation des équivalences.
- Séries. Convergence absolue, séries alternées, **sommation d'Abel** (IPP discrète).
- Produits infinis : pour justifier la convergence avoir en tête (u_k petit > 0)

$$\prod_{k=0}^{n}(1-u_k) \leqslant \prod_{k=0}^{n}\exp(-u_k) = \exp(-\sum_{k=0}^{n} u_k).$$

Exercice 21 (Suites sous-additives) Soit $(u_n)_{n\in\mathbb{N}}$ une suite telle que

$$\forall\ n, m \in \mathbb{N}, \quad u_{n+m} \leqslant u_n + u_m.$$

Démontrer que

$$\lim_{n\to\infty} \frac{u_n}{n} = \inf_{n\in\mathbb{N}} u_n.$$

Exercice 22 On note $\{x\}$, la partie fractionnaire de x (càd x auquel on a soustrait sa partie entière $[x]$). Démontrer que si α est irrationnel la suite $(\{n\alpha\})_{n\in\mathbb{N}}$ est dense dans $[0,1]$. [Penser aux sous-groupes additifs de $\mathbb{R}$.]

Exercice 23 On définit pour $x \in [0,1[$, la suite $u_n(x) = \{2^n x\}$. Démontrer qu'il existe $x \in [0,1[$ pour lequel la suite $u_n(x)$ est dense dans $[0,1]$. [Penser à la représentation dyadique de x.]

Exercice 24 Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par

$$u_{n+1} = \sin(u_n), \qquad u_0 \in [0, \pi/2].$$

Démontrer que $\lim_n u_n = 0$.

Exercice 25 1) Soit U_n une suite telle que

$$\lim_{n\to\infty} U_{n+1} - U_n = a > 0.$$

Démontrer que $U_n \sim a \times n$.

2) Soit $(u_n)_{n\in\mathbb{N}}$ une suite telle que $u_{n+1} = u_n - au_n^2$. Démontrer que si u_0 est suffisamment petit, on a $u_n \sim 1/(an)$. [On montrera que $\lim u_n = 0$ puis on pourra poser $U_n = 1/u_n$ afin d'utiliser la question 1.]

Exercice 26 Soit $(u_n)_{n\in\mathbb{N}}$ une suite de nombres réels bornée telle que

$$\lim_{n\to\infty} (u_n + \frac{1}{2}u_{2n}) = 1.$$

Que dire de $(u_n)_{n\in\mathbb{N}}$?

Exercice 27 1) Soit $(u_n)_{n\in\mathbb{N}}$ une suite définie dans $[0, 1]$ telle que $\lim_n(u_{n+1} - u_n) = 0$. Montrer que l'ensemble des valeurs d'adhérence de $(u_n)_{n\in\mathbb{N}}$ est un intervalle compact.

2) Soit une suite u_n, définie par $u_{n+1} = f(u_n)$ où $f : [0, 1] \to [0, 1]$ est continue et $u_0 \in [0, 1]$. Démontrer que si $\lim_n(u_{n+1} - u_n) = 0$ alors la suite u_n converge.

Exercice 28 Convergence de $\sum_{k=1}^{\infty}(1/k^\alpha)\sin(\sqrt{k})$ pour $\alpha = 0$, $\alpha = 1$, $\alpha = 1/2 - \epsilon$.

2.2 Fonctions continues

- Fonctions continue en un point. Une fonction $f : X \to Y$ (X et Y deux espaces topologiques) est continue si elle est continue en tout point de X.
- Une fonction $f : X \to Y$ est continue ssi la préimage de tout ouvert (resp. fermé) est un ouvert (resp. fermé).

– Si $f : X \to Y$ est continue et X est compact alors $f(X)$ est compact. Application : une application continue $X \to \mathbb{R}$ définie sur X compact atteint son inf et son sup.
– Une conséquence du résultat précédent est qu'une application continue bijective entre deux compacts est un homéomorphisme (son inverse pour la composition est aussi continu).
– Si $f : X \to Y$ est continue et X est connexe alors $f(X)$ est connexe. Application : une application continue $X \to \mathbb{R}$ définie sur X connexe vérifie le théorème des valeurs intermédiaires.

2.3 Fonctions dérivables

– Définition : $f(a+h) = f(a) + f'(a)h + o(h)$.
– Somme, produit, quotient, composition, inverse pour la composition...
– **Rolle** (connaitre la preuve) : $f : [a,b] \to \mathbb{R}$ continue, dérivable sur $]a,b[$. Si $f(a) = f(b)$ alors, il existe $c \in]a,b[$ tel que $f'(c) = 0$.
– Penser à **itérer** Rolle si on a des dérivées supplémentaires. Si f est n-fois dérivable sur $]a,b[$ et f s'annule en $n+1$ points, alors $f^{(n)}$ d'annule en un point.
– Théorème des **valeurs intermédiaires** : $f : [a,b] \to \mathbb{R}$ continue, dérivable sur $]a,b[$. Alors, il existe $c \in]a,b[$ tel que $f'(c) = (f(b) - f(a))/(b-a)$.
– Lien avec l'intégration

$$f(b) - f(a) = \int_a^b f'(t)dt.$$

Exercice 29 1) Soient $\lambda_1, \ldots, \lambda_n$ des nombres complexes distincts deux à deux. Démontrer que la fonction

$$f(t) = \sum_{k=1}^{n} c_k \exp(t\lambda_k)$$

est identiquement nulle si et seulement si $c_1 = \cdots = c_n = 0$. [Dérivation et Vandermonde.]

2) Démontrer que si les $\lambda_1, \ldots, \lambda_n$ sont réels la fonction précédente est nulle si et seulement si elle s'annule au moins n fois sur $\mathbb{R}$. [Récurrence et Rolle itéré.]

2.4 Les formules de Taylor

– Si $f : [a, b] \to \mathbb{R}$ continue, n fois dérivable sur $]a, b[$ alors il existe $c \in]a, b[$ tq

$$f(a+h) = f(a)+f'(a)h+\cdots+(f^{(n-1)}(a)/(n-1)!)h^{n-1}+(f^{(n)}(c)/n!)h^n.$$

– Taylor-Young : Si $f :]a-\epsilon, a+\epsilon[\to \mathbb{R}$ est n fois dérivable en a

$$f(a+h) = f(a) + f'(a)h + \cdots + (f^{(n)}(a)/n!)h^n + o(h^n).$$

– Taylor-Lagrange : Si f est C^n sur $[a, b]$

$$\left| f(a+h) - \left(f(a)+f'(a)h+\cdots+(f^{(n-1)}(a)/(n-1)!)h^{n-1} \right) \right| \leqslant (\sup_{[a,b]} |f^{(n)}|)\frac{h^n}{n!}.$$

– **Taylor-Reste intégral** : Si f est C^n sur $[a, b]$

$$f(a+h) = f(a)+f'(a)h+\cdots+\frac{f^{(n-1)}(a)}{(n-1)!}h^{n-1}+h^n\int_0^1 \frac{(1-t)^{n-1}}{(n-1)!}f^{(n)}(a+th)dt.$$

– **Développements limités** : connaître ceux de exp, ln, sin, cos, cosh, sinh, $(1+x)^{-1}$, $(1+x)^\alpha$, $(\alpha \in \mathbb{R})$, tan à l'ordre 3.

$$\forall\, x \in]-1, 1[, \quad (1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k \quad \text{où } \binom{\alpha}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}.$$

Exercice 30 Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction C^∞ telle que $f(0) = 0$. Démontrer qu'il existe une fonction $g : \mathbb{R} \to \mathbb{R}$, C^∞, telle que $f(x) = xg(x)$.

Exercice 31 Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction de classe C^2 telle que $\|f\|_2 := \sup_{x\in\mathbb{R}} \max_{j=0,1,2} |f^{(j)}(x)| < \infty$. Démontrer que

$$\|f'\|_0 \leqslant 2\|f\|_0^{1/2}\|f''\|_0^{1/2}.$$

Exercice 32 Trouver un équivalent de la suite $(u_n)_{n\in\mathbb{Z}}$ définie dans l'exercice 24. [Faire un DL de $\sin u_n$ et utiliser la méthode de l'exercice 25.]

2.5 L'intégration

2.5.1 Au sens de Cauchy

- **(Au sens de Cauchy)** Si $f : [a, b] \to \mathbb{R}$ est continue la suite

$$\sum_{k=0}^{n-1} f(a + \frac{k}{n}(b-a)) \times \frac{b-a}{n}$$

est de Cauchy et sa limite est l'intégrale $\int_a^b f(x)dx$.

2.5.2 Au sens de Riemann

- **(Au sens de Riemann)** : Toute fonction continue par morceaux est Riemann intégrable (nombre fini de morceaux).
- **Intégrale impropre.** Exemple : $\int_0^\infty (\sin x/x)dx$. La fonction sous l'intégrale n'est pas L^1 mais $I(a) := \int_0^a (\sin x/x)dx$ vérifie le critère de Cauchy :

$$\lim_{\min(a_1,a_2)\to\infty} |I(a_2) - I(a_1)| = 0.$$

- Reconnaître des primitives classiques :

$$\int \frac{dx}{1+x^2} \quad (\arctan), \qquad \int \frac{dx}{\sqrt{1-x^2}} \quad (\arcsin), \qquad \int \frac{dx}{\sqrt{1+x^2}} \quad (\sinh^{-1})$$

Pour les fractions rationnelles penser à une décomposition en éléments simples.
- Comparaison somme / intégrale (toujours faire un dessin).

2.5.3 Au sens de Lebesgue

- Tribu **borélienne** $Bor(\mathbb{R})$: la plus petite tribu engendrée par les ouverts de $\mathbb{R}$ (ou les intervalles).
- **Mesure de Lebesgue** : l'**unique** mesure sur $Bor(\mathbb{R})$ telle que pour tout intervalle $I \subset \mathbb{R}$,

$$\mu(I) = \text{longueur}(I).$$

- Fonctions **mesurables** : f est mesurable ssi la préimage de tout ouvert (ou de tout intervalle) est dans la tribu borélienne.
- Intégrale des fonctions **étagées** $f := \sum_{i=1}^n \lambda_i \mathbf{1}_{A_i}$ (A_i boréliens) : $\int_{\mathbb{R}} f d\mu = \sum_{i=1}^n \lambda_i \mu(A_i)$.
- Pour toute fonction mesurable f **positive** on peut définir $\int_{\mathbb{R}} f d\mu \in [0, \infty]$. (Rappel sur la convention $\infty + \infty = \infty \times \infty = \infty$ et $0 \times \infty = 0$).

– Fonctions **intégrables** : $\int_{\mathbb{R}} |f| d\mu < \infty$. On définit

$$\mathbb{R} \ni \int_{\mathbb{R}} f d\mu = \int_{\mathbb{R}} \max(f, 0) d\mu - \int_{\mathbb{R}} \max(-f, 0) d\mu.$$

– Une fonction intégrable prend des valeurs finies μ-pp.
– Convergence **monotone** : Si les f_n sont positives, mesurables, et $f_n \leqslant f_{n+1}$

$$\lim \int_{\mathbb{R}} f_n d\mu = \int_{\mathbb{R}} \lim f_n d\mu.$$

– Convergence **dominée** : Les f_n sont dans $L^1(\mathbb{R}, \mu)$, f_n converge simplement vers f μ-pp, il existe $g \in L^1(\mathbb{R}, \mu)$ tq pour tout n, $|f_n| \leqslant g$ et μ-pp $\lim f_n$ existe. Alors, f est dans L^1 et

$$\lim \int_{\mathbb{R}} f_n d\mu = \int_{\mathbb{R}} \lim f_n d\mu.$$

– (Lemme de Fatou) : Si les f_n sont positives

$$\limsup \int_{\mathbb{R}} f_n d\mu \leqslant \int_{\mathbb{R}} (\limsup f_n) d\mu.$$

– Théorèmes de **continuité et de dérivation sous le signe intégral**.
– **Mesure produit** : sur $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ on définit $Bor(\mathbb{R} \times \mathbb{R})$ comme la plus petite tribu qui contient les rectangles $I \times J$, I, J intervalles de $\mathbb{R}$. Il existe une unique mesure $\mu \otimes \mu$ définie sur $Bor(\mathbb{R} \times \mathbb{R})$ qui vérifie pour I, J intervalles de $\mathbb{R}$ (ou boréliens)

$$\mu(I \times J) = \mu(I) \times \mu(J).$$

– **Fubini positif** : Si $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ est mesurable, positive on peut définir pour μ-pt $x \in \mathbb{R}$ (resp. $y \in \mathbb{R}$), l'application $x \mapsto \int_{\mathbb{R}} f(x, y) d\mu(y)$ (resp. $y \mapsto \int_{\mathbb{R}} f(x, y) d\mu(x)$), ces applications sont mesurables positives et

$$\int_{\mathbb{R}} f d(\mu \otimes \mu) = \int_{\mathbb{R}} \left(\int_{\mathbb{R}} (f(x, y) d\mu(y) \right) d\mu(x) = \int_{\mathbb{R}} \left(\int_{\mathbb{R}} (f(x, y) d\mu(x) \right) d\mu(y)$$

– **Fubini** L^1 Si f est de signe quelconque mais $f \in L^1(\mathbb{R} \times \mathbb{R}, \mu \otimes \mu)$ la formule précédente reste vraie. En plus, les applications $x \mapsto \int_{\mathbb{R}} f(x, y) d\mu(y)$, $y \mapsto \int_{\mathbb{R}} f(x, y) d\mu(x)$ sont L^1 donc finie μ-pp. Pour vérifier $f \in L^1(\mathbb{R} \times \mathbb{R}, \mu \otimes \mu)$ on applique Fubini **positif** à $|f|$.

– **Changement de variables** Soit $f : U \to \mathbb{R}^n$, U ouvert de $\mathbb{R}^n$ dans $L^1(U, \mathbb{R}^n)$. On suppose qu'il existe un difféomorphisme $\varphi : U \to V$ (d'image V), $(x_1, \ldots, x_n) \mapsto (\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_n(x_1, \ldots, x_n))$. On a toutes les fois où cela a un sens

$$\int_V f(v)d\mu(v) = \int_U (f \circ \varphi)(u)\left|\frac{d\mu(v)}{d\mu(u)}\right| d\mu(u) = \int_U (f \circ \varphi)(u)|Jac(\varphi)|d\mu(u)$$

où $J(u) = \det D\varphi(u)$ est le jacobien (le déterminant de l'endomorphisme $h \mapsto D\varphi(u) \cdot h$ ou encore de la matrice $(\partial\varphi_i/\partial x_j)_{1 \leqslant i,j \leqslant n}$).

2.5.4 Quelques réflexes à avoir

– **Réflexes** à avoir (p.ex. cas $f : \mathbb{R} \to \mathbb{R}$)
  – Faire un dessin.
  – Intégration par parties
  – Fubini
  – Changement de variables
  – Convergence dominée
  – Dérivations par rapport à un paramètre (couplé en général à IPP).
  – (pour des inégalités) Cauchy-Schwartz.
  – Convexité.

Exercice 33 Soit $f : [0, 1] \to [0, 1]$ une fonction continue strictement croissante telle que $f(0) = 0$, $f(1) = 1$ et f^{-1} son inverse pour la composition. Démontrer que

$$1 = \int_0^1 f(x)dx + \int_0^1 f^{-1}(y)dy.$$

[Faire un dessin.]

Exercice 34 1) Montrer que l'intégrale impropre $\int_0^\infty (\sin x/x)dx$ converge. 2) Calculer sa valeur. [On introduira pour $t > 0$, $I(t) = \int_0^\infty e^{-xt}\frac{\sin x}{x}dx$ que l'on dérivera.]

Exercice 35 Montrer que l'on peut établir l'égalité

$$\frac{\pi^2}{6} = \sum_{n=1}^{\infty} \frac{1}{n^2}$$

en considérant l'intégrale double

$$\int_{[0,1]^2} \frac{dxdy}{1 - xy}.$$

Exercice 36 Soit $f \in C^2(]0,\infty[,\mathbb{R})$ vérifiant $f(0)f'(0) = 0$ et telle que les intégrales $\int_0^\infty f^2$ et $\int_0^\infty (f'')^2$ convergent. Démontrer que $\int_0^\infty (f')^2$ converge et que $\|f'\|_2^2 \leqslant \|f\|_2 \|f''\|_2$. [IPP, Cauchy-Schwarz]

Exercice 37 Soient $a > 0$ et $f : \mathbb{R} \to \mathbb{R}$ continue telle que $\int_{\mathbb{R}} f^2(t)dt < \infty$. Démonter qu'il existe une unique solution $y : \mathbb{R} \to \mathbb{R}$, continue telle que $\int_{\mathbb{R}} y^2(t)dt < \infty$ à l'équation $y'(t) - ay(t) = f(t)$. [La formule de variation de la constante montre que $y(t) = -e^{at}\int_t^\infty e^{-as} f(s)ds$; il s'agit de montrer que cette expression définit bien une fonction L^2.]

Exercice 38 1) Trouver un équivalent de $\int_{-\infty}^{\infty} e^{-tu^2/2}du$ quand t tend vers l'infini.
2) Même question pour $\int_{-\pi/2}^{\pi/2} e^{-t\cos x}dx$.

