MÉTA-PLANS POUR LES LEÇONS DE MATHÉMATIQUES POUR L'AGRÉGATION DE MATHÉMATIQUES OPTION D

Table des matières

Introduction 3
104. Groupes finis. Exemples et applications 3
105. Groupe des permutations d'un ensemble fini. Applications 5
106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous groupes de $GL(E)$. Applications. 6
108. Exemples de parties génératrices d'un groupe. Applications. 8
120. Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications. 10
121. Nombres premiers. Applications. 12
123. Corps finis. Applications. 14
141. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications. 16
150. Exemples d'actions de groupes sur les espaces de matrices 18
151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications. 20
152. Déterminant. Exemples et applications. 22
153. Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications 24
157. Endomorphismes trigonalisables. Endomorphismes nilpotents. 26
159. Formes linéaires et dualité en dimension finie. Exemples et applications. 28
162. Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques. 30
170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications 32
181. Barycentres dans un espace affine réel de dimension finie, convexité. Applications. 34
182. Applications des nombres complexes à la géométrie. 35
183. Utilisation de nombres complexes en géométrie. 37
190. Méthodes combinatoires, problèmes de dénombrement. 38
203. Utilisation de la notion de compacité. 40
208. Espaces vectoriels normés, applications linéaires continues. Exemples. 41
214. Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie. 43
215. Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications. 44
218. Applications des formules de Taylor. 46
219. Extremums : existence, caractérisation, recherche. Exemples et applications. 48
220. Equations différentielles $X' = f(X, t)$. Exemples d'étude des solutions en dimension 1 et 2. 50
221. Equations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications. 50
223. Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications. 51
224. Exemples de développements asymptotiques de suites et de fonctions. 53
226. Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations. 55
228. Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications. 56
229. Fonctions monotones. Fonctions convexes. Exemples et applications. 56
230. Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des suites numériques. Exemples. 57
233. Méthodes itératives en analyse numérique matricielle 59

236. Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables. 61
239. Fonctions définies par une intégrale dépendant paramètre. Exemples et applications. 62
243. Convergence des séries entières, propriétés de la somme. Exemples et applications. 63
246. Séries de Fourier. Exemples et applications. 65
250. Transformation de Fourier. Applications. 67
260. Espérance, variance et moments d'une variable aléatoire. 68
264. Variables aléatoires discrètes. Exemples et applications. 70
Bibliographie 72

Introduction

Voici la liste des mes méta-plans pour les leçons de mathématiques de l'option D. Ils contiennent les grandes lignes de ce que je comptais mettre dans mes leçons le jour de l'oral, les références permettant de construire ce plan et deux développements référencés. J'indique pour certaines parties la référence plus ou moins précise d'où je la tire entre crochets. Pour six des leçons, je n'ai pas de plan ; à savoir les leçons 183, 220, 221, 228, 229 et 250. Pour ces leçons, vous trouverez néanmoins mes développements. J'espère que ce document vous aidera à élaborer vos propres plans !

104. Groupes finis. Exemples et applications

Plan :

I/Définitions [Ulmer]

1) Ordres

→ Définition d'un groupe fini (+ exemple S_n ou $\mathbb{Z}/n\mathbb{Z}$), définition de l'ordre d'un élément (+ exemple : ordre d'une transposition)
→ Définition de l'exposant, exposant fini
→ Théorème de Burnside (+ contre exemple quand on est pas dans $GL_n(\mathbb{C})$ $\boxed{\text{DEV1}}$

2) Indices et théorème de Lagrange

→ Définition de l'indice d'un groupe + exemple + notation
→ Prop : $|G| = [G : H]|H|$ puis théorème de Lagrange + contre exemple à la réciproque (A_4 n'a pas de sous groupe d'ordre 6)
→ Appli : L'ordre d'un élément divise l'ordre du groupe
→ Appli : Si G est d'ordre premier alors il est cyclique

3) Actions de groupe

→ Définition d'une action de groupe, d'une orbite, d'un stabilisateur + relation orbite-stabilisateur
→ Prop : Formule des classes et formule de Burnside
→ Appli : Théorème de Cauchy
→ Appli : Une démonstration de la réciprocité quadratique [H2G2]
→ Appli : Nombre de coloriage du cube avec trois couleurs

II/Groupes abéliens [Com]

1) Groupes cycliques

→ Définition d'un groupe cyclique + ex ; définition d'un générateur + ex
→ Prop : G et G' cycliques sont isomorphes ssi ils ont même ordre (donc G est cyclique d'ordre $n \Rightarrow G \simeq \mathbb{Z}/n\mathbb{Z}$)
→ Conséquence : Un groupe cyclique d'ordre n a $\varphi(n)$ générateurs
→ Prop : Réciproque au théorème de Lagrange dans le cas des groupes cycliques + ex sous groupes de $\mathbb{Z}/\mathbb{Z}$ + appli $n = \sum_{d|n} \varphi(d)$

2) Structure des groupes abéliens finis

→ Théorème chinois
→ Décomposition en facteurs invariants + ex

III/Groupes non abéliens [Ulm] [Per]

1) Sylow

→ Définition d'un p-groupe et d'un p-Sylow
→ Théorèmes de Sylow
→ Prop : Si il y a un unique p-Sylow il est distingué

→ Applis : Un groupe d'ordre 63 n'est pas simple / un groupe d'ordre 15 est isomorphe à $\mathbb{Z}/15\mathbb{Z}$

2) Groupe symétrique

→ Définiton de S_n

→ Prop : Décomposition en cycles à supports disjoints + ex + calcul de l'ordre d'une permutation à partir de la décomposition

→ Définition de la signature et de A_n

→ Prop : A_n est engendré par les 3-cycles + A_n est simple pour $n \geqslant 5$ $\boxed{\text{DEV2}}$

3) Eventuellement parler des groupes diédraux

Références : Combes [Com], Ulmer [Ulm], Perrin [Per], H2G2 [H2G2] et XENS algèbre 2 (pour Burnside) [FGNal2]

Développements :

→ A_n est simple pour $n \leqslant 5$ [Ulm p 53]

→ Théorème du Burnside [FGNal2 p 185]

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

Plan :

I/Le groupe symétrique

1) Définitions

- → Définition de $S(X = \text{ensemble})$
- → Prop : $|X| = |Y| \Rightarrow S(X) \simeq S(Y)$ d'où la définition de S_n
- → Prop : Cardinal et centre de S_n (réduit à id pour $n \geqslant 3$)
- → Lien avec les actions de groupe + théorème de Cayley

2) Cycles

- → Définition du support d'une permutation + prop : quand les supports sont disjoints les permutations commutent
- → Définition d'un cycle + cas particulier d'une transposition
- → Prop : Décomposition en cycles à supports disjoints (+ lien avec les orbites de l'action de $< \sigma >$ sur $[\![1, n]\!]$)
- → Définition du type d'une permutation + calcul de l'ordre d'une permutation selon son type
- → Prop σ et σ' sont conjuguées ssi elles ont le même type

3) Générateurs

- → Props : Les transpositions, $\{(1,i)|i\}$ et $\{(i,i+1)|i\}$ engendrent S_n

II/Le groupe alterné

1) Signature

- → Définition de la signature + prop : c'est un morphisme de groupes + ex de calcul
- → Définition d'une permutation paire/impaire

2) A_n

- → Définition du groupe alterné A_n
- → Props : Cardinal de A_n + il est distingué en tant que noyau d'un morphisme
- → Prop : Les 3-cycles engendrent A_n
- → Appli : A_n est simple pour $n \geqslant 5$ $\boxed{\text{DEV1}}$
- → Rq : Discuter les cas pour $n \leqslant 5$

III/Applis

1) Déterminant [GouAl p 134]

- → Définition d'une forme alternée/antisymétrique (+ c'est la même chose en caractéristique $\neq 2$)
- → Caractérisation de l'antisymétrie avec les permutations
- → Définition du déterminant + formule avec la somme sur les permutations

2) Polynômes symétriques

- → Définition polynômes symétriques (élémentaires)
- → Prop et appli du [GouAl p 78]

3) Groupes d'isométries

- → Définition d'un groupe d'isométries
- → Calcul du groupe des isométries du tétraèdre et du cube $\boxed{\text{DEV2}}$
- → Appli : Nombre de coloriages du cube avec trois couleurs

Références : Ulmer [Ulm], Perrin [Per], Gourdon algèbre [GouAl], H2G2 [H2G2]

Développements :

→ A_n est simple pour $n \leqslant 5$ [Ulm p 53]
→ Groupe des isométries du cube [H2G2 p 365]

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

Plan :

Cadre : E est un espace vectoriel de dimension n sur le corps $\mathbb{K}$.

I/Groupe linéaire / spécial linéaire
1) GL et SL

- → Définition de $GL(E)$ + prop : c'est un groupe
- → Définition de $GL_n(\mathbb{K})$ + isomorphisme entre $GL(E)$ et $GL_n(\mathbb{K})$ via le choix d'une base
- → Prop : $u \in GL(E)$ ssi u est injective ssi u est surjective ssi $\det(u) \neq 0$ ssi u envoie une base sur une base + C'est faux en dimension infinie (dans $\mathbb{R}[X]$, $P \mapsto XP$ est injective mais pas bijective et $P \mapsto P'$ est surjective mais pas bijective)
- → Prop : Le déterminant est un morphisme de groupes
- → Définition de $SL(E)/SL_n(\mathbb{K})$ comme noyau du déterminant

2) Générateurs

- → Définitions d'une dilatation + ex
- → Définitions d'une transvection + ex
- → Prop : $SL(E)$ est engendré par les transvections et $GL(E)$ par les transvections et dilatations $\boxed{\text{DEV1}}$
- → Appli : Algo du pivot de Gauss (+ applis du pivot de Gauss)
- → Appli : Centre de $GL_n(\mathbb{K}) = \{$ homothéties $\}$ et centre de $SL_n(\mathbb{K}) = \{\lambda I_n | \lambda^n = 1\}$

3) Topologie

- → Ici, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ muni de la topologie induite par la norme subordonnée à la norme euclidienne
- → Prop : $GL(E) =$ ouvert dense de $L(E)$
- → Appli : $\chi_{AB} = \chi_{BA}$
- → Prop : Si $\mathbb{K} = \mathbb{C}$ alors $SL(E)$ et $GL(E)$ sont connexes par arcs $\boxed{\text{DEV1}}$ + rq : $GL(E)$ pas connexe si $\mathbb{K} = \mathbb{R}$

II/D'autres sous groupes de $GL(E)$
1) Sous groupes finis

- → Définition d'une matrice de permutation + ex
- → Prop : $\sigma \mapsto M_\sigma$ est un morphisme de groupes
- → Théorème de Cayley + appli : G est un groupe de cardinal $n \Rightarrow G \simeq$ sous groupe de $GL_n(\mathbb{K})$
- → Prop : Cardinal de $GL_n(\mathbb{F}_p)$ + appli : exhiber un p-Sylow dans $GL_n(\mathbb{F}_p)$ + csqc : existence d'un p-Sylow dans tout groupe de cardinal divisible par p [Per]
- → Théorème de Burnside $\boxed{\text{DEV2}}$

  + contre-ex : si $\mathbb{K} = \mathbb{F}_2(X)$ alors $\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} | a \in K\}$ est un sous groupe infini de $GL_2(\mathbb{K})$ mais est d'exposant fini

2) $O(q)$

- → Ici, $\mathbb{K}$ est de caractéristique différente de 2 et $q =$ forme quadratique définie positive sur E
- → Définition de $O(q)$ + prop : déterminant d'un élément de $O(q)$ d'où définition de $SO(q)$
- → Définition d'une symétrie orthogonale u + prop : $\exists E^+ \oplus E^-$ tels que $u_{|E^+} = id_{|E^+}$ et $u_{|E^-} = id_{E^-}$
- → Définition réflexion orthogonale / renversement orthogonal

- → Théorème de Cartan Dieudonné + cor : $SO(q)$ est engendré par les renversements si $n \geqslant 3$

3) Cas de $O_n(\mathbb{R})$

- → Ici, $E = \mathbb{R}$ ev avec la norme euclidienne
- → Th : Réduction orthonormée des éléments de $O_n(\mathbb{R})$
- → Cor : SO_2 est commutatif
- → Appli : $SO_n(\mathbb{R})$ est connexe par arcs
- → Th : $O_n(\mathbb{R})$ est compact
- → Théorème de décomposition polaire + appli : $GL_n(\mathbb{R})$ a deux composantes connexes + appli : calcul de l'enveloppe convexe de $O_n(\mathbb{R})$

Références : Szpirglas [Szp] (on peut faire quasi toute la leçon avec), Perrin [Per] (pour les histoires de p-Sylow), XENS algèbre 2 [FGNal2] (pour les développements), Mneimné-Testard [MT] (pour la topologie)

Développements :

- → Théorème de Burnside [FGNal2 p 185]
- → Générateurs de GL(E) et SL(E) et applications à la connexité [FGNal2 p 177]

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

Idée de défense de plan : On est contents quand on connaît un ensemble de générateurs d'un groupe car cela permet souvent de montrer des propriétés sur ce groupe en les montrant d'abord sur les générateurs puis en espérant qu'elles passent à tout le groupe.

Plan :

Intro [Ulm]

- → Définitions groupe engendré, partie génératrice, notation $<>$ + ex : le groupe dérivé $D(G)$ est le sous groupe de G engendré par les commutateurs
- → Prop : $< A >$ = l'ensemble des mots écrits comme produits d'éléments de A et d'in verses d'éléments de A

I/Groupes abéliens

1) Groupes monogènes et cycliques

- → Définition groupe monogène et groupe cyclique + ex $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$
- → Prop : Si G est de cardinal premier, il est cyclique + ctex à la réciproque
- → Prop : Le sous groupe des inversibles d'un corps fini est cyclique
- → Prop : G est monogène $\Rightarrow$ G est isomorphe à $\mathbb{Z}$ ou à un $\mathbb{Z}/n\mathbb{Z}$
- → Caractérisation des générateurs de $\mathbb{Z}/n\mathbb{Z}$ (donc de ceux des groupes cyclique) + csqc : y en a $\varphi(n)$
- → Appli : Aut($\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/n\mathbb{Z})^*$ donc est de cardinal $\varphi(n)$

2) Groupes abéliens finis

- → Théorème de structure des groupes abéliens finis + appli [Com p 66-68]

II/Groupe symétrique [Ulm]

- → Définition de S_n, de la signature et de A_n
- → Prop : S_n est engendré par les cycles à supports disjoints
- → Appli : Calcul facile de l'ordre d'une permutation via son type
- → Prop S_n est engendré par les transpositions
- → Appli : Calcul facile de la signature d'une permutation
- → Prop : S_n est aussi engendré par les $(1, i)$ ou par les $(i, i + 1)$
- → Prop : A_n est engendre par les 3-cycles
- → Appli : A_n est simple pour $n \geqslant 5$ $\boxed{\text{DEV1}}$ + rq pour les cas où $n \leqslant 4$

III/Autour du groupe linéaire

1) $GL(E)$ et $SL(E)$

- → Définition $GL(E)$ et $SL(E)$ pour E = ev de dimension n sur un corps $\mathbb{K}$
- → Définitions de transvection et dilatation
- → Prop : Les transvections engendrant $SL(E)$ et transvections et dilatations engendrent $GL(E)$ + appli connexité de $SL(E)$ $\boxed{\text{DEV2}}$
- → Appli : Calcul des centres de $GL(E)$ et de $SL(E)$
- → Appli : Pivot de Gauss

2) $O(E)$ et $SO(E)$

- → Ici, E est un $\mathbb{R}$-ev avec la norme euclidienne
- → Définition de $O(E)$ et $SO(E)$
- → Définition de symétrie orthogonale, réflexion, renversement
- → Théorème de Cartan-Dieudonné + cor : si $u \in SO(E)$ et $n \geqslant 3$ alors u est produit de moins de n renversements.
- → Appli : $SO_3(\mathbb{R})$ est simple et $SO_n(\mathbb{R})$ est connexe par arcs [FGNal3 p 63-69]

Références : Ulmer [Ulm], Combes [Com], Perrin [Per], XENS algèbre 2 [FGNal2], XENS algèbre 3 [FGNal3]

Développements :

→ A_n est simple pour $n \leqslant 5$ [Ulm p 53]
→ Générateurs de GL(E) et SL(E) et applications à la connexité [FGNal2 p 177]

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

Plan :

Cadre : On note $x \equiv y(n)$ si $x - y \in n\mathbb{Z}$.

