Développements & Leçons pour l'Agrégation de Mathématiques Option Informatique

Lopez Aliaume

6 mars 2019

TODO LIST

CHAPITRE 1

INDEX

- **LIENS**
- STATISTIQUES INFO
- DÉVELOPPEMENTS INFO
- LEÇONS INFO
- STATISTIQUES MATHS
- DÉVELOPPEMENTS MATHS
- LEÇONS MATHS

Première partie

Informatique

CHAPITRE 2

STATISTIQUES — 2019-03-06

■ **DÉVELOPPEMENTS**

Nombre de devs	23
Nombre optimal	[Désactivé à la compilation]
Recasage moyen	1.91
Rédaction	19 sur 23

■ **LEÇONS**

Sans développement (abs)	0
Un seul développement (abs)	0
Nombre moyen de développments	2.10
Écart-type σ	0.29
Rédaction	21 sur 21

■ **[DEADLINE] DÉBUT DES ORAUX AGRÉGATION**

Date	2018-06-29
Dans	-251 Jours
OVERDUE	...

■ **LIENS**

☐ DÉVELOPPEMENTS

☐ LEÇONS

CHAPITRE 3

DÉVELOPPEMENTS

3.0 ■ ANALYSE DU TRI RAPIDE

Référence : Cormen, Beauquier. Recasé 3 fois

■ **LEÇONS**

L902 DIVISER POUR RÉGNER. EXEMPLES ET APPLICATIONS ★★★★★

L903 EXEMPLES D'ALGORITHMES DE TRI. CORRECTION ET COMPLEXITÉ. ★★★★★

L926 ANALYSE DES ALGORITHMES, COMPLEXTÉ. EXEMPLES. ★★★★★

■ **RÉFÉRENCES**

Cormen

Beauquier

3.0.1 Étude préliminaire

Étape 1 Complexité de l'algorithme du pivot est exactement n opérations de comparaison. Le fait que le pivot transforme une permutation et tout.

Étape 3 (À ne pas démontrer) Étude de la complexité dans le pire des cas avec un peigne. Ceci se démontre par récurrence sur la liste constante $1,\dots,1$.

Par la suite chaque niveau fait une opération de pivot, et comme il y a exactement $n-1$ niveaux qui possèdent des listes de taille 2 à n on peut conclure pour une complexité en $\Omega(n^2)$.

Étape 4 C'est bien la pire complexité qu'on puisse atteindre, car en prenant un arbre d'appels, chaque niveau fait dans le pire des cas n comparaisons (via des appels à pivot) et la profondeur de l'arbre est plus petite que n, on a donc un $O(n^2)$ en majoration.

3.0.2 Étude en moyenne

Étape 1 On pose $\sigma \sim \mathscr{U}(S_n)$.

Notation σ^g et σ^d pour les résultats gauche et droits de l'opération de pivot ainsi que $r(\sigma) = \sigma(1)$ le rang du pivot dans la permutation.

Étape 2 L'opération pivot "conserve le tirage uniforme".

Pour cela on fixe $r(\sigma) = k$ et on regarde la probabilité conditionnelle. On veut montrer

$$\mathbb{P}(\sigma^g = \square \mid r(\sigma) = k) \sim \mathscr{U}(S_{k-1}) \tag{3.1}$$

Démonstration. On commence par remarquer que l'algorithme de pivot possède certaines propriétés intéressantes, en effet il est surjectif et l'ensemble des permutations ayant pour image (σ^g, k, σ^d) s'obtient assez simplement.

On le calcule comme suit : Pour avoir cette image-ci il faut que l'ensemble des éléments dans σ^g soient ordonnés comme dans σ^g (idem pour σ^d) et donc comme k est nécessairement en première position, on sait qu'il suffit de placer les éléments de σ^g dans les $n-1$ cases restantes (l'ordre étant imposé).

On a donc

$$pivot^{-1}(\sigma^g, k, \sigma^d) = \binom{n-1}{k-1} \tag{3.2}$$

Il est donc clair que pour $\rho \in S_{k-1}$ on a

$$\left|\{\sigma \in S_n \mid r(\sigma) = k \wedge \sigma^g = \rho\}\right| = \binom{n-1}{k-1} \times |S_{n-k}| = \frac{|S_{n-1}|}{|S_k|} \tag{3.3}$$

On a donc bien une distribution uniforme (utiliser la formule des probabilités conditionnelles !).

□

Étape 3 On peut faire notre étude en moyenne en posant $X(\sigma)$ le nombre de comparaisons effectuées par le tri rapide sur la permutation σ.

On pose $M_n = \mathbb{E}(X(\sigma))$ avec σ suivant une distribution uniforme sur S_n.

On a

$$\begin{aligned} M_n &= \sum_{k=1}^{n} \mathbb{E}(X(\sigma)|r(\sigma)=k)\frac{1}{n} \\ &= \frac{1}{n}\sum_{k=1}^{n} \mathbb{E}(X(\sigma^g)+X(\sigma^d)+n+1) \\ &= \frac{1}{n}\sum_{k=1}^{n} M_{k-1}+M_{n-k}+n+1 \\ &\leq n+1+\frac{2}{n}\sum_{k=1}^{n-1} M_k \end{aligned}$$

Étape 4 Résolution par substitution.

On recherche un α tel que $M_k \leq \alpha k \log k$.

Pour cela on injecte dans l'équation de récurrence et on trouve

$$M_n \leq n+1+\frac{2\alpha}{n}\sum_{k=1}^{n-1} k\log k \tag{3.4}$$

On peut majorer cette somme via une comparaison série-intégrale

$$\sum_{k=1}^{n} k\log k \leq \int_1^n t\log t\,dt = \frac{1}{2}n^2\log n - \frac{n^2}{4} \tag{3.5}$$

En injectant on trouve alors

$$M_n \leq n+1+\alpha n\log n - \frac{\alpha}{2}n \tag{3.6}$$

Il suffit donc de choisir $\alpha \geq 4$ pour déduire

$$M_n \leq \alpha n\log n \tag{3.7}$$

On peut ensuite vérifier que cela fonctionne pour les cas de base, et c'est effectivement vrai.

3.1 ■ ARBRES AVL

Référence : Beauquier. Recasé 3 fois

■ **LEÇONS**

L901 STRUCTURES DE DONNÉES. EXEMPLES ET APPLICATIONS. ★★★★★

L921 ALGORITHMES DE RECHERCHE ET STRUCTURES DE DONNÉES ASSOCIÉES. ★★★★★

L926 ANALYSE DES ALGORITHMES, COMPLEXTÉ. EXEMPLES. ★★★★

■ **RÉFÉRENCES**

Éléments d'algorithmique page 152

Objectif Améliorer les ABR en conservant une propriété d'équilibrage

Définition On note h la fonction hauteur, g et d les fonctions sous arbre gauche et sous arbre droit.

$$\delta(A) = h(g(A)) - h(d(A))$$

On dit qu'un arbre A est AVL (Adelson-Velskii et Landis) ssi $\delta(A) \in \{-1, 0+1\}$

Utilisation de l'espace On veut savoir si cette restriction contrôle effectivement la hauteur maximale d'un arbre AVL, ce qui permettra ultimement de garantir les complexités optimales des ABR.

On pose $N(h)$ le nombre minimal de sommet d'un AVL de hauteur h. On constate que N vérifie l'équation de récurrence

$$\begin{cases} N(0) = 0 \\ N(h+1) = 1 + N(h) + N(h-1) \end{cases} \tag{3.8}$$

En posant $F(h) = N(h) + 1$ on constate que F est précisément la suite de Fibonacci.

Or on sait que $F(h) \geq \frac{1}{\sqrt{5}}\phi^h$.

On a donc $h \leq O(\log_2(n))$ où n est le nombre de clefs dans l'arbre AVL.

Implémentation On considère la définition récursive

$$t := \emptyset \mid \text{Noeud}(x, h, t, t)$$

Avec h la hauteur de l'arbre t, afin d'éviter de la recalculer.

On suppose que la fonction δ est définie sur ce type de données, ainsi que les fonctions g et d.

Rotations Afin de ré-équilibrer un arbre binaire, on introduit des opérations qui s'effectuent en temps constant et diminuent $\delta(A)$.

DESSIN ROTATION GAUCHE/DROITE

DESSIN ROTATION GAUCHE–DROITE

DESSIN ROTATION DROITE–GAUCHE

Theoreme Les rotations se font en temps constant, et ré-équilibrent quand le besoin se fait sentir.

On définit la fonction Balance qui permet de ré-équilibrer n'importe quel arbre AVL partout sauf pour sa racine, avec $\delta(A) \in \{-2, -1, 0, +1, +2\}$, via une rotation, une double-rotation.

On ne le fait que sur un exemple où le déséquilibrage est de 2 puis 1 avec une rotation gauche. Les autres cas sont laissés admis.

Insertion On traite le cas de l'insertion dans un AVL pour illustrer l'utilisation des rotations.

Cet algorithme est correct, car il conserve l'invariant des ABR, et que l'ajout d'un nœud ne peut augmenter h que de 1, donc l'opération Balance donne bien un AVL en sortie car on lui fournit un AVL +1 en entrée.

De plus cette opération se fait en $O(\log(n))$ puisqu'en temps constant sur tout un chemin de taille au plus h qui est un $O(\log n)$.

Algorithm 1 Insertion dans un AVL

```
INSERT(x,t) := case t of
    | VIDE -> Noeud (x,0,VIDE,VIDE)
    | _    ->
        if x < clef(t) then
            g' := INSERT (x,g(t))
            BALANCE (Noeud (clef(t),
                     max (1 + h(g'(t)), h(t)),
                     g', d(t)))
        else if x > clef (t) then
            d' := INSERT (x,d(t))
            BALANCE (Noeud (clef(t),
                     max (1 + h(d'(t)), h(t)),
                     g(t), d'))
        else
            t
        end;;
```

Remarque On a besoin d'au plus une rotation, en effet, une fois corrigée, l'erreur ne se propage pas ! Ce n'est en revanche pas le cas pour la suppression, qui peut nécessiter plusieurs rotations.

3.2 ■ HIÉRARCHIE EN ESPACE ET EN TEMPS

Référence : Arora Barack. Recasé 2 fois

■ **LEÇONS**

L913 MACHINES DE TURING. APPLICATIONS. ★★★★★

L915 CLASSES DE COMPLEXITÉ. EXEMPLES. ★★★★★

■ **RÉFÉRENCES**

Arora Barack

Carton

On fixe un alphabet $\Sigma = \Sigma' \uplus \{\$\}$, et on considère uniquement des machines avec alphabet d'entrée Σ avec k-bandes de travail d'alphabet non fixé.

On fixe un codage des machines concernées sur l'alphabet Σ' (attention, sans le \$).

3.2.1 En espace

Théorème 1. *Soient f, g propres en espace avec $f = o(g)$ alors $SPACE(f) \subsetneq SPACE(g)$*

On construit pour cela la machine suivante.

```
M(w) =
    Si w = <M'>$^k alors
        Simule M' sur w avec un espace/temps
        de g(|w|) AU NIVEAU DE LA MACHINE
                  VIRTUELLE !!!!!
        Si la simulation termine correctement
            retourne l'opposé
        Sinon
            retourne Faux
    Sinon
        Faux
```

1. La machine M est dans $SPACE(g)$. En effet, la simulation ne prend par construction qu'un espace inférieur à g, et le surcoût pour le faire est un compteur qui prend un espace $O(g)$ car g est propre.
2. La machine M n'est pas dans $SPACE(f)$. Par l'absurde, si elle l'était, elle calculerait en espace inférieur à $Cf(n)$.
   Le coût de simulation de $< M >$ serait alors de $C'f(n)$.
   Mais comme $f = o(g)$ on a un k tel que

$$C'f(|< M >\$^k|) < g(|< M >\$^k|) \tag{3.9}$$

   Ainsi sur ce code la simulation ne dépasse pas les bords et on peut écrire

$$M(< M >\$^k) = \neg M(< M >\$^k) \tag{3.10}$$

   Ce qui est absurde.

3.2.2 En temps

On peut adapter la machine M pour fonctionner avec un *timeout* de $g(|w|)$.

Si une machine M' calcule en temps Cf alors sa simulation prend un temps inférieur à $C'f^2$, et donc on demande dans le théorème $f^2 = o(g)$.

Théorème 2. *Si f, g sont propres en temps et $f^2 = o(g)$ alors $TIME(f) \subsetneq TIME(g)$.*

3.2.3 En espace non-déterministe

Théorème 3. *Si f, g sont propres en espace avec $f = o(g)$ alors $NSPACE(f) \subsetneq NSPACE(g)$.*

On ne peut pas utiliser la même réduction, car le code de M ne donnerait alors pas la négation au sens non-déterministe !

En revanche on peut construire la machine sans la négation.

```
M(w) =
    Si w = <M'>$^k alors
        Simule M' sur w avec un espace/temps
        de g(|w|) AU NIVEAU DE LA MACHINE
                  VIRTUELLE !!!!!
        Si la simulation termine correctement
            retourne le même résultat
        Sinon
            retourne Faux
    Sinon
        Faux
```

1. Pour les mêmes raisons que l'espace déterministe, M est dans $NSPACE(g)$
2. Comme g est propre, on a $g \geq \log n$ et donc $NSPACE(g) = coNPSPACE(g)$.
   On a alors une machine M' dans $NSPACE(g)$ qui reconnaît le complémentaire de M.
3. Supposons par l'absurde que M' soit dans $NSPACE(f)$.
   Alors M' calcule en espace Cf, et le coût de simulation de $< M' >$ est en $C'f$ qui pour un certain k vérifie comme $f = o(g)$:

$$C'f(|< M' >\$^k|) < g(|< M' >\$^k|) \tag{3.11}$$

   Ainsi, en posant $w =< M' >\$^k$

$$M'(w) = \neg M(w) = \neg M'(w) \tag{3.12}$$

   La première égalité est par définition de M' et la seconde parce que la simulation dans M se fait bien en temps suffisant pour retourner le même résultat.
   Absurde.

NE PAS FAIRE LE TEMPS NON DÉTERMINISTE

3.2.4 En temps non-déterministe

On ne peut pas utiliser un théorème de type Immermann-Szelepscnenyi. En revanche on peut utiliser la méthode de la "réduction lente". Au lieu de retourner exactement ce que fait la machine M' en un temps n, on va calculer "par palliers" cette valeur.

On suppose que $f(n+1) = o(g(n))$. On pose une fonction h strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$ à déterminer explicitement plus tard.

```
M(w) =
    Si |w| = <M'>$^k alors
        Trouver i tel que h(i) < k <= h(i+1)
        Si k = f(i+1)
            Simuler NON(M') de manière déterminisée pour
            sur <M'>$^(h(i) + 1) avec g(|w|) étapes
```

```
        Sinon
            Simuler de manière non déterministe M' sur
            <M'>$^(k+1) avec g(|w|) étapes
    Sinon
        Retourner Vrai
```

Le temps de simulation en non déterministe se fait très bien par hypothèse, et le coût déterministe est exponentiel en $h(i)+1$.

Pour que cela reste majoré par g on construit donc h telle que $2^{h(i)+1} \leq g(h(i+1))$. On pose alors $h(i+1) = 2^{g(h(i))}$. Trouver le i se fait très bien en temps $O(g)$, et on constate que $2^{h(i)+1} \leq g(h(i+1))$.

Reste à conclure. Si M est dans $SPACE(f)$, alors à partir d'un certain rang, M s'auto-simule sans "timeout". Notons $k = h(i)+1$.

$$M(< M > \$^k) = M(< M > \$^{k+1}) = ... = M(< M > \$^{h(i+1)}) = NON(M(< M > \$^k)) \tag{3.13}$$

Et donc c'est absurde.

3.3 ■ ALGORITHME DE DIJKSTRA

Référence : Cormen / Beauquier. Recasé 2 fois

■ **LEÇONS**

L925 GRAPHES. REPRÉSENTATIONS ET ALGORITHMES. ★★★★★

L927 EXEMPLES DE PREUVE D'ALGORITHME, CORRECTION, TERMINAISON. ★★★★★

■ **RÉFÉRENCES**

Beauquier

Cormen

Dalapgusta

```
Dijkstra (G,s)
    d <- tableau de taille |v|
         initialisé à +infty
    F <- FilePrio (V,d)

    d[s] <- 0
    MODKEY (F,v,0)

    tant que nonVide (F) faire
        u <- depileMin (F)
        pour (u,v) dans E faire
            d[v] <- min (d[v], d[u] + w(u,v))
            MODKEY (F,v,d[v])

    renvoie d
```

3.3.1 Terminaison

Démonstration. Le programme termine car $|F|$ décroit de 1 à chaque tour de boucle □

3.3.2 Correction

Definition 4. On note $\delta_W(u)$ l'infimum des poids des chemins de s à u dont tous les éléments sauf éventuellement u sont dans W.

Remarque. *On constate $\delta_V(u) = \delta(u)$ le poids d'un chemin minimal. De plus $\delta_W(s) = 0$ quelque soit W.*

On liste les invariants du programme, en ayant noté $M = V - F$.

(I1)

$$\forall v \in V, d[v] \geq \delta(v)$$

(I2)

$$\forall v \in M, d[v] = \delta(v) = \delta_M(v)$$

(I3)

$$\forall v \in F, d[v] = \delta_M(v)$$

Théorème 5. *Avant le début de la boucle, tous les invariants sont vérifiés*

Démonstration. Immédiat □

Lemme 6.

$$\delta_{M\uplus\{u\}}(v) = \min\{\delta_M(v), \delta_M(u) + w(u,v)\}$$

Démonstration. Par l'absurde soit p un chemin optimal de s vers v qui passe par u mais ne termine pas avec l'arc (u,v).

On découpe donc le chemin $p = qxury v$. Comme les poids sont positifs on sait que :

La preuve est horrible ?! □

Théorème 7. *Les invariants sont préservés par la boucle*

Démonstration. **(I1)** Supposons $d[v] \geq \delta(v)$ alors comme les poids sont positifs

$$\delta(v) \leq \delta(u) + w(u,v)$$

Ainsi, comme $\delta(u) \geq d[u]$ on constate

$$\delta(v) \leq \min\{d[u] + w(u,v), d[v]\}$$

(Les relaxations conservent la sur-approximation)

(I2) Soit $v \in M\uplus\{u\}$. Si $v \neq u$, on sait que $d[v] = \delta(v)$ avant la modification de $d[v]$. Or après la relaxation on a $d[v] \geq \delta(v)$ (invariant **(I1)**) et la relaxation prend le minimum entre $\delta(v)$ et quelque chose. Donc $d[v]$ reste inchangé et la propriété est vraie.

Si $v = u$, et $M = \emptyset$ alors $u = s$ et $d[u] = \delta(u)$. Si $M \neq \emptyset$, on sait que M contient s. Par l'absurde, supposons que $d[u] > \delta(u)$. On considère p un chemin de s vers u de poids minimal. Il existe un préfixe du chemin q qui est intégralement dans M, et un point y hors de M tel que qy soit un préfixe de p. [1]

On note alors que par positivité des poids et par définition de δ_M :

$$d[u] = \delta(u) = w(p) \geq w(qy) \geq \delta_M(y)$$

Mais l'invariant **(I4)** associé au fait que $y \in F$ permet de conclure que $d[u] > d[y]$ ce qui est absurde au vu du choix de u.

(I3) On utilise le fait qu'un plus court chemin restant dans $M \cup \{u\}$ pour arriver à v passe soit par u, soit n'utilise pas l'arête (u,v).

Soit $v \in F$. Si v n'est pas un voisin de u, alors $d[v]$ reste inchangé par le tour de boucle. Or $d[v] = \delta_M(v)$ avant le tour de boucle. Le lemme permet de conclure car il n'y a pas d'arc (u,v) donc $d[u] = \delta_M(v) = \delta_{M\uplus\{u\}}(v)$

Soit v est un voisin de u, et alors après la mise à jour de $d[v]$ on a l'égalité suivante car $d[u] = \delta_M(u)$ (par l'invariant **(I4)**) :

$$d[v] = \min\{\delta_M(v), \delta_M(u), +w(u,v)\}$$

Ce qui permet directement de conclure avec le lemme.

□

On peut alors prouver la correction du programme

Démonstration. Quand le programme termine $M = V$ donc le tableau d contient bien les plus courtes distances de s à tout élément. □

1. En effet, u n'est pas dans M et s est dans M.

3.3.3 Annexe Dynamique

On peut, comme dans tout programme dynamique, retrouver à partir du tableau des valeurs des chemins optimaux de s vers tous les sommets.

On peut aussi ajouter un tableau de pères qui se met à jour au fur et à mesure du truc.

```
Dijkstra (G,s)
    d <- tableau de taille |v|
         initialisé à +infty
    F <- FilePrio (V,d)
    p <- tableau de taille |v|
         initialisé à NIL

    d[s] <- 0
    MODKEY (F,v,0)

    tant que nonVide (F) faire
        u <- depileMin (F)
        pour (u,v) dans E faire
            d[v] <- min (d[v], d[u] + w(u,v))
            p[v] <- u
            MODKEY (F,v,d[v])

    renvoie d,p
```

3.3.4 Annexe complexité

On analyse rapidement la complexité en comptant le nombre d'opérations. Chaque arête est relâchée au plus une fois, chaque sommet est dépilé au plus une fois, et donc on a en fonction de la file utilisée les complexités suivantes

Tableau $|V|^2+|E|+|E||S|$

Tas binaire $(|V|+|E|)\log|S|$

Tas fibonacci $|E|+|S|\log|S|$

3.4 ■ AUTOMATE D'AHO-CORASICK

Référence : Text Algorithm, Crochemore / Beauquier. Recasé 1 fois

■ **LEÇONS**

L907 ALGORITHMIQUE DU TEXTE. EXEMPLES ET APPLICATIONS. ★★★★★

■ **RÉFÉRENCES**

Crochemore

Beauquier

On se fixe m un motif et on veut construire un automate déterministe reconnaissant $\Sigma^* m$.

Étape 1 : Analyse de cas On fait le cas ε, puis a, puis ab. pour illustrer les deux opérations importantes.

Étape 2 : Formalisation On étiquète les états par les préfixes de m pour simplifier.