2.6 Convexité

- Une fonction $f : \mathbb{R} \to \mathbb{R}$ est convexe si

$$\forall\ x, y \in \mathbb{R},\ \forall t \in [0,1], \quad f(tx + (1-t)y) \leqslant tf(x) + (1-t)f(y).$$

- Une fonction convexe est toujours continue.
- Si f est dérivable par morceaux, la convexité est équivalente à la croissance de $x \mapsto f'(x)$.
- Si f est convexe dérivable alors pour $x \leqslant z \leqslant y$, le graphe de f est toujours au dessous de la corde $[(x, f(x)), (y, f(y))]$ et en dessous de la tangente passant par $(z, f(z))$.
- Si f est deux fois dérivable la convexité est équivalente à $f'' \geqslant 0$. Utile quand on couple à un DL à l'ordre 2 en un point où la dérivée s'annule.
- Quand on veut utiliser la convexité (pour des inégalités p.ex.) toujours **faire un dessin !** Ce que l'on voit est pratiquement toujours vrai.
- Applications : comparaison des moyennes arithmétique, géométrique et harmonique. Des inégalités de la forme $(2/\pi)x \leqslant \sin x \leqslant x$ pour $x \in [0, \pi/2]$ ou $xy \leqslant (x^a/a) + (x^b/b)$ $(a + b = 1,\ a, b \geqslant 0)$ etc.
- Mêmes résultats en dimension plus grande (fonctions $\mathbb{R}^n \to \mathbb{R}$).

Exercice 39 Démontrer que si un polynôme réel Q n'a que des zéros réels alors la fonction $-\ln|Q|$ est convexe. En déduire que pour tout $x \in \mathbb{R}$, $Q(x)''Q(x) \leqslant (Q'(x))^2$.

Exercice 40 Existe-t-il une fonction $f : \mathbb{R} \to \mathbb{R}$ de classe C^2 telle que pour tout $x \in \mathbb{R}$

$$1 + \frac{1}{1+|x|}(f(x)f'(x))^2 + f''(x) = 0 \ ?$$

3 Espaces fonctionnels

- Cadre général : **Banach** vs. **Hilbert**.
- Les sev ne sont intéressants que s'ils sont fermés et les applications linéaires que si elles sont continues.

3.1 Banach

3.1.1 Espaces Fonctionnels

- Les espaces de **fonctions** C^k, $k \in \mathbb{N}$ (ou $k \in \mathbb{R}_+$). Si U est un ouvert de $\mathbb{R}^n$ on note $C^k(U)$ l'ensemble des fonctions k-fois dérivables dont la dérivée k-ième est continue et pour avoir une norme on suppose que
$$\|f\|_{C^k(U)} := \max_{0 \leqslant l \leqslant k} \sup_{x \in U} |D^l f(x)| < \infty.$$
- Rappel sur $D^l f$. Si $f : U \to \mathbb{R}$ (ou $f : U \to \mathbb{R}^d$), $D^l f(x)$ est une forme (ou application) n-linéaire symétrique $\mathbb{R}^n \to \mathbb{R}$ (ou $\mathbb{R}^n \to \mathbb{R}^d$), $(h_1, \ldots, h_n) \mapsto D^l f(x) \cdot (h_1, \ldots, h_n)$. Cf. Rappels sur le calcul différentiel.
- L'espace $C^k(U)$ muni de $\|\cdot\|_{C^k(U)}$ est un espace de Banach. A rapprocher du fait que si f_n est une suite de fonctions dérivables qui converge uniformément ainsi que ses dérivées alors la limite simple des f_n est continue et dérivable.
- Les espaces de **fonctions** L^p, $p \in [1, \infty]$:
$$L^p(U) = \{f : U \to \mathbb{R}, \text{ mesurable}, \int_U |f|^p dx < \infty\}, \quad \|f\|_{L^p(U)} = (\int_U |f|^p dx)^{1/p}.$$
Si $p \geqslant 1$, muni de cette norme c'est un espace de Banach.
- Connaître les inégalités de **Minkowski** ($\|\cdot\|_{L^p}$ est une norme) et les inégalités de **Hölder**.
- Si f_n converge vers f dans L^p, il existe une sous-suite n_k telle que $f_{n_k}(x)$ converge vers $f(x)$ pour μ-pt x.
- Les espaces de **suites** l^p, $p \in [1, \infty]$: $l^p(\mathbb{Z}) = \{(u_n)_{n \in \mathbb{Z}}, \quad \sum_{n \in \mathbb{Z}} |u|^p < \infty\}$.

3.1.2 Convolution et régularisation

- $L^1(\mathbb{R})$ (ou $l^1(\mathbb{Z})$) peut-être muni d'un **produit de convolution** qui est **commutatif** et **associatif**.
$$f * g(x) = \int_{\mathbb{R}} f(x-y) g(y) dy = g * f(x) \qquad ((u * v)_n = \sum_{n \in \mathbb{Z}} u_k v_{n-k})$$
$$\|f * g\|_{L^1} \leqslant \|f\|_{L^1} \|g\|_{L^1} \qquad (\|u * v\|_{l^1} \leqslant \|u\|_{l^1} \|v\|_{l^1}).$$

Le produit de convolution dans $l^1(\mathbb{Z})$ admet un élément neutre, la suite $n \mapsto \delta(n)$ qui vaut 1 en $n = 0$ et 0 partout ailleurs (fonction δ de **Dirac** dans le cas $l^1(\mathbb{Z})$). En revanche, l'élément neutre pour le produit de convolution dans $L^1(\mathbb{R})$ est la distribution δ de Dirac qui est une mesure mais n'est pas une fonction dans L^1.

– L'opération de convolution est commutative, associative et **commutent avec la dérivation** : toutes les fois où cela a un sens

$$\partial(f * g) = (\partial f) * g = f * (\partial g).$$

– Les espaces $C^k([0,1])$ ($k \in \mathbb{N}$) et $L^p([0,1])$ ($p \geqslant 1$) sont **séparables**, càd admettent un sous-espace dense engendré par un ensemble dénombrable, par exemple l'espace des fonctions polynomiales. Ce n'est pas le cas de $L^\infty([0,1])$.

3.1.3 Approximation de l'identité

– Si $f \in L^1(\mathbb{R})$ et χ est C^∞ à support compact la fonction $\chi * f$ est C^∞.

– **Approximation de l'identité.** Soit χ une fonction C^∞, positive, à support compact et telle que

$$\int_{\mathbb{R}} \chi(x)dx = 1.$$

On pose pour $\epsilon > 0$

$$\chi_\epsilon(x) = \frac{1}{\epsilon}\chi(x/\epsilon).$$

Les fonction $\chi_\epsilon * f$ sont C^∞ et :

– Si f est L^1, $\chi_\epsilon * f$ converge vers f en norme L^1 quand $\epsilon \to 0$.

– Si f est continue en plus d'être L^1, $\chi_\epsilon * f$ converge uniformément vers f sur tout compact.

Voir exercice 42 pour une version sur le cercle $\mathbb{R}/\mathbb{Z}$.

3.1.4 Théorèmes de densité des polynômes dans $C^0(K)$.

– Théorème de **Stone-Weirestrass** : Une algèbre de fonctions continues sur un compact K contenant 1, stable par conjugaison complexe et qui **sépare les points** est dense dans $C^0(K)$. En particulier, toute fonction continue sur $[a,b]$ (resp. toute fonction continue 1-périodique) peut-être approchée uniformément par des polynômes (resp. polynômes trigonométriques).

– Les polynômes de **Bernstein** donne une approximation explicite $B_n(f)(x) = \sum_{k=0}^n \binom{n}{k} f(k/n)x^k(1-x)^{n-k}$ converge uniformément vers f sur $[0,1]$.

– Les sommes de **Féjer** (exercice 42).

3.1.5 Théorèmes généraux des espaces de Banach

- Théorème de **Baire** (vrai dans les espaces complets ou compacts)
- Théorème de **Banach-Steinhaus**
- Théorème de **l'application ouverte ou théorème du graphe fermé**.
- Remarque : le théorème de **Hahn-Banach** (très utile pour démontrer des résultats de densité) est vrai dans le cadre des espaces vectoriels normés (pas forcément Banach).

3.2 Espaces de Hilbert

- $L^2(\mathbb{R})$, $l^2(\mathbb{R})$. Dans le cadre des séries de Fourier $L^2(\mathbb{R}/\mathbb{Z})$ qui est l'espace des fonctions L^2, $f : \mathbb{R} \to \mathbb{R}$ qui sont 1-périodiques càd $f(x+1) = f(x)$, Lebesgue-pp.
- **Cauchy-Schwarz**
- Le théorème de **projection orthogonale** : si $F \subset E$ (E Hilbert) SEV fermé alors il existe $P : E \to F$ projection orthogonale $\|P\|_{op} \leqslant 1$.
- **Riesz-Fisher** : si $\Lambda : E \to \mathbb{R}$ est une forme linéaire continue, il existe $v \in E$ tq pour tout $u \in E$, $\Lambda u = \langle v, u \rangle$.
- Si $T : E \to E$ linéaire continue, $\ker T^* = (\mathrm{Im}T)^\perp$ ($\langle u, Tv \rangle = \langle T^* u, v \rangle$).

Exercice 41 Soit $f : [0,1] \to \mathbb{R}$ continue. Démontrer que

$$\lim_{p \to \infty} \left(\int_0^1 |f(x)|^p dx \right)^{1/p} = \sup_{x \in [0,1]} |f(x)|.$$

4 Analyse de Fourier

Référence : Le cours de F.Golse à l'adresse
http ://www.cmls.polytechnique.fr/perso/golse/MAT431-10/POLY431.pdf.

4.1 Séries de Fourier

On note $L^2(\mathbb{R}/Z)$ l'espace des fonctions $f : \mathbb{R} \to \mathbb{R}$ qui vérifient $f(\cdot+1) = f(\cdot)$ et qui sont L^2.
[De façon équivalente ce sont les fonctions $f : \mathbb{R}/\mathbb{Z} \to \mathbb{R}$ qui sont L^2 pour la **mesure de Haar** sur le groupe topologique $(\mathbb{R}/\mathbb{Z}, +)$.]
Si $f \in L^2(\mathbb{R}/\mathbb{Z})$ on définit pour $n \in \mathbb{Z}$

$$\hat{f}(n) = \int_0^1 f(x)e^{-2\pi inx}dx = \int_{\mathbb{R}/\mathbb{Z}} f(x)e^{-2\pi inx}dx.$$

4.1.1 Convergence L^2 (Parseval-Bessel)

- Les fonctions $(x \mapsto e^{2\pi inx})_{n\in\mathbb{Z}}$ forment un **système complet orthonormal** dans $L^2(\mathbb{R}/\mathbb{Z})$ (le produit hermitien est $\langle f, g\rangle = \int_0^1 \bar{f}(x)g(x)dx$).
- La suite de fonctions $\sum_{n=-N_1}^{N_2} \hat{f}(n)e^{2\pi inx}$ converge dans $L^2(\mathbb{R}/\mathbb{Z})$ vers f quand $\min(N_1, N_2) \to \infty$:

$$\sum_{n\in\mathbb{Z}} \hat{f}(n)e^{2\pi inx} \underset{L^2}{=} f(x).$$

- **Parseval-Bessel** : Isométrie $L^2 \longleftrightarrow l^2$:

$$\|f\|_{L^2} = \left(\int_0^1 |f(x)|^2 dx\right)^{1/2} = \sum_{n\in\mathbb{Z}} |\hat{f}(n)|^2 = \|\hat{f}\|_{l^2}.$$

- Quand on parle de séries de Fourier on fait en général allusion aux séries où la sommation est **symétrique**

$$S_N(f)(x) = \sum_{-N}^{N} \hat{f}(k)e^{2\pi ikx}.$$

(Pour le théorème de convergence en norme L^2 cela n'a pas d'importance).

4.1.2 Autour de la convergence simple

- La convergence **presque partout** (et pas seulement L^2) des séries de Fourier d'une fonction L^2 est vraie mais est un théorème difficile de **Carleson**.
- Il y a plusieurs **critère de convergence simple** des séries de Fourier. Le plus simple est le suivant : si f est 1-périodique et de classe C^1 alors pour tout x, $f(x)$ est égale à $\lim_{N\to\infty} \sum_{n=-N}^{N} \hat{f}(n)e^{2\pi inx}$.
- Critère de convergence simple **Dirichlet**. Si f est dérivable par morceaux et admet en x_0 des limites à droites et à gauche

$$S_N(f)(x) = \sum_{k=-N}^{N} \hat{f}(k)e^{2\pi ikx} \underset{N\to\infty}{\longrightarrow} \frac{1}{2}(f(x_0^+) + f(x_0^-)).$$

  [La preuve se fait par convolution avec le noyau de Dirichlet $D_n(x) = (\sin(2\pi x(N+1/2)))/(\sin(2\pi x))$.]
- Les **moyennes de Fejér**

$$\frac{1}{N}\sum_{n=1}^{N}\sum_{k=-n}^{n} e^{2\pi ikx}\hat{f}(k)$$

  convergent **uniformément** vers f si f est continue. [La preuve se fait par convolution avec le noyau de Fejér $(1/N)\sum_{n=1}^{N} D_n(x)$ *cf.* Exercice 42.]
- La **régularité** d'une fonction périodique se lit sur la vitesse de **décroissance** de ses coefficients de Fourier (faire une IPP) : si $\partial f = f'$

$$\widehat{\partial^k f}(n) = (2\pi i)^k \hat{f}(n)$$

  et en utilisant Parseval-Bessel

$$f \in C^k_{1-per} \implies |\hat{f}(n)| \leqslant \|f\|_{C^k} \times |n|^{-k}$$

4.2 Transformée de Fourier

Si $f \in L^1(\mathbb{R})$ on peut définir

$$\hat{f}(\xi) = \mathcal{F}f(\xi) = \int_{\mathbb{R}} f(x)e^{-ix\xi}dx.$$

- On pose parfois $\check{\mathcal{F}}(f)(\xi) = \mathcal{F}(f)(-\xi) = \int_{\mathbb{R}} f(x)e^{ix\xi}dx$. Formellement pour le produit hermitien $\langle f, g\rangle = \int_{\mathbb{R}} \bar{f}(x)g(x)dx$

$$\langle f, \mathcal{F}g\rangle = \langle \check{\mathcal{F}}f, g\rangle \Longrightarrow \mathcal{F}^* = \check{\mathcal{F}}.$$

- $\hat{f}(0) = \int_{\mathbb{R}} f$.
- $\hat{f}$ est continue et tend vers 0 en $\pm\infty$.
- Si f est dans la **classe de Schwartz** $\mathcal{S}$ (f est C^∞, f et ses dérivées tendent vers 0 en l'infini plus rapidement que tout polynôme) il en est de même de $\hat{f}$.

4.2.1 Inversion de Fourier

- **Inversion de Fourier** : si $f \in \mathcal{S}$

$$f(x) = \frac{1}{2\pi}\int_{\mathbb{R}} \hat{f}(\xi) e^{ix\xi} d\xi. \qquad (\mathcal{F}^{-1} = \frac{1}{2\pi}\check{\mathcal{F}} = \frac{1}{2\pi}\mathcal{F}^*).$$

- Si $f \in \mathcal{S}$

$$\|\hat{f}\|_{L^2} = (2\pi)^{1/2}\|f\|_{L^2}.$$

- Comme $\mathcal{S}$ est dense dans $L^2(\mathbb{R})$ on peut prolonger $\mathcal{F}$ à $L^2(\mathbb{R})$:**$\mathcal{F}$ est (à un facteur 2π près) une isométrie inversible de** $L^2(\mathbb{R})$:

$$\mathcal{F}^*\mathcal{F} = \mathcal{F}\mathcal{F}^* = 2\pi \times id.$$

  Attention si $f \in L^2$, la façon dont est définie $\mathcal{F}(f)$ est abstraite (obtenue par limite L^2).

4.2.2 $L^2 \cap L^1$

- **Invariance de $L^2 \cap L^1$ par Fourier.** Si $f \in L^2 \cap L^1$ alors
  - $\hat{f} \in L^2 \cap L^1$;
  - la formule d'inversion est vraie ;
  - l'identité L^2 est vraie.

  L'intérêt de cet espace est que l'on a affaire à de vraies fonctions.

4.2.3 Dualité convolution / différentiation

- **Fourier et convolution** :

$$\mathcal{F}(f * g) = \mathcal{F}(f) \times \mathcal{F}(g).$$

- **Fourier et dérivation** : IPP, dérivation sous $\int$

$$\mathcal{F}(\partial^k f)(\xi) = (i\xi)^k \mathcal{F}(f)(\xi), \qquad \partial^k(\mathcal{F}f)(x) = (-ix)^k \mathcal{F}(f)(x)$$

4.3 Fourier et distributions

4.3.1 Distributions tempérées

- **Distributions tempérées.** Ce sont les distributions qui sont dans le dual de la **classe de Schwartz**, $\mathcal{S}$. On note leur espace $\mathcal{S}'$. Comme pour les distributions, on ne peut pas multiplier deux distributions tempérées.
  - On peut en revanche **multiplier** une distribution tempérée par une fonction C^∞ dont la **croissance ainsi que celle de ses dérivées est au plus polynomiale**.
  - On peut aussi définir la **convolution** d'une distribution tempérée avec une fonction de **la classe de Schwartz** (on obtient alors une fonction C^∞).
  - On peut plus généralement définir la **convolution** d'une distribution tempérée avec **distribution à support compact**. Une distribution à support compact est une distribution qui agit sur les fonctions tests $C^\infty(\mathbb{R})$ (et pas seulement $C_c^\infty(\mathbb{R})$). Des exemples typiques sont les mesures de Dirac et leurs dérivées. On note $\mathcal{E}'$ l'espace des distributions à support compact.
- La **transformée de Fourier** est bien définie dans l'espace des **distributions tempérées** par **dualité** :

$$\langle \mathcal{F}T, \varphi \rangle = \langle T, \hat{\varphi} \rangle, \qquad T \in \mathcal{S}', \quad \varphi \in \mathcal{S}.$$

  - Cette définition **étend** la définition de la transformée de Fourier dans L^2 :

$$\mathcal{F}f \underset{\mathcal{D}'}{=} \hat{f}, \qquad \text{pour } f \in L^2.$$

  - Les formules d'inversion de Fourier, de convolution (commutativité, associativité) et de dérivation sont vraies toutes le fois où elles ont un sens.
  - La transformée de Fourier d'une distribution S à **support compact** est la fonction C^∞ **à croissance polynomiale** (ains que toutes ses dérivées)

$$C^\infty(\mathbb{R}) \ni \mathcal{F}S(\xi) = \langle S, e^{-ix\xi} \rangle.$$

  - La formule $\mathcal{F}(T * S) = \mathcal{F}T \times \mathcal{F}S$ a donc bien un sens.