I/Structures et $\mathbb{Z}/n\mathbb{Z}$ [RB]

1) Groupe

- → Prop : Les sous groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ (tous commutatifs donc distingués)
- → Prop : $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif et même cyclique dont les générateurs sont les éléments premiers avec n
- → Prop : Tout groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ + ex $\mathbb{U}_n$
- → Prop : Calcul des sous groupes de $\mathbb{Z}/n\mathbb{Z}$ + ex avec $\mathbb{Z}/6\mathbb{Z}$

2) Anneau

- → Prop : Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$
- → Prop : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif
- → Prop : Ses inversibles sont les éléments premiers à n + calcul effectif de l'inverse via Bézout + ex
- → Csqc : $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier
- → Definition de l'indicatrice d'Euler φ + valeur pour les puissances d'un nombre premier + rq : $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$

3) Morphismes

- → Lemme puis théorème chinois
- → Appli : Résolution de systèmes de congruence [GouAl]
- → Appli : $n \wedge m = 1 \Rightarrow (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/nm\mathbb{Z})^*$
- → Csqc : φ est multiplicative + calcul de $\varphi(n)$ pour n quelconque
- → Prop : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$
- → Théorème de structure des groupes abéliens finis [Com]

II/Arithmétique

1) Primalité

- → Théorème d'Euler et petit théorème de Fermat
- → Rq : la réciproque de Fermat est fausse (nombres de Carmichael)
- → Critère de "primalité" de Fermat

2) Equations diophantiennes

- → Définition équation diophantienne [Com]
- → Ex : $ax + by = c$ a une solution ssi $a \wedge b | c$ + ex de résolution avec Gauss et Bézout
- → Grand théorème de Fermat (admis)
- → Théorème de Chevalley-Warning [Ser] + application EGZ $\boxed{\text{DEV1}}$

3) Carrés

- → Ici, $n = p \in \mathbb{P}$
- → Définition du symbole de Legendre
- → Prop diverses du symbole de Legendre (multiplicativité...)
- → Appli : -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ ssi $p = 2$ ou $p \equiv 1(4)$ d'où théorème des deux carrés [Per p 57]
- → loi de réciprocité quadratique

4) Cryptographie (attention, pour les deux premiers, je ne connais pas de référence écrite pratique)

- → Identification de Fiat Shamir : $n = pq$ avec $p, q \in \mathbb{P}$. Alice connaît ses identifiants $s_1, ..., s_k$. Elle envoie les $v_i = s_i^2 \bmod n$ à Bob. Bob lui envoie $a_1, ..., a_k \in \{0, 1\}$. Alice lui envoie $y = s_1^{a_1} \times ... \times s_k^{a_k} \mod n$. Bob vérifie alors que $y^2 = v_1^{a_1}...v_k^{a_k} \mod n$. Ainsi, Bob a bien vérifié l'identité d'Alice sans que cette dernière ne lui envoie ses vrais identifiants (qui doivent rester secrets). Quelqu'un voulant usurper l'identité d'Alice doit calculer des racines carrées modulo n (difficile)

→ Cryptosystème de ElGamal : G = groupe cyclique ; g = générateur de G d'ordre q connu de tous. Clé privée = $x \in [\![1, q-1]\!]$; clé publique = $h = g^x$. Pour envoyer un message m, Bob choisit une clé éphémère $k \in [\![1, q-1]\!]$ et envoie le couple $c_1 = g^k$, $c_2 = h^k m$. Alice peut facilement déchiffre en calculant $(c_1^x)^{-1} c_2 = m$. Un espion pour trouver la clé privée et déchiffrer doit calculer un logarithme discret. C'est difficile par exemple si $G = (\mathbb{F}_{p^n})^*$.

→ Cryptosystème RSA [GouAl]

III/Polynômes irréductibles

1) Irréductibilité sur $\mathbb{Z}$

→ Critère d'Eisenstein + ex

→ Critère de réduction modulo p + ex

2) Factorisation

→ Définition des $\mathbb{F}_q$ comme corps de décomposition

→ Algorithme de Berlekamp $\boxed{\text{DEV2}}$

Références : OA [OA], Combes [Com], Risler-Boyer [RB], Serre [Ser], Gourdon algèbre [GouAl], Zavidovique [Zav]

Développements :

→ Algorithme de Berlekamp [OA p 244]

→ Application Erdös-Ginzburg-Ziv [Zav p 32]

121. Nombres premiers. Applications.

Plan :

I/Généralités

1) La base

- → Définition : nombre premier + ex et contre ex (1 n'est pas premier). On note $\mathbb{P}$ leur ensemble.
- → Définition : nombres premiers entre eux
- → Calcul du pgcd avec Euclide
- → Théorème de Bézout, théorème de Gauss + appli : $p \in \mathbb{P}$ et $k \in [\![1, p-1]\!] \Rightarrow p|\binom{p}{k}$

2) Décomposition

- → Prop : Si $n \geqslant 2$, il existe $p \in \mathbb{P}$ tel que $p|n$
- → Csqc : Déconposition en facteurs premiers
- → Appli : EGZ $\boxed{\text{DEV1}}$

3) Répartition des nombres premiers

- → Prop : $\mathbb{P}$ est infini
- → Théorème de Dirichlet (admis)
- → Théorème des nombres premiers (admis)

4) Indicatrice d'Euler

- → Définition de l'indicatrice d'Euler φ + multiplicativité
- → Calcul explicite de $\varphi(n)$ + $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$
- → Csqc : Théorème d'Euler puis de Fermat
- → Appli : Critère de primalité de Fermat
- → Appli : Fonctionnement de RSA

II/Applis en théorie des groupes

1) p-groupes

- → Prop : Si G est de cardinal premier alors il est cyclique
- → Prop : Le centre d'un p-groupe est non trivial
- → Prop : Un groupe d'ordre p^2 est abélien

2) p-Sylow

- → Définition d'un p-Sylow
- → Théorèmes de Sylow + appli : un groupe d'ordre 63 n'est pas simple

III/Corps finis

1) Construction et propriétés

- → Définition : caractéristique d'un corps + prop : la caractéristique p d'un corps fini est première et son cardinal est une puissance de p
- → Th : Existence et unicité à isomorphisme près d'un corps à p^n éléments (pour $p \in \mathbb{P}$) noté $\mathbb{F}_{p^n}$
- → Prop : $\mathbb{F}_{p^n}^*$ est cyclique
- → Appli : Théorème de Chevalley-Warning + appli : EGZ (dont l'énoncé a déjà été donné)

2) Polynômes sur les corps finis [Per]

- → Critère d'Eisenstein + ex
- → Critère de réduction modulo p + ct ex : $X^4 + 1$ est réductible modulo tous les p premiers mais est irréductible dans $\mathbb{Q}$
- → Algorithme de Berlekamp $\boxed{\text{DEV2}}$

3) Carrés

- → Prop : Tout élément de $\mathbb{F}_{2^n}$ est un carré

→ Définition : symbole de Legendre + prop de base
→ Lois de réciprocité quadratique

Références : Demazure [Dem], Serre [Ser], Gourdon algèbre [GouAl], OA [OA], Perrin [Per]

Développements :
→ Algorithme de Berlekamp [OA p 244]
→ Application Erdös-Ginzburg-Ziv [Zav p 32]

123. Corps finis. Applications.

Plan :

Cadre : Un corps est un anneau commutatif non nul A tel que $A^* = A\backslash\{0\}$. Il est dit fini si $|A|$ est fini.

I/Corps finis et structures

- → Rq : il existe des corps finis car :
- → Prop : $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi $\mathbb{Z}/p\mathbb{Z}$ est intègre ssi $p \in \mathbb{P}$
- → Dans la suite, K est un corps fini : on en cherche les propriétés

1) Caractéristique et cardinal

- → $c : \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & K \\ k & \longmapsto & k.1_K \end{array} \right.$ est un morphisme d'anneaux de noyau $p\mathbb{Z}$ où p est premier
- → Définition de la caractéristique + rq : $\mathbb{Z}/p\mathbb{Z}$ est le sous corps premier de K
- → Prop : K est un $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel de dimension finie
- → Csqc : $K = p^n$ + rq : il n'existe donc pas de corps à 6 éléments

2) Groupe des inversibles

- → K^* est cyclique + ex
- → Rq : En fait, tout sous groupe de K^* est cyclique
- → Rq : En fait, tout sous groupe fini de L^* est cyclique même si L est un corps infini

3) Automorphismes de K

- → Définition de l'automorphisme de Frobenius φ + cas particulier : si $K = \mathbb{Z}/p\mathbb{Z}$ alors $\varphi =$ identité
- → Prop : Si $Q \in K[X]$, $Q(X^p) = Q(X)^p$ ssi les coefficients de Q sont dans $\mathbb{Z}/p\mathbb{Z}$
- → Prop : Les deux pros de [Dem p 211 et 212]
- → Csqc : $Aut(K) =< \varphi >\simeq \mathbb{Z}/n\mathbb{Z}$

4) Existence et sous corps

- → Th : pour tout $p \in \mathbb{P}$, pour tout $n \geqslant 1$, il existe un unique (à isomorphisme près) corps de cardinal p^n, noté $\mathbb{F}_{p^n}$
- → Construction de ce corps comme quotient de $\mathbb{Z}/p\mathbb{Z}[X]$ par un polynôme irréductible de degré n + ex : construction de $\mathbb{F}_4$
- → Prop : $\mathbb{F}_{p^d}$ est un sous corps de $\mathbb{F}_{p^n}$ ssi $d|n$ + ex : calcul des sous corps de $\mathbb{F}_8$

II/Polynômes sur les corps finis

1) Polynômes sur $\mathbb{F}_q$ avec $q = p^n$

- → Prop : Critère de réduction modulo p pour décider l'irréductibilité dans $\mathbb{Z}[X]$ (cela motive le fait de vouloir connaître les polynômes irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$) + ex + ct-ex : X^4+1 est irréductible sur $\mathbb{Z}$ mais réductible modulo tous les p [Per p 78]
- → Prop : [Per p 78] + ex
- → $X^{q^n} - X = \prod_{d|n} \prod_{P \in P_d} P$ pour $P_d = \{$polynômes irréductibles unitaires de degré $d\}$
- → Prop : Critère de Rabin pour l'irréductibilité des polynômes sur $\mathbb{F}_q$

2) Algorithme de factorisation

- → Algorithme de Berlekamp $\boxed{\text{DEV1}}$
- → Expliquer comment cet algo permet de factoriser n'importe quel polynômes

3) Equations polynomiales

- → Théorème de Chevalley-Warning + appli EGZ $\boxed{\text{DEV2}}$
- → Rq : Cas où les polynômes dans Chevalley-Warning ont un zéro non trivial

III/Corps finis et arithmétique

1) Primalité

→ Critère de primalité de Fermat et de Miller Rabin

2) Carrés dans $\mathbb{F}_p$ pour $p \in \mathbb{P}$

→ Rq : Tout élément de $\mathbb{F}_{2^n}$ est un carré
→ Définition du symbole de Legendre + prop + ex de calcul
→ Prop : -1 est un carré modulo p ssi $p = 2$ ou $p \equiv 1(4)$
→ Appli : Il existe une infinité de nombres premiers congrus à 1 modulo 4
→ Prop : Loi de réciprocité quadratique

3) Cryptographie (voir la leçon 120)

→ Identification Fiat-Shamir
→ Cryptosystème d'ElGamal

Références : OA [OA], Serre [Ser], Zavidovique [Zav], Perrin [Per], Demazure [Dem]

Développements :

→ Algorithme de Berlekamp [OA p 244]
→ Théorème de Chevalley-Warning [Ser p 12]

141. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Plan :

Cadre : A est un anneau commutatif unitaire factoriel et K est un corps

I/Polynômes irréductibles [Per]

1) Définition et exemples

- → Rappel : A est factoriel $\Rightarrow A[X]$ est factoriel et $A[X]^* = A^*$
- → Définition de "$P \in A[X]$ est irréductible"
- → Ex : $2X$ est irréductible dans $\mathbb{Z}[X]$ mais pas dans $\mathbb{Q}[X]$
- → Ex : Tout polynôme de degré 1 de $K[X]$ est irréductible

2) Irréductibilité et racines

- → Prop : Si $P \in K[X]$ admet une racine dans K alors il est réductible + ex
- → Csqc : P est irréductible $\Rightarrow P$ n'a pas de racine dans K
- → Théorème de d'Alembert-Gauss
- → Prop : Si $P \in K[X]$ est de degré 2 ou 3 alors P est irréductible ssi il n'a pas de racine dans K + ex avec $X^2 + 1$ dans $\mathbb{R}[X]$
- → Ct-ex : Ça ne marche plus pour les polynômes de degré plus haut : $(2X+1)^2$ n'a pas de recine dans $\mathbb{Z}$ mais y est réductible

3) Critères d'irréductibilité

- → Définition du contenu d'un polynôme + prop : il est multiplicatif
- → Définition d'un polynôme primitif
- → Th : A est factoriel ; $K = \mathrm{Frac}(A)$. Les irréductibles de $A[X]$ sont les irréductibles de A + les polynômes non constants, primitifs et irréductibles dans $K[X]$
- → Prop : $P \in K[X]$ est irréductible ssi $K[X]/(P)$ est un corps
- → Critère d'Eisenstein + ex
- → Critère de réduction modulo p + ex + ct-ex $X^4 + 1$ [Per p 78]

II/Adjonction de racines [Per]

1) Extensions de corps, éléments algébriques

Soit L/K une extension de K

- → Prop : L est un K espace vectoriel + définition degré d'une extension + notation $[\ :\ ]$ + ex $[\mathbb{C} : \mathbb{R}] = 2$
- → Théorème de la base télescopique + appli : multiplicativité des degrés
- → Définitions : élément transcendant, élément algébrique + ex
- → Prop : x est algébrique sur K ssi $K(X) = K[X]$ ssi $\dim_K K[x]$ est finie. Dans ce cas on peut donner une base de $K[x]$ et $[K[x] : K] =$ degré du polynôme minimal de x
- → Appli : $\{x \in L | x \text{ est algébrique sur } K\}$ est un sous corps de L

2) Corps de rupture

- → Définition : corps de rupture + ex $\mathbb{Q}(\sqrt[3]{2})$ pour $X^3 - 2$
- → Th : Existence et unicité à isomorphisme près du corps de rupture pour tout polynôme irréductible sur K
- → Appli : $P \in k[X]$ de degré $n > 0$. P est irréductible ssi P n'a pas de racines dans les extensions K de k telles que $[K : k] \leqslant \frac{n}{2}$

3) Corps de décomposition

- → Définition : corps de décomposition + ex
- → Prop : Existence et unicité à isomorphisme près du corps de décomposition
- → Appli : Construction "du" corps à p^n éléments comme corps de décomposition + ex

III/Polynômes irréductibles sur les corps finis ($p \in \mathbb{P}, q = p^r$) [Goz à partir de p 87]

→ Prop : Factorisation de $X^{q^n} - X$ [FG p 189]
→ Appli : Critère d'irréductibilité de Rabin
→ Définition de la fonction de Möbius + quelques prop
→ Dénombrement des polynômes irréductibles de $\mathbb{F}_q$ $\boxed{\text{DEV1}}$
→ Algorithme de Berlekamp $\boxed{\text{DEV2}}$

Références : OA [OA], Perrin [Per], Gozard [Goz], Francinou [FG]

Développements :

→ Algorithme de Berlekamp [OA p 244]
→ Nombre de polynômes sur $\mathbb{F}_q$ [FG p 189]

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

Plan :

Prérequis : notions d'action, d'une orbite, d'un stabilisateur.