Si A est l'automate précédent pour le mot m, le nouvel automate A' possède un nouvel état q_{ma}

Et on pose

$$\forall b \in \Sigma - \{a\}, q_m \to^a q_{ma} \to^b q' \iff q_m \to^a q'' \to^b q' \tag{3.14}$$

Avec un cas particulier si $b = a$ où l'on fait la distinction Si $q_m \to^a q_m$ on pose

$$q_{ma} \to^a q_{ma} \tag{3.15}$$

Et sinon on fait comme pour le truc précédent.

Toutes les autres transitions sont identiques à A.

Étape 3 : Le lemme

$$q_0 \cdot_{A'} u = q' \iff \begin{cases} u = u'a \wedge q_0 \cdot_A u' = q_m \wedge q' = q_{ma} \\ q_0 \cdot_A u = q' \end{cases} \tag{3.16}$$

Ce lemme se démontre par induction sur la dérivation de manière très simple.

Étape 4 : La construction inducitve Une fois le lemme prouvé, il ne reste plus grand chose à faire.

Étape 5 : Retour sur la propriété On a montré qu'on pouvait faire de la ré-écriture sur les dévirations, c'est une autre manière de faire le lemme 3 qui se comprend particulièrement bien dans le cas où $q_m \to^a q_m$ n'arrive pas.

Étape 6 : C'est l'automate minimal La preuve habituelle en prenant deux préfixes.

Étape 7 : Généralisation On peut constater que l'arc retour est en fait celui de l'automate des motifs et que l'on calcule $bord(xa)$.

Cela se généralise à un ensemble de motifs, ce qui constitue le véritable algortihme d'Aho-Corasick.

3.5 ■ DISTANCE D'ÉDITION ET FACTEURS À DISTANCE k

Référence : Text Algorithm, Crochemore. Recasé 2 fois

■ **LEÇONS**

L906 PROGRAMMATION DYNAMIQUE. EXEMPLES ET APPLICATIONS. ★★★★★

L907 ALGORITHMIQUE DU TEXTE. EXEMPLES ET APPLICATIONS. ★★★★★

■ **RÉFÉRENCES**

Crochemore

■ **OUVERTURE**

Dans les recherches Google on fait des fautes de frappe, et donc on veut parfois chercher des motifs avec une distance d'édition raisonnable. C'est cool, c'est sympathique, et la distance d'édition est née. On traite dans un premier temps la distance d'édition avec un unique mot, que l'on généralise aussitôt à l'extraction des mots à distance k du motif dans un dictionnaire.

Cette dernière étape se fait en suivant le paradigme général suivant : représenter des données comme des modèles de calcul. Ainsi, comme l'automate de Simon transforme un motif en un automate, on transforme ici le motif en un automate de Levenshtein et le dictionnaire en un Trie (ou mieux encore). C'est à mettre en parallèle avec la construction de l'arbre des suffixes.

On se place sur un alphabet fini Σ.

3.5.1 Introduction

Definition 8 (Édition)**.** Soit $u, v \in \Sigma^*$ et $a, b \in \Sigma$, une édition est de la forme :

(i) Ajout $uv \to uav$

(ii) Suppression $uav \to uv$

(iii) Modification $uav \to ubv$

La relation $(\to)$ sur Σ^* définit un système de réécriture.

Definition 9 (Distance d'édition)**.** On définit la distance d'édition $d_E(u, v)$ comme la taille de la plus petite dérivation $u \to^* v$ si elle existe, et $+\infty$ sinon.

Exemple 10. *Il existe une édition de taille* 3 *qui mène de « rotis » à « sortie »*

$$\text{rotis} \to \text{sotis} \to \text{sortis} \to \text{sortie}$$

Remarque. *Ce système de ré-écriture n'est pas facile à étudier. Il existe beaucoup de dérivations d'un mot vers un autre, et l'ordre des modifications n'est pas contrôlé.*

Lemme 11 (Algorithme Naïf)**.** *L'algorithme naïf qui trouve le plus court chemin pour aller du mot $|u|$ au mot $|v|$ se fait en taille linéaire en la taille du graphe, que l'on peut tronquer aux mots de taille inférieure à $|u|+|v|$, et donc en $\mathcal{O}\left((|u|+|v|)2^{|u|+|v|}\right)$.*

Definition 12 (Alignement)**.** Un alignement de deux mots u et v dans Σ^* est la donnée de deux mots $\hat{u}$ et $\hat{v}$ dans $(\Sigma \uplus \{\perp\})^*$ qui vérifient :

(a) $\pi_\Sigma(\hat{u}) = u$ (b) $\pi_\Sigma(\hat{v}) = v$ (c) $|\hat{u}| = |\hat{v}|$

Avec π_Σ le morphisme qui efface les $\perp$ et conserve toutes les autres lettres.

Exemple 13. *Voici un alignement possible des mots « rotis » et « sortie »*

$$\begin{array}{cccccc} r & o & \perp & t & i & s \\ s & o & r & t & i & e \end{array}$$

Definition 14 (Taille d'alignement)**.** Soit $u, v \in \Sigma^*$ et $\hat{u}, \hat{v}$ un alignement de u, v. On définit la mesure $\hat{d}(\hat{u}, \hat{v})$ comme le nombre de lettres différentes dans $\hat{u}$ et $\hat{v}$, auquel on ajoute le nombre de positions où $\hat{u}$ et $\hat{v}$ possèdent tous deux un $\perp$.

Exemple 15. *En reprenant l'alignement précédent, la distance obtenue est* 3.

r	o	$\perp$	t	i	s	
s	o	r	t	i	e	
1	0	1	0	0	1	3

En revanche si on ajoute des caractères blancs, on peut constater qu'on augmente la taille d'alignement.

r	o	$\perp$	t	i	s	$\perp$	
s	o	r	t	i	e	$\perp$	
1	0	1	0	0	1	1	4

Definition 16 (Distance d'alignement)**.** On définit la distance d_A sur les mots de Σ^* comme :

$$d_A(u, v) = \min\left\{\hat{d}(\hat{u}, \hat{v}) \mid (\hat{u}, \hat{v}) \text{ alignement de } (u, v)\right\}$$

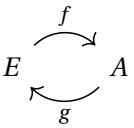
Remarque. *Il existe toujours un alignement trivial de taille $|u| + |v|$, et donc la distance d'alignement est toujours finie.*

Lemme 17 (Traduction 1)**.** *Si $u \to^k v$ alors il existe un alignement $\hat{u}, \hat{v}$ de taille inférieure à k.*

Lemme 18 (Traduction 2)**.** *Si $\hat{u}, \hat{v}$ est un alignement de u, v de taille k, alors il existe une dérivation $u \to^k v$.*

Remarque (Embedding-projection pair)**.** *Si on note E l'ensemble des traces d'édition et A l'ensemble des agencements. Les lemmes de traductions* 1 *et* 2 *fournissent de manière effective deux fonctions $f : E \to A$ et $g : A \to E$ qui vérifient :*

- *$f \circ g = Id$*
- *$g \circ f \leq Id$*
- *f et g sont des fonctions croissantes (ie : "continues")*



On a donc une construction très classique de théorie des domaines, qui permet de construire des formes normalisées.

Théorème 19 (Caractérisation de la distance d'édition)**.**

$$\forall u, v \in \Sigma^*, d_E(u, v) = d_A(u, v) < +\infty$$

On a montré plus précisément que si on considère les interprétations sémantiques dans E et A de la paire (u, v), on obtient :

$$[\![(u, v)]\!]_E = [\![(u, v)]\!]_A$$

Remarque. *Ce résultat est légèrement imprécis, et l'analogie doit en rester une. En effet, pour être particulièrement clair, il faut considérer l'interprétation de (u, v) dans E comme* l'ensemble *des dérivations de u vers v. De la même manière l'interprétation dans A comme l'ensemble des alignements de u sur v.*

Cela étant fait, on possède un préordre *sur E et A, qui à un ensemble de dérivations (resp. d'alignements) associe la plus petite (resp. celui de taille minimale). La paire f, g reste la même, mais s'applique à des ensembles, et on obtient alors :*

$$g \circ f \simeq Id \wedge f \circ g \simeq Id \quad \text{pour les préordres de } A \text{ et } E$$

3.5.2 Programme dynamique

Lemme 20 (Équation de récurrence)**.** *Soit $u, v \in \Sigma^+$. Si $w \in \Sigma^*$ on note w_i le préfixe de taille i de w.*

$$d_A(u_{i+1}, v_{i+1}) = \min \begin{cases} 1 + d_A(u_i, v_{i+1}) \\ 1 + d_A(u_{i+1}, v_i) \\ \delta_{u_{i+1}}^{v_{i+1}} + d_A(u_i, v_i) \end{cases}$$

Démonstration. Considérons un alignement optimal de u, v. Alors les dernières lettres de $\hat{u}, \hat{v}$ sont dans une des trois configurations suivantes (par optimalité) :

(i) $\perp, v_{i+1}$
(ii) $u_{i+1}, \perp$
(iii) u_{i+1}, v_{i+1}

Ce qui permet de conclure en utilisant l'optimalité de l'alignement. □

Lemme 21 (Initialisation)**.** *Soit $v \in \Sigma^+$ (attention, non vide)*

$$d(a, v) = \begin{cases} |v| - 1 & si\ a \in v \\ |v| & sinon \end{cases}$$

Algorithm 2 Distance d'Édition

Require: $u, v \in \Sigma^+$
  $T \leftarrow$ tableau $(|u|, |v|)$
  $T[0,0] \leftarrow (u_0 == v_0)$
  for $i = 1$ **to** $|u|$ **do**
    if $u_i == v_0$ **then**
      $T[i,0] \leftarrow 1$
    else
      $T[i,0] \leftarrow T[i-1,0]$.
    end if
  end for
  $T[0,0] \leftarrow (u_0 == v_0)$
  for $j = 1$ **to** $|v|$ **do**
    if $v_j == u_0$ **then**
      $T[0,j] \leftarrow 1$
    else
      $T[0,j] \leftarrow T[0,j-1]$.
    end if
  end for
  for $i = 1$ **to** $|u|$ **do**
    for $j = 1$ **to** $|v|$ **do**
      $T[i,j] \leftarrow \min\big(1 + T[i-1,j], 1 + T[i,j-1], \delta + T[i-1,j-1]\big)$
    end for
  end for

Théorème 22 (Résolution)**.** *On peut résoudre le problème de la distance d'édition avec un algorithme dynamique en temps et en espace $\mathcal{O}(|u||v|)$.*

Remarque (Optimisation spatiale)**.** *Il est possible de modifier légèrement l'algorithme pour ne retenir que la dernière ligne du tableau, et ainsi faire baisser la complexité en espace à $\mathcal{O}(|u|)$.*

3.5.3 Annexe automates de Levenshtein

Definition 23 (Automate de Levenshtein)**.** Soit u un mot k un entier plus grand que 1, l'automate non déterministe de Levenshtein est un automate A tel que $\mathscr{L}(A) = \{v \in \Sigma^* \mid d_E(u,v) \leq k\}$. Sa construction est très simple en temps $\mathcal{O}(kn)$.

Exemple 24. *TODO : à faire sur un mot court comme « sortie ».*

Remarque. *L'automate va permettre de faire quelque chose de très pertinent : si on cherche dans une base de données les mots similaires à un mot donné, l'automate de Levenshtein va permettre de les énumérer en un temps très raisonnable.*

Toutefois, le non-déterminisme fait exploser la complexité... Et déterminiser n'est pas évident.

Propriété 25 (Construction en temps linéaire)**.** *On peut construire un automate de Levenshtein déterministe en temps linéaire.*

Démonstration. Soit $u \in \Sigma^+$ avec $n = |u|$. On pose $Q = \{(m_1, \ldots, m_n) \mid 0 \leq m_i \leq k\}$ remarquons que ce n'est pas de taille linéaire par rapport à $|u|$, mais bien en k^n.

Toutefois, la table de transitions se compresse aisément grâce à l'algorithme dynamique, et il n'y a pas besoin d'enregistrer les états.

L'idée c'est simplement d'appliquer en un coup l'algorithme dynamique sur la ligne (qui est l'état q) avec la lettre c. Cela se calcule en temps linéaire en $|u|$. □

Remarque. *On peut au lieu de faire cela considérer la composition de l'automate déterministe classique du motif m avec un transducteur qui représente les différentes éditions possibles, puis minimiser.... Mais pour quelle complexité ?*

3.5.4 Annexe recherche de motif

— L'arbre des suffixes d'un texte est une sorte d'automate fini déterministe. Que se passe-t-il si on considère son intersubsection avec un automate ? Est-ce que cela donne tous les facteurs du texte qui vérifient une expression rationnelle ?

— Problème dual, l'automate de Simon permet-il de trouver un ensemble de textes pour lesquels le mot est facteur ? (donnés via une expression rationnelle) ?

Bibliographie

— http://blog.notdot.net/2010/07/Damn-Cool-Algorithms-Levenshtein-Automata.

— http://julesjacobs.github.io/2015/06/17/disqus-levenshtein-simple-and-fast.html

— https://github.com/julesjacobs/levenshtein

— ??? Jewels of Stringology ???

3.6 ■ AUTOMATES ET PRESBURGER

Référence : Carton. Recasé 3 fois

■ **LEÇONS**

L909 LANGAGES RATIONNELS ET AUTOMATES FINIS. EXEMPLES ET APPLICATIONS. ★★★★★

L914 DÉCIDABILITÉ ET INDÉCIDABILITÉ. EXEMPLES. ★★★★★

L924 THÉORIES ET MODÈLES EN LOGIQUE DU PREMIER ORDRE. EXEMPLES. ★★★★

■ **RÉFÉRENCES**

Carton

Objectif Décider la théorie au premier ordre sur $(\mathbb{N}, +)$.

Approche Considérer une formule ϕ à variables libres dans X comme un langage sur $\mathbb{N}^X$.

Pour cela, on code les entiers en binaire avec bit de poids faible à gauche, et on utilise l'opération $\otimes$ pour les "coller" avec padding.

$$\begin{aligned} 101 &\to 5 \\ 001 &\to 4 \\ 01 &\to 2 \\ 101 \otimes 001 \otimes 01 &\to \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \simeq (5,4,2) \end{aligned}$$

Ainsi, on représente $\mathbb{N}^X$ comme $(\Sigma^{|X|})^*$ avec $\Sigma = \{0,1\}$.

L'ensemble des mots qui codent une valuation ν s'écrit

$$\left(\bigotimes_i [\nu(x_i)]_2\right) \cdot 0^* \tag{3.17}$$

On note alors le langage de ϕ sur les variables X (contenant nécessairement les variables libres de ϕ) comme suit :

$$\mathscr{L}_\phi^X = \{\nu \in \mathbb{N}^X \mid \nu \models \phi\} \tag{3.18}$$

On va montrer que quelque soit X, quelque soit ϕ ce langage est rationnel, et qu'on peut consturire explicitement un automate qui le reconnaît.

On fait cela par induction sur (ϕ, X) avec l'ordre lexicographique (structurelle sur ϕ, cardinal sur X).

Remarque $\phi \equiv \psi$ si et seulement si $\mathscr{L}_\phi^X = \mathscr{L}_\psi^X$ par construction.

Opérations arithmétiques On traite ici les formules de base de l'arithmétique de Presburger

Égalité Si $\phi \equiv x + y = z$ et $X = \{x, y, z\}$ alors **DESSIN AUTOMATE ÉGALITÉ**

Addition Si $\phi \equiv x = z$ et $X = \{x, y\}$ alors **DESSIN AUTOMATE ADDITION**

Ajout de variables On veut calculer le langage de $(\phi, X \uplus \{x\})$, pour cela on remarque que

$$\mathscr{L}_\phi^{X \uplus \{x\}} = \pi_X^{-1}\left(\mathscr{L}_\phi^X\right) \tag{3.19}$$

Faire un exemple sur l'exemple de départ

Opérations booléennes Supposons que (ϕ_1, X) et (ϕ_2, Y) donnent des langages rationnels. On peut alors noter $Z = X \cup Y$ et utiliser le point précédent pour constater que (ϕ_1, Z) et (ϕ_2, Z) sont bien rationnels.

Mais alors on peut effectuer les opérations booléennes en utilisant la stabilité (constructive) des automates par ces opérations :

$$\begin{cases} \mathscr{L}^Z_{\phi_1 \wedge \phi_2} = \mathscr{L}^Z_{\phi_1} \cap \mathscr{L}^Z_{\phi_2} \\ \mathscr{L}^Z_{\phi_1 \vee \phi_2} = \mathscr{L}^Z_{\phi_1} \cup \mathscr{L}^Z_{\phi_2} \\ \mathscr{L}^Z_{\neg \phi_1} = \left(\mathscr{L}^Z_{\phi_1}\right)^c \end{cases} \tag{3.20}$$

Quantification On ne traite que le cas de $\exists x.\phi$ car on a l'équivalence logique $\forall x.\phi \equiv \neg\exists x.\neg\phi$ qui permet de s'y ramener.

On construit par hypothèse de récurrence le langage rationnel $\mathscr{L}^{X \uplus \{x\}}_\phi$, et on remarque que

$$\mathscr{L}^X_{\exists x.\phi} = \pi_X\left(\mathscr{L}^{X \uplus \{x\}}_\phi\right)\left(0^*\right)^{-1} \tag{3.21}$$

Conclusion On peut donc calculer par récurrence l'automate associée à $(\phi, FV(\phi))$ et constater que

$$SAT(\phi) \iff \mathscr{L}^{FV(\phi)}_\phi \neq \emptyset \tag{3.22}$$

$$\models \phi \iff \mathscr{L}^{FV(\phi)}_\phi = \left(\Sigma^{|FV(\phi)|}\right)^* \tag{3.23}$$

3.7 ■ AUTOMATES BOUSTROPHÉDON

Référence : Carton. Recasé 2 fois

■ **LEÇONS**

L909 LANGAGES RATIONNELS ET AUTOMATES FINIS. EXEMPLES ET APPLICATIONS. ★★★★★

L913 MACHINES DE TURING. APPLICATIONS. ★★★★★

■ **RÉFÉRENCES**

Carton

■ **OUVERTURE** On a dans le plan de leçon les égalités suivantes :

$$\mathrm{Rec}_{\mathrm{NFA}}\left(\Sigma^*\right) = \mathrm{Rec}_{\mathrm{DFA}}\left(\Sigma^*\right) = \mathrm{Rec}_{\mathrm{AFA}}\left(\Sigma^*\right) = \mathrm{Rat}\left(\Sigma^*\right)$$

Ce sont différentes manières d'exprimer une classe de langage très robuste (stabilité par opérations élémentaires) et relativement puissante (analyse lexicale).

L'objectif du développement est de montrer que modifier légèrement les automates autorisés ne change pas la classe de langage qui peuvent-êtres reconnus.

3.7.1 Définitions Préliminaires

Definition 26 (Automate Boustrophédon)**.** Un automate boustrophédon non-déterministe est un quintuplet $A = \langle \Sigma, Q, \delta, I, F \rangle$ tel que :

(i) Σ est l'alphabet fini d'entrée
(ii) Q est un ensemble fini d'états
(iii) δ est une partie de $Q \times (\Sigma \uplus \{\bot\}) \times Q \times \{\pm 1\}$

Definition 27 (Run sur un mot)**.** Un run d'un automate boustrophédon A sur un mot w en partant d'un état q et d'une position $p \in \mathbb{Z}$ est une suite $(q_n, p_n) \in Q \times \mathbb{Z}$ qui vérifie :

(i) La suite possède au moins un élément
(ii) Le premier élément de la suite est (q, p)
(iii) Si $(q_1, k_1) : (q_2, k_2)$ sont deux éléments successifs dans la suite alors

$$(q_1, w[k_1], q_2, k_2 - k_1) \in \delta$$

Avec pour convention $w[k] = \bot$ si k n'est pas une position valide dans w (sortie des bords)
(iv) Si une lettre $\bot$ est lue dans un état non final, alors la prochaine lettre est nécessairement dans le mot w

Definition 28 (Acceptation)**.** Un mot $w \in \Sigma^*$ est accepté par un automate boustrophédon A si et seulement s'il existe un run de A sur w partant d'un état initial et terminant en position $|w|$ dans un état final spécifique q_f.

Remarque. *En particulier un automate peut accepter le mot vide si l'état initial est acceptant.*

3.7.2 Preuve du théorème

Soit $A = \langle \Sigma, Q, \delta, I, F \rangle$ un automate boustrophédon que l'on suppose *complet* pour simplifier la preuve. On note $L = \mathscr{L}(A)$. On va montrer que L est saturé par une congruence d'indice fini.

Definition 29. Soit $w \in \Sigma^*$, on définit un run *dans* w de (q, p) à (q', p') comme un run partant de (q, p) et finissant en (q', p') tel que toutes les positions sauf éventuellement la dernière soient dans w.

$$\lambda^{\rightarrow}(w) = \left\{(q,q') \in Q^2 \mid \exists r \text{ run de A dans } w \text{ de } (q,0) \text{ à } (q', |w|)\right\}$$

$$\lambda^{\leftarrow}(w) = \left\{(q,q') \in Q^2 \mid \exists r \text{ run de A dans } w \text{ de } (q,|w|-1) \text{ à } (q', -1)\right\}$$

$$\lambda^{\leftrightarrow}(w) = \left\{(q,q') \in Q^2 \mid \exists r \text{ run de A dans } w \text{ de } (q,0) \text{ à } (q', -1)\right\}$$

$$\lambda^{\hookrightarrow}(w) = \left\{(q,q') \in Q^2 \mid \exists r \text{ run de A dans } w \text{ de } (q,|w|-1) \text{ à } (q', |w|)\right\}$$

Exemple 30 (Sur le mot vide)**.**

$$\lambda^{\rightarrow}(\varepsilon) = \lambda^{\leftarrow}(\varepsilon) = \lambda^{\hookrightarrow}(\varepsilon) = \lambda^{\leftrightarrow}(\varepsilon) = \emptyset$$

Exemple 31 (Sur le mot d'une lettre)**.**

$$\lambda^{\rightarrow}(a) = \left\{(q,q') \in Q^2 \mid (q,a,q',+1) \in \delta\right\}$$

$$\lambda^{\leftarrow}(a) = \left\{(q,q') \in Q^2 \mid (q,a,q',-1) \in \delta\right\}$$

$$\lambda^{\hookrightarrow}(a) = \lambda^{\leftarrow}(a)$$

$$\lambda^{\leftrightarrow}(a) = \lambda^{\rightarrow}(a)$$

Definition 32 (Relation sur Σ^*)**.** Si w et w' sont deux mots alors :

$$w \sim w' \iff \forall x \in \{\rightarrow, \leftarrow, \hookrightarrow, \leftrightarrow\}, \lambda^x(w) = \lambda^x(w')$$

Propriété 33 (Relation d'équivalence d'indice fini)**.**

1. *La relation $\sim$ est une relation d'équivalence*
2. *La relation $\sim$ est d'indice inférieur à $2^{4|Q|^2}$*

Lemme 34 (La relation $\sim$ est une congruence)**.** *Attention, la congruence se fait sur $\Sigma \uplus \{\perp\}$*

Démonstration. Soient $u_1 \sim u_2$ et $v_1 \sim v_2$ tous différents de ε. Montrons par exemple que $\lambda^{\rightarrow}(u_1 v_1) = \lambda^{\rightarrow}(u_2 v_2)$ [2].