4.3.2 Approximation de l'identité

Si $g \in \mathcal{S}(\mathbb{R})$, $\int_{\mathbb{R}} g = 1$, $g > 0$ on pose pour $\epsilon > 0$

$$g_\epsilon(x) = \frac{1}{\epsilon} g(x/\epsilon) \; ; \qquad \int_{\mathbb{R}} g_\epsilon = 1.$$

On a

$$\mathcal{F}(g_\epsilon)(\xi) = g(\epsilon\xi).$$

Au sens des distributions

$$g_\epsilon \xrightarrow[\epsilon\to 0]{\mathcal{D}'} \delta_0, \qquad g(\epsilon\cdot) \xrightarrow[\epsilon\to 0]{\mathcal{D}'} 1$$

donc, comme $\mathcal{F}$ est continue dans l'espace des distributions tempérées,

$$\mathcal{F}(\delta_0) = 1 \qquad (\text{donc } \mathcal{F}1 = 2\pi\delta_0).$$

- **Fourier et gaussiennes** :
  - Si $a > 0$ et $g_a(x) = e^{-ax^2/2}$ on a

$$\mathcal{F}(g_a) = \left(\frac{2\pi}{a}\right)^{1/2} g_{1/a} \qquad (\text{propriété modulaire } a \longleftrightarrow 1/a).$$

  - Si on prend

$$\chi(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2} \longrightarrow \mathcal{F}(\chi)(\xi) = \sqrt{2\pi} \times \chi(\xi) = e^{-\xi^2/2}.$$

  - La suite

$$\chi_\epsilon(x) := (1/\epsilon)\chi(x/\epsilon) = \frac{1}{\sqrt{2\pi\epsilon^2}} e^{-x^2/(2\epsilon^2)}$$

    est une approximation de l'identité :

$$\frac{1}{\sqrt{2\pi\epsilon^2}} e^{-x^2/(2\epsilon^2)} = \chi_\epsilon \xrightarrow[\epsilon\to 0]{\mathcal{D}'} \delta_0 \quad \text{et} \quad e^{-\epsilon^2\xi^2} = \mathcal{F}(\chi_\epsilon) = (2\pi)^{1/2}\chi_{1/\epsilon} \xrightarrow[\epsilon\to 0]{\mathcal{D}'} 1.$$

4.3.3 Valeur principale.

La distribution $vp(1/x)$ définie par

$$\langle vp(1/x), \varphi\rangle = \lim_{\epsilon\to 0} \int_{\mathbb{R}-[-\epsilon,\epsilon]} (\varphi(x)/x)dx$$

est tempérée et vérifie

$$xvp(1/x) = 1.$$

Voir l'exercice 45 pour le calcul de la transformée de Fourier de vp.

4.3.4 Fourier et EDP

Voir l'exercice 46.

4.4 Lien entre séries de Fourier et transformée de Fourier

– Ce lien est donné par la **formule sommatoire de Poisson.** : on a dans $\mathcal{S}'$

$$\mathcal{F}\left(\sum_{k\in\mathbb{Z}}\delta_k\right) = 2\pi\sum_{k\in\mathbb{Z}}\delta_{2k\pi}$$

– En particulier, si $\varphi\in\mathcal{S}$ on a

$$\sum_{k\in\mathbb{Z}}\hat{\varphi}(k) = 2\pi\sum_{k\in\mathbb{Z}}\varphi(2\pi k).$$

Exercice 42 Approximation de l'identité sur $\mathbb{R}/\mathbb{Z}$.
1) On définit pour $N\in\mathbb{N}^*$ le noyau de Fejér

$$\chi_N(x) = \left|\frac{1}{N^{1/2}}\sum_{n=0}^{N-1}e^{2\pi ikx}\right|^2 = \frac{1}{N}\left(\frac{\sin(2\pi(Nx/2))}{\sin(2\pi(x/2))}\right)^2$$

Démontrer que

$$\int_{\mathbb{R}/\mathbb{Z}}\chi_N(x)dx = 1$$

et

$$\forall\ \delta>0,\ \lim_{N\to\infty}\int_{(\mathbb{R}\setminus[-\delta,\delta])/\mathbb{Z}}\chi_N(x)dx = 0.$$

2) Soit $f:\mathbb{R}/\mathbb{Z}\to\mathbb{R}$ une fonction continue. On pose

$$F_N(x) = \int_{\mathbb{R}/\mathbb{Z}}f(x-y)\chi_N(y)dy = \int_{\mathbb{R}/\mathbb{Z}}f(y)\chi_N(x-y)dy$$

Démontrer que F_N est un polynôme trigonométrique de la forme

$$F_N(x) = \sum_{k=-(N-1)}^{N-1}a_k e^{2\pi ikx}.$$

3) Démontrer que F_n converge uniformément vers f quand $N\to\infty$.

Exercice 43 On admet qu'il existe une constant $C>0$ telle que pour tout $(p,q)\in\mathbb{Z}\times\mathbb{Z}^*$

$$|\sqrt{2}-\frac{p}{q}|\geqslant\frac{C}{|q|^2}.$$

Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction 1-périodique de classe C^∞ telle que $\int_0^1 f(t)dt = 0$. Démontrer que l'équation $g(\cdot + \sqrt{2}) - g(\cdot) = f(\cdot)$ admet une unique solution 1-périodique et C^∞.

Exercice 44 [Problème de Dirichlet sur le demi-plan] On note

$$g(x) = \frac{1}{\pi}\frac{1}{1+x^2}$$

et pour $y > 0$

$$g_y(x) = \frac{1}{y}g(x/y).$$

Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction continue à support compact et pour $(x, y) \in \mathbb{R}\times]0, \infty[$

$$F(x,y) = (g_y * f)(x) = \frac{1}{\pi}\int_{\mathbb{R}} \frac{yf(t)dt}{(x-t)^2+y^2} = \mathrm{Im}\frac{1}{\pi}\int_{\mathbb{R}} \frac{f(t)dt}{(x+iy-t)}.$$

1) Démontrer que pour $(x, y) \in \mathbb{R}\times]0, \infty[$

$$(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})F(x,y) = 0.$$

2) Démontrer que F admet un prolongement continu sur $\mathbb{R} \times [0, \infty[$ et que pour tout $x \in \mathbb{R}$, $F(x, 0) = f(x)$.

Exercice 45 Calculer $\mathcal{F}(vp(1/x))$.

[Comme $xvp(1/x) = 1$ on a $2\pi\delta_0 = \mathcal{F}(1) = \mathcal{F}(xvp(1/x)) = i\partial\mathcal{F}(vp(1/x))$ et donc $\mathcal{F}(vp(1/x)) = -2\pi i\mathbf{1}_{\mathbb{R}_+} + C$. Pour déterminer C on observe que $vp(1/x)$ est impaire et donc sa transformée de Fourier aussi.]

Exercice 46 On note pour $f : \mathbb{R}^2 \to \mathbb{R}$ de classe C^2, $\Delta f(x, y) = (\partial^2/\partial x^2 + \partial^2/\partial y^2)f(x, y)$.

1) Démontrer qu'il existe une distribution tempérée T telle que

$$(I - \Delta)T = \delta_0.$$

2) Démontrer que T est en fait une fonction de L^2.

3) Démontrer que si $f : \mathbb{R}^2 \to \mathbb{R}$ est C^∞ à support compact la distribution $T * f$ est en fait une fonction de classe C^∞ et vérifie

$$(I - \Delta)(T * f) = f.$$

4) Soit $f : \mathbb{R}^2 \to \mathbb{R}$ C^∞ à support compact. Démontrer que l'équation

$$-(\partial^2/\partial x^2 + \partial^2/\partial y^2)g(x,y) + g(x,y) = f(x,y)$$

admet une solution C^∞ sur $\mathbb{R}^2$.

Exercice 47 On note

$$\eta(y) = \sum_{n\in\mathbb{Z}} \exp(-\pi y n^2).$$

Montrer que

$$\eta(y) = \frac{1}{\sqrt{y}}\eta\left(\frac{1}{y}\right).$$

Solution – La formule de Poisson appliquée à g_a dont on connaît la transformée de Fourier, montre que

$$\sum_{n\in\mathbb{Z}} (2\pi/a)^{1/2} g_{1/a}(n) = \sum_{n\in\mathbb{Z}} \hat{g}_a(n) = 2\pi \sum_{n\in\mathbb{Z}} g_a(2\pi n).$$

On choisit $a = y/(2\pi)$. □

5 Analyse complexe

Référence : J. Dieudonné, Calcul infinitésimal.
W. Rudin, Analyse réelle et complexe.

5.1 Séries entières vs. Fonctions holomorphes

- Deux points de vue : Séries entières vs. Fonctions holomorphes.
- **Fonctions holomorphe** sur un ouvert $\Omega \subset \mathbb{C}$: fonction **dérivable au sens complexe** telle qu'en tout point $z \in \Omega$ càd

$$f'(z) := \lim_{h \to 0} \frac{f(z+h) - f(z)}{h} \quad \text{existe.}$$

  On note $\mathcal{O}(\Omega)$ l'ensemble des fonctions holomorphes sur Ω.
- Les opérations de dérivations classiques (somme, produit, quotient, composition) sont les mêmes que dans le cas réel.
- Si $[z_1, z_2] \subset \Omega$, $f \in \mathcal{O}(\Omega)$, on a $|f(z_1) - f(z_2)| \leqslant \sup_{[a,b]} |f'| \times |z_1 - z_2|$.
- **Exemples et contre exemples**
  - Polynômes en z, $a_0 + a_1 z + \cdots a_n z^n$.
  - **Séries entières** $\sum_{n=0}^{\infty} a_n z^n$ telles que $\sum_{n=0}^{\infty} |a_n| r^n < \infty$ pour un certain $r > 0$. Elles sont holomorphes sur le disque ouvert de rayon r centré en 0 $D(0, r)$. On appelle **rayon de convergence** le plus grand $r > 0$ possible. Si R est le rayon de convergence de la série précédente
$$1/R = \limsup |a_n|^{1/n}.$$
  - La fonction $z \mapsto \bar{z}$, n'est **pas** dérivable au sens complexe.
  - Une application de la forme $f : z = x + iy \mapsto \sum_{(m,n) \in \mathbb{N}^2} a_{m,n} x^m y^n$ avec $\sum_{(m,n) \in \mathbb{N}^2} |a_{m,n}| r^{n+m} < \infty$ définit une fonction dérivable au sens **réel** (et même C^∞, réelle analytique) en tout point $z = x + iy$, $\max(|x|, |y|) < r$ mais pas au sens complexe. Par exemple $z\bar{z} = x^2 + y^2$ n'est pas dérivable au sens complexe.
- **Formule de Cauchy-Riemann.** On peut lire l'holomorphie de f sur sa forme réelle. Soit $f : \Omega \ni x + iy \to f(x + iy) = P(x, y) + iQ(x, y)$. La fonction f est holomorphe sur Ω si et seulement si en tout point (x, y), $x + iy \in \Omega$ la matrice jacobienne

$$\begin{pmatrix} (\partial P/\partial x)(x,y) & (\partial P/\partial y)(x,y) \\ (\partial Q/\partial x)(x,y) & (\partial Q/\partial y)(x,y) \end{pmatrix}$$

  est une **matrice de similitude** càd

$$(\partial P/\partial x)(x,y) = (\partial Q/\partial y)(x,y), \qquad (\partial P/\partial y)(x,y) = -(\partial Q/\partial x)(x,y).$$

Si on introduit les opérateurs différentiels

$$\bar{\partial} = (1/2)(\partial_x + i\partial_y) = \partial/\partial\bar{z}, \qquad \partial = (1/2)(\partial_x - i\partial_y) = \partial/\partial z$$

il est équivalent d'écrire

$$\bar{\partial} f = (\partial f/\partial\bar{z}) = \bar{\partial}(P + iQ) = 0.$$

Quand f est dérivable au sens complexe

$$\partial f/\partial z = f'(z).$$

Remarque : Une fonction $g(x, y)$ peut s'écrire sous la forme $h(z, \bar{z})$ si on fait le changement de variables $x = (z + \bar{z})/2$, $y = (z - \bar{z})/(2i)$. Dire qu'elle est holomorphe, c'est s'assurer du fait qu'il n'y a pas de dépendance en $\bar{z}$ dans h.

– **Holomorphie sous $\int$.** Soient μ une mesure sur un espace X et $f : \Omega \times X \to \mathbb{C}$, $(z, x) \mapsto f(z, x)$, holomorphe en z pour μ-pp x et L^1 en x pour tout $z \in \Omega$. Si une hypothèse de domination $|(\partial/\partial z)f(z, x)| \leqslant g(x)$, $g \in L^1(X, \mu)$ est satisfaite, la fonction (qui est bien définie)

$$z \mapsto \int_X f(z, x)d\mu(x)$$

est holomorphe sur Ω et

$$(\partial/\partial z)\int_X f(z, x)d\mu(x) = \int_X (\partial/\partial z)f(z, x)d\mu(x).$$

– **Lien avec les fonctions harmoniques.** Si $f = P+iQ$ est holomorphe sur Ω on a (avec $\Delta = \partial^2/\partial x^2 + \partial^2/\partial y^2$, le Laplacien)

$$\Delta P = \Delta Q = 0.$$

Réciproquement, si P est harmonique ($\Delta P = 0$ avec P de classe C^2 par exemple) sur un ouvert simplement connexe alors il existe Q harmonique sur Ω telle que $f(x + iy) = P(x, y) + iQ(x, y)$ est holomorphe. On dit que Q est la fonction harmonique conjuguée de P.

5.2 La formule de Cauchy

– **Intégrale le long d'un chemin.** Soit γ un **chemin** de Ω càd $\gamma : [0, 1] \to \mathbb{C}$ de classe C^1. Si $f \in \mathcal{O}(\Omega)$ on définit

$$\int_\gamma f(z)dz = \int_0^1 f(\gamma(t))\gamma'(t)dt.$$

On dit que le chemin est **fermé** (ou que γ est un lacet) si $\gamma(0) = \gamma(1)$.

– On dit que deux chemins $\gamma_0, \gamma_A : [0,1] \to \Omega$ sont **homotopes** s'il existe $\Gamma : [0,1] \times [0,1] \to \Omega$, $(t,s) \mapsto \Gamma(t,s)$ qui est continue en (t,s) et C^1 en t telle que
$$\Gamma(\cdot, 0) = \gamma_0(\cdot) \quad \text{et} \quad \Gamma(\cdot, 1) = \gamma_1(\cdot).$$
– **Formule d'homotopie.** Fondamental. Si $f \in \mathcal{O}(\Omega)$, et $\gamma_0, \gamma_1 : [0,1] \to \Omega$ sont deux chemins fermés **homotopes** on a
$$\int_{\gamma_0} f(z)dz = \int_{\gamma_1} f(z)dz.$$
En particulier si γ est un chemin fermé **homotope à un point** dans Ω on a
$$\int_{\gamma} f(z)dz = 0.$$
– On dit que Ω est **simplement connexe** si tout chemin fermé est homotope à un point.
Exemple :
  – $\mathbb{C}$ est simplement connexe ; plus généralement un convexe est simplement connexe.
  – Un connexe n'est pas nécessairement simplement connexe : penser à un anneau.
  – $\mathbb{C}$ privé d'une demi-droite fermée est un ouvert simplement connexe.
– Si Ω est simplement connexe et $f \in \mathcal{O}(\Omega)$ alors f admet une **primitive** F càd $F \in \mathcal{O}(\Omega)$ telle que
$$F'(z) = f(z).$$
– En particulier, on peut définir un **logarithme** (càd une fonction f telle que $\exp \circ f = id$), défini à une constante près, sur tout ouvert simplement connexe ne contenant pas 0, par exemple $\Delta_\alpha := \mathbb{C}\backslash\{re^{i\alpha},\ r \in [0,\infty[\}$. Il suffit de prendre une primitive de $1/z$. On fixe en général la constante de façon que le logarithme s'annule en 1 si $1 \in \Delta_\alpha$ (p.ex. si $\alpha = -\pi$) ou vaille $i\pi$ en -1 si $-1 \in \Delta_\alpha$ (p.ex. $\alpha = 0$) de façon que la formule suivante ait lieu ($\epsilon = 0$ si $\alpha \in [-\pi, 0]$, $\epsilon = 1 =]0, \pi[$) :
$$\log_\alpha(re^{i\theta}) = \log r + i\theta, \qquad \text{si } r \in \mathbb{R}_+^*,\ \theta \in]\alpha - \epsilon\pi, \alpha + 2\pi - \epsilon\pi[$$
De la même manière, sur tout ouvert simplement connexe, on peut définir z^s sur Δ_α par $\exp(s \log_\alpha z)$.
– **Indice d'un point par rapport à un lacet.** Si $\gamma : [0,1] \to \mathbb{C}$ est un lacet on définit pour $z_0 \in \Omega\backslash\gamma([0,1])$
$$\mathrm{Ind}(z_0; \gamma) = \frac{1}{2\pi i} \int_\gamma \frac{1}{z - z_0} dz.$$

On a toujours

$$\mathrm{Ind}(z_0;\gamma) \in \mathbb{Z} \quad \text{et} \quad \Omega\backslash\gamma([0,1]) \ni z_0 \mapsto \mathrm{Ind}(z_0;\gamma) \text{ est continue.}$$

Remarque : Si γ est le cercle $C_{z_0,r} : [0,1] \to \mathbb{C}$, $t \mapsto z_* + re^{2\pi it}$ (le cercle de centre z_* et de rayon r parcouru une seule fois dans le sens trigonométrique direct) on a $(C_{z_*,r}(t) - z_*)^{-1} = r^{-1}e^{-2\pi it}$, $C'_{z_*,r}(t) = 2\pi ire^{2\pi it}$ et donc

$$\mathrm{Ind}(z_*; C_{z_*,r}) = 1.$$

De façon plus générale

$$\begin{cases} \mathrm{Ind}(z_0; C_{z_*,r}) = 1 \iff z_0 \in D(z_*, r) \\ \mathrm{Ind}(z_0; C_{z_*,r}) = 0 \iff z_0 \in \mathbb{C}\backslash\overline{D(z_*, r)}. \end{cases}$$

Si γ est un lacet dans $\mathbb{C}$ son complémentaire $\mathbb{C}\backslash\gamma([0,1])$ est un ouvert qui a un nombre au plus dénombrable de composantes connexes. Cet ouvert a une seule composante connexe non bornée (et l'indice de tout point dans cette cc par rapport à γ est nul).