I/Action par translation

→ Définition de l'action A de GL_n sur $M_{n,m}$ à gauche
→ Définition d'une matrice échelonnée
→ Prop : Deux matrices sont dans la même orbite pour A ssi elles ont même noyau + toute matrice est dans l'orbite d'une matrice échelonnée
→ Pivot de Gauss et ses applications (calcul de rang, déterminant, dimension, résolution d'équations linéaires...)
→ Rq : On a une action similaire à droite

II/Action de Steinitz

1) Définition

→ Définition : c'est l'action $\left\{ \begin{array}{lll} (GL_n \times GL_m) \times M_{n,m} & \longrightarrow & M_{n,m} \\ (P,Q), A & \longmapsto & PAQ^{-1} \end{array} \right.$
→ Rq : Les orbites sont les classes d'équivalence
→ Rq : Elle traduit un changement de base : A et B sont dans la même orbite ssi ce sont les matrices du même endomorphisme dans deux bases

2) Caractérisation des orbites par le rang

→ Prop : Si deux matrices sont équivalents alors elles ont même rang
→ Prop : Si M est de rang r, M est équivalente à la matrice $J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$
→ Conclusion : A et B sont équivalentes (cad sont dans la même orbite) ssi $rg(A) = rg(B)$ $\boxed{\text{DEV1}}$ + les orbites sont donc paramétrées par le rang $\in [\![0, \min(n,m)]\!]$
→ Appli : $rg(A) = rg({}^tA)$ [OA p 155-156]
→ Appli : Indépendance de la notion d'équivalence para rapport au corps [OA p 155-156]
→ Appli : Dénombrement des matrices de rang r sur un corps fini $\boxed{\text{DEV1}}$

III/Action par conjugaison

1) Définition

→ Définition : c'est l'action $\left\{ \begin{array}{lll} (GL_n)^2 \times M_n & \longrightarrow & M_n \\ P, A & \longmapsto & PAP^{-1} \end{array} \right.$
→ Rq : Deux matrices sont dans la même orbite sont dites semblables

2) Caractérisation de l'orbite

→ Prop : Deux matrices sont semblables ssi elles ont même valeurs propres avec mêmes multiplicités (elles caractérisent les orbites)
→ Prop : Le polynôme caractéristique caractérise donc l'orbite
→ Prop : La trace, le déterminant et le polynôme minimal sont des invariants de similitude. Attention aucun des trois objets précédents ne caractérise l'orbite + ct-ex

3) Action sur $O_n(\mathbb{R})$

→ Prop : Réduction des endomorphismes normaux $\boxed{\text{DEV2}}$
→ Appli : Réduction des matrices réelles symétriques (dans chaque orbite de l'action par conjugaison de $O_(\mathbb{R})$ sur $S_n(\mathbb{R})$ il y a donc une matrice diagonale)

IV/Action par congruence

1) Définition

→ Définition : c'est l'action $\left\{ \begin{array}{lll} GL_n \times S_n & \longrightarrow & S_n \\ P, S & \longmapsto & PS^tP \end{array} \right.$

→ Rq : Deux matrices sont dans la même orbite ssi ce sont les matrices de la même forme quadratique dans deux bases différentes

2) Classification

→ Cas complexe : deux matrices sont dans la même orbite ssi elles sont dégénérées de la même façon
→ Cas réel : théorème d'inertie de Sylvester
→ Cas sur un corps fini : deux orbites

Références : H2G2 [H2G2] (on peut quasi tout faire avec celui là), Gourdon algèbre [GouAl], OA [OA]

Développements :

→ Nombre de matrices de rang r [H2G2 p 151]
→ Réductions des endomorphismes normaux [GouAl p 260]

151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

Plan :

I/Dimension
1) Familles de vecteurs

- → Définitions : famille libre, liée, génératrice, base + exs
- → Prop : Toute sur famille d'une famille liée est liée / toute sous famille d'une famille libre est libre

2) Dimension finie

- → Définition : Un ev est de dimension finie s'il possède une famille génératrice finie
- → Prop : Si E est de dimension finie ; si (L = famille libre) $\subset$ (G = famille génératrice) alors il existe une base B telle qu $L \subset B \subset G$
- → Théorème de la base incomplète

3) Notion de dimension

- → Prop : Dans un ev de dimension finie, toutes les bases ont le même cardinal. On en déduit la bonne définition de la dimension = cardinal commun de ces bases + exs
- → Prop : Dans un ev de dimension n, un e famille libre ou liée qui a n éléments est une base
- → Calcul pratique de la dimension d'un ev par Gauss (mise sous forme échelonnée)
- → Appli : Démonstrations par récurrence (par ex pour les résultats de réduction)
- → Appli : Algorithme de Berlekamp $\boxed{\text{DEV1}}$

4) Calculs de dimensions

- → Prop : Dimension d'un produit d'ev
- → Prop : Dimension de $L(E, F)$ et de E^*
- → Prop : Si F est un sev de E alors $\dim(F) \leqslant \dim(E)$
- → Prop : Formule de Grassmann

5) Cas particulier des extensions de corps

- → Définition du degré d'une extension de corps (c'est la dimension d'un ev particulier !)
- → Théorème de la base télescopique + appli : multiplicativité des degrés
- → Définition d'un élément algébrique (et du polynôme minimal)
- → Prop : a est algébrique sur k ssi $k[a]$ est de dimension finie et alors $[k[a] : k]$ = degré du polynôme minimal de a
- → Appli : L'ensemble des éléments algébriques sur k est un corps

II/Rang
1) Définition

- → Définition du rang d'une famille de vecteurs, d'une matrice, d'une application linéaire
- → Prop : $rg(f) = rg(\mathrm{Mat}(f))$
- → Théorème du rang
- → Appli : Si E et F sont deux ev de même dimension et $f \in L(E, F)$ alors f est surjective ssi f est injective ssi f est bijective
- → Autre appli : Polynômes interpolateurs de Lagrange

2) Calcul de rang

- → Prop : Le rang d'une matrice est égal à celui de sa transposée
- → Calcul effectif du rang par Gauss
- → Prop : Le rang d'une matrice est aussi la taille du plus grand mineur non nul extrait de celle ci

3) Rang et action de groupe

→ Si A est de rang r, A est équivalente à J_r
→ En fait A et B sont équivalents ssi elles ont même rang + appli : calcul du nombre de matrices de rang r $\boxed{\text{DEV2}}$
→ Prop : Nombre de classes d'équivalences selon le rang

Références : Grifone [Gri] (y a quasi tout ce qu'il faut), OA [OA] (pour développement), Perrin [Per] (pour les extensions de corps), Gourdon algèbre [GouAl], H2G2 [H2G2] (pour développement)

Développements :
→ Algorithme de Berlekamp [OA p 244]
→ Nombre de matrices de rang r [H2G2 p 251]

152. Déterminant. Exemples et applications.

Plan :

Cadre : $\mathbb{K}$ est un corps et E un $\mathbb{K}$ espace vectoriel de dimension n.

I/Définitions [GouAl]

1) Déterminant d'une famille de vecteurs

- → Définition d'une forme n-linéaire alternée / antisymétrique + prop : quand la caractéristique de K est différente de 2 c'est la même chose
- → Prop : L'ensemble des formes n-linéaires alternées est un $\mathbb{K}$ espace vectoriel de dimension 1. On nomme $\det_B$ l'unique telle forme qui prend la valeur 1 sur la base B
- → Expression du déterminant : $\det_B(x_1, ..., x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) x_{\sigma(1)} ... x_{\sigma(n)}$ $(\star)$
- → Prop : Changement de base : $\det_{B'}(x_1, ..., x_n) = \det_{B'}(B)\det_B(x_1, ..., x_n)$ + cas particulier si $B' = (x_1, ... x_n)$
- → Prop : Si $(x_1, ... x_n)$ est liée, son déterminant est nul. La réciproque est vraie.
- → Csqc : On ne change pas le déterminant en ajoutant à l'un des x_i une combinaison linéaire des autres

2) Déterminant d'un endomorphisme

- → Définition : Si f est un endomorphisme et $B = (e_1, ..., e_n)$ est une base, $\det_B(f) = \det_B(f(e_1), ..., f(e_n))$
- → Prop : Cette quantité ne dépend pas de la base B
- → Prop : Le déterminant de l'identité vaut 1. Le déterminant de f est nul ssi f n'est pas bijective
- → Prop : Déterminant d'une composée et d'un inverse

3) Déterminant d'une matrice carrée

- → Déf : Si $A \in M_n(\mathbb{K})$, le déterminant de A est le déterminant de l'endomorphisme qui lui est canoniquement associée
- → Prop : On retrouve toutes celles qui valent pour les endomorphismes + $\det(A) = \det({}^tA)$ (par la formule $\star$)

II/Calcul de déterminants [GouAl]

1) Théorie

- → Calcul brut avec $(\star)$ en $n \times n!$
- → Définition d'un mineur, cofacteur, comatrice
- → Prop : Développement selon une ligne ou une colonne (toujours en $n!$)
- → Appli : Calcul du déterminant d'une matrice triangulaire + $\det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det(A)$C (avec A, B, C des matrices
- → Prop : $A^t\mathrm{com}(A) = \det(A) I_n$
- → Méthode de l'élimination de Gauss pour le calcul des déterminants (en n^3)

2) Quelques déterminants particuliers

- → Prop : Déterminant de Vandermonde
- → Prop : Déterminant de Cauchy
- → Prop : Déterminant circulant + appli : suite de polygones $\boxed{\text{DEV1}}$

III/Applications en algèbre [GouAl]

1) Systèmes linéaires

- → Prop : Formules de Cramer + ex

2) Polynôme caractéristique

- → Définition du polynôme caractéristique

→ Prop : Etre une valeur propre équivaut à être racine du polynôme caractéristique
→ Th de Cayley Hamilton

3) Mesurer des choses

→ Interprétation du déterminant comme un volume
→ Prop : Inégalité de Hadamard + cas d'égalité
→ Déf : matrices et déterminants de Gram
→ Th de Muntz

IV/Applications en analyse [GouAn]

1) Régularité

→ Prop : Le déterminant est C^{∞} car polynomiale + différentielle du déterminant
→ Appli : Si $A, B \in M_n(\mathbb{R})$ sont $\mathbb{C}$ semblables alors elles sont $\mathbb{R}$ semblables

2) Changement de variables

→ Définition du jacobien
→ Prop : Changement de variable
→ Appli : John-Loewner $\boxed{\text{DEV2}}$

Références : Gourdon Algèbre [GouAl] (principalement), Gourdon Analyse [GouAn], XENS algèbre 3 [FGNal3]

Développements :

→ Ellipsoïde de John-Loewner [FGNal3 p 229]
→ Suite de polygones [Sans ref, trouvé sur le site de Théo Pierron]

153. Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications

Plan :

Cadre : u est un endomorphisme du $\mathbb{K}$ espace vectoriel E de dimension n. On note M_u sa matrice dans une certaine base. Rappel : λ est valeur propre de u si il existe $x \neq 0$ tel que $u(x) = \lambda x$.

I/Polynômes d'endomorphismes

1) Algèbre $\mathbb{K}[u]$

→ Définition du morphisme d'algèbre $\varphi(u) : \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[u] \subset L(E) \\ P & \longmapsto & P(u) \end{cases}$

→ Prop $\mathbb{K}[u]$ est une sous algèbre commutative de $L(E)$

→ Théorème de décomposition des noyaux + ex pour une symétrie et une projection

2) Polynôme minimal

→ Définition idéal des polynômes annulateurs I_u

→ Prop : Il est engendré par π_u (car $\mathbb{K}[X]$) puis définition du polynôme minimal

→ Appli : Calcul des puissances de u par $X_n = \pi_u(X)P + R$ donc $u^n = 0 + R(u)$ (donc chute du degré)

→ Appli : Calcul de l'inverse de u : $0 = \pi_u(u) = \sum_{i=0}^{n} a_i u^i = \sum_{i=k}^{n} a_i u^i$ où a_k est le premier a_i non nul. Si $k = 0$ on a $u^{-1} = \frac{-1}{a_0} \sum_{i=1}^{n} a_i u^i$

→ Prop $\mathbb{K}[u] \simeq \mathbb{K}[X]/(\pi_u)$ est de dimension $\deg(\pi_u)$ et une base en est $(id, u, u^2, ...u^{\deg(\pi_u)-1}$

→ Prop : λ est valeur propre ssi $\pi_u(\lambda) = 0$

→ Prop : Si F est un sous espace u-stable, $\pi_{u_{|F}} | \pi_u$

3) Polynôme caractéristique

→ Définition du polynôme caractéristique χ_u

→ Prop : $\deg(\chi_u) = n$ + coefficient dominant $= (-1)^n$ puis $(-1)^{n-1}\mathrm{tr}(u)$ ... puis $\det(u)$

→ Prop : λ est valeur propre ssi $\chi_u(\lambda) = 0$

→ Th de Cayley Hamilton don c $\pi_u | \chi_u$ (et d'ailleurs $\chi_u | \pi_u^n$)

→ Csqc : u est nilpotent ssi $\chi_u = (-1)^n X^n$

→ Prop : Si F est un sous espace vectoriel u-stable alors $\chi_{u_{|F}} | \chi_u$

II/Un outil pour la réduction

1) Diagonalisabilité

→ Prop : u est diagonalisable ssi π_u est scindé à racines simples ssi il existe $P \in I_u$ qui est scindé à racines simples ssi χ_u est scindé et pour toute valeur propre, sa multiplicité géométrique est égale à sa multiplicité algébrique.

→ Ex : Un projecteur est toujours diagonalisable

→ Csqc : Si F est u-stable et u est diagonalisable alors $u_{|F}$ aussi

→ Prop : Familles codiagonalisables

→ Appli : Théorème de Burnside

2) Trigonalisabilité

→ Prop : u est trigonalisable ssi χ_u est scindé ssi π_u est scindé ssi il existe $P \in I_u$ qui est scindé

→ Csqc : Si $\mathbb{K}$ est algébriquement clos alors tout le monde est trigonalisable

→ Prop : Si F est u-stable et u est trigonalisable alors $u_{|F}$ aussi

3) Réduction

→ Th : Décomposition de Dunford $\boxed{\text{DEV2}}$

→ Appli : Calcul de l'exponentielle matricielle avec Dunford (même si ce n'est pas efficace) (ça peut servir en equa diff)
→ Définition d'un endomorphisme normal
→ Th : Réduction des endomorphismes normaux $\boxed{\text{DEV2}}$
→ Appli : Réduction des matrices symétriques et antisymétriques réelles

Références : Gourdon Algèbre [GouAl], OA [OA], XENS algèbre 2 [FGNal2]

Développements :
→ Réduction de Dunford [GouAl p 193]
→ Réductions des endomorphismes normaux [GouAl p 259]

157. Endomorphismes trigonalisables. Endomorphismes nilpotents.

Plan :

Cadre : E est un $\mathbb{K}$ espace vectoriel de dimension n et u un endomorphisme de E

I/Outils

- → Définition d'une valeur propre, vecteur propre, sous espace propre / caractéristique
- → Définition du polynôme minimal π_u / caractéristique χ_u
- → Prop : λ est valeur propre ssi λ est racine de π_u ssi λ est racine de χ_u
- → Prop : Si F est u-stable alors $\chi_{u_{|F}} | \chi_u$ et $\pi_{u_{|F}} | \pi_u$
- → Appli : Démonstrations par récurrence possibles
- → Théorème de décomposition des noyaux (expliquer que si on a un polynôme annulateur de u, on peut décomposer E en somme directe de sous espaces u-stables et que si on concatène des bases de ces sous espaces, on obtient une base dans laquelle la matrice de u est diagonale par blocs cad simple)

II/Endomorphismes trigonalisables

1) Résultats classiques

- → Définition matrice / endo trigonalisable
- → Prop : u est trigonalisable ssi χ_u est scindé ssi π_u est scindé
- → Csqc : Si $\mathbb{K}$ est algébriquement clos, tout le monde est trigonalisable + ct-ex : dans $\mathbb{R}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ n'est pas trigonalisable
- → Appli : $\forall A \in M_n(\mathbb{C})$, $\det(e^A) = \exp(\mathrm{tr} A)$

2) Cotrigonalisbilité

- → Prop : Si u et v commutent, les sous espaces caractéristiques de u sont v-stables
- → Prop : Si u et v commutent et sont trigonalisables, ils sont cotrigonalisables
- → Prop : Même résultat pour une famille quelconque d'endomorphismes qui commutent entre eux
- → Appli : Si u et v commutent et sont trigonalisables, $u + v$ est trigonalisable

III/Endomorphismes nilpotents

1) Définition et caractérisations

- → Définition endo nilpotent + indice de nilpotence + ex
- → Prop : u est nilpotent ssi $\chi_u = (-1)^n X^n$ ssi il existe $p \in \mathbb{N}$ tel que $\pi_u = X^p$ ssi u est trigonalisable avec des zéros sur sa diagonale ssi u est trigonalisable et sa seule valeur propre est zéro
- → Attention : 0 est la seule valeur propre de u n'implique pas que u est nilpotent : ct-ex dans $M_n(\mathbb{R})$ avec $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$ dont le spectre est nul mais qui n'est pas nilpotente
- → Prop : Si la caractéristique de $\mathbb{K}$ n'est pas nulle, u est nilpotent ssi $\forall k \in \mathbb{N}^*$ on a $\mathrm{tr}(u^k) = 0$
- → Appli : Théorème de Burnside $\boxed{\text{DEV1}}$

2) Structure

- → Prop : L'ensemble N des nilpotents n'est pas un sev : $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \notin N$
- → Rq : En revanche si $u, v \in N$ commutent alors $u + v \in N$
- → Prop : $\mathrm{Vect}(N) = \mathrm{Ker}(\mathrm{tr})$ + structure de cône de N

3) Applications à la réduction

→ Prop : Décomposition de Dunford $\boxed{\text{DEV2}}$
→ Appli : Calcul de e^A
→ Théorème de Jordan

Références : Gourdon algèbre [GouAl], Grifone [Gri] (pour quelques exemples), XENS algèbre 2 [FGNal2]

Développements :

→ Théorème de Burnside [FGNal2 p 185]
→ Réduction de Dunford [GouAl p 193]

159. Formes linéaires et dualité en dimension finie. Exemples et applications.

Plan :

Cadre : E est un $\mathbb{R}$ ou $\mathbb{C}$ espace vectoriel de dimension n

I/Formes linéaires et hyperplans
1) Définition et exemples

- → Définition d'une forme linéaire + de E^*
- → prop : Si $(e_1, ..., e_n)$ est une base de E une forme linéaire est du type $\varphi : \sum x_i e_i \longmapsto \sum a_i x_i$ où $a_i = \varphi(e_i) \in \mathbb{K}$
- → Exs : formes linéaires coordonnées, trace, différentielle d'un fonction