On montre le résultat suivant par induction sur les runs de A :

$$\lambda^{\rightarrow}(u_1 v_1) \subseteq \lambda^{\rightarrow}(u_1)(\lambda^{\leftrightarrow}(v_1)\lambda^{\hookrightarrow}(u_1))^* \lambda^{\rightarrow}(v_1)$$

On montre par induction l'inclusion réciproque :

$$\lambda^{\rightarrow}(u_1)(\lambda^{\leftrightarrow}(v_1)\lambda^{\hookrightarrow}(u_1))^* \lambda^{\rightarrow}(v_1) \subseteq \lambda^{\rightarrow}(u_1 v_1)$$

Cela permet de conclure.

Pour les cas contenant ε : Si $u_1 = \varepsilon$, alors $u_1 v_1 = v_1$ et donc $\lambda^{\rightarrow}(u_1 v_1) = \lambda^{\rightarrow}(v_1) = \lambda^{\rightarrow}(v_2)$. Quitte à supposer l'automate complet, $\lambda^{\rightarrow}(u_2) = \emptyset$ implique $u_2 = \varepsilon$. On peut alors conclure. Les autres cas se traitent de manière similaire. □

Lemme 35 (La relation $\sim$ sature L)**.**

2. Les autres cas se traitent de manière similaire

Démonstration. Soit $w \sim w'$ et $w \in L - \{\varepsilon\}$, on a un run acceptant pour w qui part de $(q_0, 0)$ et termine en $(q_f, |w|)$. Cela revient à dire que

$$(q_0, q_f) \in \lambda^{\rightarrow}(w)(\lambda^{\leftharpoondown}(w)\lambda^{\rightharpoonup}(w))^*\lambda^{\rightarrow}(w)$$

On déduit donc par la congruence

$$(q_0, q_f) \in \lambda^{\rightarrow}(w')(\lambda^{\leftharpoondown}(w')\lambda^{\rightharpoonup}(w'))^*\lambda^{\rightarrow}(w')$$

Or à partir de cela on peut reconstruire un calcul acceptant de l'automate A sur w'. On a donc bien $w' \in L$.

Si $w = \varepsilon$, alors $w \sim w'$ force $w' = \varepsilon$. On a donc $w' = w \in L$. □

3.7.3 Annexe palindromes

Lemme 36. *Un automate déterministe qui reconnait mots dont les préfixes de taille n sont des palindromes possède au moins $2^{n/2}$ états si n est impair (sur l'alphabet $\{a, b\}$)*

Démonstration. Si $n = 2m + 1$ on construit $f : \Sigma^m \to Q$ qui à u associe le $m+1$-ème état dans un run de l'automate sur $u0\overline{u}$.

Cette fonction est injective et cela donne directement la minoration attendue. □

Lemme 37. *On peut construire un automate boustrophédon qui reconnait mots dont les préfixes de taille n sont des palindromes avec $n(n+1)/2+1$ états*

Remarque (Serge)**.** *Via Wikipedia, j'ai appris que la complexité de la déterminisation d'u automate boustrophédon est un problème ouvert depuis un papier STOC 1978 : polynomiale ou exponentielle ?*

3.7.4 Annexe Effectivité

On peut effectivement construire les classes d'équivalence comme des quadruplets de parties de Q^2.

L'état initial est la classe du mot ε qui a déjà été calculée. Les états finaux sont les états (A, B, C, D) tels que

$$\exists q_0 \in I, (q_0, q_f) \in A(CD)^*A$$

Ce qui se calcule simplement car on sait calculer la clôture transitive d'une relation.

De plus, on sait que $[ua] = [u] \cdot [a]$ et comme on a calculé la classe d'une lettre on a un moyen effectif pour calculer la classe d'un mot w.

3.8 ■ PROBLÈME NP-COMPLET UNAIRE

Référence : Aucune. Recasé 2 fois

■ **LEÇONS**

L906 PROGRAMMATION DYNAMIQUE. EXEMPLES ET APPLICATIONS. ★★★★

L928 PROBLÈMES NP-COMPLETS. EXEMPLES ET RÉDUCTION. ★★★★

■ **RÉFÉRENCES**

AUCUNE

SAT est NP-dur Admis

S'il existe un langage NP-dur unaire Alors on dispose d'une réduction polynômiale h de SAT dans ce langage $L \subseteq \{0\}^*$, et d'un polynôme P tel que $|h(\phi)| \leq P(|\phi|)$.

On constate de plus que $|\phi[x \mapsto \top]| \leq |\phi|$ et $|\phi[x \mapsto \bot]| \leq |\phi|$.

On peut écrire l'algorithme récursif suivant

```
SAT (phi):
    si phi sans variables alors
        evalue (phi)
    sinon
        SAT (phi[x -> True]) OU SAT(phi[x -> False])
```

C'est un algorithme récursif qui fonctionne en temps exponentiel. On va utiliser une table pour mémoïzer les résultats intermédiaires.

On utilise la fonction h comme une fonction de haschage qui envoie une formule ϕ sur un entier n_ϕ écrit en unaire.

On modifie donc le code

```
T tableau de taille P(|phi|) initialisé à Undefined
SAT (phi):
    n_p <- h(|phi|)
    si T[n_p] non défini alors
        b <- False
        si phi sans variables alors
            b <- evalue (phi)
        sinon
            b <- SAT (phi[x -> True]) OU SAT(phi[x -> False])
        T[n_p] <- b
    finsi
    T[n_p]
```

1. L'algorithme termine sur toute entrée
2. L'algorithme est correct car le hashage respecte la satisfiabilité
3. L'algorithme est en temps polynômial puisque chaque appel à h se fait sur des entrées de taille inférieure à $|\phi|$ et donc chaque étape est polynômiale.

   Les noeuds *internes* de l'arbre des appels récursifs définissent tous *une valeur différente dans le tableau T* et donc son en nombre inférieur à $P(|\phi|)$. Le nombre total d'appels est donc polynômial en $|\phi|$.

   Au total l'algorithme est bien polynômial.

BONUS. SAT est auto-réductible *Démonstration.* Supposons qu'un oracle O pour SAT existe, alors on peut utiliser cet oracle pour construire en temps polynômial une valuation satisfaisant une formule ϕ.

L'algoritme est le suivant :

```
valuation (phi):
    si phi = x     alors (x -> True)
    si phi = non x alors (x -> False)
    sinon
        si O(phi[x -> True]) alors
            valuation(phi[x->True])(x -> True)
        si O(phi[x -> False]) alors
            valuation(phi[x->False])(x -> False)
        sinon
            ERROR
```

On constate bien que cet algorithme tourne en temps polynômial puisque qu'on effectue n étapes au plus, et chaque étape est un appel à P (constant) et un appel à la substitution (aussi polynômial).

De plus il construit bien une instance si et seulement si elle existe par induction sur le nombre de variables dans ϕ.

Cela foncitonne encore si l'appel à O utilise un temps polynômial puisque la taille des arguments est toujours inférieure à la taille de ϕ.

Constatons que cela donne un algorithme exponentiel pour résoudre SAT en remplaçant O par $valuation$. □

3.9 ■ COMPLÉTUDE DE LA LOGIQUE DE HOARE

Référence : Glynn Winskel. Recasé 2 fois

■ **LEÇONS**

L927 EXEMPLES DE PREUVE D'ALGORITHME, CORRECTION, TERMINAISON. ★★★★★

L930 SÉMANTIQUE DES LANGAGES DE PROGRAMMATION. EXEMPLES. ★★★★★

■ **RÉFÉRENCES**

Glynn Winskel

Definition 38. On considère le langage logique de l'arithmétique au premier ordre. On différencie dans les formules deux types de variables, les variables *de programme* et les variables *logiques*. L'interprétation d'une formule est donc l'interprétation standard dans $\mathbb{N}$ qui nécessite l'environment σ du programme et une interprétation I des variables logiques. On prend comme convention que $\bot \models^I A$ pour tout I et tout A.

Classiquement, on écrit $\models A$ pour dire que pour tout σ, I $\sigma \models^I A$.

Definition 39. On écrit $\models \{P\}\ c\ \{Q\}$ pour signifier que $\forall \sigma, \forall I, \sigma \models^I P \implies [\![c]\!]_\sigma \models^I Q$.

Definition 40 (Logique de Hoare)**.**

$$\frac{}{\{P\}\ \textbf{skip}\ \{P\}} \qquad \frac{\{P \wedge e \neq 0\}\ c\ \{Q\} \qquad \{P \wedge e = 0\}\ c'\ \{Q\}}{\{P\}\ \textbf{if}\ e\ \textbf{then}\ c\ \textbf{else}\ c'\ \{Q\}}$$

$$\frac{}{\{P[x \mapsto e]\}\ x := e\ \{P\}} \qquad \frac{\{P \wedge e \neq 0\}\ c\ \{P\}}{\{P\}\ \textbf{while}\ e\ \textbf{do}\ c\ \textbf{end}\ \{P \wedge e = 0\}}$$

$$\frac{\{P\}\ c\ \{Q'\} \qquad \{Q'\}\ c'\ \{Q\}}{\{P\}\ c; c'\ \{Q\}} \qquad \frac{\models P \implies P' \qquad \{P'\}\ c\ \{Q'\} \qquad \models Q' \implies Q}{\{P\}\ c\ \{Q\}}$$

Théorème 41. *Pour toute formule A plus faible précondition de c et B, le séquent $\vdash \{A\}\ c\ \{B\}$ est démontrable.*

Lemme 42. *$\rho[x \mapsto [\![e]\!]_\rho] \models^I B$ si et seulement si $\rho \models^I B[x \mapsto e]$*

Démonstration. On procède par récurrence sur le programme c.

Soit A une formule telle que $\rho \models^I A$ si et seulement si $[\![c]\!]_\rho \models^I B$, montrons que $\{A\}\ c\ \{B\}$ est démontrable.

Skip On a $[\![c]\!]_\rho = \rho$, donc $\rho \models^I A$ si et seulemnt si $\rho \models^I B$, ce qui prouve $\models A \iff B$.

On peut donc conclure via la règle skip avec B puis la règle d'affaiblissement.

$$\frac{\models A \implies B \qquad \dfrac{}{\{B\}\ \textbf{skip}\ \{B\}} \qquad \models B \implies B}{\{A\}\ \textbf{skip}\ \{B\}}$$

Affectation On sait que $[\![c]\!]_\rho = \rho[x \mapsto [\![e]\!]_\rho]$. Ainsi $\rho \models^I A$ si et seulement si $\rho[x \mapsto [\![e]\!]_\rho] \models^I B$, en utilisant le lemme, on déduit que $\rho \models^I A$ si et seulement si $\rho \models^I B[x \mapsto e]$

Cela signifique que $\models A \iff B[x \mapsto e]$, et donc on peut faire la preuve

$$\frac{\models A \implies B[x \mapsto e] \qquad \dfrac{}{\{B[x \mapsto e]\}\ x := e\ \{B\}} \qquad \models B \implies B}{\{A\}\ x := e\ \{B\}}$$

Séquence On introduit C une plus faible précondition pour (c_2, B), on a donc la dérivation $\vdash \{C\}\ c_2\ \{B\}$ par hypothèse de récurrence.

On sait que $[\![c]\!]_\rho = [\![c_2]\!]_{[\![c_1]\!]_\rho}$, si $[\![c_1]\!]_\rho \neq \bot$ et $\bot$ sinon.

Dans le premier cas on a bien $\rho \models^I A$ si et seulement si $[\![c_2]\!]_{[\![c_1]\!]_\rho} \models^I B$ et par construction cela veut dire que $[\![c_1]\!]_\rho \models^I C$.

Dans le second cas on a $\rho \models^I A$ si et seulement si $\bot \models^I B$, si et seulement si $\bot \models^I C$, si et seulement si $[\![c_1]\!]_\rho \models^I C$.

On conclut donc que A est une plus faible précondition de (c_1, C).

Alors par hypothèse de récurrence on a $\vdash \{A\}\ c_1\ \{C\}$.

On peut donc conclure via la règle de séquence.

De manière générale $[\![c_1; c_2]\!]_\rho \models^I A$ si et seulement si $[\![c_2]\!]_{[\![c_1]\!]_\rho} \models^I A$

Condition **Ne pas faire la condition, c'est pas intéressant**

Boucle On va montrer que $\models \{A \wedge e \neq 0\}\ c_1\ \{A\}$, puis que $A \wedge e = 0$ implique B.

En effet, $\rho \models^I A \wedge e \neq 0$ si et seulement si $\rho \models^I A$ et $[\![e]\!]_\rho \neq 0$, si et seulement si $[\![c]\!]_\rho \models^I B$ et $[\![e]\!]_\rho \neq 0$ et $[\![c]\!]_\rho = [\![c_1; c]\!]_\rho$. Si et seulement si $[\![e]\!]_\rho \neq 0$ et $[\![c]\!]_{[\![c_1]\!]_\rho} \models^I B$. Si et seulement si $[\![c_1]\!]_\rho \models^I A$ et $[\![e]\!]_\rho \neq 0$.

On peut appliquer l'hypothèse de récurrence à une plus faible précondition C de A pour c_1, et utiliser $\models A \wedge e \neq 0 \implies C$ pour $\vdash \{A \wedge e \neq 0\}\ c_1\ \{A\}$.

De plus, si $\rho \models^I A \wedge e = 0$ alors $\rho \models^I B \wedge e = 0$ par la sémantique du while.

On peut donc utiliser cela pour déduire $\vdash \{A\}\ c\ \{B\}$.

□

3.10 ■ ÉQUIVALENCE ENTRE SÉMANTIQUE OPÉRATIONNELLE ET DÉNOTATIONNELLE

Référence : Glynn Winskel. Recasé 1 fois

■ **LEÇONS**

L930 SÉMANTIQUE DES LANGAGES DE PROGRAMMATION. EXEMPLES. ★★★★★

■ **RÉFÉRENCES**

Glynn Winskel

On montre le théorème suivant

$$\forall \rho, \rho' \in Env, \quad (\rho, c) \Downarrow \rho' \iff [\![c]\!]_\rho = \rho' \tag{3.24}$$

3.10.1 Le sens implique

Les points clefs

1. On fait une récurrence sur la dérivation dans la sémantique opérationnelle et non pas sur l'expression
2. On utilise crucialement le fait que $[\![\textbf{while } e \textbf{ do } c \textbf{ end}]\!]_\rho = [\![\textbf{if } e \textbf{ then } c; \textbf{while } e \textbf{ do } c \textbf{ end else skip}]\!]_\rho$ qui est la propriété *de point fixe* mais n'utilise *pas* la minimalité du point fixe.

On traite le cas du **skip**, du $x := e$ et du **while** e **do** c **end** seulement.

3.10.2 Le sens récuproque

Les points clefs

1. On fait une récurrence sur l'expression c
2. Tout se passe comme dans l'autre cas sauf pour le **while** e **do** c **end**
3. On montre que les **while** e **do** c **end** sont obtenus avec un nombre fini d'itérations car $Env_\perp$ est plat
4. On fait une autre récurrence pour déduire que $F^n_{e,c}(\perp)\rho = \rho' \neq \perp$ implique $(\rho, \textbf{while } e \textbf{ do } c \textbf{ end}) \Downarrow \rho'$ pour tout ρ et ρ'. Attention aux conflits de notations !

On traite le cas du **skip**, du $x := e$ et du **while** e **do** c **end** seulement.

3.11 ■ BORNE INFÉRIEURE TRI PAR COMPARAISON

Référence : Cormen ?. Recasé 1 fois

■ **LEÇONS**

L903 EXEMPLES D'ALGORITHMES DE TRI. CORRECTION ET COMPLEXITÉ. ★★★★★

■ **RÉFÉRENCES**

TODO

■ **OUVERTURE** Des algorithmes de tri en $\mathcal{O}(n \log n)$ sont connus et réputés pour être optimaux. Quel argument permet de constater cette optimalité ? Quid des algorithmes en temps « linéaire » (tri par paquets, tri par base, ...) ?

3.11.1 Introduction

Definition 43. Soit T un arbre binaire qui possède n feuilles, on peut définir la profondeur moyenne de T comme ceci :

(i) On construit X une variable aléatoire uniforme sur $[\![1, n]\!]$
(ii) On contsruit la fonction profondeur p qui à i associe la profondeur de la $i$ème feuille.
(iii) La profondeur moyenne est alors $\mathbb{E}(p(X))$

Une expression directe est la suivante :

$$m(T) = \frac{1}{n} \sum_{i=1}^{n} p(i)$$

Théorème 44. *La profondeur moyenne d'un arbre qui possède n feuilles est supérieure à* $\log_2 n$.

Démonstration. Par induction sur la structure de l'arbre.

Si l'arbre est une feuille Alors sa profondeur est 0, la profondeur moyenne est aussi 0 et $\log_2 1 = 0$ donc $m(T) \geq \log_2 n$

Si l'arbre possède une racine non triviale Notons T_1 et T_2 les deux sous arbres (potentiellement réduits à une feuille) de T. Notons n_1 le nombre de feuilles de T_1 et n_2 le nombre de feuilles de T_2, par construction on a $n_1 + n_2 = n$.

Par hypothèse de récurrence $m(T_1) \geq \log_2 n_1$ et $m(T_2) \geq \log_2 n_2$.

$$\begin{aligned}
m(T) &= \frac{1}{n} \sum_{i=1}^{n} p(i) \\
&= \frac{1}{n} \sum_{i=1}^{n_1} (p_1(i) + 1) + \frac{1}{n} \sum_{i=n_1+}^{n_2} (p_2(i) + 1) \\
&= \frac{1}{n} (n_1 m(T_1) + n_1 + n_2 m(T_2) + n_2) \\
&= 1 + \frac{n_1}{n} m(T_1) + \frac{n - n_1}{n} m(T_2) \\
&\geq 1 + \frac{n_1}{n} \log_2(n_1) + \frac{n - n_1}{n} \log_2(n - n_1)
\end{aligned}$$

Étudions alors la fonction f définie sur $]0, n[$ [3] par :

3. On traite bien tous les cas, car $n_1 > 0$ et $n_1 < n$, puisque chaque sous arbre possède au moins une feuille

$$f(x) = 1 + \frac{x}{n}\log_2 x + \frac{n-x}{n}\log_2(n-x)$$

On calcule

$$f'(x) = \frac{\log_2 x}{n} + \frac{1}{n} - \frac{\log_2(n-x)}{n} - \frac{1}{n}$$

Ce qui donne après simplification :

$$f'(x) = \frac{1}{n}\log_2 \frac{x}{n-x}$$

On a donc le tableau de variation suivant :

x	0	$n/2$	n
$f'(x)$	$-$	0	$+$

Et on constate alors que le minimum de cette fonction est en $n/2$, ce qui signifie :

$$m(T) \geq f(n/2) = 1 + \frac{1}{2}\log_2 \frac{n}{2} + \frac{1}{2}\log_2 \frac{n}{2}$$

Or $1 = \log_2 2$ donc $f(n/2) = \log_2 n$, ce qui permet de conclure.

□

Lemme 45. *La profondeur maximale d'un arbre qui possède n feuilles est supérieure à* $\log_2 n$.

3.11.2 Tris

Lemme 46 (Stirling)**.** *La formule de Stirling donne un équivalent de n! :*

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

Et permet donc de justifier .

$$\log_2 n! \sim n\log_2 n$$

Definition 47 (Arbre de décision)**.** Soit $n \in \mathbb{N}$, un arbre de décision pour les données de taille n est un arbre qui vérifie :

1. Les nœuds sont étiquetés par des comparaisons de la forme $i < j$ (avec $0 \leq i, j \leq n-1$)
2. Les feuilles sont étiquetées par des éléments de $\mathfrak{S}_n$ ou par $\perp$

Definition 48 (Tri par comparaison)**.** Soit P un algorithme de tri, et $n \in \mathbb{N}$. Comme P est un algorithme déterministe, on peut sur une entrée T (un tableau de n entiers) construire la suite des comparaisons $i < j$ effectuées par l'algorithme, et enregistrer dans une permutation l'ensemble des opérations effectuées sur le tableau. On note $\mathrm{tr}_P\, T$ cette trace.

Si l'ensemble des traces de P forme un arbre binaire, alors P est dit *tri par comparaison*. On note A_P^n l'arbre formé par les traces de P sur les tableaux de taille n.

Propriété 49. *Un arbre sémantique d'un algorithme de tri par comparaison possède au moins n! feuilles*

Démonstration. La fonction f qui à une permutation σ dans $\mathfrak{S}_n$ associe la trace $\mathrm{tr}_P\, \sigma$ est injective.