– **Formule de Cauchy.** Si $f \in \mathcal{O}(\Omega)$ et γ est un chemin fermé de Ω on a pour tout $z \in \Omega\backslash\gamma([0,1])$

$$f(z) = \frac{\mathrm{Ind(z;\gamma)}}{2\pi i} \int_\gamma \frac{f(w)}{z-w} dw.$$

– **Conséquences de la formule de Cauchy.**
  – **Contrôle des dérivées.** En particulier

$$(1/k!)\partial^k f(z) = \frac{\mathrm{Ind(z;\gamma)}}{2\pi i} \int_\gamma \frac{f(w)}{(z-w)^{k+1}} dw \qquad (1)$$

  ce qui implique que pour tout compact $K \subset \Omega$ et tout $k \in \mathbb{N}^*$ il existe une constante $C_{K,k}$ telle que

$$\sup_K |f^{(k)}| \leqslant C_{K,k} \sup_\Omega |f|.$$

  – **Presque compacité de $\mathcal{O}(\Omega)$.** Soit $K \subset \Omega$ un compact non vide, $C > 0$ et $H_{K,C} \subset \mathcal{O}(\Omega)$ un ensemble de fonctions holomorphes telle que

$$f \in H_{K,C} \implies \sup_K |f| \leqslant C.$$

  Alors, pour tout ouvert $U \subset K$ et toute suite $(f_n)_n$, $f_n \in H_{K,C}$ on peut extraire une sous-suite qui **converge uniformément** sur U vers une fonction holomorphe $f \in \mathcal{O}(U)$.
  Par ailleurs, une suite de fonctions holomorphes qui converge uniformément sur un ouvert converge vers une fonction holomorphe.

– **Holomorphe $\Longrightarrow$ DSE**. Pour tout $z_0 \in \Omega$, $r > 0$ tels que $D(z_0, r) \subset \Omega$ on a la formule de Taylor

$$\forall\ z \in D(z_0, r), \quad f(z) = \sum_{k=0}^{\infty} \frac{f^{(k)}(z_0)}{k!}(z - z_0)^k.$$

– **Principe des zéros isolés.** Une fonction holomorphe sur un ouvert **connexe** Ω qui est nulle sur un sous-ensemble de Ω qui possède un point d'accumulation est nulle sur Ω tout entier.

Application : **Recollement des applications holomorphes :** si U_1 et U_2 sont deux ouverts de $\mathbf{C}$ et $f_1 : U_1 \to \mathbb{C}$, $f_2 : U_2 \to \mathbb{C}$ sont deux fonctions holomorphes qui coïncident sur $U_1 \cap U_2$ alors il existe une fonction f holomorphe sur $U_1 \cup U_2$ qui prolonge f_1 et f_2.

– **Principe du maximum.** Soit $f \in \mathcal{O}(\Omega)$, Ω ouvert connexe. Alors,

$$\exists\ z_0 \in \Omega,\ |f(z_0)| = \sup_{\Omega} |f| \implies f \equiv f(z_0).$$

– **Théorème de Liouville.** Une fonction entière ($f \in \mathcal{O}(\mathbb{C})$) bornée sur $\mathbb{C}$ tout entier est constante. [Appliquer (1) avec $k = 1$ sur un cercle centré en z de rayon tendant vers l'infini.]

5.3 Singularités et fonctions méromorphes

– **Singularités.** Soit $f \in \mathcal{O}(\Omega \backslash \{z_0\})$. On a trois possibilités : (1), (2.a) ou (2.b).
  – (1) **(Riemann)** Si $\sup_{\Omega\backslash\{z_0\}} |f| < \infty$ alors il existe $\hat{f} \in \mathcal{O}(\Omega)$ telle qui étend f (pour tout $z \in \Omega\backslash\{z_0\}$, $\hat{f}(z) = f(z)$).
  – (2) **(Weierstrass)** Si $\sup_{\Omega\backslash\{z_0\}} |f| = \infty$ (on dit que z_0 est une **singularité** de f) alors
    – (2.a) **(Singularité essentielle)** soit pour tout $\epsilon > 0$ suffisamment petit $f(D(z_0, \epsilon))$ est **dense** dans $\mathbb{C}$;
    – (2.b) **(Pôle)** Soit z_0 est un pôle de f càd il existe $g \in \mathcal{O}(\Omega)$ et $N \in \mathbb{N}^*$ tels que

$$\forall\ z \in \Omega\backslash\{z_0\},\ f(z) = \frac{g(z)}{(z - z_0)^N}, \qquad g(z_0) \neq 0.$$

    (N est **l'ordre** du pôle.)

– **Séries de Laurent.** Si $z_0 \in \Omega$ est une singularité de f il existe un anneau $A(z_0; r, R) = \{r < |z - z_0| < R\}$ et des nombres complexes $(a_n)_{n\in\mathbb{Z}}$ tels que la série suivante converge absolument

$$\forall\ z \in A(z_0; r, R) \quad f(z) = \sum_{n=-\infty}^{\infty} a_n (z - z_0)^n.$$

Le point z_0 est un pôle d'ordre N de f si et seulement si il existe $N \in \mathbb{N}^*$ tel que pour tout $n \leqslant -(N+1)$, $a_n = 0$.

- **Fonctions méromorphes.** Une fonction f est méromorphe sur Ω si elle est holomorphe sur Ω privé d'un nombre fini de points et ces points sont des pôles de f.
- **La formule des résidus.**
  - Si z_0 est un pôle de f d'ordre 1 on appelle résidu de f en z_0, le nombre $a \in \mathbb{C}$ pour lequel $f(z) - a/(z - z_0)$ se prolonge en une fonction holomorphe au voisinage de z_0. Si z_0 n'est pas singulier ou est un pôle d'ordre $\geqslant 2$ le résidu de f en z_0 est par définition nul. On note $\mathrm{Res}(f, z_0)$ le résidu.
  - On a la formule des résidus. Soit Ω un ouvert simplement connexe. Si $S \subset \Omega$ est un ensemble fini et f est une fonction méromorphe sur Ω avec des pôles aux points de S, on a pour tout cheminγ tel que $\gamma([0,1]) \subset \Omega \backslash S$

$$\int_\gamma f(z)dz = 2\pi i \sum_{s \in S} \mathrm{Res}(f, s)\mathrm{Ind}(s; \gamma).$$

5.4 Culture générale

- Les théorèmes de Picard.
  - **(Petit théorème de Picard)** Si f est entière ($f \in \mathcal{O}(\mathbb{C})$),

$$\mathrm{card}(\mathbb{C} \backslash f(\mathbb{C})) \leqslant 1.$$

  - **(Grand théorème de Picard)** Si z_0 est une singularité essentielle de f,

$$\forall\ \epsilon > 0,\ \mathrm{card}(\mathbb{C} \backslash f(D(z_0, \epsilon))) \leqslant 1.$$

- **Le théorème d'uniformisation.** Un ouvert simplement connexe de $\mathbb{C}$ peut-être envoyé par un homéomorphisme qui est holomorphe ainsi que son inverse pour la composition, sur le disque unité ouvert.

Exercice 48 En utilisant la formule des résidus, calculer

$$\int_{-\infty}^{\infty} \frac{dx}{1 + x^4}.$$

Exercice 49 Soit $f \in \mathcal{O}(\Omega)$ telle que $|f| =$ constante. Démontrer que $f =$ constante.

Exercice 50 On note $\mathbb{H}$ le demi-plan supérieur $\mathbb{H} = \{x + iy,\ x \in \mathbb{R},\ y > 0\}$ et on introduit la fonction

$$z \in \mathbb{H}, \qquad \theta(z) = \sum_{n \in \mathbb{Z}} \exp(\pi i z n^2).$$

1) Montrer que si $z \in \mathbb{H}$, alors $z + 2$ et $-1/z$ sont dans $\mathbb{H}$. Montrer que θ est bien définie sur $\mathbb{H}$ et y est holomorphe.

2) Expliquer pourquoi on peut définir une fonction holomorphe $r(z) = z^{1/2}$ sur $\mathbb{H}$ qui vérifie $r(z)^2 = z$ et $\lim_{y \to 0} r(x + iy) = x^{1/2}$ quand $x > 0$.

3) Démontrer que $\theta(z + 2) = \theta(z)$.

4) Démontrer que pour $z = iy$, $y > 0$

$$\theta(z) = (i/z)^{1/2} \theta(-1/z).$$

[On pourra utiliser la formule de Poisson, cf. exercice 47.]

5) Démontrer que la formule précédente est vraie pour tout $z \in \mathbb{H}$.

Exercice 51 1) Montrer que la suite de polynôme

$$S_N(z) = z \prod_{n=1}^{N} (1 - \frac{z^2}{\pi^2 n^2})$$

converge uniformément sur tout compact de $\mathbb{C}$ et que sa limite est une fonction entière que l'on notera $S(z)$.

2) Démontrer que l'ensemble des zéros de $S(z)$ est $\pi\mathbb{Z}$.

3) Démontrer que la fonction méromorphe $\frac{\sin z}{S(z)}$ est en fait holomorphe.

4) Etablir l'égalité

$$\forall\ z \in \mathbb{C},\ \sin z = z \prod_{n=1}^{\infty} (1 - \frac{z^2}{\pi^2 n^2}).$$

5) En déduire que

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Exercice 52 Regarder quelques exercices sur la méthode de la phase stationnaire et la méthode du col dans Dieudonné.

6 Calcul différentiel

6.1 Application linéaire tangente

- **Notion d'application linéaire tangente (ou dérivée).** Si E et F sont deux espaces de Banach et U est un ouvert de E on dit que $f : U \to F$ est dérivable en $x \in U$ s'il existe une application **linéaire continue** $Df(x) : E \to F$ (qui est alors nécessairement unique) telle que
$$f(x+h) = f(x) + Df(x) \cdot h + o(h).$$
On dit que $Df(x)$ est l'application linéaire tangente ou la dérivée de f en x.
- Quand $E = \mathbb{R}^n$ et $F = \mathbb{R}^m$, $Df(x)$ s'identifie à une matrice dans $M_{m,n}(\mathbb{R})$ la **matrice jacobienne** $Df(x) = (\partial f_i/\partial x_j)_{i,j}$.
- On a $D(g \circ f)(x) = Dg(f(x)) \circ Df(x)$.
- **Inégalité des accroissements finis** Si f est dérivable sur un ouvert convexe on a pour tous $a, b \in U$
$$\|f(b) - f(a)\| \leqslant \sup_{x \in U} \|Df(x)\| \times \|b - a\|.$$

6.2 Applications C^p

- On dit que f est C^1 sur U si elle est dérivable en tout point de U et $U \ni x \mapsto Df(x) \in L_c(E, F)$ est continue.
- Si cette dernière application est elle-même dérivable on a
$$Df(x+h) = Df(x) + D^2 f(x) \cdot h + o(h)$$
où $D^2 f(x) \cdot h : k \mapsto (D^2 f(x) \cdot h) \cdot k$ définit une forme **bilinéaire continue** $E \times E \to F$. Cette dernière est toujours **symétrique** (théorème de Schwarz).
- On peut définir plus généralement
$$D^p f(x) : E^p \ni (h_1, \ldots, h_p) \to D^p f(x)(h_1, \ldots, h_p) \in F$$
qui est une application p-linéaire symétrique.

6.3 Formules de Taylor

Elles prennent la forme

– **Taylor-Young.**

$$f(x+h) = f(x) + Df(x)\cdot h + \cdots \frac{1}{n!} D^n f(x)\cdot(h,\cdots,h) + o(\|h\|^n)$$

– **Taylor-Reste intégral** : Si f est C^n sur $[a,b]$

$$f(x+h) = f(x) + Df(x)h + \cdots + \frac{1}{(n-1)!} D^{n-1} f(x)\cdot(h,\ldots,h) + \int_0^1 \frac{(1-t)^{n-1}}{(n-1)!} D^n f(x+th)\cdot(h,\ldots,h)dt.$$

6.4 Inversion locale et fonctions implicites.

6.4.1 Rappels : théorème du point fixe de Picard.

– Soit (X,d) un espace métrique **complet** et $f : X \to X$ une application **κ-contractante** : càd pour $0 \leqslant \kappa < 1$ on a

$$\forall\ x,y \in X, \quad d(f(x),f(y)) \leqslant \kappa d(x,y).$$

Alors, f admet un **unique point fixe** : il existe $x_* \in X$ tel que $f(x_*) = x_*$. Par ailleurs, pour tout $x \in X$ la suite x_n définie par $x_0 = x$, $x_{n+1} = f(x_n)$ converge vers x_*.

– Si f dépend *continûment* (resp. Lipschitz, resp C^k) d'un **paramètre** $\lambda \in \Lambda$ dans un espace topologique (resp. métrique, resp. un ouvert d'un Banach) le point fixe $x_* = x_\lambda$ dépend de façon continue (resp. Lipschitz, resp. C^k) pourvu que f_λ soit **uniformément contractante** en λ.

6.4.2 Inversion locale.

– Soit $f : U \to F$ de classe C^1 et $x \in U$. On suppose que $Df(x) \in L_c(E,F)$ est inversible.
– Par un théorème de Banach son inverse est automatiquement continu.
– **Inversion locale** : Il existe alors des ouverts V, W, $x \in V \subset U$, $f(x) \in W \subset F$ telle que f soit un diiféomorphisme de V sur $f(V) = W$.

6.4.3 Fonctions implicites.

– Soient E, F, G trois espaces de Banach et $f : U \times V \to W$ une application de classe C^1. On suppose que

$$D_y f(x_0,y_0) : F \to G \quad \text{est inversible.}$$

– Alors, il existe des ouverts $\tilde{U}$, $x_0 \in \tilde{U} \subset U$ et $\tilde{V}$, $y_0 \in \tilde{V} \subset V$ et une fonction de classe C^1, $\eta : \tilde{U} \to \tilde{V}$ telle que $\eta(x_0) = y_0$ et

$$\forall\ (x, y) \in \tilde{U} \times \tilde{V} \quad f(x, y) = f(x_0, y_0) \iff y = \eta(x).$$

Si f est C^k, $k \geqslant 1$, on peut remplacer C^1 par C^k dans les énoncés précédents.

6.5 Problème d'extremum

– Supposons que $f : \mathbb{R}^n \to \mathbb{R}$ de classe C^2 admette un point critique $x_0 : Df(x_0) = 0$. Alors, si $D^2 f(x_0)$ est une forme bilinéaire symétrique **définie positive** (resp. définie négative) alors x_0 est un **minimum** (resp. maximum) local de f.
– Si en plus f est **convexe** ce minimum est **global**.
– **Extrema liés.** Soit en plus $g : \mathbb{R}^n \to \mathbb{R}^p$ une fonction C^1 (une contrainte) telle que $Dg(x_0) : \mathbb{R}^n \to \mathbb{R}^p$ soit de rang p. Si x_0 est une solution du problème

$$\min\{f(x),\ g(x) = 0\} = f(x_0)$$

alors il existe $\lambda \in \mathbb{R}^p$ tel que

$$Df(x_0) + \langle \lambda, Dg(x_0) \rangle = 0.$$

En d'autres termes pour trouver x_0 il suffit de chercher un extremum x_λ de $f + \langle \lambda, g \rangle$ pour un certain $\lambda \in \mathbb{R}^p$ tel que $g(x_\lambda) = 0$.

Exercice 53 Lemme de Morse.