2) Lien avec les hyperplans

- → Définition d'un hyperplan par la dimension + ex
- → Prop : $\varphi \in E^* \backslash \{0\} \Rightarrow \mathrm{Ker}(\varphi)$ est un hyperplan
- → Prop : Réciproquement, si H est un hyperplan, il existe une forme linéaire non nulle de noyau H
- → Prop : φ et ψ sont deux formes linéaires non nulles de même noyau ssi elles sont proportionnelles
- → Cor : $\{x | \sum x_i a_i\}$ avec $(a_1, ..., a_n) \neq 0$ est un hyperplan. D'ailleurs, tout hyperplan est de cette forme
- → Rq : Résoudre un système d'équations linéaires revient à calculer une intersection d'hyperplans
- → Illustration : Méthode de Kaczmarz $\boxed{\text{DEV1}}$

II/Dualité
1) Dual

- → Définition d'une base duale + notation e_i^* + ex de calcul $(X^k)^* : P \longmapsto \frac{P^{(k)}(0)}{k!}$ [Gri]
- → Prop $E \simeq E^*$ via le choix d'une base
- → Prop : Dans le cadre euclidien, le théorème de Riesz donne un isomorphisme entre E et E^* sans dépendance à une base
- → Prop : Cas de $M_n(\mathbb{R})$: $A \longmapsto \mathrm{tr}(AM)$ est un isomorphisme entre $M_n(\mathbb{R})$ et $M_n(\mathbb{R})^*$) $\boxed{\text{DEV1}}$
- → Applis : Prop sur les formes linéaires centrales + $GL_n(\mathbb{R})$ rencontre tout hyperplan de $M_n(\mathbb{R})$ $\boxed{\text{DEV1}}$

2) Bidual

- → Définition du bidual
- → Prop : Isomorphisme canonique entre E et E^{**}
- → Définition : bas antéduale
- → Ex : La base des polynômes de Lagrange avec les a_i comme points d'évaluation est la base antéduale de la base (φ_i) pour $i = 0..n$ où $\varphi_i : P \longmapsto P(a_i)$

III/Applications
1) Orthogonalité

- → Définition : $x \in E$ et $\varphi \in E^*$ sont orthogonaux si $\varphi(x) = 0$
- → Rq : Cette définition correspond à la définition classique dans le cadre euclidien (via Riesz)
- → Définition des deux orthogonaux

2) Formes linéaires indépendantes

- → Prop : Réduction de Gauss des formes quadratiques

→ Th des extrema liés + appli : diagonalisation des endomorphismes symétriques + appli : inégalité arithmético-géométrique

3) On peut éventuellement parler de transposée [GouAl]

Références : Gourdon algèbre [GouAl], XENS algèbre 1 [FGNal1], OA [OA], Grifone [Gri] (pour les calculs pratiques)

Développements :

→ Dual de $M_n(\mathbb{K})$ [FGNal1 p 329]

→ Méthode de Kaczmarz [Sans ref, trouvé sur le site de Théo Pierron]

162. Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

Plan :

I/Théorie générale des systèmes linéaires [Gri p 141-147]

1) Définition

→ Définition d'un système linéaire + représentation matricielle $Ax = b$

→ Définition d'un système compatible + le rang d'un système + ex : un système homogène $AX = 0$ est compatible

→ Prop : Un système est compatible ssi $b \in \mathrm{Im}(A)$ ssi b est engendré par les vecteurs colonnes de A

2) Cramer

→ Définition d'un système de Cramer ($= A \in GL_n(\mathbb{K})$) + prop : il admet une unique solution. Rq : on se place dans ce cas dans les parties II, III et IV

→ Th : Cette solution est donnée par les déterminants de Cramer + ex + complexité naïve en $n!$ (mais si on calcule les déterminants avec Gauss, on descend à $n \times n^3 = n^4$

3) Rouché-Fontené

→ théorème de Rouché-Fontené + ex + cas particulier des systèmes homogènes

II/Opérations élémentaires et pivot de Gauss [OA]

1) Opérations élémentaires

→ Définition : matrices élémentaires = matrices de dilatation, de transvection et de permutation

→ Prop : La multiplication à gauche (resp droite) de A par une matrice élémentaire revient à effectuer une opération sur les lignes (resp colonnes) de A

→ Th : $SL_n(\mathbb{K})$ est engendré par les matrices de transvection et $GL_n(\mathbb{K})$ par celle de transvection et dilatation + appli connexité de $SL_n(\mathbb{K})$ $\boxed{\text{DEV1}}$

2) Méthode de Gauss

→ Prop : $A \in M_n(\mathbb{K})$ de première colonne non nulle peut être transformée en $\begin{pmatrix} \alpha & *...* \\ 0 & A' \end{pmatrix}$ par multiplication à gauche par des matrices élémentaires

→ Algorithme de Gauss

→ Rq : Complexité en n^3 + attention quand les pivots sont petits on peut faire des grosses erreurs d'arrondi [Gri]

→ Prop : Grâce à Gauss, le système $Ax = b$ devient $Tx = Mb$ avec T triangulaire

→ Prop : On peut maintenant utiliser la méthode de remontée (en $O(n^2)$) pour calculer la solution en $O(n^3)$

→ Appli de Gauss : calcul de rang, de l'inverse d'une matrice, recherche d'une base d'un sev, calcul de déterminant...

III/Autres méthodes de résolution directe [Gri p 363] [Cia]

But : Se ramener à des systèmes triangulaires qui sont faciles à résoudre

1) Méthode LU

→ Prop : Décomposition LU : existence et unicité sous conditions

→ Calcul effectif avec Gauss + ex

→ Expliquer comment on revient à résoudre deux systèmes triangulaires + complexité

→ Rq : Si A est tridiagonale, le calcul de LU se fait en $O(n)$ d'où calcul d'une solution en $O(n^2)$ + ex matrice du laplacien discret relève de ce cas

2) Cholesky

→ Prop : Décomposition de Cholesky

→ Calcul explicite en $O(n^3)$ mais un peu mieux en mémoire que LU car on ne conserve qu'une seule matrice et pas deux

IV/ Méthodes itératives [Cia p 95-103]

But : Construire $(x_k)_k$ qui converge vers la solution

→ Th : Si $A = M - N$ avec $M \in GL_n$ et $N \in M_n$ la suite définie par $x_0 \in \mathbb{K}^n$ et $x_{n+1} = M^{-1}(Nx_k + b)$ converge vers la solution de $Ax = b$ ssi $\rho(M^{-1}N) < 1$

→ Ex : méthode de Jacobi, de Gauss-Siedel, de relaxation : donner les matrices M et N et des exs

→ Méthode de Kaczmarz $\boxed{\text{DEV2}}$

→ Prop : Gradient à pas optimal [HU p 53]

Références : Grifone [Gri], Ciarlet [Cia], XENS algèbre 2 [FGNal2] (pour le dev), [HU]

Développements :

→ Générateurs de GL(E) et SL(E) et applications à la connexité [FGNal2 p 177]

→ Méthode de Kaczmarz [Sans ref, trouvé sur le site de Théo Pierron]

170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications

Plan :

Cadre : $\mathbb{K}$ est un corps de caractéristique différente de deux et E un $\mathbb{K}$ ev de dimension n

I/Généralités

1) Définitions

- → Définition d'une forme bilinéaire symétrique (= fbs) + ex, et d'une forme quadratique (= fq) comme polynôme homogène de degré deux
- → Prop : Lien entre les deux, forme polaire
- → Définitions : matrice d'une fbs b et matrice d'une fq q + expression de $b(x, y)$ et de $q(x)$ avec ces matrices
- → Prop : Changement de base + définition de matrices congruentes

2) Noyau et rang

- → Définition du noyau et du rang d'une forme quadratique + ex + prop : c'est stable par congruence
- → Définition d'une forme dégénérée / non dégénérée + caractérisation

3) "Norme"

- → Définition d'un fq définie et positive (= fqdp)
- → Prop : Inégalité de Cauchy-Schwartz + csqc =
- → Prop : Si q est un fqdp alors $\sqrt{q}$ est une norme
- → Théorème de Schwarz pour une fonction deux fois différentiable + $D^2f(a)$ est un exemple de fqdp + application à la recherche d'extremums

II/Orthogonalité et isotropie

1) Orthogonalité

- → définition de vecteurs orthogonaux, de l'orthogonal d'un sev
- → Théorème de Pythagore

2) Diagonalisation

- → Définition d'une base orthogonale / base orthonormée (dans le cas d'une forme bilinéaire symétrique définie positive)
- → Th : Pour toute fq q il existe une base q orthogonale + calcul effectif (et preuve) via la méthode de Gauss de réduction des formes quadratiques + ex + csqc : orthodiagonalisation des matrices symétriques
- → Théorème de pseudo réduction simultanée
- → Appli : John-Loewner $\boxed{\text{DEV1}}$

3) Isotropie

- → Définition d'un vecteur isotrope, du cône isotrope (ce n'est pas un sev !) + ex avec $(x, y) \longmapsto xy$
- → Prop : $\mathrm{Ker}(q) \subset$ cône isotrope de q + réciproque fausse avec la forme associée à $\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$

III/Classification des formes quadratiques

- → Rappel de la définition de congruence + notation M et M' sont congruentes = $M \equiv M'$
- → Prop : Si $\mathbb{K}$ est algébriquement clos, $M \equiv M'$ ssi elles ont même rang
- → Prop : Dans le cas où $\mathbb{K} = \mathbb{R}$, théorème d'inertie de Sylvester = classification grâce à la signature
- → Rq : Lien entre positivité de la forme et sa signature + calcul de la signature via la réduction de Gauss

→ Appli : Lemme de Morse $\boxed{\text{DEV2}}$
→ Prop : Classification lorsque le corps est fini = il y a deux classes de congruence
→ Appli : Une démonstration de la réciprocité quadratique [H2G2]

Références : [dSP] (principalement), Rouvière [Rou] (pour l'analyse), XENS algèbre 3 [FGNal3] (pour le dev), Gourdon algèbre [GouAl]

Développements :
→ Ellipsoïde de John-Loewner [FGNal3 p 229]
→ Lemme de Morse [Rou p 209 et 354]

181. Barycentres dans un espace affine réel de dimension finie, convexité. Applications.

Idée de défense de plan : Le centre de gravité d'un ensemble de points pondérés est un barycentre → utile en physique

Plan :

Cadre : E est un espace affine réel de dimension n

I/Barycentres [DJM]

1) Définition

- → Définition + expression
- → Prop : homogénéité, commutativité et associativité du barycentre
- → Appli (de l'associativité) : Suite de polygones $\boxed{\text{DEV1}}$

2) Isobarycentre

- → Définition isobarycentre + ex : pour un segment c'est son milieu
- → Appli : Les médianes d'un triangle sont concourantes

II/Convexité [Tau p 75-87]

1) La base

- → Définition d'une combinaison convexe, d'une partie convexe, d'une partie étoilée
- → Prop : Une intersection de convexe est convexe ; convexe implique connexe par arcs ; A est convexe ssi toute combinaison convexe de points de A reste dans A ; si A est convexe, $\overline{A}$ aussi ...

2) Enveloppe convexe

- → Définition de l'enveloppe convexe de $A = \text{cv}(A)$
- → Théorème de Carathéodory [Tau p77]
- → Théorème de projection sur un convexe fermé (+ réciproque = théorème de Motzkin) + appli : approximation par les moindres carrés
- → Théorème de séparation (stricte) par un hyperplan
- → Théorème de Hahn Banach géométrique [Bre] + appli : calcul de l'enveloppe convexe de $O_n(\mathbb{R})$ pour la norme euclidienne
- → Définition de point extrémal + ex pour un segment + caractérisation des points extrémaux
- → Théorème de Krein-Milman

3) Lien avec les fonctions convexes

- → Définition d'une fonction convexe (stricte) via la convexité de son épigraphe
- → Définition d'une fonction convexe (stricte) classique + ce sont les mêmes
- → Prop : Si f est strictement convexe et admet un minimum local il est unique
- → Appli : Ellipsoïde de John-Loewner $\boxed{\text{DEV2}}$

Références : Brézis [Bre], [DJM], [Tau], XENS algèbre 3 [FGNal3] (pour le dev)

Développements :

- → Suite de polygones [Sans ref, trouvé sur le site de Théo Pierron]
- → Ellipsoïde de John-Loewner [FGNal3 p 229]

182. Applications des nombres complexes à la géométrie.

Idée de défense de plan : Définir le plan comme étant $\mathbb{C}$ peut être mieux que par $\mathbb{R}^2$ car $\mathbb{C}$ est un corps commutatif et ça c'est cool. D'ailleurs, on a essayé de faire pareil en dimension supérieure (3) ce qui a donné les quaternions mais là ça marche moins bien car ils ne forment pas un corps.

Plan :

I/Géométrie euclidienne

1) Lien $\mathbb{R}^2$ et $\mathbb{C}$ [Eid]

- → On représente le plan euclidien $\mathbb{R}^2$ par $\mathbb{C}$ via $(x, y) \longmapsto x + iy$
- → Définition de l'affixe d'un point / d'un vecteur (+ par la suite point et affixe de ce point)
- → Ex : Calcul de l'affixe de l'isobarycentre de $z_1, ...z_n$
- → Appli : Suite de polygones $\boxed{\text{DEV1}}$
- → Prop : Expression d'une longueur d'un segment, d'un produit scalaire, d'un produit mixte avec les affixes des points concernés
- → Appli : CNS de colinéarité + équation d'une droite avec les affixes

2) Angles [Aud p 73-77]

- → Prop : Si $u, v \in S^1$ (le cercle unité) il existe une unique rotation qui envoie u sur v. Ça donne donc une relation d'équivalence R sur $S^1 \times S^1$: $(u, v)R(u', v')$ ssi il existe une rotation qui envoie u sur u' et v sur v'
- → Définition : L'angle orienté de vecteur $(\overrightarrow{u}, \overrightarrow{v}$ est la classe de (u, v) modulo R
- → Prop : Relation de Chasles
- → Def : On oriente le plan. On note $\varphi : (u, u') \longmapsto$ l'unique rotation de $SO_2(\mathbb{R})$ qui envoie u sur u', de matrice $\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$. La mesure de l'angle (u, u') est θ (bien définie modulo 2π)
- → Appli : Coordonnées polaires

3) Transformations [Aud]

- → définition d'une similitude directe, de son rapport, de son angle
- → Prop : L'ensemble des similitudes directes est le groupe engendré par les translations, rotations et homothéties
- → Csqc : Les similitudes directes préservent les angles orientés et les distance (+ réciproque)
- → Définition de la conjugaison $z \longmapsto \overline{z}$
- → Définition des isométries affines + prop : elles sont engendrées par la conjugaison, et les similitudes directes dont le module du rapport vaut 1

II/Droite projective complexe et homogrphies [Aud]

1) Définitions

- → Définition de $\mathbb{P}1(\mathbb{C})$ comme $\frac{\mathbb{C}^2 \setminus \{(0,0)\}}{\sim}$ où $\sim$ est la relation de colinéarité
- → Prop : $\mathbb{P}_1(\mathbb{C})$ est homéomorphe à $\mathbb{C} \cup \{\infty\}$ ainsi qu'à la sphère de Riemann + dessins

2) Homographies

- → Prop : $GL_2(\mathbb{C})$ préserve les droites ce qui donne une action de $GL_2(\mathbb{C})$ sur $\mathbb{P}_1(\mathbb{C})$: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, [z : z'] \longmapsto [az + bz' : cz + dz']$
- → Définition du groupe linéaire projectif = $$PGL_2(\mathbb{C}) = \frac{GL_2(\mathbb{C})}{\mathbb{C}I_2} \simeq \{f : \left\{ \begin{array}{ccc} \mathbb{C} \cup \{\infty\} & \longrightarrow & \mathbb{C} \cup \{\infty\} \\ z & \longmapsto & \frac{az+b}{cz+d} \end{array} \right. |ad - bc \neq 0\}.$$ c'est le groupe des homographies
- → Conventions : $0 \times \infty = 0$ et $\frac{1}{0} = \infty$

→ Prop : Une homographie est une bijection et l'inverse d'une homographie est une homographie (structure de groupe)

→ Th : Si $a_1, a_2, a_3 \in \mathbb{P}_1(\mathbb{C})$ sont deux à deux distincts et $b_1, b_2, b_3 \in \mathbb{P}_1(\mathbb{C})$, il existe une unique homographie h tel que $h(a_1) = b_1, h(a_2) = b_2$ et $h(a_3) = b_3$

3) Birapport

→ Définition : Soit (a, b, c, d) où a, b, c sont deux à deux distincts. Alors il existe une unique homographie h telle que $h(a) = \infty$, $h(b) = 0$ et $h(c) = 1$. Le birapport de a, b, c, d est $[a, b, c, d] = h(d)$ + ex

→ Prop : Calcul du birapport : $[a, b, c, d] = \frac{(c-a)/(c-b)}{(d-a)/(d-b)}$ d'où le nom

→ Prop : Si $a, b, c \in \mathbb{P}_1(\mathbb{C})$ sont deux à deux distincts et $d \in \mathbb{P}_1(\mathbb{C})$, $[a, b, c, d] \in \overline{\mathbb{R}}$ ssi a, b, c, d sont alignés ou cocycliques