En effet, la feuille (dernier élément) de $\mathrm{tr}_P\, \sigma$ correspond à la permutation σ^{-1}, puisque c'est précisément la suite d'opérations qui permet de trier σ. □

Propriété 50 (Bornes inférieures)**.** *Un algorithme de tri par comparaison fait en moyenne* $\Omega(n\log n)$ *comparaison. Un algorithme de tri par comparaison fait dans le pire des cas* $\Omega(n\log n)$ *comparaison.*

Démonstration. On combine simplement les lemmes précédent avec la formule de Stirling. □

3.12 ■ THÉORÈME DE COMPLÉTUDE

Référence : Dowek. Recasé 2 fois

■ **LEÇONS**

L918 SYSTÈMES FORMELS DE PREUVES EN LOGIQUE DU PREMIER ORDRE. EXEMPLES.★★★★★

L924 THÉORIES ET MODÈLES EN LOGIQUE DU PREMIER ORDRE. EXEMPLES. ★★★★★

■ **RÉFÉRENCES**

Gilles Dowek

3.12.1 Trois formulations équivalentes

(i) $T \vDash A$ implique $T \vdash A$

(ii) $T \nvdash A$ implique $T \nvDash A$

(iii) $T \nvdash \bot$ implique $T \nvDash \bot$ ie, T a un modèle

Démonstration. Les deux premières propositions sont clairement équivalentes, la troisième est impliquée par la deuxième de manière aussi simple. La réciproque est facile : Si $T \nvdash A$ alors $T, \neg A \nvdash \bot$ en raisonnant par l'absurde, et donc $T, \neg A$ a un modèle, donc T a un modèle qui satisfait $\neg A$, donc A n'est pas valide pour T. □

3.12.2 Le modèle syntaxique

On suppose T cohérente dans le reste du développement.
On pose $M = \{t\sigma \mid t \in T_X(\Sigma), \sigma \text{ close}\}$.

$$[\![f]\!]_M(t_1,\dots,t_n) = f(t_1,\dots,t_n) \qquad [\![P]\!]_M(t_1,\dots,t_n) = T \vdash P(t_1,\dots t_n) \tag{3.25}$$

Exemple 51. *Prenons* $T = \{P(c) \vee Q(c), \exists x.P(x)\}$ *On a*

$$[\![P(c)]\!]_M = [\![Q(c)]\!]_M = \bot \qquad [\![P(c) \vee Q(c)]\!]_M = [\![\exists x.P(x)]\!]_M = \bot \tag{3.26}$$

Cela pose problème ...

3.12.3 Si la théorie est saturée

Supposons de plus que T est saturée. C'est-à-dire

1. T est complète
2. Si $T \vdash \exists x.\phi$ alors il existe un terme clos t tel que $T \vdash (t/x)\phi$.

Le modèle M satisfait alors la théorie T.

Démonstration. Par induction sur ϕ on montre que $T \vdash \phi \iff [\![\phi]\!]_M = \top$.

Formules atomiques C'est évident par construction de M

Conjonction Si $T \vdash \phi \wedge \psi$ alors via la règle $\wedge$-elim on déduit $T \vdash \phi$ et $T \vdash \psi$.
Par hypothèse de récurrence $[\![\phi]\!]_M = [\![\psi]\!]_M = \top$ puis $[\![\phi \wedge \psi]\!]_M = \top$.
Réciproquement on procède de même avec la règle $\wedge$-intro.

Négation Si $T \vdash \neg\phi$, alors on ne peut pas avoir $T \vdash \phi$ par cohérence. Donc par hypothèse de récurrence $[\![\phi]\!]_M = \bot$, ce qui prouve $[\![\neg\phi]\!]_M = \top$.
Si $[\![\neg\phi]\!]_M = \top$, alors $[\![\phi]\!]_M = \bot$ et donc T ne prouve pas ϕ. Comme T est complète, cela force T à prouver $\neg\phi$.

Existence On procède par équivalence.

$T \vdash \exists \phi$ si et seulement si $\exists t \in M, T \vdash (t/x)\phi$ si et seulement si $\exists t \in M, [\![\phi]\!]_M(t) = \top$ si et seulement si $[\![\exists x.\phi]\!]_M = \top$.

□

3.12.4 Saturation d'une théorie cohérente

On suppose Σ dénombrable. On pose U un ensemble dénombrable de constantes. On numérote les formules par ϕ_i, les constantes via c_i.

On construit par itérativement une théorie T_i sur le langage $\Sigma \uplus U$ comme suit.

$$T_0 = T \tag{3.27}$$

1. Si $T_i \vdash \phi_{i+1}$ alors $T_{i+1} = T_i \cup \{\phi_{i+1}\}$.
2. Si $T_i \nvdash \phi_{i+1}$ alors $T_{i+1} = T_i \cup \{\neg\phi_{i+1}\}$.
3. Si $\phi_{i+1} = \exists x.\phi$ alors ajouter en plus l'axiome $(c_{i+1}/x)\phi_{i+1}$ à la théorie T_i

On pose alors $T' = \bigcup_i T_i$.

T' est saturée Par construction, une formule ϕ est soit un axiome, soit n'est pas démontrable. De plus on a bien les témoins de Henkin.

Les T_i sont cohérentes Par récurrence sur i. C'est le cas pour $i = 0$ par hypothèse. Si T_i est cohérente, alors T_{i+1} est cohérente car

1. Si $T_i \vdash \phi_{i+1}$ alors $T_{i+1} \vdash \bot$ implique $T_i, \phi_{i+1} \vdash \bot$ puis $T_i \vdash \bot$ en substituant la règle axiome par la preuve de ϕ_{i+1}.
2. Si $T_i \nvdash \phi_{i+1}$ alors $T_{i+1} \vdash \bot$ implique $T_i, \neg\phi_{i+1} \vdash \bot$ puis $T_i \vdash \phi$ (par récurrence sur la dérivation) puis $T_i \vdash \bot$.
3. Si $T_i, (c_{i+1}/x)\phi \vdash \bot$ alors en utilisant la règle $\exists$-elim on peut déduire $\bot$ depuis la théorie T_i.

La théorie T' est cohérente En effet, une théorie est incohérente si et seulement si une partie finie de la théorie est incohérente. Donc T' incohérente si et seulement si une T_i est incohérente.

On peut donc conclure.

3.13 ■ COMPLÉTUDE DE LA RÉSOLUTION

Référence : Aucune ? Goubault ? Logique Résolution Réduction. Recasé 2 fois

■ **LEÇONS**

L916 FORMULES DU CALCUL PROPOSITIONNEL : REPRÉSENTATION, FORMES NORMALES, SATISFIABILITÉ. APPLICATIONS. ★★★★★

L918 SYSTÈMES FORMELS DE PREUVES EN LOGIQUE DU PREMIER ORDRE. EXEMPLES. ★★★

■ **RÉFÉRENCES**

Logique réduction résolution R. Lalement

On considère ϕ une formule

$$\phi = \bigwedge_i C_i \tag{3.28}$$

Où les C_i sont représentées comme des ensembles de littéraux.
La seule règle de résolution est la règle de coupure.

$$\frac{C, \neg l_i \qquad l_i, C'}{C, C'}$$

Attention, tout se fait avec des notations *ensemblistes*.
On note $R(\phi)$ l'ensemble la clôture de ϕ par résoluiton.
On va démontrer que ϕ est insatisfiable si et seulement si $\bot \in R(\phi)$.

1. On sait déjà que le calcul des séquents est correct, donc en particulier que la règle de coupure est correcte. Le sens réciproque est donc évident.
2. On va montrer le sens implique qui est plus dur.

Supposons donc ϕ insatisfiable. Il est clair que $R(\phi)$ reste insatisfiable car il y a plus de clauses.

Definition 52. Arbre sémantique Soit I un ensemble de littéraux (positifs ou négatifs). On dit que I est une interprétation *partielle* si elle ne fournit pas une interprétation totale des littéraux du langage L.

On ordonne tous les littéraux du langage L pour construire un arbre sémantique comme suit : **IMAGE**.

Un nœud est une interprétation partielle. Une branche infinie permet de définir une interprétation totale.

Definition 53. Noeud d'échec On dit que I est un noeud d'échec si et seulement s'il existe une clause C dans $R(\phi)$ telle que $I \models \neg\phi$.

Notation on écrit $I \models C$ pour dire qu'il existe une interprétation partielle contenant I satisfaisant C.

On peut désormais prouver le théorème.
Considérons l'arbre sémantique A, où l'on élague les branches à partir des nœuds d'échec.

1. L'arbre A est fini. En effet, $R(\phi)$ est insatisfiable, et donc il n'y a pas de branches infinies. Comme l'arbre est binaire, le lemme de König permet de conclure.
2. L'arbre A est vide. Par l'absurde, considérons un élément I de profondeur maximale.
   On a alors un littéral l, une clause C_1, une clause C_2 telles que

$$I, \neg l \models \neg C_1 \qquad I, l \models \neg C_2 \qquad I \models C_1 \qquad I \models C_2 \tag{3.29}$$

Une simple analyse de cas montre que cela force

$$C_1 = l, C_1' \qquad C_2 = \neg l, C_2' \tag{3.30}$$

On constate de plus que

$$I \not\models C_1' \qquad I \not\models C_2' \tag{3.31}$$

Mais la règle de résolution permet de déduire que C_1', C_2' est dans $R(\phi)$ or $I \not\models C_1', C_2'$, ce qui est absurde.

3. $\bot \in R(\phi)$. Comme l'arbre est vide, cela veut dire que $\emptyset$ est un nœud d'échec. Il existe donc une clause C telle que $\emptyset \not\models C$, c'est-à-dire, aucune valuation ne satisfait la clause C, et donc nécessairement $C = \bot$.

On a donc déduit $\bot \in R(\phi)$.

3.13.1 Post-requis

On peut adapter cette construction à la logique du premier ordre via la règle :

$$\frac{C}{C\theta}$$

La preuve est quasi-identique. Et permet en particulier de montrer le théorème de Herbrand, à savoir

$$\models \exists \bar{x}.\phi(\bar{x}) \iff \models_H \exists \bar{x}.\phi(\bar{x}) \iff \exists \theta_1, \ldots, \theta_n \models \bigvee_i \phi\theta_i \tag{3.32}$$

3.14 ■ HACHAGE PARFAIT

Référence : Cormen. Recasé 2 fois

■ **LEÇONS**

L901 STRUCTURES DE DONNÉES. EXEMPLES ET APPLICATIONS. ⋆⋆⋆⋆⋆

L921 ALGORITHMES DE RECHERCHE ET STRUCTURES DE DONNÉES ASSOCIÉES. ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Cormen

Objectifs Description des objectifs avec un dessin

Famille universelle Définition, construction admise.

Étape 1 : Le faire en espace quadratique Tire h uniformément dans $\mathscr{H}_{p,n^2}$. Variable aléatoire du nombre de collisions. Espérance du nombre de collision est $< 1/2$

Hachage parfait avec un espace n^2

Écriture de l'algorithme. Digression sur le nombre de tours de boucle.

Étape 2 : Amélioration Double hachage. On utilise un hacahge avec seulement n cases. On note $n_1, \dots, n_n$ le nombre de collisions dans les cellules 1 à n. On effectue ensuite un hachage parfait (comme précédent) sur les n_i.

L'espérance de la complexité spatiale est linéaire.

Encore une fois avec espérance puis Markov.

Refait un peu de blabla sur l'algorithme, précise bien que les tests se font en temps linéaire !

Conclusion La probabilité que le nombre de tours soit plus grand que 10 est inférieure à 2^{-10} qui est négligeable et donc voilà on est content.

3.15 ■ 2SAT NL-COMPLET ET TEMPS POLY

Référence : Carton/Cormen. Recasé 4 fois

■ **LEÇONS**

L915 CLASSES DE COMPLEXITÉ. EXEMPLES. ★★★★★

L916 FORMULES DU CALCUL PROPOSITIONNEL : REPRÉSENTATION, FORMES NORMALES, SATISFIABILITÉ. APPLICATIONS. ★★★★★

L925 GRAPHES. REPRÉSENTATIONS ET ALGORITHMES. ★★★★★

L928 PROBLÈMES NP-COMPLETS. EXEMPLES ET RÉDUCTION. ★★★

■ **RÉFÉRENCES**

Carton Pour la définition du graphe

On veut décider en temps linéaire de la satisfiabilité d'une formule ϕ sous forme $2CNF$.
Pour un littéral l on note $\bar{l}$ sa négation involutive.

Étape 1 Construction du graphe G_ϕ. On considère comme sommets $V = X \uplus \bar{X}$ avec X l'ensemble des variables de ϕ.

Pour toute clause $l_1 \vee l_2$ de ϕ on ajoute les arêtes $\bar{l_1} \to l_2$ et $\bar{l_2} \to l_1$.

Remarque On peut dire que $l_1 \implies l_2$ au sens où toute valuation satisfaisant ϕ satisfait cette implication.

On a alors par construction

$$l_1 \to^* l_2 \implies (\phi \models l_1 \implies l_2) \tag{3.33}$$

Étape 2 Si une composante fortement connexe de G contient l et $\bar{l}$ alors ϕ n'est pas satisfiable.

En effet, on obtient alors $l \to^* \bar{l} \to^* l$ et donc si ϕ était satisfiables on aurait $v(l) = 1 - v(l)$. Absurde.

Étape 3 Réciproquement, supposons que toute paire $l, \bar{l}$ se trouve dans des composantes fortement connexes distinctes.

Soit v une valuation partielle, on pose $\operatorname{dom} v$ l'ensemble des sommets de G_ϕ pour lesquels v est définie.

On va définir *itérativement* v vérifiant à chaque étape :

(I1) $\operatorname{dom} v$ est une union de composantes connexes

(I2) Si $u \to v$ et $u, v \in \operatorname{dom} v$ alors $v(u) \leq v(v)$

(I3) Si $u \to v$ et $u \notin \operatorname{dom} v$ et $v \in \operatorname{dom} v$ alors $v(v) = 1$.

Démonstration. Initialement v n'est définie sur aucun sommet de G.

Tant que $\operatorname{dom} v \neq S$.

On sait que G' a une composante connexe *terminale* T, et l'involution $x \mapsto \bar{x}$ envoie cette composante connexe sur une composante connexe *initiale* $I = \bar{T}$.

De plus, l'hypothèse sur G indique en particulier que dans G' les composantes connexes ne contiennent pas un littéral et sa négation.

Ainsi, on sait que $I \neq T$. On peut alors définir pour tout littéral dans T $v(l) = 1$ et tout littéral dans $I = \bar{T}$ $v(l) = 0$, ce qui donne bien une valuation cohérente au niveau des *variables* de la formule ϕ.

De plus, comme T est terminale et I initiale, la propriété 1. est bien vérifiée dans G'.

Le premier invariant est trivialement vérifié. Pour les autres on fait un dessin avec une bulle contenant $G_\phi - \operatorname{dom} v$, la composante T, la composante I.

Et on ne traite que deux cas.

□

De plus cette construction itérative termine.

Étape 4 En conclusion, on a construit v une valuation, définie sur toutes les variables de ϕ et vérifiant $u \to v \in G$ implique $v(u) \leq v(v)$.

Ainsi, pour une clause $l_1 \vee l_2$ de ϕ, on a bien $v(l_1 \vee l_2) = 1$, et donc $v \models \phi$.

On a donc le théorème suivant

> ϕ est satisfiable $\iff$ les composantes connexes de G ne contiennent pas x et $\bar{x}$ pour x variable.

Conclusion On peut vérifier via l'algorithme de Kosaraju/Tarjan dans chacune des composantes connexes si les littéraux apparaissent.

Bonus 1 La construction de v est explicite et encore en temps linéaire !

Bonus 2 La construction nous permet de montrer que $2SAT$ est dans $coNL$. Le fait que $2SAT$ soit $coNL$-dur étant évident.

On déduit alors que $2SAT$ est NL-complet.

3.16 ■ GRAMMAIRES ET INDÉCIDABILITÉ

Référence : Carton. Recasé 2 fois

■ **LEÇONS**

L914 DÉCIDABILITÉ ET INDÉCIDABILITÉ. EXEMPLES. ★★★★

L923 ANALYSE LEXICALE ET SYNTAXIQUE. APPLICATIONS. ★★★★

■ **RÉFÉRENCES**

Carton

Théorème 54. *Le problème suivant est indécidable*

ENTRÉE G_1, G_2 *gramaires algébriques*

SORTIE $\mathscr{L}(G_1) \cap \mathscr{L}(G_2) = \emptyset$

Démonstration. On effectue une réduction depuis le problème de correspondance de Post (PCP). On note (u_i) et (v_i) avec $i \in [\![1, n]\!]$ une instance de PCP.

On définit sur l'alphabet $\Sigma' = \Sigma \uplus \{\#\} \uplus \underline{[\![1, n]\!]}$:

$$G_1 : S \mapsto u_i S \underline{i} | u_i \# \underline{i} \tag{3.34}$$

De même on pose

$$G_2 : S \mapsto v_i S \underline{i} | v_i \# \underline{i} \tag{3.35}$$

Supposons que le langage de G_1 et le langage de G_2 aient un mot w en commun.

Alors $w = u_{i_1} \dots u_{i_k} \# \underline{i_k} \dots \underline{i_1}$ et de même avec des v. Ceci se prouve par induction sur la dérivation.

On a donc une solution au problème de correspondance de Post !

Réciproquement, il suffit de prendre une solution au problème de correspondance, et de marquer un # puis les indices correspondants dans l'ordre inverse ensuite pour trouver un mot dans l'intersection des grammaires. □

Remarque. *On peut faire la même preuve en ayant ajouté la contrainte "les grammaires sont non ambiguës".*

Théorème 55. *Le problème suivant est indécidable*

ENTRÉE *Une grammaire G*

SORTIE *G est ambigue ?*

Démonstration. On utilise la remarque et on réduit le problème de l'intersection de gramaires non ambiguës.

Soient G_1 et G_2 deux grammaires non ambiguës, d'axiomes S_1 et S_2 et de variables distinctes. On note G' la grammaire obtenue en faisant l'union des deux grammaise, avec un axiome S et deux règles $S \to S_1$ et $S \to S_2$.

On constaite aisément que G est ambiguë si et seulement si les langages des deux grammaires s'intersectent. □

Théorème 56. *Le problème suivant est indécidable*

ENTRÉE *Une grammaire G*

SORTIE $\mathscr{L}(G) = \Sigma^*$

On utilise ce théorème pour montrer le suivant

Théorème 57. *Le problème suivant est indécidable*

ENTRÉE *Une grammaire G*

SORTIE $\mathscr{L}(G)$ *est rationnel*

Démonstration. On réduit le problème précédent à celui-ci.

Soit G une grammaire sur un alphabet Σ_1. Considérons un langage L_2 algébrique mais non rationnel (qui existe) sur un alphabet disjoint noté Σ_2.

On pose

$$L = \Sigma_1^* \# L_2 \cup \mathscr{L}(G) \# \Sigma_2 \tag{3.36}$$

Avec # un nouveau symbole qui permet de séparer les deux alphabets.

Supposons L rationnel et par l'absurde que $\mathscr{L}(G)$ n'est pas Σ_1^*.

On considère $y \in \Sigma_1^* - \mathscr{L}(G)$. Il est clair que le langage suivant est rationnel

$$L \cap y\#\Sigma_2^* = y\#L_2 \tag{3.37}$$

Comme le langage $y\#L_2$ est rationnel, le langage $(y\#)^{-1} y\#L_2$ est rationnel puis L_2 est rationnel ce qui est absurde !

Réciproquement supposons que $\mathscr{L}(G) = \Sigma_1^*$, alors le lanage L est simplement

$$L = \Sigma_1^* \# \Sigma_2^* \tag{3.38}$$

En particulier il est rationnel.

On a donc bien une réduction vers la rationnalité. □

Remarque. *On peut adapter cette preuve pour faire plein de trcus, comme l'ambiguité inhérente et compagnie, en ayant une propriété P vraie sur les rationnels, stable par intersection avec un rationnel, et par quotient à droite avec un rationnel.*

3.17 ■ LEMME DES DÉVELOPPEMENTS FINIS

Référence : Barengheit. Recasé 1 fois

■ **LEÇONS**

L929 LAMBDA-CALCUL PUR COMME MODÈLE DE CALCUL. EXEMPLES. ★★★★★

■ **RÉFÉRENCES**

Barentruc Mais en fait non

On pose

$$\Lambda' := x \mid \lambda x.\Lambda' \mid \Lambda'\Lambda' \mid \text{let}\, x = \Lambda' \,\text{in}\, \Lambda' \tag{3.39}$$

On pose $\twoheadrightarrow$ comme étant la plus petite relation passant au contexte (précongruence) et vérifiant $\text{let}\, x = u \,\text{in}\, v \twoheadrightarrow v[u/x]$.

Definition 58 (Lien avec Λ)**.** On pose E la fonction surjective suivante

$$E(x) = x \quad E(uv) = E(u)E(v) \quad E(\lambda x.u) = \lambda x.E(u) \tag{3.40}$$

$$E(\text{let}\, x = u \,\text{in}\, v) = (\lambda x.E(v))E(u) \tag{3.41}$$

Lemme 59. *1. Si t let $t ='$ in alors $E(t) \to_\beta E(t')$*

2. Si $t \to_\beta t'$ alors il existe u, v tels que $E(u) = t$, $E(v) = t'$ et $u \twoheadrightarrow v$

Théorème 60. *La relation $\twoheadrightarrow$ est fortement normalisante*

Démonstration. On montre un résultat plus fort par récurrence sur t, à savoir ce qui σ est une substitution fortement normalisante alors $t\sigma$ est fortement normalisant.

Variable $x\sigma = \sigma(x)$ est fortement normalisant par hypothèse

App Une réduction d'un terme de la forme uv se fait nécessairement dans u ou dans v. Par récurrence immédiate, on déduit que $uv\sigma = (u\sigma)(v\sigma)$ est un terme fortement normalisant.

Abstr Une réduction de $\lambda x.u$ se fait nécessairement via une réduction de u. Donc comme $u\sigma$ fortement normalisant on peut conclure.

Let Considérons $t = \text{let}\, x = u \,\text{in}\, v$. Par l'absurde considérons une suite infinie de réductions. Si les réductions ne se font que dans u ou v alors il n'y en a qu'un nombre fini.

Donc il existe un moment ou cette réduction infinie réduit le let = in.

On a donc

$$t\sigma \twoheadrightarrow^* \text{let}\, x = u' \,\text{in}\, v' \twoheadrightarrow v'[u'/x] \twoheadrightarrow^\infty \tag{3.42}$$

Mais on a $u\sigma \twoheadrightarrow^* u'$ et $v\sigma \twoheadrightarrow^* v'$, en particulier $u\sigma$ est fortement normalisant. Puis u' aussi.

Donc $v\sigma[u'/x]$ est fortement normalisant par hypothèse de récurrence. Or on constate aisément (par induction structurelle) que

$$(v\sigma)[u'/x] \twoheadrightarrow^* v'[u'/x] \tag{3.43}$$

Et donc on a une absurdité.