7 Equations différentielles

7.1 Problème de Cauchy

- **Problème de Cauchy.** Soient U un ouvert d'un espace de Banach, I un intervalle ouvert de $\mathbb{R}$, $f : I \times U \to E$, $t_0 \in I$ et $x_0 \in U$. On considère le **problème de Cauchy**

$$(C(t_0, x_0)) \quad \begin{cases} x'(t) = f(t, x(t)) \\ x(0) = x_0. \end{cases}$$

- **Formulation intégrale.** Il est équivalent de résoudre

$$x(t) = x_0 + \int_{t_0}^{t} f(s, x(s))ds.$$

7.2 Cauchy-Lipschitz

- **Théorème de Cauchy-Lipschitz :** Existence et Unicité locales.
  Si f est continue et **uniformément localement Lipschitz** en x alors il existe $\delta > 0$ et $x :]t_0 - \delta, t_0 + \delta[\to E$ de classe C^1 solution du problème de Cauchy $C(t_0, x_0)$.
  La preuve repose sur le **théorème du point fixe de Picard** appliqué à la formulation intégrale du problème de Cauchy.
- **Solution maximale.** Le théorème de Cauchy-Lipschitz est un résultat d'existence en temps **local**. On peut définir une notion de solution **maximale :** une solution $x : J \to E$ de $C(t_0, x_0)$ est maximale s'il n'existe pas $\tilde{x} : \tilde{J} \to E$ solution de $C(t_0, x_0)$ telle que $\tilde{x}$ restreinte à J égale x. Une solution maximale existe toujours.
- L'existence dans le théorème de C-L reste vrai (au moins en dimension finie) si f est seulement continue : c'est le **théorème de Péano** mais l'unicité est perdue.
- On peut souvent obtenir l'existence en **temps long** en utilisant le **Théorème de sortie de tout compact :** Soit $x : J \to E$ une solution maximale de $C(t_0, x_0)$. Supposons que J soit de la forme (a, b). Alors, pour tout **compact** $K \subset I \times U$ il existe $t_n \to b$ telle que $f(t_n, x(t_n)) \notin K$.
- **Lemme de Gronwall.** Soit $x : J \to E$ solution de $C(t_0, x_0)$ pour f. Supposons que

$$\|f(t, x)\| \leqslant Ax + B.$$

Alors, x est définie sur I **tout entier** et

$$\|x(t)\| \leqslant e^{(t-t_0)A}\|x(t_0)\| + \int_{t_0}^{t} e^{(t-s)A}Bdt.$$

7.3 Linéarisation

- **Dépendance par rapport à un paramètre et aux conditions intiales.**
  Supposons que $(t,x) \mapsto f_\lambda(t,x)$ dépende C^k d'un paramètre $\lambda \in F$ (F Banach) et que pour $\lambda = \lambda^*$, $x_0 : [a,b] \to E$ ($[a,b] \subset I$) soit une solution de $C(t_0, x^*)$ pour $f_{\lambda *}$. Alors, il existe un voisinage L de λ^* et un voisinage V de x^* tel que pour tout $(\lambda^*+\Delta\lambda^*, x^*+\Delta x^*) \in L\times V$ il existe $x_{\Delta\lambda^*,\Delta x^*} : [a,b] \to E$ solution de $C(t_0, x^* + \Delta x^*)$ pour $f_{\lambda^*+\Delta\lambda^*}$. L'application $(\Delta\lambda^*, \Delta x^*) \mapsto x_{\Delta\lambda^*,\Delta x^*}(\cdot)$ est C^k et son application linéaire tangente en 0 est l'application linéaire qui à $(\Delta\lambda^*, \Delta x^*)$ associe la solution de l'EDO **linéaire** (ou plutôt affine)

$$\begin{cases} (\Delta x)'(t) = D_x f(\lambda^*, t, x_0(t)) \cdot \Delta x(t) + D_\lambda f(\lambda^*, t, x_0(t)) \cdot \Delta\lambda^* \\ \Delta x(t_0) = \Delta x^*. \end{cases}$$

- L'équation précédente s'appelle **l'équation linéarisée**.

7.4 EDO linéaires et affines

- **EDO linéaire** $X'(t) = A(t)X(t)$, $\quad A : I \to M(n,\mathbb{R})$. Solutions définies sur I tout entier.
  - **Résolvante.** C'est la famille des $R_A(t,s) \in GL(n,\mathbb{R})$, $t,s \in \mathbb{R}$ telle que
    $$X(t) = R_A(t,s)X(s)$$
    toutes les fois que $X(\cdot)$ est solution se $X'(t) = A(t)X(t)$.
  - **Chasles.** $R_A(t_2,t_0) = R_A(t_2,t_1)R_A(t_1,t_0)$.
  - R_A est solution de l'EDO dans $M(n,\mathbb{R})$
    $$\begin{cases} R'_A(t) = A(t)R_A(t) \qquad \text{(la multiplication est dans ce sens)} \\ R(0) = Id \end{cases}$$
  - $A(\cdot) \mapsto R_A(\cdot,\cdot)$ est C^k pour tout k.
  - Si $A(\cdot)$ est constante
    $$R_A(t,s) = e^{(t-s)A}.$$
    Le calcul se fait en utilisant la **forme normale de Jordan**.

– **Attention.** En dehors du cas $n = 1$ ou du cas constant, on ne sait pratiquement **jamais calculer** la résolvante. On peut en revanche souvent en calculer des expressions approchées.

– **EDO affines.** $X'(t) = A(t)X(t) + b(t)$, $A : I \to M(n, \mathbb{R})$, $b : I \to \mathbb{R}^n$. Solutions définies sur I tout entier. Si R_A est la résolvante de $X'(t) = A(t)X(t)$ on a la **formule de variation de la constante** (formule de Duhamel)

$$X(t) = R_A(t, 0)X(0) + \int_0^t R_A(t, s)b(s)ds.$$

7.5 Flots

– **Flots.** On peut définir l'analogue non-linéaire de la résolvante :

$$x(t) = \phi^{t,s}(x(s)), \qquad (\phi^{t_2,t_0} = \phi^{t_2,t_1} \circ \phi^{t_1,t_0})$$

toutes les fois où x est solution de $x'(t) = f(t, x(t))$. Pour t, s fixés, $x \mapsto \phi^{t,s}(x)$ est un **difféomorphisme local**. Quand f ne dépend pas de t on a $\phi^{t,s} = \phi^{t-s,0}$; on note alors $\phi^{t,0} = \phi^t$. C'est le **flot** au temps t du **champ de vecteurs** $x \mapsto f(x)$.

Exercice 54 Quelle est la forme générale de la solution d'une EDO linéaire à coefficients constants

$$y^{(n)}(t) + a_1 y^{(n-1)}(t) + \cdots + a_n y(t) = 0?$$

Exercice 55 On considère une EDO linéaire à coefficients 1-périodiques

$$X'(t) = A(t)X(t), \qquad A : \mathbb{R} \to M(n, \mathbb{R}), \quad A(\cdot + 1) = A(\cdot).$$

1) Les solutions de cette EDO sont elles périodiques en général ?

2) Montrer que si X est solution d'une telle EDO et $X(0) = X(1)$ alors X est 1-périodique.

3) Démontrer que si R_A est la résolvante, pour tous $t, s \in \mathbb{R}$

$$R_A(t + 1, s + 1) = R_A(t, s).$$

4) Démontrer que pour tout t le déterminant $\det R(t + 1, t)$ est indépendant de t.

8 Groupes

Référence :
- Le livre de D. Perrin.
- Le livre de P. Colmez
  https ://webusers.imj-prg.fr/ pierre.colmez/livre.pdf

8.1 Concepts et constructions générales

- Définition, sous-groupes, morphismes, conjugaison, adjoint, commutateur, groupe dérivé, centre d'un groupe, groupe cyclique, ordre d'un élément...

8.1.1 Théorème de Lagrange

- Opérations fondamentales : **quotient, produit** et leurs variantes.
- Si H est un sous groupe de G on peut construire $G/H = \{gH, g \in G\}$ ou $H\backslash G = \{Hg, g \in G\}$ **l'ensemble des classes** à droite ou à gauche. Ce ne sont que des ensembles. Intérêt : les ensembles gH (ou Hg), $g \in G$ forment une **partition** de g.
- En tant qu'ensembles : G et $H \times G/H$ sont en bijection.
- On en déduit le **théorème de Lagrange** : $|H|$ divise $|G|$ (card G = card H × card(G/H)).
- Application : l'**ordre** d'un élément divise le cardinal du groupe et donc $g^{|G|} = e$. En particulier, si p premier $a^{p-1} \equiv 1 \mod p$ (Fermat). [Le cardinal de $(\mathbb{Z}/p\mathbb{Z})^*$ vaut $p - 1$.]
- L'application $\pi : G \to G/H$, $g \mapsto gH$ est surjective.

8.1.2 Sous-groupes distingués

- Il y a un cas important où l'ensemble G/H peut-être **muni d'une structure de groupe**, c'est quand H **est distingué dans** G (on dit aussi **normal** et on note $H \lhd G$) càd $\forall\ g \in G$, $gH = Hg$ (ou encore $gHg^{-1} = H$). Dans ce cas on peut écrire $(g_1H)(g_2H) = (g_1g_2)H$ qui définit une loi de groupe sur G/H.
- **Morphismes de groupes.** Si G_1, G_2 sont deux groupes et $f : G_1 \to G_2$, l'image $f(G_1)$ est un sous-groupe de G_2 et le noyau $\ker f$ est un sous-groupe *distingué* de G_1 (si $h \in \ker f$, $f(ghg^{-1}) = f(g)e_2f(g)^{-1} = e_2$ dont $ghg^{-1} \in \ker f$). On a le **passage au quotient**

$$\text{Im } f \simeq G_1/\ker f.$$

– Quand $H \lhd G$, l'application $\pi : G \to G/H$ est un morphisme surjectif de groupe et $\ker \pi = H$. On dit que G/H est un **facteur** de G.

8.1.3 Suites exactes

– **Suites exactes.** Soient G, H, K des groupes et $i : H \to G$, $p : G \to K$ des morphismes de groupes tels que la suite suivante soit **exacte**

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{p} K \longrightarrow 1 \tag{2}$$

càd i injectif, p surjectif et $\ker p = \text{Im } i$.
  – On dit que K est un **facteur** de G et que G est une **extension** de H par K.
  – On dit que la suite exacte est **scindée** s'il existe un morphisme $s : K \to G$, appelé **section**, tel que $p \circ s = id_K$.
  – Si $H \lhd G$ on a la suite exacte (2) avec $K = G/H$.

8.2 Produits semi-directs

– Soient H, K des groupes et

$$\rho : K \to (Aut(H), \circ)$$

un morphisme de groupes. On définit le **produit semi-direct** $H \rtimes_\rho K$ de la façon suivante : c'est le produit $H \times K$ muni de la loi de composition

$$(h, k) *_\rho (h', k') = (h\ \rho(k) \cdot h', kk').$$

$H \rtimes_\rho K$ est isomorphe à $H \times K$ si et seulement si pour tout $k \in K$, $\rho(k) = id_H$.
– Quand la suite exacte (2) est **scindée** :
  – Il existe un morphisme de groupe $\rho : K \to (Aut(H), \circ)$ tel que G est isomorphe au **produit semi-direct** $H \rtimes_\rho K$
  – On a la suite exacte

$$1 \longrightarrow H \xrightarrow{i} H \rtimes_\rho K \xrightarrow{p} K \longrightarrow 1$$

avec $i(h) = (h, e_K)$, $p(h, k) = k$.

8.2.1 Une illustration "affine".

– On modélise un système (disons un solide) par la donnée d'un point $b \in \mathbb{R}^n$ (son centre de gravité) et un repère vectoriel B qui lui est attaché,

càd un n-uplet de vecteurs de $\mathbb{R}^n$ (qu'on peut supposer orthonormal). Pour déplacer le système, on peut agir par une application linéaire $A \in GL(n,\mathbb{R})$ qui fixe 0 (par exemple une rotation dans $SO(n,\mathbb{R})$) puis déplacer le système par une translation $a \in \mathbb{R}^n$.

– Après ces opérations

$$\mathbb{R}^n \times GL(n,\mathbb{R}) \ni (b,B) \mapsto (a+Ab, AB) \in \mathbb{R}^n \times GL(n,\mathbb{R}).$$

– La loi de composition

$$(a,A) * (b,B) = (a+Ab, AB)$$

sur $\mathbb{R}^n \times GL(n,\mathbb{R})$ définit une structure de groupe qui fait de $\mathbb{R}^n \times GL(n,\mathbb{R})$ un produit semi-direct $\mathbb{R}^n \rtimes_\rho GL(n,\mathbb{R})$ où $\rho : GL(n,\mathbb{R}) \to Aut(\mathbb{R}^n) \simeq GL(n,\mathbb{R})$ est l'identité (mais n'est pas triviale).

– De façon plus générale on aurait pu considérer

$$(a,A) * (b,B) = (a+\rho(A)b, AB)$$

où $\rho : GL(n,\mathbb{R}) \to GL(n,\mathbb{R})$ est un morphisme de groupe.

8.2.2 Point de vue "espaces fibrés" ($H \lhd G$).

– Si H est distingué dans G, on a la suite exacte

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{p} G/H \longrightarrow 1$$

(i est l'inclusion de H dans G). On peut alors se représenter G comme étant un **"espace fibré"** au dessus d'une "base" G/H (dans notre cas un groupe car $H \lhd G$) dont les "fibres" sont toutes "isomorphes" au groupe H.

– Pour **"recoller"** (identifier) ces fibres entre-elles on peut procéder de la façon suivante. *Choisissons* un système de représentants de G/H, $(g_\alpha)_{\alpha \in G/H}$, $g_\alpha \in G$, $\pi(g_\alpha) = \alpha$. Chaque $g_\alpha \in \alpha$ peut-être vu comme un point de marquage (en physique on dit une **"jauge"**) sur la fibre $\alpha = g_\alpha H$ et permet d'identifier $g_\alpha H$ à H. L'application entre G et le groupe produit $G/H \times H$

$$\begin{cases} G = \bigsqcup_{\alpha \in G/H} g_\alpha H & \to G/H \times H \\ g_\alpha h & \mapsto (\alpha, h) \end{cases}$$

est une bijection. Elle n'est en revanche **pas un isomorphisme** en général ; vérifions-le :

$$\begin{aligned} g_\alpha h_\alpha g_\beta h_\beta &= g_\alpha g_\beta (g_\beta^{-1} h_\alpha g_\beta) h_\beta \\ &= g_{\alpha\beta} (g_{\alpha\beta}^{-1} g_\alpha g_\beta)(g_\beta^{-1} h_\alpha g_\beta) h_\beta \end{aligned}$$

et on peut écrire

$$(g_\alpha h_\alpha)(g_\beta h_\beta) = g_{\alpha\beta} h_{\alpha,\beta} \qquad \text{où } h_{\alpha,\beta} = (g_{\alpha\beta}^{-1} g_\alpha g_\beta)(g_\beta^{-1} h_\alpha g_\beta) h_\beta \in H$$

(remarquer que $\pi(g_{\alpha\beta}^{-1} g_\alpha g_\beta) = (\alpha\beta)^{-1}\alpha\beta = e$ donc $g_{\alpha\beta}^{-1} g_\alpha g_\beta \in H$; d'autre part $(g_\beta^{-1} h_\alpha g_\beta) \in H$ car $H \lhd G$). On n'a pas en général $h_{\alpha,\beta} = h_\alpha h_\beta$.

– *S'il est possible* de choisir la "jauge" $\alpha \mapsto g_\alpha$ de façon que pour tous α, β, $g_{\alpha\beta} = g_\alpha g_\beta$, c'est-à-dire si

$$G/H \ni \alpha \mapsto g_\alpha \in G$$

est une **section** pour $\pi : G \to G/H$, on peut obtenir un isomorphisme entre G et un **groupe "tordu"** $G/H \times_\rho H := (G/H \times H, *_\rho)$, où ρ est le morphisme de groupe

$$\begin{cases} \rho : G/H & \to (Aut(H), \circ) \\ \alpha & \mapsto \rho(\alpha)\cdot : h \mapsto \rho(\alpha)\cdot h := g_\alpha h g_\alpha^{-1} \end{cases}$$

(c'est un morphisme car $g_{\alpha\beta} = g_\alpha g_\beta$) et $*_\rho$ est la loi de composition

$$(\alpha, h) *_\rho (\beta, k) = (\alpha\beta, (g_\beta^{-1} h g_\beta)k) = (\alpha\beta, (\rho(\beta^{-1})\cdot h)k).$$

– Le groupe $G/H \times_\rho H$ est isomorphe au **produit semi-direct** $H \rtimes_\rho G/H$.

8.3 Action d'un groupe

Action d'un groupe G sur un ensemble X (à droite, à gauche).

8.3.1 Exemples et formule des classes

– Action de G sur lui-même par conjugaison.
– Si H est un sous-groupe (pas nécessairement distingué) de G et $X = G/H$ on a une action à gauche par translation $g \cdot (kH) = (gk)H$.
– Si X est l'ensemble des parties A de G de cardinal r fixé ($r \in [1, |G|]$), on a une action de G sur X par translation à gauche : pour tout $A \in X$, $g \cdot A$ est l'ensemble $gA = \{ga, a \in A\}$. $\longrightarrow$ théorèmes de Sylow.
– Si $X = \mathcal{H}$ est l'ensemble des sous-groupes de G on a une action de G sur X par $g \cdot H = gHg^{-1} := \{ghg^{-1}, h \in H\}$.
– *etc.*

– Si $x \in X$ et $g \in G$ on définit

$Stab(x) = \{g \in G,\ g.x = x\}$ (stabilisateur de x) : sous-groupe de G
$Fix(g) = \{x \in X,\ g.x = x\}$ (points fixes de g) : sous-ensemble de X
$\mathcal{O}(x) = \{g.x,\ g \in G\}$ (orbite de x) : sous-ensemble de X.

– **Formule des classe.** Si on note $\bar{X}$ un système de représentant de la relation $x \sim y \iff \mathcal{O}(x) = \mathcal{O}(y)$, on a la **formule des classes**

$$X = \bigsqcup_{x \in \bar{X}} \mathcal{O}(x) \qquad \text{et} \qquad |\mathcal{O}(x)| = |(G/Stab(x)| = \frac{|G|}{|Stab(x)|}.$$

8.3.2 Formule de Burnside

C'est la formule

nombre d'orbites = nombre moyen de points fixes :

$$|\bar{X}| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

8.4 Suites de compositions

(HP)

– Une suite de compositions d'un groupe G est

$$\{1\} \lhd G_n \lhd G_{n-1} \lhd \ldots \lhd G_0 = G.$$

– Elle est dite de **Jordan-Hölder** si elle est maximale pour l'inclusion. Une telle suite existe toujours.
– Dans ce cas les quotients G_{i-1}/G_i sont des **groupes simples**, càd sans sous-groupes distingués, et sont uniquement définis à permutation près.
– Si on connaît **tous les groupes finis simples** et si on sait résoudre le **problème de l'extension**, c'est-à-dire reconstruire G à partir de la suite exacte (pas nécessairement scindée)

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{p} K \longrightarrow 1$$

on peut dire que l'on a **classifié** les groupes finis.