→ Définition d'une division harmonique

→ Prop : Si a, b, c sont deux à deux distincts, $[a, b, c, \infty] = -1$ ssi c est le milieu de $[ab]$

→ Prop : Toute homographie préserve les birapports + cor : $\mathcal{C} = \{$cercles et droites de $\mathbb{C}\}$ est préservé par toute homographie

4) Groupe circulaire

→ Définition : Le groupe circulaire G est le groupe engendré par $z \longmapsto \overline{z}$ et les homographies

→ Th : G est l'ensemble des bijections de $\mathbb{P}_1(\mathbb{C})$ qui préservent $\mathcal{C}$

Références : Eiden [Eid], Audin [Aud]

Développements :

→ Suite de polygones [Sans ref, trouvé sur le site de Théo Pierron]

→ Groupe circulaire [Aud p 204]

183. Utilisation de nombres complexes en géométrie.

Développements :

→ Groupe circulaire [Aud p 204]

→ Groupe des isométries du cube [H2G2 p 365]

190. Méthodes combinatoires, problèmes de dénombrement.

Plan :

I/Outils basiques [dB]

→ Définition d'un ensemble fini, cardinal, notation $|\ |$

1) Unions

→ Prop : Formule du crible + cas disjoint

→ Cor : Lemme des bergers = si $\varphi : A \longmapsto B$ est telle que A et B sont finis et $\forall x \in B, |\varphi^{-1}(x)| = n$ alors $|A| = n|B|$

→ Appli : $\forall p \geqslant 3$ et premier, il y a $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{F}_p$

2) Produits

→ Définition d'un produit d'ensembles finis

→ Prop : Cardinal d'un produit d'ensembles finis

→ Appli : Il y a p^n applications de X de cardinal n dans Y de cardinal p + nombre de parties d'un ensemble fini

3) Permutations

→ Définition d'un arrangement + leur nombre + appli : tiercé dans l'ordre

→ Définition d'une permutation (= cas particulier d'un arrangement) + $|S_n| = n!$

→ Définition d'une combinaison, des coeffs binomiaux + appli : tiercé dans le désordre

→ Prop sur les coeffs binomiaux + triangle de Pascal + binôme de Newton

→ Appli : inverse de la matrice de Pascal + nombre de dérangements

II/Utilisation de la théorie des groupes

1) Simple

→ Théorème d'isomorphisme

→ Prop : $|GL_n(\mathbb{F}_q)|$ + appli du th d'isomorphisme : calcul de $|SL_n(\mathbb{F}_q)|$ et recalcul du nombre de carrés de $\mathbb{F}_q$

2) Utilisation des actions de groupes

→ Définition : G agit sur X ensemble fini + stabilisateur + orbite

→ Th : $|X| = \sum_i |\text{orb}(x_i)|$ + appli : théorème de Lagrange

→ Prop : Relation orbite-stabilisateur + appli : nombre de matrice de rang r $\boxed{\text{DEV1}}$

3) Double comptage et théorie des groupes

→ Double comptage : A, B sont finis, P est un propriété sur $A \times B$. Alors $|\{(x,y) \in A \times B | (x,y) \text{ vérifie } P\}| = \sum_{y \in B} |\{x \in A | (x,y) \text{ vérifie } P\}| = \sum_{x \in A} |\{y \in B | (x,y) \text{ vérifie } P\}|$

→ Appli : Démonstration du théorème de Burnside

→ Appli de Burnside : Nombre de coloriage du cube

III/Utilisation des séries génératrices

→ Définition d'une série génératrice / série génératrice exponentielle

→ Appli : Nombres d'involutions de $[\![1, n]\!]$

→ Appli : Nombres de Catalan [Cormen p 264]

→ Appli : Nombres de Bell $\boxed{\text{DEV2}}$

IV/Fonctions arithmétiques [Per]

1) Fonction d'Euler

→ Définition de l'indicatrice d'Euler φ + expression pour une puissance d'une nombre premier

→ Prop : $\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^*| = |\text{générateurs de } \mathbb{Z}/n\mathbb{Z}|$

→ Prop : Multiplicativité de φ + expression de $\varphi(n)$

→ Prop : $\varphi(n) = \sum\limits_{d|n} \varphi(d)$ + csqc : cyclicité du groupe des inversibles d'un corps fini

2) Fonction de Moebius

→ Définition de la fonction de Moebius μ

→ Prop : Toutes celles qui permettent de montrer la

→ Prop : Formule d'inversion de Moebius

→ Appli : Calcul du nombre de polynômes irréductibles sur $\mathbb{F}_q$ [FG]

Références : De Biasi [dB], Ulmer [Ulm] (pour la théorie des groupes), Cormen [Cor], Perrin [Per], [FG], XENS algèbre 1 [FGNal1] (pour le dev), [H2G2]

Développements :

- Nombres de Bell [FGNal1 p 14]
- Nombre de matrices de rang r [H2G2 p 251]

203. Utilisation de la notion de compacité.

Plan :

Cadre : On se place dans un espace E qui est au moins métrique (sinon les deux définitions de la compacité ne sont plus équivalentes)

I/Généralités [GouAn]

1) Version Borel-Lebesgue [GouAn p 27-28]

- → Définition de la compacité via Borel-Lebesgue + ex
- → Prop : Une union finie ou une intersection quelconque de compacts reste compacte

2) Version Bolzano Weierstrass

- → Définition de la compacité séquentielle (= Bolzano-Weierstrass)
- → Csqc : Les compacts de $\mathbb{R}$, $\mathbb{R}^n$ et $\mathbb{C}^n$ sont les fermés bornés
- → Prop : E est séquentiellement compact ssi il est compact selon Borel-Lebesgue (cad les deux définitions sont équivalentes)

3) Quelques propriétés

- → Prop : Un compact est fermé borné. Réciproque fausse en général
- → Prop : Si A est une partie fermée du compact E alors A est compact
- → Prop : Une partie compacte est complète
- → Prop : Tout intervalle de $\mathbb{R}$ est union croissante de compacts
- → Appli : Une démonstration du théorème de Cauchy-Lipschitz $\boxed{\text{DEV1}}$

II/Compacité et fonctions continues

1) Extremums

- → prop : Si f est continue, l'image d'un compact par f est compacte
- → Csqc : Si f est continue sur un compact, elle est bornée et atteint ses bornes
- → Appli 1 : Théorème de Rolle puis celui des accroissements finis
- → Appli 2 : Equivalence des normes en dimension finie + csqc : en dimension finie, les fermés bornés sont les compacts + rq : théorème de Riesz : $\dim(E) < \infty$ ssi la boule unité fermée est compacte
- → Appli 3 : Ellipsoïde de John-Loewner $\boxed{\text{DEV2}}$
- → Définition d'une fonction coercive
- → Prop : Une fonction continue et coercive est minorée et atteint sa borne inf
- → Appli : Théorème de d'Alembert

2) Utilisation de la compacité dans le calcul de limites

- → Théorème de Heine = si f est continue sur un compact elle y est uniformément continue
- → Appli 1 : Densité des polynômes dans les fonctions continues sur un compact par les polynômes de Bernstein
- → Appli 2 : Sommes de Riemann pour le calcul approché d'intégrales

3) Théorèmes de points fixes [Rou]

- → Un théorème de point fixe lorsque E est compact
- → Th : Point fixe de Brouwer

- → On peut aussi parler d'uniforme équicontinuité, d'Ascoli + application au théorème de Montel

Références : Gourdon analyse [GouAn], XENs algèbre 3 [FGNal3], Rouvière [Rou], Testard [Tes]

Développements :

→ Ellipsoïde de John-Loewner [FGNal3 p 229]
→ Théorème de Cauchy-Lipschitz [Rou p 180]

208. Espaces vectoriels normés, applications linéaires continues. Exemples.

Plan :

Cadre : E est un $\mathbb{R}$ ou $\mathbb{C}$ espace vectoriel

I/Généralités
1) Normes

- → Définition d'une norme et d'un espace vectoriel normé (= evn) + ex : les normes p sur $\mathbb{C}^n$ ou les L^p + ct-ex [Hau p 318]
- → Rq : Une norme donne toujours une distance : $d(x,y) = ||x-y||$
- → Prop : Toute norme est 1-lipschitzienne donc continue
- → Définition de normes équivalentes + rq : cela signifie qu'elles font converger les mêmes suites et donc les mêmes fermés, bornés, compacts...
- → Théorème d'équivalence des normes pour les $\mathbb{R}$ ou $\mathbb{C}$ ev de dimension finie
- → Ct-ex : Sur $C^0([0,1],\mathbb{R})$ les normes $||\ ||_1$ et $||\ ||_\infty$ ne sont pas équivalentes (considérer $x \longmapsto x^n$)

2) Applications linéaires

- → Définition d'une application linéaire continue
- → Ex : $\varphi_1 : f \in C^0([0,1],\mathbb{R}) \longmapsto f(0)$ et $\varphi_2 : f \in C^0([0,1],\mathbb{R}) \longmapsto \int_0^1 f(t)\mathrm{d}t - f(0)$ sont continues pour $||\ ||_\infty$
- → Attention : La continuité dépend des normes qu'on a choisies ! Par exemple, φ_1 n'est plus continue avec $||\ ||_1$
- → Définition de $L_c(E,F)$ + norme triple $|||\ |||$ + ça donne un evn
- → Ex de calcul de normes d'applications linéaires : $|||\varphi_1||| = 1$ (avec atteinte) et $|||\varphi_2||| = 2$ (sans atteinte)
- → Prop : Sous multiplicativité de la norme triple + csqc : ça fait que $L_c(E)$ est une algèbre normée

3) Cas de la dimension finie

- → Prop : Toute application linéaire définie sur un ev de dimension finie est continue (quelle que soit la norme dessus)
- → Prop : En dimension finie, les fermés bornés sont les compacts
- → Th de Riesz : $(E, ||\ ||)$ est de dimension finie ssi $\overline{B}_{||\ ||}(0,1)$ est compacte

II/Banachs
1) Définitions et propriétés

- → Définition : Un Banach est un evn complet + ex : tout evn de dimension finie est un Banach + ex : les $(L^p, ||\ ||_p)$ pour $p \in [1,\infty]$ sont des Banachs + ex : $(C^0(K = \text{compact}, \mathbb{R}^m), ||\ ||_\infty)$ est un Banach
- → Appli : Cauchy-Lipschitz $\boxed{\text{DEV1}}$
- → Prop : Si F est un Banach alors $L_c(E,F)$ aussi + csqc E' est donc un Banach
- → Th : E = Banach, $(u_n)_n \in E^{\mathbb{N}}$. Si $\sum ||u_n||_E$ converge alors $\sum u_n$ converge dans E
- → Appli : Si E est un Banach, $GL_c(E)$ est un ouvert de $L_c(E)$

2) Baire et applications [GouAn p 397 et suivantes]

- → Lemme de Baire
- → Appli 1 : Théorème de l'application ouverte puis théorème d'isomorphisme de Banach
- → Appli 2 : Théorème de Banach-Steinhaus + appli : si E et F sont des Banachs et $(f_n)_n \in L_c(E,F)$ cvs vers f alors f est continue + autre appli : il existe une fonction continue qui diffère de sa série de Fourier $\boxed{\text{DEV2}}$

III/Hilberts

1) Définitions

→ Définition d'un espace préhilbertien + ex l^2 et L^2
→ Prop : Inégalité de Cauchy-Schwartz + csqc : le produit scalaire donne une norme
→ Définition : Un Hilbert est un préhilbertien complet pour cette fameuse norme
→ Définition d'éléments orthogonaux + théorème de Pythagore
→ Prop : identité du parallélogramme

2) Projection sur un convexe fermé

→ Théorème de projection sur un convexe fermé dans un Hilbert puis cas particulier des sev fermés (de dimension finie par exemple)
→ Appli 1 : Moindres carrés [Rou p 385]
→ Appli 2 : Théorème de représentation de Riesz + appli : existence de l'opérateur adjoint dans un Hilbert

Références : Gourdon analyse [GouAn], Hauchecorne [Hau], [OA], Rouvière [Rou]

Développements :

→ Théorème de Cauchy-Lipschitz [Rou p 180]
→ Théorème de Banach-Steinhaus [GouAn p 404-405]

214. Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie.

Plan :

Cadre : On reste en dimension finie. Prérequis : Définition d'un C^k-difféomorphisme

I/Théorème d'inversion locale (TIL) [Rou]
1) Théorème et variantes

- → Théorème d'inversion locale version C^1 + ça donne la différentielle de l'inverse + un dessin
- → Ex : $f_0 : (x, y) \longmapsto (x^2 - y^2, 2xy)$ est un difféomorphisme local en tout point de $\mathbb{R}^2 \backslash \{(0, 0)\}$
- → Ct-ex : Il faut vraiment une fonction C^1 ; D^1 ne suffit pas : $f : x \longmapsto x^2 \sin\left(\frac{\pi}{x}\right)$ vérifie $f'(0) = 0$ et n'est pas injective
- → Variantes du TIL : version C^k et version holomorphe
- → Théorème d'inversion globale + ct-ex : f_0 est un difféomorphisme local en tout point de $\mathbb{R}^2 \backslash \{(0, 0)\}$ mais pas global car pas injective
- → Rq : Montrer l'injectivité revient souvent à calculer directement l'inverse (auquel cas, plus besoin du théorème)

2) Applications

- → Appli 1 : Racine k-ème d'une matrice proche de I_n [OA p 11]
- → Appli 2 : Une application C^1 et k-dilatante est un C^1 difféomorphisme global [Rou p 221]
- → Appli 3 : Lemme de Morse $\boxed{\text{DEV1}}$ + csqc : condition suffisante de minimalité [OA p 15]
- → Appli 4 : L'exponentielle est un difféomorphisme local au voisinage de $0 \in M_n(\mathbb{K})$. D'où surjectivité de l'exponentielle matricielle complexe $\boxed{\text{DEV2}}$

II/Théorème des fonctions implicites (TFI)
1) Théorème et variantes [Rou]

- → TFI + schéma + ex avec le cercle $x^2 + y^2 - 1 = 0$
- → Rq : On peut calculer la différentielle de la fonction implicite + ex avec le cercle
- → Variantes du TFI : version C^k et version holomorphe
- → Rq : Le TIL implique le TFI et réciproquement

2) Applications

- → Appli : Polynôme scindé à racines simples [OA p 11-12]
- → Théorème des extrema liés + applis : inégalité arithmético-géométrique [GouAn], inégalité de Hadamard [Rou p 409] et diagonalisation des matrices symétriques [OA p 21]

III/Sous-variétés [Rou]

- → Définition d'une sous-variété de dimension k + ex : sphère + ct-ex : cône
- → Théorème des sous-variétés + préciser ce qu'on utilise (TIL/TFI) pour le montrer
- → Définition d'un vecteur tangent
- → Prop : {vecteurs tangents} est un ev + expression selon la façon dont on définit une sous variété
- → Rq : Interprétation géométrique des extrema liés

Références : Rouvière [Rou] (principalement), Gourdon analyse [GouAn] (pour extrema liés), [OA] (pour les applis), Zavidovique [Zav] (pour le développement)

Développements :

→ Lemme de Morse [Rou p 354 et 209]

→ Surjectivité de l'exponentielle [Zav p 49]

215. Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.