□

3.18 ■ CONFLUENCE λ-CALCUL

Référence : Krivine. Recasé 1 fois

■ **LEÇONS**

L929 LAMBDA-CALCUL PUR COMME MODÈLE DE CALCUL. EXEMPLES. ★★★★★

■ **RÉFÉRENCES**

Krivine

On veut montrer la propriété de confluence de la β-réduction.

$$\begin{array}{ccc} t & \longrightarrow & u \\ \downarrow & & \vdots \\ v & \dashrightarrow & w \end{array}$$ Les flèches représentent des réductions pour $\to_\beta^*$

Méthode 1 Montrer que $\to_\beta$ est fortement confluente. Faux pour $(\lambda x.xx)((\lambda x.x)y)$.

Méthode 2 Montrer que $\to_\beta$ termine et est localement confluente. Faux pour Ω.

3.18.1 La méthode qui marche

Définir une relation $\to_\beta \subseteq \Longrightarrow \subseteq \to_\beta^*$

$$\frac{}{t \Longrightarrow t} \qquad \frac{t \Longrightarrow t' \qquad u \Longrightarrow u'}{tu \Longrightarrow \lambda t' u'}$$

$$\frac{t \Longrightarrow t'}{\lambda x.t \Longrightarrow \lambda x.t} \qquad \frac{t \Longrightarrow t' \qquad u \Longrightarrow u'}{(\lambda x.u)t \Longrightarrow \lambda u[t/x]}$$

Remarque. *La relation $\Longrightarrow$ est la plus petite pré-congruence qui vérifie la dernière règle.*

Lemme 61. *On a bien les inclusions désirées*

Démonstration. Il est clair que $\to_\beta$ est inclue dans $\Longrightarrow$. De plus $\to_\beta^*$ est une précongruence et vérifie la dernière règle. Ce qui prouve l'inclusion désirée. □

Lemme 62. *La règle suivante est admissible*

$$\frac{t \Longrightarrow t' \qquad u \Longrightarrow u'}{u[t/x] \Longrightarrow u'[t'/x]}$$

Démonstration. Par induction sur la preuve de $u \Longrightarrow u'$, puis analyse de cas sur la dernière règle appliquée.

Ne traiter que la règle 4

Règle 1 Alors $u' = y = u$ et on a bien le résultat attendu.

Règle 2 On a $u = \lambda y.v$, et $v \Longrightarrow v'$.

Par HR on a $v[t/x] \Longrightarrow v'[t'/x]$ puis cela passe sous la λ-abstraction.

Règle 3 Pareil, c'est encore utiliser la pré-congruence.

Règle 4 $$\frac{w' \Longrightarrow w' \qquad v \Longrightarrow v'}{(\lambda y.w)v \Longrightarrow \lambda w'[v'/y]}$$

Alors on a bien

$$\begin{aligned} u[t/x] &= (\lambda y.w)[t/x]v[t/x] \\ &= (\lambda y.w[t/x])v[t/x] \end{aligned}$$

Par hypothèse de récurrence on a donc

$$\frac{w[t/x] \implies w'[t'/x] \qquad v[t/x] \implies v'[t'/x]}{(\lambda y.w[t/x])v[t/x] \implies w'[t'/x][v'[t'/x]/y]}$$

Mais on a alors la réduction désirée en remarquant que le terme obtenu est bien $u'[t'/x]$.

□

Lemme 63. *La réduction $\implies$ est fortement confluente.*

Démonstration. Par induction sur t.

Ne traiter que le cas 2

Variable C'est évident

Abstraction C'est par congrunence

Application On suppose $t = (\lambda x.w)h$ qui est le seul cas intéressant.

On a alors plusieurs possibliités de réduction pour t

Cas 1 $$\frac{w \implies w' \qquad h \implies h'}{t \implies u = (\lambda x.w')h'}$$

$$\frac{w \implies w'' \qquad h \implies h''}{t \implies v = (\lambda x.w'')h''}$$

Alors on applique l'hypothèse de récurrence w, w', w'' h, h', h''. On peut alors conclure par pré-congruence.

Cas 2 On garde u suivant la même dérivation, mais cette fois v utilise la règle 4.

$$\frac{w \implies w'' \qquad h \implies h''}{t \implies v = w''[h''/x]}$$

Alors on applique l'hypothèse de récurrence sur w, w', w'' et h, h', h''. On peut conclure parce que $u \implies \hat{w}[\hat{h}/x]$ et via le lemme précédent on a bien $v \implies \hat{w}[\hat{h}/x]$.

Cas 3 Cela se traite de la même manière, en utilisant le lemme précédent.

□

Théorème 64. *La $\to_\beta$ réduction est confluente.*

Démonstration. On a $\implies = \to_\beta^*$ et donc $\to_\beta^*$ est fortement confluente, ce qui veut exactement dire que $\to_\beta$ est confluente. □

3.18.2 Post requis

Cela permet de définir la notion de calcul, les formes normales sont toutes égales et tout est bien dans le meilleur des mondes.

3.19 ■ CALCUL PREMIER-SUIVANT

Référence : ??. Recasé 1 fois

■ **LEÇONS**

L923 ANALYSE LEXICALE ET SYNTAXIQUE. APPLICATIONS. ⋆⋆⋆⋆⋆

3.20 ■ POINTS LES PLUS PROCHES

Référence : Beauquier/Cormen. Recasé 2 fois

■ **LEÇONS**

L902 DIVISER POUR RÉGNER. EXEMPLES ET APPLICATIONS ⋆⋆⋆⋆⋆

L927 EXEMPLES DE PREUVE D'ALGORITHME, CORRECTION, TERMINAISON. ⋆⋆⋆⋆⋆

3.21 ■ CALCULABLE SSI RÉCURSIF

Référence : Wolper. Recasé 2 fois

■ **LEÇONS**

L912 FONCTIONS RÉCURSIVES PRIMITIVES ET NON PRIMITIVES. EXEMPLES. ⋆⋆⋆⋆⋆

L915 CLASSES DE COMPLEXITÉ. EXEMPLES. ⋆⋆⋆⋆⋆

3.22 ■ HIÉRARCHIE DE GREGOJURSXT

Référence : Clefs de l'agrégation. Recasé 1 fois

■ **LEÇONS**

L912 FONCTIONS RÉCURSIVES PRIMITIVES ET NON PRIMITIVES. EXEMPLES. ⋆⋆⋆⋆⋆

CHAPITRE 4

LEÇONS

■ **LEÇONS**	**9XX**
L901 STRUCTURES DE DONNÉES. EXEMPLES ET APPLICATIONS.	2D
L902 DIVISER POUR RÉGNER. EXEMPLES ET APPLICATIONS	2D
L903 EXEMPLES D'ALGORITHMES DE TRI. CORRECTION ET COMPLEXITÉ.	2D
L906 PROGRAMMATION DYNAMIQUE. EXEMPLES ET APPLICATIONS.	2D
L907 ALGORITHMIQUE DU TEXTE. EXEMPLES ET APPLICATIONS.	2D
L909 LANGAGES RATIONNELS ET AUTOMATES FINIS. EXEMPLES ET APPLICATIONS.	2D
L912 FONCTIONS RÉCURSIVES PRIMITIVES ET NON PRIMITIVES. EXEMPLES.	2D
L913 MACHINES DE TURING. APPLICATIONS.	2D
L914 DÉCIDABILITÉ ET INDÉCIDABILITÉ. EXEMPLES.	2D
L915 CLASSES DE COMPLEXITÉ. EXEMPLES.	3D
L916 FORMULES DU CALCUL PROPOSITIONNEL : REPRÉSENTATION, FORMES NORMALES, SATISFIABILITÉ. APPLICATIONS.	2D
L918 SYSTÈMES FORMELS DE PREUVES EN LOGIQUE DU PREMIER ORDRE. EXEMPLES.	2D
L921 ALGORITHMES DE RECHERCHE ET STRUCTURES DE DONNÉES ASSOCIÉES.	2D
L923 ANALYSE LEXICALE ET SYNTAXIQUE. APPLICATIONS.	2D
L924 THÉORIES ET MODÈLES EN LOGIQUE DU PREMIER ORDRE. EXEMPLES.	2D
L925 GRAPHES. REPRÉSENTATIONS ET ALGORITHMES.	2D
L926 ANALYSE DES ALGORITHMES, COMPLEXTÉ. EXEMPLES.	2D
L927 EXEMPLES DE PREUVE D'ALGORITHME, CORRECTION, TERMINAISON.	3D
L928 PROBLÈMES NP-COMPLETS. EXEMPLES ET RÉDUCTION.	2D
L929 LAMBDA-CALCUL PUR COMME MODÈLE DE CALCUL. EXEMPLES.	2D
L930 SÉMANTIQUE DES LANGAGES DE PROGRAMMATION. EXEMPLES.	2D

L901 STRUCTURES DE DONNÉES. EXEMPLES ET APPLICATIONS.
- ✓ Arbres AVL
- ✓ Hachage parfait

L902 DIVISER POUR RÉGNER. EXEMPLES ET APPLICATIONS
- ✓ Analyse du tri rapide
- ✗ Points les plus proches

L903 EXEMPLES D'ALGORITHMES DE TRI. CORRECTION ET COMPLEXITÉ.
- ✓ Analyse du tri rapide
- ✓ Borne inférieure tri par comparaison

L906 PROGRAMMATION DYNAMIQUE. EXEMPLES ET APPLICATIONS.
- ✓ Distance d'édition et facteurs à distance k
- ✓ Problème NP-complet unaire

L907 ALGORITHMIQUE DU TEXTE. EXEMPLES ET APPLICATIONS.
- ✓ Automate d'Aho-Corasick
- ✓ Distance d'édition et facteurs à distance k

L909 LANGAGES RATIONNELS ET AUTOMATES FINIS. EXEMPLES ET APPLICATIONS.
- ✓ Automates et Presburger
- ✓ Automates Boustrophédon

L912 FONCTIONS RÉCURSIVES PRIMITIVES ET NON PRIMITIVES. EXEMPLES.
- ✗ Calculable ssi récursif
- ✗ Hiérarchie de Gregojursxt

L913 MACHINES DE TURING. APPLICATIONS.
- ✓ Hiérarchie en espace et en temps
- ✓ Automates Boustrophédon

L914 DÉCIDABILITÉ ET INDÉCIDABILITÉ. EXEMPLES.
- ✓ Automates et Presburger
- ✓ Grammaires et indécidabilité

L915 CLASSES DE COMPLEXITÉ. EXEMPLES.
- ✓ Hiérarchie en espace et en temps
- ✓ 2SAT NL-complet et temps poly
- ✗ Calculable ssi récursif

L916 FORMULES DU CALCUL PROPOSITIONNEL : REPRÉSENTATION, FORMES NORMALES, SATISFIABILITÉ. APPLICATIONS.
- ✓ Complétude de la résolution
- ✓ 2SAT NL-complet et temps poly

L918 SYSTÈMES FORMELS DE PREUVES EN LOGIQUE DU PREMIER ORDRE. EXEMPLES.
- ✓ Théorème de complétude
- ✓ Complétude de la résolution

L921 ALGORITHMES DE RECHERCHE ET STRUCTURES DE DONNÉES ASSOCIÉES.
- ✓ Arbres AVL
- ✓ Hachage parfait

L923 ANALYSE LEXICALE ET SYNTAXIQUE. APPLICATIONS.
- ✓ Grammaires et indécidabilité
- ✗ Calcul premier-suivant

L924 THÉORIES ET MODÈLES EN LOGIQUE DU PREMIER ORDRE. EXEMPLES.
- ✓ Automates et Presburger
- ✓ Théorème de complétude

L925 GRAPHES. REPRÉSENTATIONS ET ALGORITHMES.
- ✓ Algorithme de Dijkstra
- ✓ 2SAT NL-complet et temps poly

L926 ANALYSE DES ALGORITHMES, COMPLEXTÉ. EXEMPLES.
- ✓ Analyse du tri rapide
- ✓ Arbres AVL

L927 EXEMPLES DE PREUVE D'ALGORITHME, CORRECTION, TERMINAISON.
- ✓ Algorithme de Dijkstra
- ✓ Complétude de la logique de Hoare
- ✗ Points les plus proches

L928 PROBLÈMES NP-COMPLETS. EXEMPLES ET RÉDUCTION.
- ✓ Problème NP-complet unaire
- ✓ 2SAT NL-complet et temps poly

L929 LAMBDA-CALCUL PUR COMME MODÈLE DE CALCUL. EXEMPLES.
- ✓ Lemme des développements finis
- ✓ Confluence λ-calcul

L930 SÉMANTIQUE DES LANGAGES DE PROGRAMMATION. EXEMPLES.
- ✓ Complétude de la logique de Hoare
- ✓ Équivalence entre sémantique opérationnelle et dénotationnelle

4.901 ■ STRUCTURES DE DONNÉES. EXEMPLES ET APPLICATIONS.

■ **DÉVELOPPEMENTS** **5.0**

D01 ARBRES AVL ⋆⋆⋆⋆⋆

D14 HACHAGE PARFAIT ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Cormen

Beauquier

Dalpagusta

■ **RAPPORT DE JURY**

> Le mot algorithme ne figure pas dans l'intitulé de cette leçon, même si l'utilisation des structures de données est évidemment fortement liée à des questions algorithmiques. La leçon doit donc être orientée plutôt sur la question du choix d'une structure de données. Le jury attend du candidat qu'il présente différents types abstraits de structures de données en donnant quelques exemples de leur usage avant de s'intéresser au choix de la structure concrète. Les notions de complexité des opérations usuelles sur la structure de données sont bien sûr essentielles dans cette leçon. Le candidat ne peut se limiter à des structures linéaires simples comme des tableaux ou des listes, mais doit présenter également quelques structures plus complexes, reposant par exemple sur des implantations à l'aide d'arbres.

■ **IDÉE DE PLAN :** Structurer en fonction des types de données abstrait.

Récupérer pour chaque structure des exemples dans la partie correspondante du Cormen pour les implémentations. Et dans les parties "analyse amortie" pour les études de complexité "pertinentes".

■ **EXEMPLES D'ALGORITHMES**

Postfixe pile
DFS pile
BFS file
Dijkstra file-prio
Kruskal union-find
Mémoïsation table de hash
Moore partitions

I. LE TYPE PILE
   A) Type de donnée abstrait
   B) Implémentation par listes
   C) Étude de complexité

II. LES STRUCTURES SÉQUENTIELLES
   A) Files
   B) Doubles files
   C) Tableaux dynamiques

III. DICTIONNAIRES
   A) ABR
   B) AVL
   C) Hachage

IV. FILE DE PRIORITÉ
   A) Tableau trié
   B) Tas binaire
   C) Tas binomial/Fibonacci

V. PARTITIONS
   A) Union-Find
   B) Partitions disjointes (cormen)

4.902 ■ DIVISER POUR RÉGNER. EXEMPLES ET APPLICATIONS

■ **DÉVELOPPEMENTS** **5.0**

D00 ANALYSE DU TRI RAPIDE ⋆⋆⋆⋆⋆

D20 POINTS LES PLUS PROCHES ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Cormen

Beauquier

Dalpagusta

■ **RAPPORT DE JURY**

> Cette leçon permet au candidat de proposer différents algorithmes utilisant le paradigme diviser pour régner. Le jury attend du candidat que ces exemples soient variés et touchent des domaines différents. Un calcul de complexité ne peut se limiter au cas où la taille du problème est une puissance exacte de 2, ni à une application directe d'un théorème très général recopié approximativement d'un ouvrage de la bibliothèque de l'agrégation.

■ **IDÉE DE PLAN :** C'est une leçon orientée sur un *paradigme*, il faut donc structurer le cours sur les applications. Faire une première partie de présentation du paradigme.

I. PRÉSENTATION DU PARADIGME
- A) Méthode générale
- B) Sur un exemple facile
- C) Étude de complexité

II. ALGORITHMES DE TRI
- A) Fusion
- B) Tri-rapide
- C) Médians
- D) Tri-bitonique

III. PRODUITS
- A) Karatsuba
- B) Strassen
- C) FFT

IV. GÉOMÉTRIE
- A) Points les plus proches
- A) Enveloppe convexe

4.903 ■ EXEMPLES D'ALGORITHMES DE TRI. CORRECTION ET COMPLEXITÉ.

■ **DÉVELOPPEMENTS** **5.0**

D00 ANALYSE DU TRI RAPIDE ★★★★★

D11 BORNE INFÉRIEURE TRI PAR COMPARAISON ★★★★★

■ **RÉFÉRENCES**

Cormen

Beauquier

■ **RAPPORT DE JURY**

> Sur un thème aussi classique, le jury attend des candidats la plus grande précision et la plus grande rigueur. Ainsi, sur l'exemple du tri rapide, il est attendu du candidat qu'il sache décrire avec soin l'algorithme de partition et en prouver la correction en exhibant un invariant adapté. L'évaluation des complexités dans le cas le pire et en moyenne devra être menée avec rigueur : si on utilise le langage des probabilités, il importe que le candidat sache sur quel espace probabilisé il travaille. On attend également du candidat qu'il évoque la question du tri en place, des tris stables, ainsi que la représentation en machine des collections triées. Le jury ne manquera pas de demander au candidat des applications non triviales du tri.

■ **IDÉE DU PLAN :** On commence par définir la notion de tri. Cela permet d'utiliser plein de tris élémentaires, puis de passer aux tris optimaux par comparaison. On peut ensuite s'intéresser aux méthodes alternatives n'utilisant pas de comparaison.

L'intérêt pédagogique du tri est que c'est une opération très simple, pour laquelle les algorithmes efficaces ne sont pas les algorithmes "naturels" pour un être humain, illustrant beaucoup de techniques de programmation.

I. NOTION DE TRI
   A) Spécification "hoare"
   B) Complexité via les comparaisons
   C) Propriétés supplémentaires (en place, stable etc...)

II. TRIS ÉLÉMENTAIRES
   A) Insertion
   B) Sélection
   C) Bubble

III. TRIS OPTIMAUX
   A) Borne inférieure (Lien avec l'enveloppe convexe)
   B) Tri fusion
   C) Tri rapide

IV. TRI PAR STRUCTURE
   A) Tri par tas
   B) Tri par AVL

V. TRIS ALTERNATIFS
   A) Tri par dénombrement
   B) Tri par base
   C) Tri par paquets
   D) Tri bitonique

4.906 ■ PROGRAMMATION DYNAMIQUE. EXEMPLES ET APPLICATIONS.

■ **DÉVELOPPEMENTS** **4.5**

D05 DISTANCE D'ÉDITION ET FACTEURS À DISTANCE k ⋆⋆⋆⋆⋆

D08 PROBLÈME NP-COMPLET UNAIRE ⋆⋆⋆⋆

■ **RÉFÉRENCES**

Cormen

Beauquier

Crochemore

■ **RAPPORT DE JURY**

> Même s'il s'agit d'une leçon d'exemples et d'applications, le jury attend des candidats qu'ils présentent les idées générales de la programmation dynamique et en particulier qu'ils aient compris le caractère générique de la technique de mémoïsation. Le jury appréciera que les exemples choisis par le candidat couvrent des domaines variés, et ne se limitent pas au calcul de la longueur de la plus grande sous-séquence commune à deux chaînes de caractères. Le jury ne manquera pas d'interroger plus particulièrement le candidat sur la question de la correction des algorithmes proposés et sur la question de leur complexité en espace.

■ **IDÉE DU PLAN :** C'est une fois de plus une leçon de *paradigme*, on fait donc un plan thématique.

Toutefois un plan thématique seul n'est pas suffisant, le paradigme étant assez riche pour avoir une véritable introduction pour lui-même.

I. PARADIGME
   A) Optimalité de Bellmann
   B) Mémoïsation, top/bottom
   C) Différences, tps/mémoire

II. EXEMPLES D'ÉCHAUFFEMENT
   A) Fibonacci
   B) Multiplication de matrices
   C) Sous séquences de palindromes

III. ALGORITMIQUE DU TEXTE
   A) PLSC
   B) Edition
   C) CYK

IV. ALGORITHMES DE GRAPHES
   (a) Dijkstra
   (b) Bellmann ford
   (c) Floyd-warshall (et généralisation)

V. NP-COMPLÉTUDE
   A) Subsetsum
   B) Knapsack
   C) SAT et Bergman

4.907 ■ ALGORITHMIQUE DU TEXTE. EXEMPLES ET APPLICATIONS.

■ **DÉVELOPPEMENTS** **5.0**

D04 AUTOMATE D'AHO-CORASICK ⋆⋆⋆⋆⋆

D05 DISTANCE D'ÉDITION ET FACTEURS À DISTANCE k ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Beauquier

Crochemore

■ **RAPPORT DE JURY**

TODO

■ **IDÉE DU PLAN :** Il faut dédier une partie de la leçon à la recherche de motif. On commence par l'algorithme naïf, puis l'amélioration jusqu'à KMP. Cela peut faire une partie. Boyer-Moore peut se faire dans un deuxième temps en reprenant les mêmes idées.

Il est judicieux d'évoquer d'autres problèmes sur les textes : plus longue sous-séquence, recherche approchée, distance d'édition.

Enfin, une dernière partie qui s'intéresse aux structures de données pour l'algorithmique du texte est d'autant plus intéressante qu'elle rentre aussi dans "structure de données pour la recherche".

Bien préciser au début de la leçon *quels domaines* seront abordés. On évite ainsi tout débordement sur la leçon analyse lexicale, automates finis, etc ...

I. RECHERCHE DE MOTIF NAÏVE
   - A) Définition du problème
   - B) Algorithme GD/DG
   - C) Rabin-Karp et hach

II. AMÉLIORATIONS : MP, KMP, BOYER-MOORE
   - A) MP
   - B) KMP
   - C) Boyer-Moore

III. COMPARAISON DE CHAÎNES
   - A) PLSC
   - B) Edition
   - C) Recherche approchée

IV. STRUCTURES DE DONNÉES
   - (a) Langages réguliers et automates
   - (b) Automate des bordures, Aho-Corasick
   - (c) Tries / Suffix Tree

4.909 ■ LANGAGES RATIONNELS ET AUTOMATES FINIS. EXEMPLES ET APPLICATIONS.

■ **DÉVELOPPEMENTS** **5.0**

D06 AUTOMATES ET PRESBURGER ⋆⋆⋆⋆⋆

D07 AUTOMATES BOUSTROPHÉDON ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Sakarovich

Carton

Beauquier

■ **RAPPORT DE JURY**

> Pour cette leçon très classique, il importe de ne pas oublier de donner exemples et applications, ainsi que le demande l'intitulé. Une approche algorithmique doit être privilégiée dans la présentation des résultats classiques (déterminisation, théorème de Kleene, etc.) qui pourra ultérieurement être illustrée par des exemples. Le jury pourra naturellement poser des questions telles que : connaissez-vous un algorithmme pour décider de l'égalité des langages reconnus par deux automates ? Quelle est sa complexité ? Des applications dans le domaine de l'analyse lexicale et de la compilation entrent naturellement dans le cadre de cette leçon.