8.5 Exemples de groupes

8.5.1 Les groupes cycliques.

- Groupes engendrés par un seul élément. Il sont isomorphes à $(\mathbb{Z}/n\mathbb{Z}, +)$.
- Un groupe de cardinal p **premier** est cyclique (Lagrange).
- En revanche, ce n'est pas automatique pour un **p-groupe** (groupe de cardinal p^α) : *cf.* exercice 58.
- **Ordre d'un élément.**
- Si d est **l'ordre** d'un élément de $\mathbb{Z}/n\mathbb{Z}$ on a $d \mid n$.
- Il y a $\varphi(d)$ élément d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ [le groupe multiplicatif $(\mathbb{Z}/d\mathbb{Z})^*$, dont le cardinal est $\varphi(d)$ agit (par multiplication) transitivement et sans point fixe sur l'ensemble des éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.]
- Rappels : si $d = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ on a

$$\varphi(d) = d \prod_{i=1}^{r} (1 - \frac{1}{p_i}), \qquad \varphi(1) = 1.$$

- Les ensembles O_d, $d \mid n$, constitués chacun des éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ constituent une partition de $\mathbb{Z}/n\mathbb{Z}$. Par conséquent

$$n = \sum_{d|n} \varphi(d).$$

8.5.2 Théorème de structure des groupes abéliens finis

- Tout groupe abélien fini est **produit de groupes cycliques**.
- **Lemme Chinois**

$$\mathbb{Z}/(p_1^{\alpha_1} \cdots p_n^{\alpha_n}\mathbb{Z}) \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_n^{\alpha_n}\mathbb{Z}).$$

  [Le même résultat est vrai si on remplace dans la formule précédente les groupes $\mathbb{Z}/n\mathbb{Z}$ par les groupes $(\mathbb{Z}/n\mathbb{Z})^*$. Lemme chinois dans les anneaux. Voir l'exercice 56.]
- Les deux derniers résultats donnent le résultat suivant : A est un groupe abélien fini, il existe une **unique** suite d'entiers

$$a_n \mid a_{n-1} \mid \ldots \mid a_1$$

  tels que A soit isomorphe à

$$(\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z}).$$

8.5.3 Les groupes de permutations

- $\mathfrak{S}_n$ et ses sous-groupes.
  - $|\mathfrak{S}_n| = n!$.
  - $\mathfrak{S}_n$ est engendré par les **transpositions** (i, j) (ou aussi $(i, i+1)$).
  - Une permutation admet une décomposition unique en produit de **cycles** de **supports** disjoints (en particulier ils commutent).
  - Deux permutations sont **conjuguées** ($\sigma_1 = \rho \circ \sigma_2 \circ \rho^{-1}$) si et seulement si elles ont le même nombre de cycles de même longueurs. $\longrightarrow$ utile pour déterminer les classes de conjugaisons des groupes de permutations.
  - **Signature.** Morphisme $\mathfrak{S}_n \to \mathbb{Z}/2\mathbb{Z} \simeq (\{-1, 1\}, \times)$ défini par
$$\epsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$
    La signature d'une transposition vaut -1.
  - **Principe de conjugaison.** Si $X \subset \{1, \ldots, n\}$ est un sous-ensemble invariant par une permutation $\sigma \in \mathfrak{S}_n$ alors pour toute permutation $\rho \in \mathfrak{S}_n$, l'ensemble $\rho(X)$ est un ensemble invariant par $\rho \circ \sigma \circ \rho^{-1}$. Si C est le support d'un cycle de σ, $\rho(C)$ est le support d'un cycle de $\rho \circ \sigma \circ \rho^{-1}$.
  - Toute groupe fini de cardinal n **s'injecte** dans un groupe de permutations $\mathfrak{S}_n$. En particulier, il s'injecte dans $GL(n, \mathbb{F}_p)$ pour tout p premier (à une permutation on associe la matrice correspondante de permutation).
- **Groupes alternés** : Sous-groupes $\mathcal{A}_n$ de $\mathfrak{S}_n$ égal à $\ker \epsilon$. On a $\mathcal{A}_n \lhd \mathfrak{S}_n$. Les groupes $\mathcal{A}_n$ pour $n \geqslant 5$ sont **simples**.

8.5.4 Les groupes de symétries

- Les groupes de symétries (linéaires, orthogonales) d'un ensemble de points de $\mathbb{R}^n$.
- Par exemple, groupe de symétrie d'un polygone ou un polyèdre régulier.
- On peut les voir comme des sous-groupes finis de $GL(n, \mathbb{R})$ ou $O(n, \mathbb{R})$.
- Ce sont les groupes **diédraux**.
- Il est parfois commode de les définir par **générateurs et relations**.

8.5.5 Les groupes de matrices sur des corps finis $GL(n, \mathbb{F}_q)$

(ou leur version projective), où $\mathbb{F}_q$, $q = p^m$, est un corps fini.

- Le groupe $GL(n, \mathbb{F}_p)$ est de cardinal $(p^n - 1) \cdots (p^n - p^{n-1})$. [Même formule avec q à la place de p].

– Si P est le sous-groupe des matrices triangulaires supérieures avec des 1 sur la diagonale, $|P| = p \times p^2 \times p^{n-1} = p^{n(n-1)/2}$. C'est un p-sous-groupe de Sylow de $GL(n, \mathbb{F}_p)$ (voir plus loin).
– Si p est premier
$$Aut((\mathbb{Z}/p\mathbb{Z})^n) = GL(n, \mathbb{F}_p).$$
[Utile quand on veut construire des **produits semi-directs**, cf. exercice 58.]

8.5.6 Les produits semi-directs

– Les **produits semi-directs** $(\mathbb{Z}/q\mathbb{Z}) \rtimes_\rho (\mathbb{Z}/p\mathbb{Z})$ où $p < q$ sont deux nombres premiers tels que $p \mid q-1$ et ρ est un morphisme **non trivial**
$$\rho : (\mathbb{Z}/p\mathbb{Z}, +) \to (\mathbb{Z}/(q-1)\mathbb{Z}, +) \simeq ((\mathbb{Z}/q\mathbb{Z})^*, \times) \simeq (Aut(\mathbb{Z}/q\mathbb{Z}), \circ).$$
– Le groupe $(\mathbb{Z}/q\mathbb{Z}) \rtimes_\rho (\mathbb{Z}/p\mathbb{Z})$ est non abélien.
– Les groupes de cardinal pq, $p < q$ premiers sont donc
  – si p ne divise pas $q-1$ le groupe cyclique $\mathbb{Z}/(pq)\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.
  – si $p \mid q-1$ le groupe cyclique $\mathbb{Z}/(pq)\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et le produit semi-direct non abélien $(\mathbb{Z}/q\mathbb{Z}) \rtimes_\rho (\mathbb{Z}/p\mathbb{Z})$ (un autre choix de ρ non trivial produit un groupe isomorphe).

8.6 Théorèmes de Sylow

– Si G est un groupe et $|G| = p^r m$ $(r \geqslant 1)$, $p \wedge m = 1$, un p-sous groupe de G est un sous-groupe de cardinal p^s, $1 \leqslant s \leqslant r$. Il est de Sylow si $s = r$.
– **Théorème de Cauchy.** Si $p \mid |G|$ alors G contient un élément d'ordre p.
– Si G contient un p-groupe de Sylow il contient, pour tout $1 \leqslant i \leqslant r$, un sous-groupe de cardinal p^i.
– **Premier théorème de Sylow** Le groupe G admet au moins un p-sous groupe de Sylow.
– **Second théorème de Sylow**
  – Les p-sous-groupes de Sylow de G sont tous conjugués entre-eux.
  – Si k est leur nombre on a
$$k \mid m \qquad \text{et} \qquad k \equiv 1 \mod p.$$
  – Si H est un p-sous-groupe de G alors il existe un p-Sylow de G contenant H.

Exercice 56 1) Soit $(\mathbb{Z}/n\mathbb{Z})^*$ le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Comment calculer son cardinal ?

2) Soient $a, b \in \mathbb{N}^*$ premiers entre-eux. Démontrer que

$$(\mathbb{Z}/ab\mathbb{Z})^* = (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*.$$

3) Soit p un nombre premier et $\alpha \in \mathbb{N}^*$. Le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est-il cyclique ?

4) Le groupe $(\mathbb{Z}/15\mathbb{Z})^*$ est-il cyclique ?

Exercice 57 Démontrer la formule de Burnside sur le nombre moyen de points fixes d'une action.

Exercice 58 1) Démontrer le théorème de Cauchy (si un nombre premier p divise l'ordre d'un groupe, il existe un élément d'ordre p) en utilisant une action de groupe judicieuse.

[Soit n l'ordre du groupe et $p|n$. On considère $X = \{(a_1, \ldots, a_p),\ a_i \in G\ :\ a_1 \cdots a_p = e\}$ et l'action de $\mathbb{Z}/p\mathbb{Z}$ sur X par permutation circulaire. On note que $|X| = n^{p-1}$ et que si $x \in X$, $|\mathcal{O}_x| = 1$ si et seulement si $x = (a, \ldots, a)$ avec $a^p = e$; sinon (Lagrange) $|\mathcal{O}_x| = p$. Si r est le nombre de solution de $a^p = e$ et s le nombre d'orbite de longueur p on a $n^{p-1} = r + sp$ et comme $p|n$ on a $p|r$ donc $r \geqslant 1$.]

2) Un groupe d'ordre p^2 est abélien.

[La formule des classes appliquée à l'action de G sur lui-même par conjugaison montre que le cardinal du centre Z_G de G est p ou p^2. Si c'est p, le groupe G/Z_G (Z_G est distingué dans G) est d'ordre premier p donc cyclique. Cela suffit pour voir que G est commutatif. On peut voir que G est égal soit à $Z/p^2\mathbb{Z}$ soit à $Z/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.]

3) Construire un groupe d'ordre p^3 non abélien. [On construira un morphisme $\rho : \mathbb{Z}/p\mathbb{Z} \to Aut((Z/p\mathbb{Z})^2) \simeq GL(2, \mathbb{F}_p)$ non trivial, par exemple $k \mapsto \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$. L'exemple est $(\mathbb{Z}/p\mathbb{Z}) \rtimes_\rho (Z/p\mathbb{Z})^2$.]

Exercice 59 1) Si $n = p^\alpha m$, p premier et p ne divise pas m, démontrer que le coefficient binomial $\binom{p^\alpha m}{p^\alpha}$ n'est pas divisible par p.

2) En considérant l'action de G sur X qui est l'ensemble des parties de G de cardinal p^α démontrer en utilisant la formule des classes que G contient un p-Sylow. [On pourra éventuellement faire une récurrence.]

Exercice 60 1) Exhiber un groupe non commutatif de cardinal 21.

2) Un groupe d'ordre 15 est-il cyclique ?

Exercice 61 Quel est le groupe de symétrie du carré ? Quel est son cardinal ? Est-il abélien ?

8.7 Représentations des groupes finis

8.7.1 Concepts et définitions de base

- Une **représentation** $Q = (G, V, \rho)$ d'un groupe fini G est une action linéaire $\rho : G \to Hom(V)$ d'un groupe G sur un K-ev V (de dim finie). De façon équivalente c'est un morphisme de groupe $\rho : G \to GL(n, K)$ ($n = \dim V$). On prend en général $K = \mathbb{C}$ (algébriquement clos). On appelle dimension de la représentation, la dimension de l'ev V.
- Les coefficients de la matrice $\rho_{ij}(g)$ sont appelés les **coefficients** de la représentation.
- L'application $g \mapsto \mathrm{tr}(\rho(g))$ est appelé le **caractère** de la représentation. On verra qu'il **caractérise** la représentation. On note $\mathcal{X}_G$ l'ensemble des caractères de G.
- On note $\langle \cdot, \cdot \rangle$ le produit hermitien sur l'espace $\mathbb{C}^G$ des fonctions $G \to \mathbb{C}$

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)}.$$

- On dit qu'une fonction $\phi \in \mathbb{C}^G$ est **centrale** si

$$\forall\ g, g' \in G, \quad \phi(gg'g^{-1}) = \phi(g').$$

- Le caractère d'une représentation est une fonction centrale (invariance de la trace par conjugaison).
- On dit que $W \subset V$ est un sev de V **ρ-invariant** si $\forall\ g \in G$, $\rho(g)W \subset W$. Ainsi, (G, W, ρ) est encore une représentation (on dit une sous-représentation de (G, V, ρ)).
- On dit que la représentation est **irreductible** s'il n'existe pas de sous-espace vectoriel $W \subset V$ non trivial ($W \neq \{0\}, V$) invariants par tous les $\rho(g)$, $g \in G$. On note Irr_G l'ensemble des représentations irréductibles de G, $\widetilde{\mathrm{Irr}}_G$ un système de représentants à équivalence près (conjugaison) de Irr_G et $\mathcal{X}_G^{\mathrm{Irr}}$ leurs caractères.
- On dit que deux représentations (G, V, ρ) et (G, V', ρ') sont **équivalentes** ou conjuguées s'il existe un **isomorphisme** linéaire $h : V \to V'$ tel que

$$\forall\ g \in G, \quad h \circ \rho(g) = \rho'(g) \circ h.$$

– **Opérations sur les représentations.** Si (G, V, ρ), (G, V', ρ') sont des représentations de G on peut construire les représentations

$$(V \oplus V', \rho \oplus \rho') := (V, \rho) \oplus (V', \rho'),$$
$$(V \otimes V', \rho \otimes \rho') := (V, \rho) \otimes (V', \rho')$$

par les formules

$$(\rho \oplus \rho')(g) = \begin{pmatrix} \rho(g) & 0 \\ 0 & \rho'(g) \end{pmatrix}$$

et

$$(\rho \otimes \rho')_{(i,i'),(j,j')}(g) = \rho_{i,j}(g)\rho'_{i',j'}(g).$$

[On rappelle que $V \otimes V'$ est l'ensemble des combinaisons linéaires $\sum \lambda_{ii'} e_i \otimes e'_{i'}$. Si on identifie les vecteurs $u = \sum_i u_i e_i \in V$, $u' = \sum_{i'} u'_i e'_i \in V$' à des applications $i \mapsto u(i) = u_i$, $i' \mapsto u'(i') = u'_{i'}$, le vecteur $u \otimes u' = \sum_{i,i'} u_i u'_{i'} e_i \otimes e'_{i'}$ s'identifie à l'application $(i, i') \mapsto u(i)u'(i')$ et de façon plus générale un vecteur $\sum \lambda_{ii'} e_i \otimes e'_{i'}$ de $V \otimes V'$ peut être vue comme une application $(i, i') \mapsto \lambda(i, i') = \lambda_{i,i'}$. L'application $\rho(g) \otimes \rho'(g)$ envoie $u \otimes u'$ sur $\rho(g)u \otimes \rho'(g)u'$.)

– On a

$$\chi_{\rho\oplus\rho'}(g) = \chi_\rho(g) + \chi_{\rho'}(g), \qquad \chi_{\rho\otimes\rho'}(g) = \chi_\rho(g)\chi_{\rho'}(g).$$

– **Restriction et représentation induite.** Soit H un **sous-groupe** de G.
  – Si (G, V, ρ) une représentation de G on peut définir par restriction à H une représentation $(H, V, \mathrm{Res}^H_G(\rho))$ de H.
  – Si (H, V, ρ) est une représentation de H on peut définir une représentation de G de la façon suivante. On introduit $W = \mathrm{Ind}^G_H(V)$ l'ensemble des applications $f : G \to V$ qui sont **H-équivariantes** :

$$\forall\ h \in H, \quad g \in G, \quad f(hg) = \rho(h)f(g)$$

  et on définit l'action $G \to Hom(W)$ par

$$\mathrm{Ind}^G_H(\rho)(g) : W \ni f(\cdot) \mapsto (G \ni x \mapsto f(xg) \in V).$$

  – Si χ est le caractère de ρ et $\chi_{\mathrm{Ind}^G_H}$ celui de $\mathrm{Ind}^G_H(\rho)$ on a

$$\chi_{\mathrm{Ind}^G_H}(g) = \frac{1}{|H|} \sum_{s\in G, sgs^{-1}\in H} \chi(sgs^{-1}).$$

– **A partir de maintenant $K = \mathbb{C}$.**

8.7.2 Exemples

- Soit $G = \mathbb{Z}/n\mathbb{Z}$. Alors, pour tout $l \in \mathbb{Z}/n\mathbb{Z}$,

$$\mathbb{Z}/n\mathbb{Z} \ni k \mapsto e^{2\pi ikl/n} \in \mathbb{U}$$

  est une représentation de $\mathbb{Z}/n\mathbb{Z}$ (irréductible car de dimension 1). Elles sont distinctes deux à deux.
- Soit $G = ((\mathbb{Z}/n\mathbb{Z})^*, \times)$ le groupe des éléments inversibles pour le produit de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Un caractère de $(\mathbb{Z}/n\mathbb{Z})^*$ peut-être assimilée à une fonction $\chi : \mathbb{Z} \to \mathbb{Z}$ qui est n-périodique, nulle sur les entiers non premiers à n et qui vérifie $\chi(kl) = \chi(k)\chi(l)$ si k et l sont premiers avec n. On les appelle les caractères de Dirichlet.
- **Représentation régulière.** Si G est un groupe on appelle représentation régulière la représentation $\mathrm{Reg}_G = (G, K^G, \mathrm{reg_G})$ qui à tout $g \in G$ et toute fonction $\psi : G \to K$ de K^G associe la fonction

$$\mathrm{reg}_G(g)(\psi) : G \ni x \mapsto \psi(xg).$$

  On peut aussi voir $\mathrm{reg}_G(g)$ comme l'endomorphisme de $\mathrm{Vect}(e_t,\ t \in G\}$ qui à $e_t \mapsto e_{gt}$.