Plan :

Cadre : Les fonctions vont de U, ouvert de $\mathbb{R}^n$ dans $\mathbb{R}^p$

I/Généralités (ordre 1)
1) Différentielles [Rou p 45-50]

- → Définition de la différentielle + unicité
- → Ex : Cas d'une fonction de $\mathbb{R}$ dans $\mathbb{R}$ + lien avec la dérivée
- → Ex : Différentielle d'une fonction linéaire
- → Ex : Différentielle d'une fonction de $\mathbb{R}^n$ dans $\mathbb{R}$ et définition du gradient
- → Prop : La différentiabilité en a implique la continuité à a
- → Prop : Différentielle de la somme, produit, composée
- → Appli : Calcul de la différentielle de la norme euclidienne

2) Lien avec les dérivées partielles [Rou] [Gou p 304-313]

- → Déf : Dérivée selon un vecteur + cas particulier quand on dérive selon un vecteur de la base canonique = dérivée partielle
- → Prop : Différentiable implique avoir des dérivées selon tout vecteur
- → Rq : la réciproque est fausse : ct ex [Rou p 49]
- → Prop : En revanche, si les dérivées selon tout vecteur sont continues, la fonction est différentiable
- → Appli : Calcul de la différentielle du déterminant

II/Fonctions C^1
1) Inégalité des accroissements finis (IAF)

- → Définition : fonction C^1
- → Prop : IAF [Rou p 104]
- → Cor : f est C^1 ssi f admet des dérivées partielles continues
- → Appli : Si U est connexe et $Df \equiv 0$ alors $f = 0$

2) TIL et TFI

- → Définition C^1 difféomorphisme
- → Théorème d'inversion locale
- → Appli : Surjectivité de l'exponentielle $\boxed{\text{DEV1}}$
- → Théorème d'inversion globale
- → Théorème des fonctions implicites
- → Ex : On peut paramétrer le cercle unité

III/Différentielles d'ordre supérieur
1) Définition [Rou p 293-296]

- → définition différentielle seconde, hessienne + ex
- → Théorème de Schwarz
- → Prop : Si $f \in C^2$ alors D^2f existe mais l'existence des dérivées partielles secondes n'impliquent pas que D^2f existe (ct-ex)
- → Définition différentielle d'ordre k par récurrence

2) Formule de Taylor

- → prop : Formule de Taylor avec reste intégral [Rou p 298]
- → Appli : Lemme de Morse $\boxed{\text{DEV2}}$

IV/Applications à l'optimisation
Mettre la partie correspondante de la leçons sur les extremums

Références : Gourdon analyse [GouAn], Rouvière [Rou], [OA]

Développements :

→ Lemme de Morse [Rou p 354 et 209]
→ Surjectivité de l'exponentielle [Zav p 49]

218. Applications des formules de Taylor.

Plan :

I/Diverses formules de Taylor

1) Pour une fonction de $\mathbb{R}$ dans $\mathbb{R}$ [GouAn p 73-75]

- → Théorème de Rolle
- → Th : Formule de Taylor-Lagrange (se déduit de Rolle avec la bonne fonction)
- → Rq : Ça redonne le théorème des accroissements finis + appli encadrement [GouAn p 75]
- → Th : Inégalité de Taylor-Lagrange + ex avec sinus (se déduit de la formule de Taylor-Lagrange)
- → Th : Formule de Taylor-Young (= TY) (se montre par récurrence)
- → Th : Formule de Taylor avec reste intégral (= FTRI) (se montre par récurrence ; on peut en déduire l'inégalité de Taylor-Lagrange)

2) Pour une fonction de $\mathbb{R}$ dans un $\mathbb{R}$ espace vectoriel de dimension d

- → Rq : En dimension d, Rolle et l'égalité des accroissements finis (donc l'égalité de Taylor-Lagrange aussi) sont faux : ct-ex $= f : t \longmapsto e^{it}$
- → Prop : L'inégalité de Taylor-Lagrange reste vraie [GouAn p 73]
- → Prop : TY et FTRI restent vraies aussi

II/Applications en analyse

1) Développements limités (dl) et équivalents

- → Prop : TY donne les dl usuels + ex
- → Appli : Démonstration du théorème central limite
- → Prop : L'existence d'un dl_1 équivaut à la dérivabilité mais ce n'est plus vrai pour les ordre supérieurs
- → Prop : TY donne aussi des équivalents + appli : calcul de limites indéterminées + ex
- → Appli : Théorème de Darboux

2) Séries entières

- → Définition : La série de Taylor de f en a est $\sum\limits_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n$
- → Rq : f ne correspond pas toujours à sa série de Taylor : ct-ex avec $x \longmapsto e^{\frac{-1}{x}}$ si $x > 0$ et 0 sinon
- → Prop : La FTRI donne certains développements en série entière (il suffit de montrer qu le reste tend vers 0) + ex
- → Théorème de Bernstein pour les séries entières +ex [GouAn p 250]

3) Recherche d'extremums

- → Conditions nécessaires / suffisantes à l'ordre 1 ou 2 pour avoir un extremum (elles viennent de Taylor-Young) : s'inspirer de la partie correspondante de la leçon sur les extremums
- → Lemme de Morse + appli extremum $\boxed{\text{DEV2}}$

III/Analyse numérique

1) Optimisation

- → Prop : Newton + dessin $\boxed{\text{DEV1}}$
- → Appli : méthode de Héron pour approximer $\sqrt{2}$

2) Calcul d'intégrales [De]

- → Définition d'une méthode d'ordre n

→ Comparaison des méthodes (avec la FTRI) rectangle à gauche, à droite, méthode des trapèzes, de Simpson pour le calcul approché d'intégrales

Références : Gourdon analyse [GouAn], Rouvière [Rou], [OA], Demailly [De]

Développements :

→ Lemme de Morse [Rou p 354 et 209]
→ Méthode de Newton [Rou p 152]

219. Extremums : existence, caractérisation, recherche. Exemples et applications.

Plan :

I/Définitions et cadre de travail [Rou]

- → Cadre : E est un $\mathbb{R}$ espace vectoriel de dimension finie muni de la norme euclidienne ; $U \subset E$; $f : U \longmapsto \mathbb{R}$
- → Définitions : Minimum global, local, strict (global ou local) + rq : pareil pour les max
- → Ex : Sinus admet un minimum global non strict (qui est un minimum local strict) en $\frac{-\pi}{2}$

II/Compacité et existence d'extremums [Tes p 44-48]

- → Prop : Si f est continue sur un compact, elle est bornée et atteint ses bornes
- → Ex : La norme $N : (\mathbb{R}^n, || \ ||_\infty \longmapsto \mathbb{R}$ est continue sur le compact $S_\infty(0,1)$ donc y atteint son minimum
- → Appli : Equivalence des normes pour les $\mathbb{R}$ espaces vectoriels de dimension finie
- → Déf : Fonction coercive + cas où $U = E$
- → Prop : Si f est continue et coercive, elle est minorée et atteint son min
- → Ex : $(x,y) \longmapsto x^2 + y^2$ est continue et coercive. Et, en effet, elle admet un min en $(0,0)$
- → Appli : Théorème de d'Alembert

III/Extremums et calcul différentiel
Ici, U est un ouvert
1) Ordre 1

- → Définition d'un point critique
- → Prop : Si y a un extremum local en a, il y a un point critique en a
- → Rq : La condition précédente est nécessaire mais pas suffisante : $\left\{ \begin{array}{lcl}]-1,1[& \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^3 \end{array} \right.$ vérifie $Df(0) = 0$ mais 0 n'est pas un extremum de cette fonction
- → Appli : Théorème de Rolle puis des accroissements finis

2) Ordre 2

- → Prop : Si a est un minimum local et $D^2f(a)$ existe, alors $Df(a) = 0$ et $D^2f(a)$ est une forme quadratique positive
- → Ex : $(x,y) \longmapsto x^2 + y^4$ a un minimum local en $(0,0)$ et en effet, $Df(0,0) = 0$ et $D^2f(0,0) = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$ est positive
- → Ct-ex : Ce n'est pas suffisant pour avoir un minimum : $(x,y) \longmapsto x^2 - y^3$ admet $(0,0)$ comme point critique et $D^2f(0,0) = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$ est positive mais $(0,0)$ n'est pas un minimum local
- → Prop : Si $Df(a) = 0$ et $D^2f(a)$ est *définie* positive alors f admet un minimum local strict en a
- → Ex : $(x,y) \longmapsto x^2 - y^2 + \frac{y^4}{4}$ vérifie ces hypothèses en $(0, \sqrt{2})$ qui est donc un minimum local strict
- → Ct-ex : Ce n'est pas nécessaire pour avoir un minimum : $(x,y) \longmapsto x^2 + y^4$ admet un minimum local strict en $(0,0)$ sans que $D^2f(0,0)$ ne soit définie
- → Rq : Cas de dimension 2 [GouAn p 317]
- → Appli : Maximum harmonique [GouAn p 318]

3) Problèmes sous contraintes

- → Théorème des extrema liés + interprétation géométrique

→ Applis : Inégalité arithmético-géométrique + diagonalisation des endomorphismes symétriques

IV/Extremums et convexité

Ici, U est convexe et non vide

→ Définition d'une fonction (strictement) convexe + ex
→ Prop : Si f est convexe et que U est ouvert, si a est un max global de f alors f est constante
→ Prop : Si f est convexe et que U est ouvert, si a est un min local de f alors a est un min global
→ Prop : Si f est convexe et différentiable, (a est un extremum local) ssi ($Df(a) = 0$)
→ Ex : exp n'a pas de min (ni local, ni global)
→ Th : Si f est strictement convexe et a un minimum alors il est unique
→ Appli : Ellipsoïde de John-Loewner $\boxed{\text{DEV1}}$
→ Théorème de projection sur un convexe fermé + appli : moindres carré [Rou p 384]

V/Deux algos de recherche

→ Algo de Newton $\boxed{\text{DEV2}}$ + dessin
→ Cor : Si $f \in C^3$ est strictement convexe, on peut appliquer Newton à f' pour connaître les points critiques
→ Algo : Gradient à pas optimal + dessin [HU p 53]

Références : Testard [Tes], Gourdon analyse [GouAn], Rouvière [Rou], [OA] (pour les exs et ct-exs), [HU], XENS algèbre 3 [FGNal3]

Développements :

→ Ellipsoïde de John-Loewner [FGNal3 p 229]
→ Méthode de Newton [Rou p 152]

220. Equations différentielles $X' = f(X,t)$. Exemples d'étude des solutions en dimension 1 et 2.

Développements :

→ Théorème de Cauchy-Lipschitz [Rou p 180]
→ Liapunov [Rou p 143]

221. Equations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

Développements :

→ Equation de Bessel [FGNan4 p 101]
→ Liapunov [Rou p 143]

223. Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.

Plan :

Intro : Une suite numérique est à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$. Dans la suite on considère qu'elles sont à valeurs dans $\mathbb{R}$ mais les résultats s'adaptent.

I/Convergence : définitions

1) Définitions

- → Définition de la convergence (vers une limite finie) + unicité quand elle existe + notation + ex
- → Prop : Caractérisation séquentielle de la continuité d'une fonction
- → Définition de la divergence vers $\pm\infty$ + notation
- → Rq : On dit qu'une suite diverge si elle tend vers $\pm\infty$ ou n'a pas de limite
- → Définition de O, o, $\sim$ à l'aide des limites

2) Premières propriétés

- → Prop : Compatibilité de la limite avec plus, fois, inégalités
- → Prop : Converger implique être bornée + pas de réciproque (penser à $(-1)^n$)
- → Prop : Si u est majorée et croît ou est minorée et décroît elle converge + ce n'est pas nécessaire : $\frac{(-1)^n}{n} \to 0$ mais n'est pas monotone

3) Valeurs d'adhérence

- → Définition d'une sous suite, d'une valeur d'adhérence (comme $\{l \in \overline{\mathbb{R}} | \exists \varphi$ strictement croissante telle que $u_{\varphi(n)}$ $l\})$
- → Prop : $\mathrm{Adh}(u) = \bigcap\limits_{N \in \mathbb{N}} \overline{\{u_n | n \geqslant N\}}$. D'où $\mathrm{Adh}(u)$ est fermée
- → Prop : Si u converge, elle admet une valeur d'adhérence (sa limite) + Si u a au moins deux valeurs d'adhérence, u diverge + ex : $\left(\cos(\frac{n\pi}{2})\right)$
- → Théorème de Bolzano-Weierstrass
- → Prop : Si une suite admet une unique valeur d'adhérence dans $\overline{\mathbb{R}}$ elle converge dans $\overline{\mathbb{R}}$

4) Limites inférieure et supérieure

- → Définition limsup et liminf
- → Prop : La limsup (resp liminf) de u est la plus grande (resp petite) valeur d'adhérence de u
- → Prop : Si limsup u = liminf u alors u converge

II/Convergence : suites particulières

- → Définition de suites adjacentes
- → Prop : Deux suites adjacentes convergent vers la même limite
- → Appli : TVI, approximation décimale, critère de convergence des séries alternées
- → Théorème des gendarmes
- → Appli : Comparaison série-intégrale + ex avec les séries de Riemann
- → Définition suite de Cauchy
- → prop : Dans notre contexte, être de Cauchy équivaut à converger
- → Appli : Les séries absolument convergentes convergent

III/Suites récurrentes

- → Définition d'une suite récurrente d'ordre k
- → Ex : Cas linéaire à coefficients constants + Fibonacci
- → Cadre : I est un intervalle fermé, $f : I \longrightarrow I$, $u_0 \in I$ et $u_{n+1} = f(u_n)$
- → Prop : Si f est croissante, (u_n) est monotone ; si f est décroissante, (u_{2n}) et (u_{2n+1}) sont monotones de sens contraire

- → Prop : Si (u_n) converge vers l, l est un point fixe de f + ct-ex : $x \longmapsto -x$ a un point fixe sans que $u_{n+1} = -u_n$ ne converge
- → Prop : Théorèmes de points fixe
- → Appli : Méthode de Newton $\boxed{\text{DEV1}}$

IV/Comportement asymptotique de suites / séries

- → Prop : Sommation des relations de comparaison + ct-ex quand les termes généraux ne sont pas positifs : $\frac{(-1)^n}{\sqrt{n}} \sim \frac{(-1)^n}{\sqrt{n}} + \frac{1}{n}$ mais l'une des séries converge et pas l'autre
- → Appli : Stirling ou développement de la série harmonique
- → Appli : Lemme de Cesàro
- → Appli de Cesàro : Suite à convergence lente $\boxed{\text{DEV2}}$

Références : Gourdon analyse [GouAn], El Amrani [ElA], XENS analyse 1 [FGNan1]

Développements :

- → Méthode de Newton [Rou p 152]
- → Convergence lente [FGNan1 p 99]

224. Exemples de développements asymptotiques de suites et de fonctions.

Idée de défense de plan : Un développement asymptotique c'est utile en physique par exemple pour calculer le potentiel créé par un dipôle électrostatique (loin des sources). Pour motiver les échelle de comparaison on peut souligner le fait qu'elles permettent de réduire des fonctions compliquées à des combinaisons linéaires de fonctions modèles plus simples.

Plan :

Cadre de la plupart des parties : f est définie sur un intervalle I différent d'un point à valeurs dans $\mathbb{R}$, $a \in \overline{I}$ et $n \in \mathbb{N}$

I/Notations [GouAn p86]

→ Définition et notation O, o, $\sim$ + rq : $f = O(g)$ est une écriture impropre
→ Rq : Quand f ne s'annule pas, on peut exprimer O, o et $\sim$ par le caractère borné ou la limite de $\frac{g}{f}$

II/Développements asymptotiques de fonction [GouAn p 86 et suivantes]
1) Développements asymptotiques

→ Définition d'une échelle de comparaison + exs classiques
→ Définition d'un développement asymptotique (DA) par rapport à une échelle de comparaison
→ Prop : Unicité du DA + ex du DA de $x^{\frac{1}{x}}$

2) Développements limités

→ Définition d'un $DL_n(a)$
→ Rq : On peut faire un changement de variable dans un DL du coup on ne donne que ceux en 0
→ Rq : Un DL est un DA avec l'échelle de comparaison $(x^n)_n$ d'où l'unicité du $DL_n(a)$
→ Prop : Taylor-Young (la régularité donne des DL) + ex DL de exp ou de $(1+x)^\alpha$
→ Appli 1 : Calcul de limites indéterminées
→ Appli 2 : Démonstration du théorème central limite
→ Prop : ("réciproque" de Taylor-Young) : f est continue (resp dérivable) en a ssi f admet un $DL_0(a)$ (resp $DL_1(a)$) mais ça devient faux pour $n \geqslant 2$ + ct-ex

3) Opérations sur les DL

→ Prop : DL d'une somme + ex : DL de ch et sh : DL d'un produit
→ Prop : DL d'une composée + appli : Dl d'un quotient

III/Développements asymptotiques et intégration
1) Intégration d'un DL

→ Prop : Intégration d'un $DL_n(a)$
→ Appli : Calcul du DL(0) de $ln(1+x)$ et de $\arctan(x)$

2) Intégration des relations de comparaison

→ Prop : Intégration des relations de comparaison [GouAn p 159]
→ Ex : On retrouve $ln(x) = o(x^\alpha)$ en ∞ pour $\alpha > 0$
→ Appli : DA du logarithme intégral [GouAn p 169]

IV/Développements asymptotiques de suites et de de séries
1) Suites récurrentes

→ Théorème de Cesàro
→ Appli : Converge lente $\boxed{\text{DEV1}}$ + ex avec sinus
→ Appli : Méthode de Newton $\boxed{\text{DEV2}}$

2) Sommation des relations de comparaison

→ Prop : Sommation des relations de comparaison
→ Attention les termes généraux doivent être positifs + ct-ex [Hau]
→ Appli : $H_n \sim ln(n)$ en $+\infty$

3) Comparaison série-intégrale

→ Prop : Comparaison série-intégrale
→ Appli : Etude des séries de Bertrand
→ Appli : Equivalent des sommes de Riemann, d'où le développement asymptotique de H_n (série harmonique)

Références : Gourdon analyse [GouAn], Rouvière [Rou], Hauchecorne [Hau] (pour le ct-exs), XENS analyse 1 [FGNan1]

Développements :

→ Méthode de Newton [Rou p 152]
→ Converge lente [FGNan1 p 99]

226. Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations.