■ **IDÉE DU PLAN :** On commence en première page avec plein d'algorithmique pour donner confiance au jury.

De manière plus générale, on fait un plan de type thématique, avec automates, expressions, monoïdes. Chaque partie étant l'occasion d'introduire de nombreux exemples : automate des motifs, model checking, grep, machines de turing, presburger et bien d'autres.

Il faut insister sur la complexité des opérations de clôture, en faisant une *table en annexe* pour ne pas rendre le texte illisible et montrer une vision globale.

I. AUTOMATES
- A) DFA. Ex et App.
- B) NFA. ε-trans.
- C) Déterminisme, complétude, algorithmes
- D) EX : Motifs

II. LANGAGES RATIONNELS
- A) Clôtures effectives
- B) APP : Presburger
- C) Expressions rationnelles
- D) Analyse lexicale
- E) Équivalence
- F) Caractérisations (pompage et compagnie)

III. ÉTUDE ALGÉBRIQUE
- A) Monoïde syntaxique
- B) EX : Boustrophédon
- C) Automate minimal

IV. ANNEXE DÉCISION
- (a) Problème du mot
- (b) Égalité de langages
- (c) Intersection vide
- (d) etc ...

4.912 ■ FONCTIONS RÉCURSIVES PRIMITIVES ET NON PRIMITIVES. EXEMPLES.

■ **DÉVELOPPEMENTS** **5.0**

D21 CALCULABLE SSI RÉCURSIF ⋆⋆⋆⋆⋆

D22 HIÉRARCHIE DE GREGOJURSXT ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Wolper

Carton

Clefs agrégation

4.913 ■ MACHINES DE TURING. APPLICATIONS.

■ **DÉVELOPPEMENTS** **5.0**

D02 HIÉRARCHIE EN ESPACE ET EN TEMPS ⋆⋆⋆⋆⋆

D07 AUTOMATES BOUSTROPHÉDON ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Wolper

Carton

Arora Barak

■ **RAPPORT DE JURY**

> Il s'agit de présenter un modèle de calcul. Le candidat doit expliquer l'intérêt de disposer d'un modèle formel de calcul et discuter le choix des machines de Turing. La leçon ne peut se réduire à la leçon 914 ou à la leçon 915, même si, bien sûr, la complexité et l'indécidabilité sont des exemples d'applications. Plusieurs développements peuvent être communs avec une des leçons 914, 915 mais il est apprécié qu'un développement spécifique soit proposé, comme le lien avec d'autres modèles de calcul, ou le lien entre diverses variantes des machines de Turing.

■ **IDÉE DU PLAN :** Pour cette leçon un plan didactique *définitions* puis *applications* semble idéal. On ne manquera pas de souligner la *diversité* des définitions, et leurs relations, en utilisant par exemple le terme de *robustesse*. Cela permet de distinguer « le » modèle de Turing, et le λ-calcul ou les fonctions récursives.

Dans la partie décidabilité, on peut par ailleurs noter la similarité avec le fonctionnement d'une machine RAM, ce qui permet d'écrire de manière *informelle* des programmes et fournir des preuves convaincantes, mais surtout très simples.

Dans la partie complexité, on peut remarquer que la notion même de complexité repose sur la sémantique petits-pas. Les fonctions récursives (dénotationnelle) et le λ-calcul (pas de configuration) ne permettent pas de définir de manière pertinente la complexité d'un calcul.

I. MODÈLE DE CALCUL
- A) Machines de turing à une bande I/O
- B) Langage d'une machine
- C) Robustesse

II. CALCULABILITÉ
- A) Lien avec récursives
- B) Récursif, rec enum
- C) Indécidabilité
- D) APP : analyse lex/synt

III. COMPLEXITÉ
- A) Lien avec le λ-calcul
- B) Raffinements robustesse
- C) Polynômial
- D) Hiérarchie

4.914 ■ DÉCIDABILITÉ ET INDÉCIDABILITÉ. EXEMPLES.

■ **DÉVELOPPEMENTS** **4.5**

D06 AUTOMATES ET PRESBURGER ⋆⋆⋆⋆⋆

D16 GRAMMAIRES ET INDÉCIDABILITÉ ⋆⋆⋆⋆

■ **RÉFÉRENCES**

Wolper pour l'indécidabilité

Carton pour l'indécidabilité

Arora Barak pour les machines

Cori pour la logique

Raffali pour la logique

Dowek pour la logique

■ **RAPPORT DE JURY**

> Le programme de l'option offre de très nombreuses possibilités d'exemples. Si les exemples classiques de problèmes sur les machines de Turing figurent naturellement dans la leçon, le jury apprécie des exemples issus d'autres parties du programme : théorie des langages, logique,... Le jury portera une attention particulière à une formalisation propre des réductions, qui sont parfois très approximatives.

■ **IDÉE DU PLAN :** Avant de parler de décidabilité, il faut parler de langage. On évoque donc naturellement les classes D, RE et leurs propriétés de clôtures. Bien entendu, la robustesse des différentes classes au modèle de calcul est un passage nécessaire.

Ensuite, on peut attaquer la partie cruciale : le résultat d'incécidabilité et ses variantes, la notion de réduction et l'impossibilité de vérifier un programme (Rice).

Une dernière partie parle alors des applications des notions, en prenant deux exemples du rapport de jury : l'analyse lexicale/syntaxique et la logique. Dans le premier on part du facile/décidable vers le pratique mais indécidable, et dans l'autre on fait l'inverse.

I. LANGAGES
   A) Décidable, clôture
   B) RE, clôture
   C) Équivalence des modèles

II. INDÉCIDABILITÉ
   A) Problème de l'arrêt
   B) Réductions
   C) PCP, riez et co

III. APPLICATIONS
   A) Analyse de texte
   B) Logique

4.915 ■ CLASSES DE COMPLEXITÉ. EXEMPLES.

■ **DÉVELOPPEMENTS** **5.0**

D02 HIÉRARCHIE EN ESPACE ET EN TEMPS ⋆⋆⋆⋆⋆

D15 2SAT NL-COMPLET ET TEMPS POLY ⋆⋆⋆⋆⋆

D21 CALCULABLE SSI RÉCURSIF ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Carton

Arora Barak

■ **RAPPORT DE JURY**

> Le jury attend que le candidat aborde à la fois la complexité en temps et en espace. Il faut naturellement exhiber des exemples de problèmes appartenant aux classes de complexité introduites, et montrer les relations d'inclusion existantes entre ces classes, en abordant le caractère strict ou non de ces inclusions. Le jury s'attend à ce que les notions de réduction polynomiale, de problème complet pour une classe, de robustesse d'une classe vis à vis des modèles de calcul soient abordées. Parler de décidabilité dans cette leçon serait hors sujet.

■ **IDÉE DU PLAN :**

On ne fait pas dans l'originalité : le plan du Barak Arora est parfait. Il se fait en quatre temps 1. Notion de complexité et robustesse 2. P et NP 3. Autres classes 4. Étude de hiérarchies .

Ne pas oublier de faire un joli dessin en annexe avec les différentes inclusions strictes ou non.

I. NOTION DE COMPLEXITÉ
   A) Complexité en temps
   B) Complexité en espace
   C) Robustesse

II. TEMPS POLYNÔMIAL
   A) P
   B) NP

III. LE PAYSAGE CLASSIQUE
   A) PSPACE et NPSPACE
   B) L et NL

IV. HIÉRARCHIES
   A) Théorèmes de hiérarchie (simulation etc)
   B) PH

4.916 ■ FORMULES DU CALCUL PROPOSITIONNEL : REPRÉSENTATION, FORMES NORMALES, SATISFIABILITÉ. APPLICATIONS.

■ **DÉVELOPPEMENTS** **5.0**

D13 COMPLÉTUDE DE LA RÉSOLUTION ★★★★★

D15 2SAT NL-COMPLET ET TEMPS POLY ★★★★★

■ **RÉFÉRENCES**

René Lalement Logique, réduction résolution

Gilles Dowek

Cori 1/2

Raffali

Goubault BDD

■ **RAPPORT DE JURY**

> Le jury attend des candidats qu'ils abordent les questions de la complexité de la satisfiabilité. Pour autant, les applications ne sauraient se réduire à la réduction de problèmes NP-complets à SAT. Une partie significative du plan doit être consacrée à la représentation des formules et à leurs formes normales.

■ **IDÉE DU PLAN :** On prend textuellement le titre de la leçon.

L'idée c'est de faire au plus simple pour ne pas surprendre le jury, tout en ayant la possibilité d'aborder plusieurs choses : la notion de formule, les formes normales, les algorithmes de satisfiabilité. Tout cela bien entendu en étudiant la complexité et la totalité des méthodes.

■ **ÉLÉMENTS CLEFS**

Table de vérité	**SAT solver**	**BDD**
Compacité logique	**Résolution**	**Substution**
Cook	**Tseitin**	**DPLL**
Graphes et SAT	**Horn**	**QBF**

I. FORMULES DU CALCUL PROPOSITIONNEL
   A) Syntaxe
   B) Sémantique
   C) Satisfiabilité 101

II. FORMES NORMALES
   A) Système de connecteurs
   B) FNC/FND
   C) BDD

III. SATISFIABILITÉ
   A) NP-complétude
   B) Déduction
   C) Variantes de SAT

4.918 ■ SYSTÈMES FORMELS DE PREUVES EN LOGIQUE DU PREMIER ORDRE. EXEMPLES.

■ **DÉVELOPPEMENTS** **4.0**

D12 THÉORÈME DE COMPLÉTUDE ⋆⋆⋆⋆⋆

D13 COMPLÉTUDE DE LA RÉSOLUTION ⋆⋆⋆

■ **RÉFÉRENCES**

René Lalement Logique, réduction résolution

Gilles Dowek

Cori 1/2

Raffali

Goubault BDD

■ **RAPPORT DE JURY**

> Le jury attend du candidat qu'il présente au moins la déduction naturelle ou un calcul de séquents et qu'il soit capable de développer des preuves dans ce système sur des exemples classiques simples. La présentation des liens entre syntaxe et sémantique, en développant en particulier les questions de correction et complétude, et de l'apport des systèmes de preuves pour l'automatisation des preuves est également attendue. Le jury appréciera naturellement si des candidats présentent des notions plus élaborées comme la stratégie d'élimination des coupures mais est bien conscient que la maîtrise de leurs subtilités va au-delà du programme.

■ **IDÉE DU PLAN :** On fait un plan quasi-thématique. Une introduction à la notion de théorie, de modèle, puis directement une partie par système de preuve.

Les exemples ne manquent pas, mais il ne faut surtout pas confondre cette leçon avec la 924. En effet il ne faut pas s'intéresser particulièrement aux propriétés d'une théorie donnée, ni même s'attarder sur la notion de modèle.

■ **ÉLÉMENTS CLEFS**

Théorie	**Déduction naturelle**	**Résolution**
Modèle	**Calcul des séquents**	**Élimination des coupures**

I. FORMULES DU CALCUL PROPOSITIONNEL
- A) Syntaxe
- B) Sémantique
- C) Satisfiabilité 101

II. FORMES NORMALES
- A) Système de connecteurs
- B) FNC/FND
- C) BDD

III. SATISFIABILITÉ
- A) NP-complétude
- B) Déduction
- C) Variantes de SAT

4.921 ■ ALGORITHMES DE RECHERCHE ET STRUCTURES DE DONNÉES ASSOCIÉES.

■ **DÉVELOPPEMENTS** **5.0**

D01 ARBRES AVL ⋆⋆⋆⋆⋆

D14 HACHAGE PARFAIT ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Cormen

Beauquier

Dalpagusta

■ **RAPPORT DE JURY**

> Le sujet de la leçon concerne les algorithmes de recherche : les structures de données proposées doivent répondre à une problématique liée aux algorithmes, et la leçon ne peut donc être structurée sur la base d'un catalogue de structures de données. La recherche d'une clé dans un dictionnaire sera ainsi par exemple l'occasion de définir la structure de données abstraite « dictionnaire », et d'en proposer plusieurs implantations concrètes. De la même façon, on peut évoquer la recherche d'un mot dans un lexique : les arbres préfixes (ou digital tries) peuvent alors être présentés. Mais on peut aussi s'intéresser à des domaines plus variés, comme la recherche d'un point dans un nuage (et les quad-trees), et bien d'autres encore.

■ **IDÉE DU PLAN :** On construit le plan par complexité croissante des éléments recherchés. Attention à bien introduire chaque partie via un algorithme ! Ainsi, on commence par tester l'égalité structurelle Par la suite on peut s'intéresser aux éléments par rapport à un ordre $\leq$ fixé. On spécifie encore et on ne veut plus trouver un élément particulier, mais un représentant d'une classe d'équivalence. On continue à enrichir la structure, on s'intéresse à l'algorithmique du texte.

■ **ÉLÉMENTS CLEFS**

Hachage	**Union Find**	**Tri**
AVL	**Partitions**	**Médian**
Suffix Tree	**Dijkstra**	**k-rank**
Aho-Corasick	**Kruskal**	
Tas	**Moore**	

I. RECHERCHE PAR ÉGALITÉ
   A) Tableau/liste
   B) Hachage

II. RECHERCHE PAR ORDRE
   A) Tris/rang k
   B) ABR/AVL
   C) Tas

III. RECHERCHE DE CLASSE
   A) Union-Find
   B) Partitions

IV. RECHERCHE DE MOTIF
   A) Automates
   B) Suffix Tree

4.923 ■ ANALYSE LEXICALE ET SYNTAXIQUE. APPLICATIONS.

■ **DÉVELOPPEMENTS** **4.5**

D16 GRAMMAIRES ET INDÉCIDABILITÉ ★★★★

D19 CALCUL PREMIER-SUIVANT ★★★★★

■ **RÉFÉRENCES**

Carton

Petits poissons

Beauquier

Autebert

Compilers, Aho, Ullman, Lam, Seth

■ **RAPPORT DE JURY**

> Cette leçon ne doit pas être confondue avec la 909, qui s'intéresse aux seuls langages rationnels, ni avec la 907, sur l'algorithmique du texte. Si les notions d'automates finis, de langages rationnels et de grammaires algébriques sont au coeur de cette leçon, l'accent doit être mis sur leur utilisation comme outils pour les analyses lexicale et syntaxique. Il s'agit donc d'insister sur la différence entre langages rationnels et algébriques, sans perdre de vue l'aspect applicatif : on pensera bien sûr à la compilation. On pourra s'intéresser à la transition entre analyse lexicale et analyse syntaxique, et on pourra présenter les outils associés classiques, sur un exemple simple. Les notions d'ambiguïté et l'aspect algorithmique doivent être développés. La présentation d'un type particulier de grammaire algébrique pour laquelle on sait décrire un algorithme d'analyse syntaxique efficace sera ainsi appréciée. Le programme 2018 permet de nouveaux développements pour cette leçon avec une ouverture sur des aspects élementaires d'analyse sémantique.

■ **IDÉE DU PLAN :** Il n'y a pas d'ambiguité dans le sujet, la compilation est un passage nécessaire. Quand le jury parle de grammaires intéressantes, il veut dire LL ou bien automates à pile déterministes. On fait donc un plan orienté compilation : définition, lexicale, syntaxique, sémantique. En prenant bien soin de soulever les difficultés dans chaque partie, et surtout *le lien entre les parties*. L'introduction peut parler d'Unix et de la propriété terrible "tout est downcasté vers du texte", ce qui justifie la nécessité d'une telle compilation dans de nombreux cadres très différents.

■ **ÉLÉMENTS CLEFS :**

Automates/piles	**CYK vs LL**	**Complexité !**
Transducteurs	**Ambiguïté/Équivalence**	**IMP/JSON/YAML**

I. COMPILATION
  A) Donnée non structurée
  B) Arbre de syntaxe
  C) Arbre sémantique
  D) Schéma global

II. ANALYSE LEXICALE
  A) Lexèmes
  B) Automates
  C) Problèmes de décision

III. ANALYSE SYNTAXIQUE
  A) Grammaires algébriques
  B) Automates à piles
  C) Problèmes de décision
  D) Analyse LL

IV. ANALYSE SÉMANTIQUE
  A) Annotations
  B) Système de type

4.924 ■ THÉORIES ET MODÈLES EN LOGIQUE DU PREMIER ORDRE. EXEMPLES.

■ **DÉVELOPPEMENTS** **4.5**

D06 AUTOMATES ET PRESBURGER ⋆⋆⋆⋆

D12 THÉORÈME DE COMPLÉTUDE ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Cori

Raffali

Goubault

Loique réduction résolution

■ **RAPPORT DE JURY**

> Le jury s'attend à ce que la leçon soit abordée dans l'esprit de l'option informatique, en insistant plus sur la décidabilité/indécidabilité des théories du premier ordre que sur la théorie des modèles. Il est attendu que le candidat donne au moins un exemple de théorie décidable (respectivement complète) et un exemple de théorie indécidable. Si le jury peut s'attendre à ce que le candidat connaisse l'existence du théorème d'incomplétude, il ne s'attend pas à ce que le candidat en maîtrise la démonstration.

■ **IDÉE DU PLAN :**

Il faut parler de théories et de modèles, donc on commence par faire une partie définitions et exemples sur les deux notions. Cela permet ensuite de s'intéresser dans une deuxième partie aux *liens* entre les notions et leurs conséquences. Enfin on s'intéresse à la décidabilité.

■ **ÉLÉMENTS CLEFS :**

Complétude	**Gödel**	**Presburger**
Lowelheim-Skolem	**Élimination Quant**	
Erenfeucht ?	**Petits modèles**	**Peano**

I. THÉORIES & MODÈLES
   A) Théories
   B) Modèles

II. LIENS ENTRE LES DEUX NOTIONS
   A) Correction & Complétude
   B) Compacité
   C) Résolution & Herbrand

III. INDÉCIDABILITÉ
   A) Peano
   B) Presburger
   C) SAT...

4.925 ■ GRAPHES. REPRÉSENTATIONS ET ALGORITHMES.

■ **DÉVELOPPEMENTS** **5.0**

D03 ALGORITHME DE DIJKSTRA ⋆⋆⋆⋆⋆

D15 2SAT NL-COMPLET ET TEMPS POLY ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Cormen

Beauquier

Dalpagusta

■ **RAPPORT DE JURY**

Cette leçon offre une grande liberté de choix au candidat, qui peut décider de présenter des algorithmes sur des problèmes variés : connexité, diamètre, arbre couvrant, flot maximal, plus court chemin, cycle eulérien, etc. mais aussi des problèmes plus difficiles, comme la couverture de sommets ou la recherche d'un cycle hamiltonien, pour lesquels il pourra proposer des algorithmes d'approximation ou des heuristiques usuelles. Une preuve de correction des algorithmes proposés sera évidemment appréciée. Il est attendu que diverses représentations des graphes soient présentées et comparées, en particulier en termes de complexité.

■ **IDÉE DU PLAN :**

On suit le jury, sinon on se fait taper sur les doigts par popol. Donc d'abord représentations, puis algorithmes en une longue liste décousue, triée approximativement.

I. REPRÉSENTATION DES GRAPHES
   A) Matrice
   B) Liste
   C) Adjacence

II. PARCOURS DE GRAPHE
   A) Parcours en largeur
   B) Parcours en profondeur
   C) Autres parcours (eulérien, hamiltonien)

III. COMPOSANTES CONNEXES
   A) Kosaraju
   B) 2SAT

IV. PLUS COURT CHEMIN
   A) Bellmann-Ford
   B) Dijkstra
   C) Floyd-Warshall

V. ARBRES COUVRANTS
   A) Kruskal
   B) Prim

VI. FLOTS (OPTS)
   A) CORMEN

4.926 ■ ANALYSE DES ALGORITHMES, COMPLEXTÉ. EXEMPLES.

■ **DÉVELOPPEMENTS** **4.5**

D00 ANALYSE DU TRI RAPIDE ⋆⋆⋆⋆⋆

D01 ARBRES AVL ⋆⋆⋆⋆

■ **RÉFÉRENCES**

Cormen

Beauquier

Dalpagusta

Flajolet Pour la méthode des séries génératrices

■ **RAPPORT DE JURY**

> Il s'agit ici d'une leçon d'exemples. Le candidat prendra soin de proposer l'analyse d'algorithmes portant sur des domaines variés, avec des méthodes d'analyse également variées : approche combinatoire ou probabiliste, analyse en moyenne ou dans le cas le pire. Si la complexité en temps est centrale dans la leçon, la complexité en espace ne doit pas être négligée. La notion de complexité amortie a également toute sa place dans cette leçon, sur un exemple bien choisi, comme union find (ce n'est qu'un exemple).

■ **IDÉE DU PLAN :**

On fait encore une fois un plan thématique, on commence par les définitions (avec exemples triviaux), puis on s'attarde sur les différentes méthodes. Les méthodes peuvent être attachée à des styles de programmation (récursif, dynamique, impératif) ou bien à des modes de complexité (amortie, en moyenne).

Attention, il ne faut surtout pas définir le modèle de calcul qui est considéré, et si la question se pose, évoquer une sémantique à petits pas pour éviter d'avoir des questions pénibles sur les modèles de machines de Turing.

I. NOTION DE COMPLEXITÉ
   - A) Notations asymptotiques
   - B) Complexité temporelle
   - C) Complexité spatiale

II. ANALYSES CLASSIQUES
   - A) Des programmes itératifs
   - B) Des programmes récursifs

III. ANALYSES ALTERNATIVES
   - A) Amortie
   - B) Moyenne

IV. COMPROMIS TEMPS/MÉMOIRE
   - A) Programmation dynamique
   - B) Structure de données 1
   - C) Structure de données 2

4.927 ■ EXEMPLES DE PREUVE D'ALGORITHME, CORRECTION, TERMINAISON.