  Le caractère de $\mathrm{reg}_G(g)$ est donné par

$$\chi_{\mathrm{reg}_G}(e) = |G|, \qquad \chi_{\mathrm{reg}_G}(g) = 0 \text{ si } g \neq e.$$

8.7.3 Résultats intermédiaires importants

- **Représentations entrelacées.** Soient (G, V, ρ) et (G, V', ρ') deux représentations de G et $h : V \to V'$ une application linéaire (pas forcément inversible) telle que

$$\forall\ g \in G, \quad h \circ \rho(g) = \rho'(g) \circ h.$$

  Alors
  - le sev $\ker h \subset V$ est **ρ-invariant** ;
  - le sev $\mathrm{Im}h \subset V'$ est **ρ'-invariant**.
- **Lemme de Schur.** Soient (G, V, ρ), (G, V', ρ') deux représentations **irréductibles** entrelacées par h.
  - Si les représentations ne sont pas équivalentes $h = 0$.
  - Si elles sont équivalentes h est un isomorphisme et quand $V = V'$, h est de la forme $\lambda \times Id$, $\lambda \in \mathbb{C}^*$.

  [Quand $V = V'$, appliquer le résultat précédent à $h - \lambda id$ où λ est une valeur propre de h.]
- **Représentations irréductibles des groupes abéliens.** Si un groupe est commutatif, ses représentations irréductibles sont de dimension 1.

– **Moyennisation.**
  – Si (G, V, ρ), (G, V', ρ') sont deux représentations et $h : V \to V'$ est une application linéaire, l'application

$$\bar{h} := \frac{1}{|G|} \sum_{g \in G} \rho'(g)^{-1} \circ h \circ \rho(g)$$

  entrelace (G, V, ρ), (G, V', ρ').
  – Si $q : V \to \mathbb{R}$ (resp. $\varphi : G \times G \to \mathbb{R}$) est une fonction alors $\bar{q}$ (resp. $\bar{\varphi}$) définie par

$$\bar{q}(v) = \frac{1}{|G|} \sum_{g \in G} q(\rho(g)v) \qquad (\text{resp.} \quad \bar{\varphi}(v_1, v_2) = \frac{1}{|G|} \sum_{g \in G} q(\rho(g)v_1, \rho(g)v_2))$$

  est G-invariante : $\bar{q}(\rho(g)v) = \bar{q}(v)$ (resp. $\bar{\varphi}(\rho(g)v_1, \rho(g)v_2) = \bar{\varphi}(v_1, v_2)$). En particulier, il existe toujours un **produit hermitien ρ-invariant** sur V et on peut donc supposer que ρ agit sur V par matrices **unitaires**.

8.7.4 Résultats

– **Théorème de Maschke.** Toute représentation se **décompose** en somme directe finie de représentations **irréductibles** :

$$(G, V, \rho) = \bigoplus_{i \in I} (G, V_i, \rho_i), \qquad (G, V_i, \rho_i) \in \mathrm{Irr}_G$$

  [Conséquence de l'existence d'un produit hermitien ρ-invariant.]
– **Orthogonalité des coefficients.** Soient (G, V, ρ), (G, V, ρ') deux représentations irréductibles.
  – Si (G, V, ρ), (G, V, ρ') ne sont pas équivalentes, alors pour tous i, j, i', j' les coefficients $g \mapsto \rho_{ij}(g)$ et $g \mapsto \rho'_{ij'}(g)$ sont orhogonaux :

$$\langle \rho_{ij}, \rho'_{i'j'} \rangle = 0.$$

  – Si (G, V, ρ), (G, V, ρ') sont équivalentes

$$\langle \rho_{ij}, \rho'_{i'j'} \rangle = \frac{1}{|\dim V|} \delta_{i,i'} \delta_{j,j'}$$

– **Orthogonalité des caractères.** Soient (G, V, ρ), (G, V, ρ') deux représentations irréductibles et $\chi = \mathrm{tr}\rho$, $\chi' = \mathrm{tr}\rho'$ leurs caractères.
  – Si (G, V, ρ) et (G, V, ρ') ne sont pas équivalentes

$$\langle \chi, \chi' \rangle = 0.$$

– Si (G, V, ρ) et (G, V, ρ') sont équivalentes

$$\langle \chi, \chi' \rangle = 1.$$

– **Théorème de Frobenius.** Les caractères irréductibles (i.e. les caractères des représentations irréductibles) d'un groupe forment une base orthonormale de l'espace $C(G)$ des fonctions centrales.
– **Caractérisation des représentations par les caractères.** Deux représentations sont équivalentes si et seulement si leurs caractères sont égaux.
– **Caractérisation des représentations irréductibles.** Une représentation est irréductible si et seulement si son caractère χ vérifie $\langle \chi, \chi \rangle = 1$.
– On peut donc indexer les classes d'équivalence des représentations irréductibles par les caractères irréductibles $\mathcal{X}_G^{\mathrm{Irr}}$.
– **Nombre de caractères irréductibles.** Le **nombre de caractères irréductibles** est égal au **nombre de classes de conjugaison** de G :

$$|\mathcal{X}_G^{\mathrm{Irr}}| = \mathrm{card}\{\{ghg^{-1},\ g \in G\},\ h \in G\}.$$

En particulier si G est abélien, il est égal à $|G|$.
– **Multiplicité.** Notons $\mathrm{Irr}(G)$ l'ensemble des représentations irréductibles de G.
  – Soient (G, V, ρ) est une représentation de G de caractère φ et $(G, V, \rho) = \bigoplus_{i \in I} (G, V_i, \rho_i)$ une décomposition en somme directe de représentations irréductibles ($(G, V_i, \rho_i) \in \mathrm{Irr}(G)$ de caractère φ_i). Alors, si $(G, W, \theta) \in \mathrm{Irr}(G)$ est une représentation irréductible de caractère φ, le nombre de i pour lesquels (G, V_i, ρ_i) est équivalent à (G, W, θ) égale $\langle \chi_i, \varphi \rangle$ (qui est donc un entier).
  – **Représentation canonique (ou isotypique).** Il existe une décomposition unique en somme directe de représentations

$$(G, V, \rho) = \bigoplus_{\chi \in \mathcal{X}_G^{Irr}} \mathrm{Iso}_G(\chi)$$

où chaque $\mathrm{Iso}_G(\chi)$ est soit nul soit la somme de $m(\chi) := \langle \mathrm{tr}(\rho), \chi \rangle \in \mathbb{N}^*$ représentations irréductibles de caractère χ.
– **Décomposition de la représentation régulière.** La décomposition régulière contient toutes les représentations irréductibles avec pour chacune une multiplicité égale sa dimension :

$$\mathrm{Reg}_G = \bigoplus_{Q \in \widetilde{\mathrm{Irr}_G}} (\dim Q)\ Q.$$

En particulier

$$\chi_{Reg_G} = \sum_{Q \in \widetilde{\mathrm{Irr}_G}} (\dim Q)\ \chi_Q$$

et

$$|G| = \sum_{Q \in \widetilde{\mathrm{Irr}_G}} (\dim Q)^2.$$

- **Propriétés d'intégralité.** La dimension d'une représentation irréductible **divise** l'ordre du groupe.
- **Théorème de réciprocité de Frobenius.** Si (H, V_1, ρ_1) et (G, V_2, ρ_2) sont deux représentations on a

$$\langle \mathrm{Ind}_H^G(\rho_1), \rho_2 \rangle_G = \langle \rho_1, \mathrm{Res}_G^H(\rho_2) \rangle_H.$$

- **Le cas des groupes abéliens : dual et Fourier.** Si A est un groupe abélien ses dimensions irréductibles sont de dimension 1. L'ensemble des caractères (forcément irréductibles) de A forment un groupe abélien (la loi est le produit des caractères) qu'on appelle **le groupe dual** $\hat{A} = \mathcal{X}_A^{\mathrm{Irr}}$ de A. Toute fonction sur A est **centrale** s'écrit comme combinaison linéaire d'éléments de $\hat{A}$ et on a l'inversion de Fourier (orthogonalité des caractères)

$$C(A) \ni f = \sum_{\chi \in \hat{A}} \hat{f}(\chi)\chi \qquad \text{où} \quad \hat{f}(\chi) = \langle f, \chi \rangle = \frac{1}{|A|} \sum_{a \in A} f(a)\overline{\chi(a)}.$$

On a l'égalité l^2 :

$$\langle f, f \rangle = \sum_{\chi \in \hat{A}} \langle \chi, \chi \rangle$$

Exercice 62 1) Démontrer qu'un sous-groupe fini de $(\mathbb{C}^*, \times)$ est en fait un sous-groupe du cercle unité $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$ (muni de la multiplication).

2) Démontrer qu'un sous-groupe fini de $\mathbb{U}$ est cyclique (de la forme $\{e^{2\pi ik/n},\ k = 0, \ldots, n-1\}$). [On pourra s'inspirer de la démonstration du théorème de classification des sous-groupes fermés de $\mathbb{R}$.]

3) Soit G un groupe fini *abélien*. Montrer que G est isomorphe à un sous-groupe abélien fini G' du sous-groupe $\Sigma_n \subset GL(n, \mathbb{C})$ constitué des matrices de permutations M_σ, $\sigma \in \mathfrak{S}_n$, où $n = |G|$.

4) Montrer que G' est conjugué dans $GL(n, \mathbb{C})$ à un sous-groupe de matrices diagonales de la forme $\{\mathrm{diag}(\lambda_1(g), \ldots, \lambda_n(g)),\ g \in G\}$ où les $G \ni g \mapsto \lambda_i(g) \in \mathbb{U}$ sont des morphismes de groupes, càd des caractères de G

5) En utilisant la question 4), la question 2) et le fait que les caractères de G forment une base des fonctions sur G démontrer que tout groupe abélien est produit de groupes cycliques.

Exercice 63 1) Déterminer les caractères du groupe $\mathbb{Z}/n\mathbb{Z}$.

2) En déduire la formule $\sum_{d|n} \varphi(d) = n$.

Exercice 64 Un groupe G non trivial est simple si et seulement si pour toute caractère irréductible distinct de 1 on

$$\forall\ g \neq e, \quad \chi(g) \neq \chi(e).$$

Exercice 65 Soit G un groupe (abélien) à 8 éléments. Déterminer (suivant les cas) ses caractères.

Exercice 66 Soit χ_1 et χ_2 deux caractères.

1) Démontrer que la fonction $\chi_1\chi_2$ est un caractère.

2) On suppose que χ_1 et χ_2 sont irréductibles, $\neq 1$ et que $\chi_1\chi_2 = \lambda_1\chi_1 + \lambda_2\chi_2$, $\lambda_1, \lambda_2 \in \mathbb{C}$. Démontrer que $\chi_1\chi_2$ n'est pas irréductible.

Exercice 67 On suppose que V est une représentation de dimension 1 et que W est une représentation irréductible. Démontrer que $V \otimes W$ est irréductible.

Exercice 68 Tables de caractères. (Groupe $\mathfrak{S}_3$).

1) Trouver des générateurs s, t de $\mathfrak{S}_3$ tels que $s^2 = 1$, $t^3 = 1$, $sts = t^{-1}$.

2) Combien de classes de conjugaisons possède $\mathfrak{S}_3$? Combien de caractères irréductibles ?

3) Démontrer que la signature est un caractère.

4) Démontrer qu'il existe un caractère irréductible associé à une représentation de dimension 2.

5) En utilisant la décomposition de la représentation régulière en sommes de représentations irréductibles (et en prenant la trace) détérminer toutes les représentations irréductibles de $\mathfrak{S}_3$. (On fera un tableau).

9 Anneaux

- **Idéaux.** Notions de base, produits d'anneaux, **idéal** d'un anneau commutatif, quotient par un idéal, anneau intègre, idéal premier (l'anneau quotient est intègre), idéal maximal (l'anneau quotient est un corps), un anneau intègre fini est un corps.
- **Théorème chinois.** Soit A un anneaux commutatif et $I_1, \ldots, I_n$ des idéaux premiers entre eux deux à deux ($I_i + I_j = A$). Alors,
  - $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.
  - l'application $x \mod I_1 \cap \cdots \cap I_n \mapsto (x \mod I_1, \ldots, x \mod I_n)$ est un isomorphisme

$$A/(I_1 \ldots I_n) \simeq (A/I_1) \times \cdots \times (A/I_n).$$

- **Divisibilité.**
  - Anneau factoriel ; si A est factoriel alors $A[X]$ aussi.
  - Anneau principal : théorème de **Bezout**.
  - Pour les polynômes : critère d'Eisenstein, contenant de Gauss.
- **Polynômes.**
  - Relations racines / coefficients.

$$(X - \lambda_1) \cdots (X - \lambda_n) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n$$

    σ_j est un polynôme symétrique en les $(\lambda_1, \cdots, \lambda_n)$ de degré j. Ce sont les **fonctions symétriques élémentaires**.
  - **Polynômes symétriques.** Si $P(X_1, \ldots, X_n)$ est un polynôme dans $A[X_1, \ldots, X_n]$ on définit pour $\rho \in \mathfrak{S}_n$, $P^\rho(X_1, \ldots, X_n) = P(X_{\rho(1)}, \ldots, X_{\rho(n)})$. On dit que P est **symétrique** si pour tout $\rho \in \mathfrak{S}_n$ on a $P^\rho = P$.
    On a alors le théorème important : tout polynôme symétrique P à coefficients dans A s'écrit comme polynôme à coefficients dans A des polynômes symétriques élémentaires : il existe $Q \in A[X_1, \ldots, X_n]$ tel que

$$P(X_1, \ldots, X_n) = Q(\sigma_1(X_1, \ldots, X_n), \ldots, \sigma_n(X_1, \ldots, X_n)).$$

  - **Applications :**
    - **Discriminant** : teste si les racines d'un polynôme sont simples. Si $P = X^n + a_1 X + \cdots + a_n$ et $\lambda_1, \ldots, \lambda_n$ sont ses racines comptées avec multiplicités on a

$$\prod_{1 \leqslant i,j \leqslant n} (\lambda_i - \lambda_j) = D(a_1, \ldots, a_n)$$

      où $D \in \mathbb{Z}[X_1, \ldots, X_n]$ est à coefficients **entiers** en les $a_1, \ldots, a_n$.

- **Résultant** : teste si deux polynômes ont des racines en commun. Si $P = X^n + a_1X^{n-1} + \cdots + a_n$ a pour racines $\lambda_1, \ldots, \lambda_n$ et $Q = X^m + b_1X^{m-1} + \cdots + b_m$ a pour racines $\mu_1, \ldots, \mu_m$ on a

$$\prod_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m} (\lambda_i - \mu_j) = R_{n,m}(a_1, \ldots, a_n, b_1, \ldots, b_m)$$

  où $R_{n,m} \in \mathbb{Z}[X_1, \ldots, X_{n+m}]$ est à coefficients **entiers** en les $a_1, \ldots, a_n$, $b_1, \ldots, b_m$.
- **Sommes de Newton.** La somme $N_k = \sum_{j=1}^{n} \lambda_j^k$ des puissances k-ièmes d'un polynôme $P(X) = X^n + a_1X^{n-1} + a_n$ est un polynôme en ses coefficients.

- **Décomposition en éléments simples.**

Exercice 69 Soient $a_1, \ldots, a_d$ des entiers positifs premiers entre-eux deux à deux. On note p_n le nombre de façons d'écrire n comme somme $n = \sum_{i=1}^{d} n_i a_i$.
1) Démontrer que

$$\frac{1}{1 - X^{a_1}} \cdots \frac{1}{1 - X^{a_d}} = \sum_{k=0}^{\infty} p_k X^k.$$

2) Décomposer le membre de gauche de l'identité précédente en éléments simples et démontrer qu'il existe N tel que pour tout $k \geqslant N$, $p_k \neq 0$.

Module sur un anneau principal

10 Corps

10.1 Caractéristique d'un corps

- **Caractéristique.** L'ensemble des $n \in \mathbb{Z}$ pour lesquels $n \cdot 1 = 0$ est un idéal de $\mathbb{Z}$ de la forme $p\mathbb{Z}$, avec $p = 0$ ou p un nombre premier. On dit que p est la caractéristique du corps.
- Si la caractéristique d'un corps est nulle alors son plus petit sous-corps (pour l'inclusion) est isomorphe à $(\mathbb{Q}, +, \times)$.
- Si la caractéristique d'un corps est p non nul alors son plus petit sous-corps (pour l'inclusion) est isomorphe à $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ (qu'on note $\mathbb{F}_p$).

10.2 Extensions de corps

- **Extension de corps.** Si $K \subset L$ est un sous corps de L on dit que L est une extension de K. On note en général L/K. Dans ce cas L est un K-espace vectoriel. Sa dimension se note $[L : K]$ et est appelée le **degré** de l'extension.
- **Théorème de la base télescopique.** Si L/K est une extension de K et M/L une extension de L alors M/K est une extension de K et

$$[M : K] = [M : L] \times [L : K].$$

- **Constructions d'extensions.**
  - Si L/K est une extension de corps et S est une partie d'éléments de L on peut construire $K(S)$, le plus petit corps contenant K et S. Si par exemple $\alpha \in L$:
    - Soit il existe un polynôme $\mu \in K[X]$ tel que $\mu(\alpha) = 0$ et on a $K(\alpha) = K[\alpha] = \{P(\alpha),\ P \in K(X)\} = \{P(\alpha),\ P \in K[X]\}$; le corps $K(\alpha)$ est alors isomorphe à $K[X]/(\mu_\alpha)$ où μ_α est le **polynôme minimal** de α (le polynôme unitaire de plus petit degré à coefficients dans K qui annule α). On a

$$[K(\alpha) : K] = \deg \mu_\alpha.$$

      On dit que α est **algébrique** sur K.
    - soit ce n'est pas le cas et $K(\alpha)$ est isomorphe à $K(X)$ (le corps des fractions rationnelles sur K). On dit que α est **transcendant** sur K.
  - Une extension L/K est **algébrique** si tout élément de L est algébrique sur K.