Plan :

Cadre : $(E, || \ ||)$ est un evn de dimension finie, $f : I \longrightarrow E$ tel que $f(I) \subset I$, $u_0 \in I$ et $\forall n \geqslant 0, u_{n+1} = f(u_n)$

I/Généralités : l'étude de f donne des infos sur (u_n)

1) Monotonie et convergence

→ Prop : Si f est croissante, (u_n) est monotone +ex

→ Prop : Si f est décroissante, (u_{2n}) et (u_{2n+1}) sont monotones de sens contraire +ex

→ Si (u_n) converge vers l et f est continue, l est un point fixe de u + csqc : si f est continue, u ne peut converger que vers un point fixe

→ Ex d'étude : [GouAn p 194]

2) Suites particulières

→ Cas des suites arithmétiques, géométriques, arithmético-géométriques

→ Cas des suites homographiques

→ Cas des suites récurrentes à coeffs constants + ex Fibonacci

II/Points fixes et limites

1) Théorème de point fixe

→ Théorème de point fixe

→ Attention, il faut bien toutes les hypothèses [Rou]

→ Variantes du théorème du point fixe lorsque f^p est contractante ou lorsqu'elle contracte strictement les distances et qu'on est sur un compact à la place d'un complet + ex

→ Rq : pour aller plus loin que la convergence : Suite à convergence lente $\boxed{\text{DEV1}}$

2) Classification des points fixes [De p 95-97 et 106-109]

→ Déf : Points fixes attractifs, super attractifs, répulsifs + dessins dans le cas $E = \mathbb{R}$

→ Déf : Rayon spectral + point fixe attractif lorsque $E = \mathbb{R}^n$

III/Résolution approchée de systèmes

1) Systèmes linéaires [Cia]

→ Définition d'une méthode itérative

→ Théorème : Une méthode itérative converge ssi le rayon spectral d'une certaine matrice est < 1

→ Exs : Méthodes de Jacobi, Gauss-Siedel, de relaxation

2) Systèmes non linéaires

→ Méthode de dichotomie

→ Méthode de Newton + dessin $\boxed{\text{DEV2}}$

→ Rq : On peut lui préférer la méthode de la sécante quand la dérivée de la fonction considérée est dure à calculer

Références : Gourdon analyse [GouAn], Demailly [De], Rouvière [Rou], Ciarlet [Cia], XENS analyse 1 [FGNan1]

Développements :

→ Méthode de Newton [Rou p 152]

→ Converge lente [FGNan1 p 99]

228. Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications.

Développements :

→ Polynômes de Bernstein [BL p 59]
→ Un calcul de l'intégral de Gauss [GouAn p 163]

229. Fonctions monotones. Fonctions convexes. Exemples et applications.

Développements :

→ Méthode de Newton [Rou p 152]
→ Ellipsoïde de John-Loewner [FGNal3 p229]

230. Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des suites numériques. Exemples.

Plan :

I/Vocabulaire
1) Convergence

- → Défs : terme général (= TG) de série, série, série convergente et dans ce cas définition du reste
- → Ex : Série géométrique : selon sa raison elle converge (et dans ce cas on donne sa somme) ou non
- → Prop : Si $\sum u_n$ converge, le reste tend vers 0 et $(u_n$ aussi + réciproque fausse avec le ct-ex de la série harmonique
- → Rq : Ce fait peut permettre de montrer la convergence vers 0 de certaines suites

2) Absolue convergence

- → Définition d'une suite absolument convergente
- → Prop : L'absolue convergence implique la convergence + la réciproque est faussu (ct-ex avec la série harmonique alternée)

II/Convergence des séries à TG positif
1) Convergence

- → Définition d'un TG positif (= ultimement positif) + ex : $u_0 = -2$ et $u_{n+1} = \frac{1}{2^n}$ est un TG positif
- → Prop : Comparaison : $0 \leqslant u_n \leqslant v_n$ et $\sum v_n$ converge implique $\sum u_n$ converge + ct-ex quand les termes ne sont pas positifs
- → Appli : Si $\frac{u_{n+1}}{u_n} \to l < 1$ alors $\sum u_n$ converge et si $\frac{u_{n+1}}{u_n} \to l > 1$, $\sum u_n$ diverge (comparaison avec une série géométrique)

2) Comparaison série-intégrale

- → Prop : Comparaison série-intégrale + encadrement du reste dans le cas convergent
- → Rq : Attention, cet encadrement ne donne pas forcément un équivalent du reste (considérer $x \longmapsto e^{-x^2}$
- → Appli : Etude des séries de Riemann et de Bertrand (+ ici on peut déduire un équivalent des restes avec la comparaison série-intégrale)
- → Appli : Régle $(n^\alpha u_n)$

III/Comparaison et TG positifs
1) Comparaison

- → Théorème de comparaison
- → Appli : Théorème de Cesàro
- → Appli : Calcul d'un équivalent de u avec $u_{n+1} = \sin(u_n)$ en cherchant α tel que $(u_{n+1}^\alpha - u_n^\alpha)$ converge + généralisation : th de convergence lente

2) Le point de vue des séries

- → Méthode : Pour montrer que (u_n) converge, montrer que $u_{n+1} - u_n$ est un TG de série convergente
- → Appli : $H_n = ln(n) + \gamma + o(1)$ + on peut continuer ce développement asymptotique
- → Appli : Une démonstration de la formule de Stirling

IV/Convergence pour un TG quelconque
1) Montrer une convergence

- → On peut observer $|u_n|$ et lui appliquer toute la partie précédente
- → définition d'une série alternée

→ Prop : Critère spécial pour les séries alternées
→ Ex : Ça marche pour $\frac{(-1)^n}{n}$ + ct-ex
→ Généralisation : critère d'Abel + appli : $\sum \frac{\sin(nx)}{n}$ converge

2) Produit de Cauchy

→ Définition produit de Cauchy
→ Prop : Si $u, v \in l^1$, le produit de Cauchy de u et v appartient à l^1 et on a égalité des sommes
→ Appli : $e^{z+z'} = e^z \times e^{z'}$

V/Séries de Fourier, séries entières

1) Séries entières

→ Définition d'un SE, rayon de convergence
→ Prop : Unicité du DES, caractère C^∞ de la somme sur le disque ouvert de convergence
→ Appli : Nombres de Bell $\boxed{\text{DEV1}}$

2) Séries de Fourier

→ Définition coeffs et série de Fourier
→ Prop :formule de Parseval + appli : calcul de $\zeta(2)$
→ Prop : Formule de Poisson + appli $\boxed{\text{DEV2}}$

Références : Gourdon analyse [GouAn], XENS algèbre 1 [FGNal1], El Amrani [ElA] (surtout)

Développements :

→ Nombres de Bell [FGNal1 p 14]
→ Formule sommatoire de Poisson [GouAn p 272 et 164]

Idée de défense de plan : Pourquoi peut on préférer les méthodes itératives aux méthodes exactes ? Un : si on a un gros système linéaire, on va faire beaucoup d'opérations donc potentiellement beaucoup d'erreurs. Deux : les méthodes exactes exigent parfois des calculs exacts ce qui est impossible à faire informatiquement.

Plan :

I/Outils

1) Normes matricielles

→ définition d'une norme matricielle (= sous multiplicative) + rq pour une telle norme, $||A^k|| \leqslant ||A||^k$ ce qui permet d'établir des convergences

→ Définition d'une norme subordonnée + prop : elles sont matricielles

→ Ex : $|||A|||_1 = \max_j \sum_i |a_{i,j}|$

2) Rayon spectral

→ Définition du rayon spectral d'une matrice ρ

→ Ex : Le rayon spectral d'une matrice orthogonale vaut 1

→ Th : Pour tout norme matricielle $|||\ |||$, $\rho(A) \leqslant |||A|||$ et $\forall \varepsilon > 0$, il existe une norme subordonnée $|||\ |||$ telle que $|||A||| \leqslant \rho(A) + \varepsilon$ $\boxed{\text{DEV1}}$

→ Th : Conditions de convergence : $A^k \to 0$ ssi $\rho(A) < 1$ ssi $\exists ||\ ||$ tel que $||A|| < 1$

3) Conditionnement

→ Ex : [Cia p 27] : Une petite erreur peut se répercuter beaucoup

→ Définition du conditionnement + ex : $\text{cond}_2(O \in O_n(\mathbb{R})) = 1$ + prop de base

→ Th : Les deux théorèmes reliant erreur relative et conditionnement [Cia p 28-29]

→ Interprétation : Un conditionnement petit c'est bien car ça permet de ne pas amplifier les erreurs

→ Rq : ($\text{cond}_2(O \in O_n(\mathbb{R})) = 1$ + sous multiplicativité + interprétation) $\Rightarrow$ les changements de base orthogonaux n'amplifient pas les erreurs !

II/Résolution de systèmes linéaires

Cadre : $A \in GL_n(\mathbb{K})$. On veut résoudre $Ax = b$. Dessin de la décomposition E/D/F de A. On décompose $A = M - N$ avec M inversible

1) Description et théorème de convergence

→ Définition d'une méthode itérative, de la matrice d'itération ($= M^{-1}N$), du fait qu'une méthode itérative converge

→ Th : La méthode est convergente ssi $\rho(M^{-1}N) < 1$ $\boxed{\text{DEV1}}$

→ Co : Si A est hermitienne définie positive et $M^* + N$ aussi, la méthode converge

2) Exemples de méthodes itératives

→ Définition : Méthode de Jacobi + matrice d'itération = J

→ Prop : Si A est à diagonale strictement dominante, la méthode de Jacobi converge + ex

→ Définiton : Méthode de Gauss-Siedel (= GS) + matrice d'itération = L_1 + rq : c'est un cas particulier de la méthode de relaxation

→ Prop : Si A est tridiagonale, $\rho(L_1) = \rho(J)^2$ donc Jacobi converge dès que GS converge et GS est meilleure

→ Définitin : Méthode de relaxation + matrice d'itération = L_ω

→ Prop : Si la relaxation converge, $\omega \in]0, 2[$ et c'est même une équivalence si $A \in H_n^{++}$

→ Ex : La matrice du Laplacien discret est hermitienne définie positive donc fait converger toutes les méthodes

→ Rq : Le but avec la relaxation, c'est de trouver le ω optimal (celui pour lequel $\rho(L_\omega)$ est le plus petit possible)

→ Méthode de Kaczmarz $\boxed{\text{DEV2}}$

3) Méthodes variationnelles [HU]

Ici, $A \in S_n^{++}(\mathbb{R})$

→ Gradient à pas fixe

→ Gradient à pas optimal + dessin

III/Recherche de valeurs propres

→ On recherche les valeurs propres dans $D(0, |||A|||)$ où $|||\ \ |||$ est subordonnée

→ Prop : On recherche les valeurs propres dans les disques de Gershgörin

→ Méthode de la puissance pour la recherche de valeurs propres

→ Rq : On applique cette méthode à A^{-1} pour avoir la plus petite valeur propre de A

→ Rq : On applique cette méthode à $A - \alpha I_n$ pour avoir les autres

Références : Ciarlet [Cia] (principalement), [HU]

Développements :

→ Méthode de Kaczmarz [Sans ref, trouvé sur le site de Théo Pierron]

→ Convergence des méthodes itératives [Cia p 96]

236. Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables.

Plan :

I/Méthodes directes

1) Par connaissance d'une primitive

→ Définition primitive + ex

→ Ex : Calcul d'intégrale d'une fraction rationnelle = décomposition en éléments simples

→ Ex : Calcul d'intégrale en sinus et cosinus = linéariser

2) Intégration par parties

→ Th : Intégration partie

→ Ex : Calcul d'une intégrale dont l'intégrande est le produit d'une exponentielle et d'un polynôme

→ Appli : Calcul de la formule de récurrence pour les intégrales de Wallis + csqc : $\Gamma(n+1) = n\Gamma(n)$

→ Théorème de Fubini + appli : dans la partie suivante

3) Changement de variables

→ Prop : Changement de variables (cas à une variable puis à plusieurs variables)

→ Ex : Changement de coordonnées polaire / sphérique

→ Appli : Un calcul de l'intégrale de Gauss + volume de la boule euclidienne dans $\mathbb{R}^n$ [BP p 246]

II/Méthodes utilisant une convergence

1) Convergence uniforme sur un compact

→ Prop : Si (f_n) converge uniformément vers f sur le compact $[a, b]$ alors $\int_a^b f(t)\mathrm{d}t = \lim \int_a^b f_n(t)\mathrm{d}t$

→ Appli 1 : Sommes de Riemann [GouAn p 124] + calcul de sommes [GouAn p 129]

→ Appli 2 : Formule sommatoire de Poisson + appli $\boxed{\text{DEV1}}$

2) Convergence dominée

→ Théorème de convergence dominée [BP p 134] ou [GouAn pour une version plus facile]

→ Ex : Calcul de l'intégrale de Fresnel

→ Csqc : Inversion somme et intégrale sous hypothèses

3) Passage par les fonctions définies par une intégrale à paramètre

→ Prop : Théorème de continuité / dérivabilité d'une fonction définie par une intégrale à paramètre

→ Appli : Un autre calcul de l'intégrale de Gauss $\boxed{\text{DEV2}}$

→ Appli : Calcul de $\int_0^\infty \frac{\sin(xt)}{t} e^{-t}\mathrm{d}t$ [GouAn]

III/Calcul approché

→ Définition de l'ordre d'une méthode d'approximation

→ Méthode des rectangles, des trapèzes... + comparaison

→ Méthode de Monte Carlo

On peut aussi parler de l'utilisation de l'analyse complexe, mentionner le théorème des résidus qui permet de calculer pas mal de types d'intégrales.

Références : Gourdon analyse [GouAn], [BP], Demailly [De]

Développements :

→ Un calcul de l'intégrale de Gauss [GouAn p 163]

$\rightarrow$ Formule sommatoire de Poisson [GouAn p 272 et 164]

239. Fonctions définies par une intégrale dépendant paramètre. Exemples et applications.

Plan :

I/Régularité [ZQ]
1) Continuité

→ Th : Continuité sous l'intégrale
→ Ex : La fonction Γ d'Euler est continue
→ Ct-ex : $x \longmapsto \in_0^{+\infty} xe^{-xt}\mathrm{d}t$ n'est pas continue en 0 alors que l'intégrande l'est (il manque la domination) + ct-ex quand il manque la continuité [Hau]

2) Régularité d'ordre supérieure

→ Th : Dérivabilité sous l'intégrale + extension à C^k sous l'intégrale
→ Ex : Γ est de classe C^∞
→ Appli : Un calcul de l'intégrale de Gauss $\boxed{\text{DEV1}}$

II/Convolution
1) Définition + props

→ Définition de la convolution (cas L^1) + commutativité
→ Prop : Comportement de la convolution para rapport aux normes p
→ prop : Comportement de la convolution par rapport à la dérivation
→ Appli : Régularisation de f en convolant avec une fonction C^∞ à support compact (+ ex d'une telle fonction)

2) Approximation de l'unité

→ Définition d'une approximation de l'unité + ex
→ Prop : Construction approximation de l'unité
→ Appli : Densité des fonctions C^∞ à support compact dans L^p (pour $1 \leqslant p < \infty$ (résultat difficile et faux pour $p = \infty$)

III/Deux intégrales à paramètre célèbres (qui sont en fait les mêmes)
1) Transformation de Fourier

→ Définition de la transformation de Fourier (TF) + TF de la gaussienne
→ Prop : La TF est continue, linéaire, tend vers 0 à l'infini
→ Prop : Lien dérivation et TF / convolution et TF
→ Prop : Injectivité et inversion de Fourier
→ Appli : Formule de Poisson + appli $\boxed{\text{DEV2}}$

2) Fonction caractéristique

→ Définition de la fonction caractéristique
→ Prop : Elle caractérise la loi d'une variable aléatoire

Références : [OA], [ZQ], Gourdon analyse [GouAn], Hauchecorne [Hau]

Développements :

→ Un calcul de l'intégrale de Gauss [GouAn p 163]
→ Formule sommatoire de Poisson [GouAn p 272 et 164]

243. Convergence des séries entières, propriétés de la somme. Exemples et applications.

Plan :

Cadre : Les coefficients ici considérés sont a priori complexes même si on se concentrera surtout sur ceux réels

I/Rayon de convergence

Dans la suite $(a_n)_n$ et $(b_n)_n \in \mathbb{C}^n$

1) Définition

- → Définition : La série entière associée à $(a_n)_n$ est la série des fonctions $\left\{ \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & a_n z \end{array} \right.$
- → Lemme d'Abel
- → Définition du rayon de convergence R + dessin rappelant les diverses propriétés de la somme selon l'endroit où on se trouve par rapport au disque de convergence + rappeler qu'on ne peut rien dire sur ce qui se passe sur le cercle de convergence
- → Ex : Pour $\sum \frac{z^n}{n!}$, $R = +\infty$; pour $\sum \frac{z^n}{n}$, $R = 1$; pour $\sum n! z^n$, $R = 0$
- → Prop : Le domaine de définition de $\sum a_n z^n$, U, est tel que $\overset{D}{(}\ 0,1) \subset U \subset \overline{D}(0,1)$
- → Rq : On peut avoir inclusion stricte des deux côtés ($\sum \frac{z^n}{n}$), égalité à gauche ($\sum z^n$) ou égalité à droite ($\sum \frac{z^n}{n^2}$)