■ **DÉVELOPPEMENTS** **5.0**

D03 ALGORITHME DE DIJKSTRA ⋆⋆⋆⋆⋆

D09 COMPLÉTUDE DE LA LOGIQUE DE HOARE ⋆⋆⋆⋆⋆

D20 POINTS LES PLUS PROCHES ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Cormen

Beauquier

Dalpagusta

■ **RAPPORT DE JURY**

> Le jury attend du candidat qu'il traite des exemples d'algorithmes récursifs et des exemples d'algorithmes itératifs. En particulier, le candidat doit présenter des exemples mettant en évidence l'intérêt de la notion d'invariant pour la correction partielle et celle de variant pour la terminaison des segments itératifs. Une formalisation comme la logique de Hoare pourra utilement être introduite dans cette leçon, à condition toutefois que le candidat en maîtrise le langage. Des exemples non triviaux de correction d'algorithmes seront proposés. Un exemple de raisonnement type pour prouver la correction des algorithmes gloutons pourra éventuellement faire l'objet d'un développement.

■ **IDÉE DU PLAN :**

On ne peut pas éviter une présentation "formaliste" de la notion de programme. Toutefois, la sémantique effective est reléguée à une dernière partie, justifiant la correction des raisonnements effectués avant elle.

I. TERMINAISON
   A) Propriétés des ordres et ré-écriture
   B) Dans un programme itératif
   C) Dans un programme récursif

II. CORRECTION
   A) Correction totale, partielle
   B) Récursif
   C) Itératif
   D) Gloutons

III. RÈGLES DE HOARE
   A) IMP
   B) Hoare
   C) Complétude

4.928 ■ PROBLÈMES NP-COMPLETS. EXEMPLES ET RÉDUCTION.

■ **DÉVELOPPEMENTS** **3.5**

D08 PROBLÈME NP-COMPLET UNAIRE ⋆⋆⋆⋆

D15 2SAT NL-COMPLET ET TEMPS POLY ⋆⋆⋆

■ **RÉFÉRENCES**

Cormen

Beauquier

Dalpagusta

■ **RAPPORT DE JURY**

L'objectif ne doit pas être de dresser un catalogue le plus exhaustif possible ; en revanche, pour chaque exemple, il est attendu que le candidat puisse au moins expliquer clairement le problème considéré, et indiquer de quel autre problème une réduction permet de prouver sa NP-complétude. Les exemples de réduction polynomiale seront autant que possible choisis dans des domaines variés : graphes, arithmétique, logique, etc. Un exemple de problème NP-complet dans sa généralité qui devient P si on contraint davantage les hypothèses pourra être présenté, ou encore un algorithme P approximant un problème NP-complet. Si les dessins sont les bienvenus lors du développement, le jury attend une définition claire et concise de la fonction associant, à toute instance du premier problème, une instance du second ainsi que la preuve rigoureuse que cette fonction permet la réduction choisie.

■ **IDÉE DU PLAN :**

On suit le plan du jury. D'abord la définition de P et NP, la notion de réduciton, des exemples. Ensuite la NP-complétude, en long en large et en travers. Enfin, les limites de la complétude.

■ **ÉLÉMENTS CLEFS :**

logique	**knapsack**	**VC**
graphes	**2-approx**	
bin packing	**DPLL**	

I. LA CLASSE NP
- A) La classe P et NP
- B) Notion de certificat
- C) Réduction poly

II. *NP*-COMPLÉTUDE
- A) Logique
- B) Graphes
- C) Arithmétique
- D) Langages

III. AU DELÀ DE NP
- A) Restrictions
- B) Approximations
- C) SAT-solvers

4.929 ■ LAMBDA-CALCUL PUR COMME MODÈLE DE CALCUL. EXEMPLES.

■ **DÉVELOPPEMENTS** **5.0**

D17 LEMME DES DÉVELOPPEMENTS FINIS ⋆⋆⋆⋆⋆

D18 CONFLUENCE λ-CALCUL ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

J.L. Krivine Lambda-calcul types et modèles

Henk Barendregt The Lambda Calculus, Its Syntax and Semantics

R. Lalement Logique réduction résolution

■ **RAPPORT DE JURY**

Il s'agit de présenter un modèle de calcul : le lambda-calcul pur. Il est important de faire le lien avec au moins un autre modèle de calcul, par exemple les machines de Turing ou les fonctions récursives. Néanmoins, la leçon doit traiter des spécificités du lambda-calcul. Ainsi le candidat doit motiver l'intérêt du lambda-calcul pur sur les entiers et pourra aborder la façon dont il permet de définir et d'utiliser des types de données (booléens, couples, listes, arbres).

■ **IDÉE DU PLAN :**

On doit se concentrer sur la partie *calcul*. Il est donc naturel de comparer régulièrement le lambda-calcul aux autres modèles : turing, fonctions récursives ... mais aussi OCaml/Scheme par exemple.

Si la notion de type est hors-sujet, l'encodage des données et sa philosophie est centrale dans la leçon. On a donc un plan très simple. D'abord définir les termes, ce qui contient déjà son lot de subtilités. Ensuite parler de réduction, et *dès lors* encoder des données ! On peut faire une seconde partie pour expliquer formellement les différentes réductions et leurs propriétés. En terminant bien sûr sur l'équivalence avec les autres modèles de calcul.

I. LES λ-TERMES
   A) Syntaxe
   B) α-équivalence
   C) Exemples

II. LA β-RÉDUCTION
   A) Définition
   B) Codages
   C) Points fixes

III. LES β-RÉDUCTIONS
   A) Confluence
   B) Développements finis
   C) Réductions alternatives

IV. STATUT DU MODÈLE DE CALCUL
   A) Équivalence avec recursives
   B) Petites propriétés de décidabilité
   C) Ouverture : système de typage ...

4.930 ■ SÉMANTIQUE DES LANGAGES DE PROGRAMMATION. EXEMPLES.

■ **DÉVELOPPEMENTS** **5.0**

D09 COMPLÉTUDE DE LA LOGIQUE DE HOARE ⋆⋆⋆⋆⋆

D10 ÉQUIVALENCE ENTRE SÉMANTIQUE OPÉRATIONNELLE ET DÉNOTATIONNELLE ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Winskel

■ **RAPPORT DE JURY**

L'objectif est de formaliser ce qu'est un programme : introduction des sémantiques opérationnelle et dénotationnelle, dans le but de pouvoir faire des preuves de programmes, des preuves d'équivalence, des preuves de correction de traduction. Ces notions sont typiquement introduites sur un langage de programmation (impératif) jouet. On peut tout à fait se limiter à un langage qui ne nécessite pas l'introduction des CPOs et des théorèmes de point fixe généraux. En revanche, on s'attend ici à ce que les liens entre sémantique opérationnelle et dénotationnelle soient étudiés (toujours dans le cas d'un langage jouet). Il est aussi important que la leçon présente des exemples d'utilisation des notions introduites, comme des preuves d'équivalence de programmes ou des preuves de correction de programmes.

■ **IDÉE DU PLAN :**

On ne suit *surtout pas* la recommandation du jury qui obfusque les preuves de correction/adéquation. En revanche, on découpe soigneusement la partie expression de la partie commandes. Enfin, on évoque l'utilisation pour les preuves de hoare.

Il *faut* évoquer les différentes utilisations des différentes sémantiques. Les opérationnelles sont pratiques pour implémenter, les dénotationnelles pour raisonner. La notion de calcul permet-elle de définir une complexité ? Peut-on décrire le comportement de programmes qui ne terminent pas ?

Attention, l'introduction de CPO peut amener à des questions triviales, mais auxquelles il faut savoir répondre : pourquoi le sup dans les fonctions est le sup terme à terme ? Propriété de la chaine croissante ? etc ...

I. LE LANGAGE IMP
   A) Expressions
   B) Commandes
   C) Exemples

II. EXPRESSIONS
   A) Dénotation
   B) Grand pas
   C) Petit pas

III. COMMANDES
   A) Petit pas
   B) Grand pas
   C) Dénotation

IV. HOARE
   A) Langage logique
   B) Règles de hoare
   C) Complétude

Deuxième partie

Mathématiques

CHAPITRE 5

STATISTIQUES — 2019-03-06

■ **DÉVELOPPEMENTS**

Nombre de devs	29
Nombre optimal	[Désactivé à la compilation]
Recasage moyen	2.97
Rédaction	27 sur 29

■ **LEÇONS**

Sans développement (abs)	0
Un seul développement (abs)	1
Nombre moyen de développments	2.05
Écart-type σ	0.30
Rédaction	40 sur 42

■ **[DEADLINE] LEÇONS BLANCHES MATHÉMATIQUES**

Date	2018-05-30
Dans	-281 Jours
OVERDUE	...

■ **[DEADLINE] DÉBUT DES ORAUX AGRÉGATION**

Date	2018-06-29
Dans	-251 Jours
OVERDUE	...

■ **LIENS**

☐ DÉVELOPPEMENTS

☐ LEÇONS

CHAPITRE 6

DÉVELOPPEMENTS

6.0 ■ FROBÉNIUS-ZOLOTAREV

Référence : Beck. Recasé 5 fois

■ **LEÇONS**

L105 GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI. APPLICATIONS ★★★★★

L106 GROUPE LINÉAIRE D'UN ESPACE VECTORIEL DE DIMENSION FINIE, SOUS GROUPES. APPLICATIONS ★★★★

L120 ANNEAUX Z/NZ. APPLICATIONS ★★★★

L121 NOMBRES PREMIERS. APPLICATIONS ★★★★

L152 DÉTERMINANT. EXEMPLES ET APPLICATIONS ★★★★★

■ **RÉFÉRENCES**

Objectif Agrégation

Rombaldi l'application est en exercice page 440 !

Risler Boyer (mauvaise idée)

6.0.1 Prérequis

Théorème 65 (Perrin page 101)**.** *$D(GL_n(k)) = SL_n(k)$ sauf si $n = 2$ et $k = \mathbb{F}_2$.*

Faire la démonstration

6.0.2 Développement

Théorème 66. *Soit p un nombre premier impair, et $u \in GL_n(\mathbb{F}_p)$.*

$$\varepsilon(u) = \left(\frac{\det u}{p}\right) \tag{6.1}$$

Lemme 67. *Soit k un corps, M un groupe abélien, avec $k \neq \mathbb{F}_2$ ou $n > 2$. Pour tout morphisme ϕ : $GL_n(k) \to M$ il existe un unique morphisme $\delta : k^* \to M$ tel que $\phi = \delta \circ \det$.*

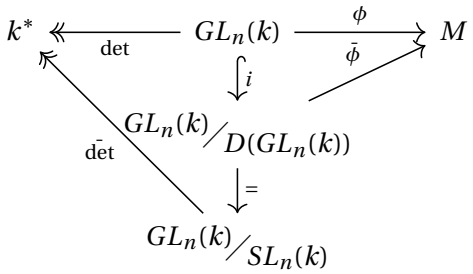
Démonstration. On utilise dans un premier temps la propriété universelle du groupe dérivé

$$\begin{array}{ccc} GL_n(k) & \xrightarrow{\phi} & M \\ \downarrow{\scriptstyle i} & \nearrow_{\bar{\phi}} & \\ GL_n(k)/D(GL_n(k)) & & \end{array}$$

Puis on utilise le fait que $D(GL_n(k)) = SL_n(k)$ dans notre cas.

$$\begin{array}{ccc} GL_n(k) & \xrightarrow{\phi} & M \\ \downarrow{\scriptstyle i} & \nearrow_{\bar{\phi}} & \\ GL_n(k)/D(GL_n(k)) & & \\ \downarrow{\scriptstyle =} & & \\ GL_n(k)/SL_n(k) & & \end{array}$$

Enfin, on peut compléter le diagramme en faisant passer le déterminant au quotient par $SL_n(k)$.



On a remarqué que $\bar{\det}$ est une bijection, et donc on pose très naturellement $\delta = \bar{\phi} \circ \bar{\det}^{-1}$.
Cela prouve l'existence de δ, son unicité venant du fait que det est surjectif sur k^*. □

Lemme 68. *Le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^*$ vers $(\{-1,+1\},\times)$.*

Démonstration.
1. Le symbole de Legendre est bien un morphisme de groupes car $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ dans $\mathbb{F}_p^*$.
2. Le symbole de Legendre n'est pas trivial puisqu'il existe des non-carrés dans $\mathbb{F}_p^*$. En effet, l'ensemble des carrés est l'image de $x \mapsto x^2$ qui est un morphisme de noyau $\{-1,+1\}$ et donc il n'y a que $(p-1)/2 < p$ carrés dans $\mathbb{F}_p^*$. [1]
3. Soit $\alpha : \mathbb{F}_p^* \to \{-1,+1\}$ un morphisme non trivial. Comme $\mathbb{F}_p^*$ est cyclique, il est engendré par un ω. Par non-trivialité, $\alpha(\omega) = -1$, puis, $\alpha(x) = 1$ pour tout x carré dans $\mathbb{F}_p^*$. Si au contraire x n'est pas un carré, alors $x = \omega^k$ avec k impair, et on peut encore conclure.

□

On peut désormais attaquer la preuve du théorème

Démonstration. On considère $M = \{-1,+1\}$ et $\phi = \varepsilon$. Il est clair qu'il suffit de montrer que δ est non trivial pour déduire $\delta(\cdot) = \left(\frac{\cdot}{p}\right)$.

Pour cela on remarque qu'en tant qu'espaces vectoriels, $\mathbb{F}_p^n$ et $\mathbb{F}_{p^n}$ sont isomorphes. Il suffit de trouver une bijection $\mathbb{F}_p$-linéaire sur $\mathbb{F}_{p^n}$ de signature -1.

On considère ω un générateur de $\mathbb{F}_{p^n}^*$, la permutation $x \mapsto \omega x$ agit comme le p^n-1 cycle $(\omega, \omega^2, \ldots, \omega^{p^n-1})$ (qui fixe 0). Sa signature est donc -1 car p^n-1 est pair, et que la signature d'un cycle de longueur r est $(-1)^{r-1}$.

□

6.0.3 Application Première

Soit p un nombre premier impair, on a

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \tag{6.2}$$

De même on peut retrouver

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{6.3}$$

Démonstration. On utilise l'isomorphisme de $\mathbb{F}_p$ suivant : $x \mapsto 2x$. Son déterminant est trivialement 2. Il ne reste plus qu'à calculer sa signature. Pour cela on compte le nombre d'inversions.

x	0	1	…	$\frac{p-1}{2}$	$\frac{p+1}{2}$	…	$p-2$	$p-1$
$u(x)$	0	2	…	$p-1$	1	$\ldots p-2$		

(6.4)

1. En effet p est impair donc plus grand que 2 et ça marche...!!!

On remarque que les seules inversions sont entre les deux blocs "pairs" et "impairs". Soit $k \leq (p-1)/2$, cet élément se voit inversé par rapport à k éléments dans le bloc impair (les k impairs au inférieurs à $2k$).

On a donc $\left(\frac{2}{p}\right) = (-1)^{\delta}$ avec

$$\delta = \sum_{k=0}^{(p-1)/2} k = \frac{p^2-1}{8} \tag{6.5}$$

On peut procéder de même pour $\left(\frac{-1}{p}\right)$ via l'application $x \mapsto -x$, même si dans ce cas il existe un résultat plus élémentaire.

□

Exemple 69. *On veut savoir si le polynôme X^2+2X+5 possède une racine dans $\mathbb{F}_7$.*

Pour cela on regarde $\Delta = -16$ et on veut savoir si Δ est un carré.

$$\left(\frac{-16}{7}\right) = \left(\frac{-2}{7}\right) \tag{6.6}$$

$$= \left(\frac{5}{7}\right) \tag{6.7}$$

$$= 1 \times \left(\frac{7}{5}\right) \tag{6.8}$$

$$= 1 \times \left(\frac{2}{5}\right) \tag{6.9}$$

$$= -1 \qquad \text{Car } 5^2 - 1 = 24 = 3 * 8 \tag{6.10}$$

$$\tag{6.11}$$

Donc le polynôme est irréductible sur $\mathbb{F}_7$.

6.0.4 Application Seconde

On regarde le morphisme de Frobénius F sur $\mathbb{F}_q$ avec $q = p^n$.

On sait que le morphisme de Frobénius est d'ordre exactement n, car $\mathbb{F}_q$ est exactement l'ensemble des racines de $X^{p^n} - X$, c'est à dire de $F^n - id$.

Ainsi, on c'est un endomorphisme cyclique sur $\mathbb{F}_q$ en tant que $\mathbb{F}_p$ espace vectoriel, et il existe un x tel que $(x, F(x), \dots, F^{n-1}(x))$ soit une base de $\mathbb{F}_q$.

La matrice de l'endomorphisme dans cette base est celle correspondant à l'action d'une permutation circulaire d'ordre n, et donc son déterminant est $(-1)^{n+1}$.

Lier ça avec l'action du groupe symétrique sur un espace vectoriel, où déterminant et signature coïncident

On a donc dans $\mathbb{F}_p$:

$$\varepsilon(F) = \left(\frac{(-1)^{n+1}}{p}\right) = (-1)^{\frac{(p-1)(n+1)}{2}} \tag{6.12}$$

6.1 ■ SOUS GROUPES COMPACTS DE GLN(R)

Référence : Szpirglas Algèbre L3. Recasé 5 fois

■ **LEÇONS**

L106 GROUPE LINÉAIRE D'UN ESPACE VECTORIEL DE DIMENSION FINIE, SOUS GROUPES. APPLICATIONS ⋆⋆⋆⋆⋆

L150 EXEMPLES D'ACTIONS DE GROUPES SUR LES ESPACES DE MATRICES ⋆⋆⋆⋆⋆

L181 BARYCENTRES DANS UN ESPACE AFFINE RÉEL DE DIMENSION FINIE, CONVEXITÉ ,APPLICATIONS ⋆⋆⋆⋆⋆

L203 UTILISATION DE LA NOTION DE COMPACITÉ. ⋆⋆⋆⋆⋆

L208 ESPACES VECTORIELS NORMÉS, APPLICATIONS LINÉAIRES CONTINUES. EXEMPLES.⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Spizgrals L3

Rombaldi page 155

On étudie les sous groupes compacts de $GL_n(\mathbb{R})$, en particulier on veut démontrer le théorème suivant.

Théorème 70. *Tout sous groupe compact de $GL_n(\mathbb{R})$ est conjugué à un sous groupe de $O_n(\mathbb{R})$.*

6.1.1 Préliminaires

On rappelle que si q et q' sont deux formes quadratiques équivalentes, alors $O(q)$ est conjugué à $O(q')$, c'est le petit calcul trivial qui dit que

$$q'(x,y) = q(u(x),u(x)) \implies uO(q')u^{-1} = O(q) \tag{6.13}$$

Lemme 71 (Carathéodory)**.** *Soit E un $\mathbb{R}$ espace vectoriel de dimension n, A une partie de E.*

$$Conv(A) = \left\{ \sum_{i=1}^{n+1} \alpha_i x_i \mid x_i \in A \right\} \tag{6.14}$$

Démonstration. Soit $x = \sum_{i=1}^{p} \alpha_i x_i$ un élément de Conv(A) avec p minimal.

Supposons par l'absurde que $p \geq n+2$. En fixant x_1, on sait que la famille $(x_i - x_1)_{i>1}$ est liée dans E car de taille plus grande que $n+1$ [2].

Il existe donc des λ_i tels que

$$\sum_{i=2}^{p} \lambda_i (x_i - x_1) = 0 \tag{6.15}$$

C'est à dire,

$$\sum_{i=2}^{p} \lambda_i x_i = \left(\sum_{i=2}^{p} \lambda_i \right) x_i \tag{6.16}$$

On pose $\lambda_1 = -\sum_{i=2}^{p} \lambda_i$ pour que $\sum \lambda_i = 0$.

On remarque alors que

$$\sum_{i=1}^{p} (\alpha_i + \lambda_i) x_i = x \tag{6.17}$$

2. L'idée est de se servir du fait que $(x_1,\dots,x_p)$ n'est pas un repère affine, et pour cela, il faut se ramener au cas linéaire en fixant un des points

Malheureusement, ce n'est pas nécessairement une combinaison convexe. D'un côté, on sait que $\sum(\alpha_i + \lambda_i) = 1$ ce qui est bien, mais de l'autre $\alpha_i + \lambda_i$ peut être négatif ...

On va donc pondérer par un paramètre t les λ_i afin de s'assurer que tous les termes de cette combinaison soient positifs.

$$\forall t \in \mathbb{R}, \sum_{i=1}^{p} (\alpha_i + t\lambda_i) x_i = x \tag{6.18}$$

En posant $t = \inf\{\tau \mid \forall i, \alpha_i + \tau\lambda_i \geq 0\}$ on peut presque conclure.

(i) L'ensemble sur lequel on considère l'inf n'est pas vide car il contient 0

(ii) L'ensemble sur lequel on considère l'inf est minoré par le minimum des $-\alpha_i/\lambda_i$ pour λ_i non nul.

En réalité, cet inf est atteint pour un des $-\alpha_j/\lambda_j$ [3].

En posant $t = -\alpha_j/\lambda_j$ on a donc non seulement une combinaison convexe, mais on annule un terme dans la somme.

$$\sum_{i=1 \wedge i \neq j}^{p} (\alpha_i + t\lambda_i) x_i = \sum_{i=1}^{p} (\alpha_i + t\lambda_i) x_i = x \tag{6.19}$$

Ce qui contredit la minimalité de p. □

Remarque. *En conséquence* l'enveloppe convexe d'un compact en dimension finie est compacte, *en effet on remarque que l'application continue suivante est aussi* surjective

$$\begin{array}{rccc} \Phi : & A^{n+1} \times \{(\alpha_i) \mid \alpha_i \geq 0, \sum \alpha_i = 1\} & \longrightarrow & Conv(A) \\ & ((x_i), (\alpha_i)) & \mapsto & \sum \alpha_i x_i \end{array} \tag{6.20}$$

Donc comme image d'un compact par une application continue, Conv(A) *est compacte.*

6.1.2 Cas des groupes finis

Remarque. *C'est vrai pour tout groupe fini de manière évidente en considérant le produit scalaire renormalisé comme dans la preuve de Machke*

$$\phi(x, y) = \frac{1}{|G|} \sum_{g \in G} \langle gx \mid gy \rangle \tag{6.21}$$

C'est bien un produit scalaire, et celui-ci rend tous les éléments de G orthogonaux.

On a donc $G \subseteq O(\phi)$*, mais comme* ϕ *est un produit scalaire,* ϕ *est congrue à* $\langle\cdot|\cdot\rangle$*. Ainsi,* $u^{-1}Gu \subseteq u^{-1}O(\phi)u = O(E)$.