- Si K est un corps et $P \in K[X]$ est un polynôme, on peut construire le **corps de décomposition** de P dans K qui est le plus petit corps contenant toutes les racines de P, c'est-à-dire sur lequel P est scindé (i.e. produit de monômes de degré 1). Ce corps existe toujours. Pour le construire on produit des extensions successives de **corps de rupture** : si P est un polynôme irréductible sur K, l'idéal $(P) \subset K[X]$ est premier et $K[X]/(P)$ est un corps dans lequel $X + (P)$ est une racine de P.
  Exemple : $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$.
- **Clôture algébrique.** Tout corps admet une clôture algébrique, càd une extension dans laquelle tout polynôme admet une racine (est scindé). Deux clôtures algébriques d'un corps sont isomorphes (mais l'isomorphisme n'est pas unique).
  $\mathbb{C}$ est algébriquement clos.

- Une extension L/K est **séparable** si elle est algébrique et le polynôme minimal sur K de tout élément de L n'admet que des racines simples. Si K est de **caractéristique nulle ou est un corps fini** il est parfait, càd que toute extension de K est séparable.
- **Théoréme de l'élément primitif.** Toute extension séparable est **simple**, càd engendré par un seul élément. En particulier, si L/K est une extension d'un corps de caractéristique nulle ou d'un corps fini, il existe $\alpha \in L$ tel que $L = K[\alpha]$.

10.3 Théorie de Galois

- **Extension galoisienne.**
  - Un automorphisme de L/K est un automorphisme de corps $L \to L$ qui vaut l'identité sur K. L'ensemble $Gal(L/K)$ de ces automorphismes est le **groupe de Galois**. Si $P \in K[X]$, $\alpha \in L$ et $\sigma \in Gal(L/K)$ on a $P(\alpha) = 0 \implies P(\sigma(\alpha)) = 0$. En particulier, si l'extension est séparable on a toujours
  $$|Gal(L/K)| \leqslant [L : K];$$
  (pour le voir considérer α un élément primitif de L/K, $L = K[\alpha]$).
  - On dit que l'extension L/K est **normale** si pour tout élément $\alpha \in L$, l'ensemble $\{\sigma(\alpha), \sigma \in Gal(L/K)\}$ est l'ensemble des racines du polynôme minimal de α (et pas seulement une partie).
  - Une extension L/K est dite **galoisienne** si elle est normale et séparable.
  - L'extension L/K est galoisienne si et seulement si
  $$|Gal(L/K)| = [L : K].$$

– **Théorie de Galois.** Correspondance entre corps intermédiaire d'une extension et sous-groupe du groupe de Galois. Soit L/K une extension galoisienne. A tout sous-groupe H de $Gal(L/K)$ on associe le sous-corps

$$L^H = \{x \in L,\ \forall\ \sigma \in H,\ \sigma(x) = x\}, \qquad K \subset L^H \subset L.$$

L'ensemble L^H est un corps intermédiaire $K \subset L^H \subset L$.

1. L'application qui à H associe L^H est une **bijection** de l'ensemble des **sous-groupes** de $Gal(L/K)$ sur l'ensemble des **corps intermédiaires** entre K et L.
2. L/L^H est galoisienne et $Gal(L/L^H) = H$.
3. L^H/K est galoisienne si et seulement si $H \lhd Gal(L/K)$. Dans ce cas
$$Gal(L^H/K) = Gal(L/K)/H.$$

10.4 Corps finis

– Le groupe multiplicatif d'un corps fini est cyclique.
– Si un corps K est fini, il est de caractéristique p non-nulle (p nombre premier). Si on note $n = [K : \mathbb{F}_p]$, K est de cardinal $q = p^n$.
– **Frobenius**. Si K est un corps fini, on a pour tout $x, y \in K$, l'identité $(x + y)^p = x^p + y^p$ (car p divise les coefficients binomiaux $\binom{p}{k}$ pour $k \neq 0, p$). En particulier,
$$\varphi_p : x \mapsto x^p$$
est un endomorphisme de corps bijectif[1] qui fixe $\mathbb{F}_p$. On a donc $\varphi_p \in Gal(K/\mathbb{F}_p)$. On l'appelle l'**automorphisme de Frobenius**.
– **Structure des corps finis.** Il existe un corps de cardinal $q = p^n$, unique à isomorphisme près, qui est le corps de décomposition du polynôme $X^q - X$.
– **Structure des extensions de corps finis.** Les extensions de corps finis sont galoisiennes et leur groupe de Galois est cyclique :
$$Gal(\mathbb{F}_{p^n} : \mathbb{F}_p) = \{\varphi_p^j,\ 0 \leqslant j \leqslant n-1\} \simeq (\mathbb{Z}/n\mathbb{Z}, +).$$
Les corps intermédiaires entre $\mathbb{F}_p$ et $\mathbb{F}_{p^n}$ sont donc de la forme $\mathbb{F}_{p^d}$ avec $d|n$ (ils sont en correspondance bijective avec les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$).

1. Il est injectif car si $x^p = y^p$ on a $(x - y)^p = 0$ et donc $x = y$. Comme K est fini, il est bijectif.

Exercice 70 Construire un corps de rupture de $P(X) = X^3 - 2 \in \mathbb{Q}[X]$. Donner un corps de décomposition L de P ? Quel est le degré de l'extension $L/\mathbb{Q}$?

11 Probabilités

11.1 Espace probabilisé

- **Espace probabilisé.** C'est la donnée $(\Omega, \mathcal{B}, \mathbb{P})$ d'un ensemble Ω, l'espace des états (ou univers), d'une tribu $\mathcal{B}$ (l'espace des événements) et d'une probabilité $\mathbb{P} : \mathcal{B} \to [0,1]$ (fonction σ-additive d'ensemble).
- On n'a en général jamais accès à Ω.
- Le fait que $\mathcal{B}$ soit invariant par intersection, union, complémentaire, permet de former des phrases avec des "et", "ou", "non" (de façon dénombrable) et souvent de coder les quantificateurs "il existe" et "pour tout". Par exemple, l'ensemble défini par "la suite de variables aléatoires X_n converge vers l" signifie "pour tout $q \in \mathbb{N}^*$ il existe $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$ $X_n \in]l - 1/q, l + 1/q[$" ce qui s'écrit

$$\bigcap_{q \in \mathbb{N}^*} \bigcup_{N \in \mathbb{N}} \bigcap_{n \geqslant N} \Big\{ \omega \in \Omega,\ X_n(\omega) \in]l - 1/q, l + 1/q[\Big\}.$$

11.2 Variable aléatoire

- **Variable aléatoire.** C'est une application $X : \Omega \to \mathbb{R}$ qui est $\mathcal{B}$-mesurable (la préimage de tout ouvert est un événement de la tribu $\mathcal{B}$).
- **Vecteur aléatoire.** C'est une application $\mathcal{B}$-mesurable $X : \Omega \to \mathbb{R}^n$, $\omega \mapsto (X_1(\omega), \ldots, X_n(\omega))$. Le vecteur X est aléatoire ssi ses composantes X_i le sont.
- **Loi d'une v.a.** C'est la **probabilité** μ_X définie sur $(\mathbb{R}, Bor(\mathbb{R}))$ (où $Bor(\mathbb{R})$ est la tribu borélienne de $\mathbb{R}$, càd la tribu engendré par les ouverts de $\mathbb{R}$) par :

$$\forall\ I \in Bor(\mathbb{R}) \text{ (ou } \forall\ I \text{ intervalle)} \quad \mu_X(I) = \mathbb{P}(\{\omega \in \Omega,\ X(\omega) \in I\}.$$

On note souvent $\{X \in I\}$ l'événement

$$\{X \in I\} := X^{-1}(I) = \{\omega \in \Omega,\ X(\omega) \in I\}.$$

L'intérêt de considérer ces lois, c'est que l'on a affaire à des probabilités définies sur un espace beaucoup plus concret que l'espace Ω.
Si la mesure μ_X (la loi de X) est **absolument continue** par rapport à la mesure de Lebesgue, ce qui est équivalent au fait qu'il existe une fonction positive $\rho : \mathbb{R} \to \mathbb{R}$ telle que $\int_{\mathbb{R}} \rho(x)dx = 1$ telle que $d\mu(x) = \rho(x)dx$, on dit que X admet une **densité** (ρ en l'occurrence).
On définit de la même manière la loi d'un **vecteur aléatoire**.

– **Fonction de répartition.** Si X est une v.a. à valeurs réelles c'est la fonction $F_X : \mathbb{R} \to [0,1]$

$$F_X(t) = \mu_X(]-\infty, t]) = \mathbb{P}(X \leqslant t).$$

Ce sont des fonctions **càdlàg** (continues à droite qui admettent des limites à gauche).

11.3 Indépendance

– **Indépendance.** Un ensemble de variables aléatoires $(X_i)_{i\in I}$ est dit **indépendant dans son ensemble** si pour tout sous-ensemble fini $\{i_1, \ldots, i_n\} \subset I$ et tous boréliens ou intevalles $U_1, \ldots, U_n$ de $\mathbb{R}$ on a

$$\mathbb{P}(\{X_{i_1} \in U_1\} \cap \ldots \cap \{X_{i_n} \in U_n\}) = \mathbb{P}(\{X_{i_1} \in U_1\}) \cdots \mathbb{P}(\{X_{i_n} \in U_n\}).$$

On utilise souvent le résultat **d'indépendance par paquets** : si les ensembles I_α, $\alpha \in A$ forment une partition de I et si $(X_i)_{i\in I}$ est indépendant dans son ensemble, les variables aléatoires $(Y_\alpha)_{\alpha\in A}$ de la forme $Y_\alpha = F_\alpha(X_i,\ i \in I_\alpha)$ sont indépendantes dans leur ensemble.

– **Produits de v.a. indépendantes.** Les v.a. $X_1, \ldots, X_n$ sont indépendantes dans leur ensemble si et seulement si pour toutes fonctions continues bornées $f_1, \ldots, f_n : \mathbb{R} \to \mathbb{R}$

$$\mathbb{E}(f_1(X_1) \ldots f_n(X_n)) = \mathbb{E}(f_1(X_1)) \cdots \mathbb{E}(f_n(X_n)).$$

– **Jeu de pile ou face infini.** On pose $\Omega = \{0,1\}^{\mathbb{N}}$ et $\mathcal{B}$ la tribu engendrée par les **cylindres** càd les ensembles de la forme

$$C_{\epsilon_0,\ldots,\epsilon_k} = \{(x_n)_{n\in\mathbb{N}} \in \Omega,\ \forall\ n \in [0,k] \cap \mathbb{N},\ x_n = \epsilon_n\}.$$

Il existe alors (ce n'est pas si facile à démontrer) une **unique** mesure de probabilité $\mathbb{P}$ sur $\mathcal{B}$ qui a la propriété que pour tout cylindre $C_{\epsilon_0,\ldots,\epsilon_k}$

$$\mathbb{P}(C_{\epsilon_0,\ldots,\epsilon_k}) = p^{\sum_{j=0}^k \epsilon_j}(1-p)^{\sum_{j=0}^k (1-\epsilon_j)}.$$

Les fonctions $X_n : \omega = (\omega_n)_{n\in\mathbb{N}} \mapsto \omega_n$ sont des v.a. indépendantes dans leur ensemble. Elles ont toutes la même **loi de Bernoulli** de paramètre $p \in [0,1] : \mathbb{P}(X_n = 1) = p$.

– **Borel-Cantelli.**
  – Si $(A)_{n\in\mathbb{N}}$ est une suite d'événements telle que

$$\sum_{n\in\mathbb{N}} \mathbb{P}(A_n) < \infty,$$

alors, $\mathbb{P}$-presque tout $\omega \in \Omega$ appartient à un nombre fini de A_n.

– Si les $(A_n)_{n\in\mathbb{N}}$ sont **indépendants** (càd les $\mathbf{1}_{A_n}$ le sont) et

$$\sum_{n\in\mathbb{N}} \mathbb{P}(A_n) = \infty,$$

alors, $\mathbb{P}$-presque tout $\omega \in \Omega$ appartient à une infinité de A_n.

11.4 Lois classiques

– **Lois classiques.** Bernoulli, Binomiale (somme de Bernoulli i.i.d.), Exponentielle, Géométrique, Poisson, Normale.
La loi Normale $\mathcal{N}(0, \sigma^2)$ (centrée) :

$$\mathbb{P}(X \in [a, b]) = \frac{1}{\sqrt{2\pi\sigma^2}} \int_a^b \exp(-t^2/(2\sigma^2))dt.$$

11.5 Espérance

– **v.a. dans** L^p On dit que $X \in L^p(\Omega, \mathbb{P})$ si

$$\mathbb{E}(|X|^p) := \int_\Omega |X|^p d\mathbb{P}(\omega) < \infty.$$

Si $p = 1$ on peut définir **l'espérance** de X

$$\mathbb{E}(X) := \int_\Omega X d\mathbb{P}(\omega) < \infty$$

et si $p = 2$ la **variance** de X

$$\mathrm{Var}(X) = \mathbb{E}(|X - \mathbb{E}(X)|^2) = \mathbb{E}(X^2) - \mathbb{E}(X)^2.$$

L'écart type de X est $\sigma(X) := \mathrm{Var}(X)^{1/2}$.

– **Théorème de transfert** Soit X une v.a. de loi μ_X. Toutes les fois où cela a un sens

$$\mathbb{E}(f(X)) = \int_{\mathbb{R}} f(x) d\mu_X.$$

11.6 Convergence

– **Divers type de convergence.** Si $(X_n)_n$ est une suite de v.a.
  – **Convergence presque-sûre (p.s)** : $(X_n)_n$ converge p.s. vers X si

$$\mathbb{P}(\lim_{n\to\infty} X_n = X) = 1.$$

– **Convergence en probabilité** :

$$\forall\ \epsilon > 0, \quad \lim_{n\to\infty} \mathbb{P}(|X_n - X| \geqslant \epsilon) = 0.$$

– **Convergence L^p** :

$$\mathbb{E}(|X_n - X|^p) = 0.$$

– **Convergence en loi.**

$$\forall\ I \text{ intervalle} \quad \lim_{n\to\infty} \mathbb{P}(X_n \in I) = \mathbb{P}(X \in I).$$

Connaître les implications reliant ces propriétés.

– **Fonction caractéristique.** C'est la fonction (toujours définie)

$$\forall\ t \in \mathbb{R}, \quad \phi_X(t) = \mathbb{E}(\exp(itX)).$$

– Elle caractérise la **loi** de X : si pour tout $t \in \mathbb{R}$, $\phi_X(t) = \phi_Y(t)$ alors les v.a. X et Y ont même loi.

– Une suite de v.a. $(X_n)_{n\in\mathbb{N}}$ converge en loi vers X si et seulement si

$$\forall\ t \in \mathbb{R}, \quad \phi_{X_n}(t) = \phi_X(t).$$

– Une suite de v.a $(X_n)_{n\in\mathbb{N}}$ est indépendante dans son ensemble si et seulement si pour tout $t_1, \ldots, t_n \in \mathbb{R}$

$$\phi_{(X_1,\ldots,X_n)}(t_1, \ldots, t_n) = \phi_{X_1}(t_1) \cdots \phi_{X_n}(t_n).$$

– Si X et Y sont deux v.a. indépendantes

$$\phi_{X+Y} = \phi_X \times \phi_Y.$$

– Si X suit une loi normale $\mathcal{N}(0, \sigma^2)$

$$\phi_X(t) = e^{-t^2\sigma^2/2}.$$

– Quand X prend ses valeurs dans $\mathbb{N}$

$$\phi_X(t) = \sum_{n\in\mathbb{N}} \mathbb{P}(X = n)e^{itn} = G_X(e^{it})$$

où G est la **fonction génératrice** de X, $G(z) = \sum_{n\in\mathbb{N}} \mathbb{P}(X = n)z^n$.

11.7 Les théorèmes limites

– **Loi des grands nombres.** Si les $(X_n)_{n\in\mathbb{N}}$ forment une suite de v.a. indépendantes identiquement distribuées (on écrit i.i.d.) dans L^1 alors

$$\frac{1}{n}\sum_{k=1}^{n} X_k \xrightarrow[n\to\infty]{p.s.} \mathbb{E}(X_1).$$

– **Théorème "Central Limit".** Si les $(X_n)_{n\in\mathbb{N}}$ forment une suite de v.a. indépendantes identiquement distribuées (on écrit i.i.d.) dans L^2 alors

$$\sqrt{n}\left(\frac{1}{n}\sum_{k=1}^{n} X_k - \mathbb{E}(X_1)\right) \xrightarrow[n\to\infty]{loi} \mathcal{N}(0,\sigma^2), \qquad \sigma^2 = \mathrm{Var}(X_1).$$

Exercice 71 Soit $(\Phi_n)_{n\geqslant 1}$ une suite de v.a. indépendantes à valeurs dans $\{k/q,\ 0 \leqslant k \leqslant q-1\}$ (où $q \geqslant 3$ est un entier) uniformément répartie. On considère la suite de v.a. $(T_n)_{n\geqslant 0}$ définie par $T_0 = 0$ et pour $n \geqslant 0$, $T_{n+1} = T_n + \tau + \sin(2\pi(T_n - \Phi_n))$.

1) Calculer $\mathbb{E}(T_n)$.

2) Démontrer qu'il existe $\lambda \in \mathbb{R}$ tel que pour tout $\epsilon > 0$, $\lim_{n\to\infty} \mathbb{P}(|\frac{T_n}{n} - \lambda| \geqslant \epsilon) = 0$.