2) Calcul de rayons de convergence

- → Prop : Si $\sum a_n z_0^n$ converge alors $R \geqslant |z_0|$ et si $\sum a_n z_0^n$ diverge alors $R \leqslant |z_0|$
- → Prop : Règle de d'Alembert + ex + attention elle ne s'applique pas toujours (séries lacunaires)
- → Prop : Règle de Hadamard + ex
- → Prop : Dans le cas général, considérer la suite sumérique $\sum a_n z^n$ et lui appliquer tous les critères qu'on connaît pour les séries numériques
- → Prop : Comparaison : Si $a_n = O(n^\alpha b_n)$ alors $R_b \leqslant R_a$

3) Opérations sur les séries entières

- → Prop : Rayon de convergence d'une somme de séries entières en fonction des rayons de convergence des deux séries impliquées
- → Prop : Produit de Cauchy de séries entières + rayon de convergence de ce produit

II/Propriété de la somme

On note s la somme de la série entière $\sum a_n z^n$ de rayon $R > 0$ donc définie au moins sur $D(0, R)$

1) Régularité

- → Prop : Convergence normale de la série sur tout compact inclus dans $D(0, R)$
- → Csqc : s est continue sur $D(0, R)$ + appli : principe des zéros isolés
- → Prop : s est C^∞ sur $]-R, R[$ + expressions des dérivées + les dérivées successives ont même rayon de convergence que s
- → Rq : On en déduit par récurrence que $a_n = \frac{s^{(n)}(0)}{n!}$ $(\star)$
- → Appli : On en déduit le DSE de $\frac{1}{(1-x)^p}$ par dérivation

2) Intégration

- → Prop : Intégration d'une série entière
- → Appli : Calcul du DSE de $ln(1+x)$ et de $\arctan(x)$

3) Le problème général du DSE

- → définition d'une fonction DSE en z_0 + définition fonction analytique = DSE en tout point

→ Prop : Si f est DSE en a, f est C^∞ sur $]-R,R[$ et égale à sa série de Taylor par $(\star)$

→ Rq : La réciproque est fausse : $x \longmapsto e^{\frac{-1}{x^2}}$ prolongée en 0 par 0 est de classe C^∞ mais est différente de sa série de Taylor

→ Rq : Ça donne l'unicité du DSE

→ Appli 1 : Nombres de Bell $\boxed{\text{DEV1}}$

→ Appli 2 : Equation de Bessel $\boxed{\text{DEV2}}$

→ Th : Les fonctions analytiques sur un ouvert Ω sont exactement les fonctions holomorphes sur Ω

Références : El Amrani [ElA], Gourdon analyse [GouAn], XENS algèbre 1 [FGNal1], XENS analyse 4 [FGNan4]

Développements :

→ Nombres de Bell [FGNal1 p 14]

→ Equation de Bessel [FGNan4 p 101]

246. Séries de Fourier. Exemples et applications.

Idée de défense de plan : Les séries de Fourier ont été introduites pour résoudre des équations aux dérivées partielles (équation de la chaleur). L'avantage c'est que cette théorie transforme les équations différentielles en équations polynomiales.

Plan :

Cadre : $f : \mathbb{R} \longrightarrow \mathbb{C}$, 2π périodique + rappel de la définition d'une fonction de classe C^k par morceaux [GouAn p 258]

I/Coefficients de Fourier

1) Définitions [GouAn]

- → Définition des a_n, b_n, c_n dès que $f \in L^1$
- → Définition des séries de Fourier (version complexe et version réelle) $S_n(f)$
- → Prop : Relation entre les a_n/b_n et les c_n
- → Rq : Si f est paire, les b_n sont nuls et si f est impaire, les a_n sont nuls
- → Ex : Calcul des coeffs de Fourier de $f_0 : \left\{ \begin{array}{lcl}]-\pi,\pi] & \longrightarrow & \mathbb{C} \\ x & \longmapsto & |x| \end{array} \right.$ prolongée 2π périodiquement (faire un dessin de la fonction)

2) Propriétés

- → Prop : Calcul des $c_n(\overline{f})$, de $c_n(t \mapsto f(-t))$... en fonction de $c_n(f)$
- → Prop : Lemme de Riemann-Lebesgue
- → Csqc : $F : \left\{ \begin{array}{lcl} (L^1([0,2\pi]), || \ ||_1) & \longrightarrow & (c_0(\mathbb{Z}), || \ ||_\infty) \\ f & \longmapsto & (c_n(f))_{n\in\mathbb{Z}} \end{array} \right.$ est bien définie, linéaire, continue et de norme 1
- → Prop : Si f est C^{k-1} et C^k par morceaux, $c_n(f^{(k)} = (in)^k c_n(f)$ d'où $c_n(f^{(k)}) = o(\frac{1}{n^k})$ donc lus f est régulière plus ses coefficient de Fourier sont petits

II/Convergences

1) Un cas de divergence

- → Théorème de Banach Steinhaus + appli : il existe une fonction continue différente de sa série de Fourier $\boxed{\text{DEV1}}$

2) Convergence au sens de Cesàro [OA]

- → Définition noyau de Dirichlet $D_n(t)$ et noyau de Féjer et $K_n(t)$
- → Définition sommes de Cesàro $\sigma_n(f)$
- → Prop : $S_n(f)$ est la convolution de f et D_n et $\sigma_n(f)$ est la convolution de f et de K_n
- → Théorème de Féjer : Si f est continue, $\sigma_n(f)$ converge uniformément vers f
- → Appli : Densité des polynômes trigonométriques + infectivité de F

3) Convergence de la série de Fourier

- → Théorème de Dirichlet
- → Ex : $S_n(f_0)(0) = f(0)$ d'où un calcul de $\sum \frac{1}{(2n+1)^2}$ puis de $\zeta(2)$
- → Théorème de Dirichlet uniforme
- → Appli : Formule sommatoire de Poisson + appli $\boxed{\text{DEV2}}$
- → Appli : Utilisation dans la résolution d'équations différentielles + ex : $y^{(4)} + 5y'' + 4y = sin(t)$ devient une équation polynomiale : $n^4 c_n(f) + 5n^2 c_n(f) + 4c_n(f) = c_n(t \mapsto \sin(t))$ d'où les c_n puis une solution f si f est suffisamment régulière pour être égale à sa série de Fourier

4) Convergence dans L^2 [OA]

- → Définition du produit scalaire sur L^2 + rq : $c_n(f) =< f, e_n >$ et $S_n(f)$ est la projection de f sur le sous espace $\{e_k | k \leqslant |n|\}$ où $e_n : t \longmapsto e^{int}$

→ Th : Si $f \in L^2$, $S_n(f)$ converge vers f pour la norme 2
→ Prop : Formule de Parseval
→ Appl : Exo [GouAn p 262]

Références : [OA] (principalement), Gourdon analyse [GouAn]

Développements :

→ Théorème de Banach-Steinhaus [GouAn p 404-405]
→ Formule sommatoire de Poisson [GouAn p 272 et 164]

250. Transformation de Fourier. Applications.

IMPASSE

260. Espérance, variance et moments d'une variable aléatoire.

Plan :

Cadre : X est une variable aléatoire réelle sur un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$

I/Espérance

1) Définition

- → Définition de l'espérance de X et d'un vecteur aléatoire
- → Rq : Définition d'une variable centrée
- → Ex : Espérance d'une variable presque constante, espérance d'une indicatrice
- → Théorème de transfert

2) Exemples de calcul

- → Prop : Si X est discrète, $\mathbb{E}(X) = \sum\limits_{x \in V} x\mathbb{P}(X = x)$ où $V = \{x \in \mathbb{R} | \mathbb{P}(X = x) > 0\}$
- → Ex : Espérance d'une Bernoulli, binomiale, Poisson, géométrique
- → Prop : Si X est à densité f, $\mathbb{E}(X) = \int_{\mathbb{R}} xf(x)\mathrm{d}x$
- → Ex : Espérance d'un loi normale, exponentielle, uniforme
- → Ex : Une loi de Cauchy n'a pas d'espérance

3) Propriétés

- → Prop : L'espérance est linéaire
- → Prop : Inégalité de Jensen
- → Prop : Inégalité de Markov + appli : hachage parfait $\boxed{\text{DEV1}}$
- → Définition de variables mutuellement indépendantes via l'espérance
- → Prop : Si les variables sont indépendantes, $\mathbb{E}(\prod X_i) = \prod \mathbb{E}(X_i)$ + réciproque fausse

II/Moment d'ordre 2, variance

1) Variance

- → Définitions : moment d'ordre 2, variance, variable réduite, écart type
- → Prop : Expression de la variance + la variance est positive
- → Ex : Variance d'une binomiale / loi normale
- → Prop : Calcul de $\mathrm{Var}(X + a)$ et $\mathrm{Var}(aX)$
- → Prop : Inégalité de Tchebychev + appli : Stone-Weierstrass par les polynômes de Bernstein

2) Covariance [Ouv]

- → Prop : Inégalité de Cauchy-Schwartz (ce qui permet de définir la covariance)
- → Définition covariance + rq : généralisation avec la matrice de covariance pour les vecteurs aléatoires

3) Lien avec l'indépendance

- → Définition : Variables non corrélées
- → Prop : L'indépendance implique la non corrélation + la réciproque est fausse (sauf pour des vecteurs gaussiens)
- → Prop : Identité de Bienaymé + Inégalité de Bienaymé-Tchebychev

III/Moments d'ordre p

1) Définition

- → Définition + ex pour la loi normale
- → Prop : Inégalité de Hölder + implique les inclusion des L^p
- → Prop : Inégalité de Minkowski + ça implique que $|| \ ||_p = (\mathbb{E}| \ |^p)^{\frac{1}{p}}$ est une norme

2) Fonction caractéristique

- → Définition fonction caractéristique

→ Prop : $\varphi_X = \varphi_Y$ implique X et Y ont même loi (+ appli : démo du TCL)
→ Prop : φ_X caractérise la loi de X
→ Prop : Lien entre φ_X et moment s de X [BL p 64]
→ Prop : Si φ_X est analytique, la loi de X est caractérisée par ses moments + attention ce n'est pas le cas en général

IV/Moments et théorèmes limites

→ Th : Loi faible des grands nombres, loi forte des grands nombres (admis)
→ Appli : Méthode de Monte Carlo pour le calcul approché d'intégrale
→ Théorème central limite (TCL) $\boxed{\text{DEV2}}$

Références : Barbe-Ledoux [BL], Ouvrard [Ouv], Cormen [Cor] (pour le développement), Zuily-Queffélec [ZQ] (pour le développement)

Développements :

→ Hachage parfait [Cor p 258-262]
→ Théorème central limite [ZQ p 540]

264. Variables aléatoires discrètes. Exemples et applications.

Plan :

Cadre : $(\Omega, \mathcal{F})$ est un espace probabilisé

I/Variables aléatoires (= va) et lois discrètes

1) Définitions

- → Définition d'un va discrète = une fonction $X : \Omega \longrightarrow E$ mesurable et telle que $X(\Omega)$ est dénombrable
- → Rq : Souvent, $E = \mathbb{N}/\mathbb{Z}/\mathbb{N}^n$
- → Définition d'un loi d'une va discrète + il suffit de connaître $\mathbb{P}(X = x)$ pour $x \in X(\Omega)$ pour la connaître

2) Exemples

- → Déf : Loi uniforme + ex X = chiffre obtenu en lançant un dé 6 suit une loi uniforme sur $[\![1, 6]\!]$
- → Déf : Loi de Bernoulli $\mathcal{B}(p)$ + ex $X : \Omega \longrightarrow \{P, F\}$ donnant le lancer d'une pièce suit une binomiale de paramètre $\frac{1}{2}$
- → Déf : Loi binomiale $\mathcal{B}(n, p)$ = nombre de succès dans une suite de n Bernoulli indépendantes de paramètre p + ex : Si on a n boules dont p noirs et qu'on les tire avec remise, X = nombre de boules noires suit un binomiale de paramètres n et p
- → Déf : Loi géométrique $\mathcal{G}(p)$: compte le nombre d'échec avec succès dans une répétition de Bernoulli indépendantes + ex : on lance une pièce jusqu'à avoir un pile et on gagne X = le nombre de lancers euros ; alors $X \sim \mathcal{G}(p)$
- → Déf : Loi de Poisson + ex : décrit le nombre d'événements rares qui arrivent dans un intervalle de temps donné (nombre d'accidents / erreurs de fabrication)

II/Moments d'un va discrète

1) Espérance

- → Définition de l'espérance + quelques prop
- → Lemme de transfert + appli : polynômes de Bernstein et théorème de Weierstrass
- → Ex : Calcul des espérances des loi du I/
- → Prop : Inégalité de Markov + appli : hachage parfait $\boxed{\text{DEV1}}$

2) Fonction caractéristique

- → Définition variance, expression + moments d'ordre p
- → Définition fonction caractéristique φ + prop : elle caractérise la loi

III/Indépendance et sommes de va

- → Définition de va indépendantes dans le cas discret
- → Csqc : Si les X_i sont indépendantes, $\mathbb{E}(\prod X_i) = \prod \mathbb{E}(X_i)$ et $\varphi_{(X_1,\dots,X_n)} = \prod \varphi_{X_i}$
- → Prop : Loi d'une somme de va discrètes indépendantes [Ouv p 61 et suivantes]
- → Ex : Somme de va de Bernoulli indépendant = une binomiale

IV/ Théorèmes limites

- → Prop : Approximation loi de Poisson par une suit de géométriques + ex paradoxe des anniversaires [Ouv p 220]
- → Prop : Loi des grands nombres faible puis forte (admise)
- → Appli 1 : Méthode de Monte Carlo
- → Appli 2 : Calcul d'une proba du nombre de pièces défectueuses à partir d'un échantillon
- → Théorème central limite $\boxed{\text{DEV2}}$

Références : Barbe-Ledoux [BL], Ouvrard [Ouv], Cormen [Cor] (pour le développement), Zuily-Queffélec [ZQ] (pour le développement)

Développements :

→ Hachage parfait [Cor p 258-262]

→ Théorème central limite [ZQ p 540]

Bibliographie

[Aud] Audin, *Géométrie*
[BL] Barbe et Ledoux, *Probabilité*
[BP] Briane et Pagès, *Théorie de l'intégration*
[Bre] Brézis, *Analyse fonctionnelle*
[Cia] Ciarlet, *Introduction à l'analyse numérique matricielle et à l'optimisation*
[Com] Combes, *Algèbre et géométrie*
[Cor] Cormen et alii, *Algorithmique*
[dB] De Biasi, *Mathématiques pour le CAPES et l'agrégation interne*
[De] Demailly, *Elements d'analyse réelle*
[Dem] Demazure, *Cours d'algèbre*
[DJM] Dany-Jack Mercier, *Cours de géométrie, préparation au CAPES et à l'agrégation*
[dSP] de Seguin Pazzis, *Invitation aux formes quadratiques*
[Eid] Eiden, *Géométrie analytique classique*
[ElA] El Amrani, *Suites et séries numériques, suites et séries de fonctions*
[FG] Francinou, Gianella, *Exercices de mathématiques pour l'agrégation, algèbre 1*
[FGNal1] Francinou, Gianella, Nicolas, *Oraux XENS algèbre 1*
[FGNal2] Francinou, Gianella, Nicolas, *Oraux XENS algèbre 2*
[FGNal3] Francinou, Gianella, Nicolas, *Oraux XENS algèbre 3*
[FGNan1] Francinou, Gianella, Nicolas, *Oraux XENS analyse 1*
[FGNan4] Francinou, Gianella, Nicolas, *Oraux XENS analyse 4*
[GouAl] Gourdon, *Algèbre*
[GouAn] Gourdon, *Analyse*
[Goz] Gozard, *Théorie de Galois*
[Gri] Grifone, *Algèbre linéaire*
[Hau] Hauchecorne, *Les contre exemples en mathématiques*
[HU] Hiriart et Urruty, *Optimisation et analyse convexe*
[H2G2] Caldero et Germoni, *Histoire hédoniste de groupes et de géométrie*
[MT] Mneimné et Testard *Introduction à la théorie des groupes de Lie classiques*
[OA] Beck, Malick et Peyré, *Objectif agrégation*
[Ouv] Ouvrard, *Probabilités : tome 1*
[Per] Perrin, *Cours d'algèbre*
[RB] Risler et Boyer, *Algèbre pour la licence 3, groupes, anneaux, corps*
[Rou] Rouvière, *Petit guide de calcul différentiel à l'usage de la licence et de l'agrégation*
[Ser] Serre, *Cours d'arithmétique*
[Szp] Szpirglas, *Mathématiques Algèbre L3*
[Tau] Tauvel, *Géométrie*
[Tes] Testard, *Analyse mathématique : la maîtrise de l'implicite*
[Ulm] Ulmer, *Théorie des groupes : Cours et exercices*
[Zav] Zavidovique, *Un max de maths : problèmes pour agrégatifs et mathématiciens, en herbe ou confirmés*
[ZQ] Zuily et Queffélec, *Analyse pour l'agrégation*