La méthode générale est donc de trouver une forme quadratique définie positive ϕ invariante par G. Après cela, en utilisant le changement de base u adapté à ϕ on passe de $G \subseteq O(\phi)$ à $u^{-1}Gu \subseteq O(\mathbb{R})$ pour le produit scalaire canonique.

On peut comprendre la méthode comme suit : G agit sur l'espace des formes quadratiques sur E via [4] $q(\cdot,\cdot) \mapsto q(g\cdot, g\cdot)$. Pour construire une forme invariante par l'action à droite de G on considère la moyenne de l'orbite du produit scalaire canonique par G. C'est clairement quelque chose qui est invariant, c'est un produit scalaire, et donc on peut se ramener au petit calcul de changement de base.

3. C'est assez clair si on regarde l'ensemble comme une intersection d'intervalles de $\mathbb{R}$

4. C'est une action à *droite*!!!

6.1.3 Kakutani

Lemme 72. *Soit H un sous groupe compact de $GL(E)$, K un compact convexe non vide de E stable par H. Alors H a un point fixe dans K*

Démonstration. On fixe une norme euclidienne $\|\cdot\|_2$ sur E et on pose

$$\|x\| = \max_{h\in H} \|h(x)\|_2 \tag{6.22}$$

Cette définition est légitime car H est compact et que les opérateurs sont continus.

(i) Cela définit une norme sur E (vérifications laissées au lecteur)

(ii) Cette norme est invariante par H car $\|h(x)\| = \max_{h'\in H} \|hh'(x)\|_2 = \|x\|$ car H est un groupe

(iii) Cette norme est strictement convexe, en effet si $x \neq y$ en utilisant la stricte convexité de $\|\cdot\|_2$ on peut conclure :

$$\left\|\frac{x+y}{2}\right\| = \left\|h_0\left(\frac{x+y}{2}\right)\right\|_2 = \left\|\frac{h_0(x)+h_0(y)}{2}\right\|_2 < \frac{\|h_0(x)\|_2 + \|h_0(y)\|_2}{2} \leq \frac{\|x\|+\|y\|}{2} \tag{6.23}$$

Choisissons alors $s \in K$ avec $\|s\|$ minimale, c'est possible car K est compact non vide. Comme K est convexe, et par stricte convexité de $\|\cdot\|$ cet élément est unique.

Puisque K est stable par H $h(s) \in K$. De plus $\|\cdot\|$ est invariant par H, on déduit que $\|h(s)\| = \|s\|$, c'est-à-dire via l'unicité évoquée plus haut, que s est un point fixe de H dans K. □

6.1.4 Utilisation

Tout refaire sans matrices ... c'est inutile

L'idée dans le cas non fini est de trouver un point fixe pour l'action de G via le théorème de Kakutani. Pour cela on va utiliser fortement la représentation matricielle est l'espace S_n des matrices symétriques.

On fait donc agir[5] G représenté matriciellement sur S_n via

$$\rho : g \cdot s \mapsto {}^t gsg \tag{6.24}$$

Le sous ensemble des matrices symétriques définies positives est convexe et stable sous l'action de G. Toutefois il n'est pas compact ce qui ne permet pas d'appliquer directement le lemme.

Le compact naturel à considérer au vu des explications précédentes est l'orbite de I_n par l'action de G. C'est bien un compact contenu dans l'ensemble des matrices symétriques définies positives. On considère donc $K = \mathrm{Conv}(G \cdot I_n)$, par le théorème de Carathéodory c'est un convexe compact, contenu dans SDP car SDP est convexe.

Préciser l'action affine préserve l'enveloppe convexe ...

L'ensemble K reste stable sous l'action de G car $g \cdot K = g \cdot (\mathrm{Conv}(G \cdot I_n)) = \mathrm{Conv}(g \cdot G \cdot I_n) = K$. En effet l'action de G est affine.

On a donc bien $H = \rho(G)$ un sous groupe compact de $GL(E)$, K compact convexe non vide, stable par H. En utilisant le point fixe de Kakutani on possède donc bien un élément $s \in K$ fixé par H.

En sélectionnant une base orthogonale pour s, et en notant P la matrice de changement de base associée, on constate via la formule du changement de base pour les formes quadratiques

$${}^t PsP = Id_n \tag{6.25}$$

Cela se traduit par $P^{-1}gP \in O(\mathbb{R})$, via

$${}^t(P^{-1}gP)(P^{-1}gP) = {}^t P {}^t g {}^t P^{-1} P^{-1} gP = {}^t PsP = I_n \tag{6.26}$$

5. C'est encore une action à *droite* ... il faut changer ?

6.1.5 Remarques post développement

En réalité, on peut continuer sur la lancée "je prends le barycentre sur l'orbite de l'identité" pour conclure, en "reprouvant localement" le théorème de point fixe.

La solution est la suivante dans les grandes lignes

1. On peut recouvrir G par un nombre fini de boules ouvertes de rayon R, telles que pour deux éléments g, g' dans une boule, la distance des formes quadratiques q_g, $g_{g'}$ soit inférieure à ε.

   Avec bien entendu $q_g(x) = \langle gx \mid gx \rangle$ C'est possible par compacité et parce qu'on est en dimension finie du coup il n'y a aucun problème avec les normes en général.

2. Étant donné un tel recouvrement $U_1, \dots, U_n$ on sélectionne dans chaque U_i un élément g_i. On pose alors
$$\phi_\varepsilon(x,y) = \frac{1}{n}\sum_{i=1}^{n} \langle g_i x \mid g_i y \rangle \tag{6.27}$$
   Bien entendu le n dépend du ε.

3. On constate immédiatement que les éléments de G, bien que n'étant pas des isométries pour ϕ_ε, sont des *quasi*-isométries, puisque
$$|\phi_\varepsilon(gx, gx) - \phi_\varepsilon(x,x)| \leq \varepsilon \tag{6.28}$$
   Il suffit de remarquer que si $g_i \in U_i$, alors $g_i g \in U_i g$, or la multiplication par g est une bijection de G dans G, donc $U_i g = U_j$ pour un certain j, et réciproquement. Chaque différence étant alors majorée par ε, on conclut.

4. On remarque que ϕ_ε est toujours dans un compact. En effet c'est le barycentre d'éléments dans l'orbite du produit scalaire usuel pour l'action de G. Or, G est compact, et son action est continue, donc ϕ_ε évolue dans un *compact* contenu dans l'ensemble des formes quadratiques définies positives.

5. En considérant une suite extraite, on fait converger ϕ_ε vers ϕ, ce qui permet en passant à la limite de conclure que tout élément de G est une isométrie pour ϕ, qui est un produit scalaire, et hop on a conclu.

C'est encore plus fait à la main, mais cela illustre parfaitement l'idée générale de la moyenne, et l'utilisation de l'enveloppe convexe devient particulièrement claire.

6.1.6 Applications et conséquences

Compléter et détailler cette liste

1. Sous groupes compacts maximaux ?
2. Enveloppe convexe de la boule unité ?
3. autres ?

Exercice FGN Algèbre 3 page 231 Une norme N telle que le groupe d'isométries G_N associé à N agit transitivement sur S_N la sphère unité pour cette norme est euclidienne.

En effet, G_N est un sous groupe compact car fermé borné, donc $G_N \subseteq O(q)$ pour une certaine forme quadratique définie positive q.

Mais alors, si G agit transitivement sur S_N, on a
$$\forall x \in S_N, \exists g \in G_N, \exists y \in S_N, q(x) = q(g(y)) = q(y) \tag{6.29}$$
Ainsi q est constante sur S_N, mais par "quadraticité"

$$q\left(\frac{x}{N(x)}\right) = \frac{1}{N(x)^2} q(x) \tag{6.30}$$

Donc pour tout x on a $q(x) = N(x)^2\alpha$, avec α la constante de q sur S_N. Ainsi, $N(x)$ est proportionnelle à $\sqrt{q}$ qui est une norme euclidienne.

6.2 ■ THÉORÈME DE BRAUER EN CAR QCQ

Référence : Bonne question ... FGN pour smyth. Recasé 3 fois

■ **LEÇONS**

L104 GROUPES FINIS. EXEMPLES ET APPLICATIONS ★★★★★

L105 GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI. APPLICATIONS ★★★★★

L108 EXEMPLE DE PARTIES GÉNÉRATRICES D'UN GROUPE. APPLICATIONS ★★★★★

■ **RÉFÉRENCES**

Rombaldi Pour les choses sur S_n

FGN Algèbre 2 Pour le déterminant de smith

On a un morphisme $P : S_n \to GL_n(k)$ qui correspond à l'action du groupe symétrique sur les vecteurs de k^n. On sait que si σ est conjugée à τ alors P_σ est conjugée à P_τ. On se demande s'il y a une réciproque.

On suppose $P_\sigma = QP_\tau Q^{-1}$.

On note δ_σ^k le nombre de cycles de taille k dans la décomposition en cycles à support disjoints de σ, *en comptant les cycles de taille* 1.

Il suffit de montrer que $\delta_\sigma^k = \delta_\tau^k$ pour conclure, car on connaît les classes de conjugaison dans S_n grâce au type de la signature.

6.2.1 Fixateur

On étudie le fixateur de P_σ et P_τ, c'est à dire $\mathrm{Fix}\, P = \mathrm{Ker}(P - id_E)$. Comme les deux endomorphismes sont congugués on trouve :

$$\dim \mathrm{Fix}\, P_\sigma = \dim \mathrm{Fix}\, P_\tau \tag{6.31}$$

Supposons alors que σ se décompose en cycles à support disjoints $c_1 \dots c_l$. Une base de $\mathrm{Fix}\, P_\sigma$ est alors $(\varepsilon_1, \dots, \varepsilon_l)$ où ε_i est le vecteur indicateur du support de c_i.

(i) Cette famille est libre car les c_i sont à support disjoints

(ii) Elle est bien fixée par l'action de σ

(iii) Elle est génératrice, car si $P_\sigma x = x$, pour tout c_i, et j dans le support de c_i on obtient $x_j = x_{c_i(j)}$. Donc le vecteur est constant sur chaque support par transitivité.

On obtient donc, si l est le nombre de cycles dans la décomposition en cycles à support disjoints de σ :

$$\dim \mathrm{Fix}\, P_\sigma = l \tag{6.32}$$

On remarque que l'égalité des dimensions s'étend aux itérées de σ et τ :

$$\dim \mathrm{Fix}\, P_{\sigma^k} = \dim \mathrm{Fix}(P_\sigma)^k = \dim \mathrm{Fix}(P_\tau)^k = \dim \mathrm{Fix}\, P_{\tau^k} \tag{6.33}$$

6.2.2 Décompte des cycles

Lemme 73. *Si c est un cycle de longueur r alors c^m possède exactement $r \wedge m$ cycles de longueur $r/(r \wedge m)$.*

Démonstration.

$$(c^m)^k(x) = x \iff c^{mk}(x) = x \tag{6.34}$$
$$\iff r | mk \tag{6.35}$$
$$\iff r/(r \wedge m) | km/(r \wedge m) \tag{6.36}$$
$$\iff r/(r \wedge m) | k \tag{6.37}$$

Par définition de l'ordre d'un élément, on obtient que l'ordre de x est $r/(r \wedge m)$, ceci étant vrai pour chaque x, on déduit qu'il y a exactement $r \wedge m$ cycles de taille $r/(r \wedge m)$ dans la décomposition de c^m en cycles à support disjoints. □

Ainsi, on peut compter le nombre de cycles dans la décomposition en cycles à support disjoints de σ^m : chaque cycle de taille i se découpe en exactement $(i \wedge m)$ cycles [6].

$$\dim \mathrm{Fix}\, P_{\sigma^m} = \sum_{i=1}^{n} (i \wedge m)\delta_\sigma^i \tag{6.38}$$

On a donc le système d'équations suivant :

$$\forall m \in \mathbb{N}^*, \sum_{i=1}^{n} (i \wedge m)\delta_\sigma^i = \sum_{i=1}^{n} (i \wedge m)\delta_\tau^i \tag{6.39}$$

6.2.3 Résolution du déterminant

On déduit alors que si l'on pose $A_{i,j} = (i \wedge j)$ et $X_i = \delta_\sigma^i - \delta_\tau^i$ on veut résoudre $AX = 0$. Si l'unique solution est $X = 0$ alors on déduit σ conjuguée à τ.

Or la matrice A correspond à un déterminant de Smith.

Lemme 74 (Déterminant de Smith)**.** $\det A = \prod_{i=1}^{k} \phi(i) > 0$

Démonstration. On remarque que $A_{i,j} = (i \wedge j) = \sum_{d|(i \wedge j)} \phi(d)$

Mais d divise le pgcd si et seulement s'il divise les deux, donc $A_{i,j} = \sum_{d=1}^{n} \phi(d)\chi_{d|i}\chi_{d|j}$.

En posant $B_{i,j} = \chi_{i|j}$ on obtient $A = {}^tBD(\phi(1)\dots\phi(n))B$.

Or la matrice B est triangulaire supérieure et de diagonale 1 donc on obtient le déterminant désiré. □

En conclusion les deux permutations ont même type et sont donc bien conjuguées.

6. Les supports étant disjoints on peut raisonner indépendamment sur chaque cycle

6.3 ■ SO3(R) ET LES QUATERNIONS

Référence : H2G2, Perrin. Recasé 3 fois

■ **LEÇONS**

L108 EXEMPLE DE PARTIES GÉNÉRATRICES D'UN GROUPE. APPLICATIONS ★★★

L182 APPLICATIONS DES NOMBRES COMPLEXES À LA GÉOMÉTRIE ★★★★★

L183 UTILISATION DES GROUPES EN GÉOMÉTRIE ★★★★★

■ **RÉFÉRENCES**

Perrin Partie quaternions

6.3.1 Prérequis

Lemme 75 (Isométries)**.** *On fait un bref rappel des éléments dans* $O(\mathbb{R})$.

Symétrie *c'est semblable à* $I_p, -I_{n-p}$

Réflexion orthogonale *c'est diagonalisable, de spectre* $\{\pm 1\}$ *avec un seul* -1.

Un retournement *c'est pareil qu'un renversement ou une rotation d'angle* π*, c'est de spectre* $\{\pm 1\}$ *avec exactement* deux -1.

SO3 *tous les gens dans* SO_3 *sont des rotations !*

Lemme 76. *On montre que* $O_n(\mathbb{R})$ *est engendré par les produits de n réflexions*

Démonstration. Soit u un endomorphisme orthogonal, et considérons $\operatorname{Fix} u$ l'espace vectoriel des points fixes de u. On pose $p_u = n - \dim \operatorname{Fix} u$, et on montre par récurrence que u est un produit d'au plus p_u réflexions orthogonales.

Si $p_u = 0$ alors $u = id$, c'est terminé.

Sinon. $E = \operatorname{Fix} u \oplus (\operatorname{Fix} u)^\perp$, et on a un $x \neq 0$ dans $(\operatorname{Fix} u)^\perp$.

On pose $y = u(x)$, et comme $x \notin \operatorname{Fix} u$, $x \neq u(x) = y$. Toutefois, comme $\operatorname{Fix} u$ est u-stable et u orthogonal, $(\operatorname{Fix} u)^\perp$ est u-stable et $y \in (\operatorname{Fix} u)^\perp$.

On considère la réflexion orthogonale définie par le vecteur $x - y$. Elle vérifie trivialement les propriétés suivantes

— Elle fixe $\operatorname{Fix} u$, car $x - y \in (\operatorname{Fix} u)^\perp$

— Elle fixe $x + y$ car $x + y$ est orthogonal à $x - y$

— Elle envoie y sur x, car $\tau(x - y) = y - x$ et $\tau(x + y) = x + y$.

Ainsi τu est un élément de $O_n(\mathbb{R})$ avec $\dim \operatorname{Fix}(\tau u) > \dim \operatorname{Fix} u$ puisque $\operatorname{Fix} u \subseteq \operatorname{Fix}(\tau u)$ et $\tau(u(x)) = x$.

On peut donc se ramener à l'hypothèse de récurrence sur $\tau u = \tau_1 \dots \tau_r$, puis $u = \tau\tau_1 \dots \tau_r$.

□

Lemme 77. *On déduit que* $SO_n(\mathbb{R})$ *est engendré par les produits de n* retournements

Démonstration. On découpe la preuve en deux, car le cas $n = 3$ est particulièrement facile.

Le cas $n = 3$ Si τ est une réflexion, alors $-\tau$ est un retournement, car on est en dimension 3.

Or, un élément dans $SO_n(\mathbb{R})$ ne peut être qu'un produit *pair* de réflexions à cause de son déterminant positif.

Donc en remplaçant τ par $-\tau$ dans l'expression de u on obtient bien u comme un produit de n retournements

Le cas $n > 3$ Cette fois il faut prouver un lemme un peu plus fort, qui montre qu'un produit de deux réflexions peut s'écrire comme un produit de deux retournements.

Soit $u = \tau_1\tau_2$, d'hyperplans respectifs H_1, H_2. On considère V un sous espace vectoriel de $H_1 \cap H_2$ de dimension $n-3$ possible car $n \geq 3$.

On a $u_{|V} = id_V$ par composition, et donc u laisse stable $V^\perp$. Or $V^\perp$ est de dimension précisément 3, et on peut écrire $u_{|V^\perp}$ comme un produit de deux retournements. En prolongeant ces retournements par l'identité sur V, on peut conclure.

□

Remarque. *$SO_3(\mathbb{R})$ est un connexe (par arcs) compact.*

Lemme 78. *Si $h \in H$ est quaternion pur alors $h^2 = -1$.*

Lemme 79. *Les quaternions de norme 1 forment un ensemble connexe.*

Lemme 80. *Parler des endomorphismes orthogonaux, des isomorphismes de H avec les matrices parce que sinon le développement ne tient pas debout*

6.3.2 Développement

On note G le groupe des quaternions de norme 1.

Théorème 81. *Il existe un isomorphisme "calculable"* $G/_{\{\pm 1\}} \simeq SO_3(\mathbb{R})$

Le point clef de la preuve est de remarquer que G agit sur H par automorphisme intérieur.

$$\begin{array}{rccl} S: & G & \to & \mathrm{Aut}(H) \\ & h & \mapsto & S_h: \quad \begin{array}{ll} H & \to H \\ q & \mapsto hqh^{-1} \end{array} \end{array} \tag{6.40}$$

Démonstration. C'est bien une action de G sur H par automorphisme intérieur.

S_h est un automorphisme son inverse étant $S_{h^{-1}}$

C'est bien une action En effet $hh' \cdot q = hh'qh'^{-1}h^{-1} = h \cdot (h' \cdot q)$. De plus $1 \cdot q = q$.

□

Remarque. *On remarque que $hqh^{-1} = hq\bar{h}$ car h est de norme 1.*

Démonstration. On va transformer cette action en une action de G sur $\mathbb{R}^3$ via le groupe spécial orthogonal.

(i) L'action par automorphisme intérieur correspond a un morphisme $G \to GL_4(\mathbb{R})$.

(ii) Pour $h \in G$ l'application S_h respecte la norme.

$$N(S_h(q)) = N(hq\bar{h}) = N(h)N(q)N(\bar{h}) = N(q) \tag{6.41}$$

Ainsi $S_h \in O_4(N)$.

(iii) L'application S a pour noyau $Z(H) \cap G = \mathbb{R} \cap G = \{\pm 1\}$.

(iv) Pour la norme N, l'espace des quaternions purs P est l'orthogonal de $\mathbb{R}$. Comme S_h fixe $\mathbb{R}$ et est un endomorphisme orthogonal, on déduit que P est stable par S_h, pour tout $h \in G$.

On pose $s_h = (S_h)_{|P}$, qui correspond donc à un élément de $O(N_{|P}) \simeq O(3,\mathbb{R})$.

(v) On désire montrer que ce morphisme est en réalité vers $SO_3(\mathbb{R})$. Pour cela on munit $O(3,\mathbb{R})$ de la topologie induite par $\mathcal{M}_3(\mathbb{R})$ et on constate alors que l'application S est continue : il suffit de remarquer que $S_h(q)$ est un polynôme de degré 2 en les coordonnées de h, et linéaire en les coordonnées de q.

Préciser cette chose

En remarquant que G est isomorphe à S^3 (la sphère unité en dimension 4) est connexe, on constate alors que l'image de G par l'homéomorphisme puis par le déterminant est connexe. Or G étant un groupe cela force $G \subseteq SO_3(\mathbb{R})$.

(vi) Reste à montrer la surjectivité vers $SO_3(\mathbb{R})$. Pour cela on utilise le fait que $SO_3(\mathbb{R})$ est engendré par les *renversements*.

On considère donc un élément $h \in P \cap G$, et on construit le retournement d'axe $\mathbb{R}h$.

En réalité on montre même $S_h = r_h$, car S_h laisse clairement stable l'axe désiré, et que $(S_h)^2 = S_{h^2} = S_{-1} = Id_H$ car h est un quaternion *pur*.

Ainsi on a montré que S_h était un élément de $O(3,\mathbb{R})$ avec un axe fixe, et donc une rotation autour de cet axe. De plus S_h est une involution, donc c'est nécessairement le renversement d'axe h.

En conclusion, on a bien un morphisme surjectif $\phi : G \twoheadrightarrow SO_3(\mathbb{R})$ de noyau $\{\pm 1\}$, ce qui donne l'isomorphisme attendu. □

6.3.3 Post-requis

On peut aussi décrire les isométries négatives En effet, sur l'exemple d'une réflexion de droite q et d'hyperplan $q^\perp$ on sait que la réflexion τ_q est donnée par

$$\tau_q(x) = x - 2\frac{\phi(q,x)}{\phi(q,q)}q \tag{6.42}$$

Or ici le produit scalaire est simplement $\frac{1}{2}\left(q\bar{x} + \bar{q}x\right)$ et la norme de q vaut 1. Ainsi

$$\tau_q(x) = x - (q\bar{x} - \bar{q})x = -q\bar{x}q \tag{6.43}$$

Ainsi, en faisant agir q sur les quaternions purs, on obtient $\tau_q(x) = qxq$. Ce qui veut dire qu'il "suffit de ne pas conjuguer".

Comme on considère la réflexion de droite q, q est de plus un quaternion pur, et on peut se ramener à s_q via $\tau_q(x) = -s_q(x)$.

Application aux automorphismes de H tout automorphisme de H est intérieur, c'est-à-dire de la forme S_q.

Éléments de preuve

- Un automorphisme doit conserver le centre, donc il fixe $\mathbb{R}$, mais alors restreint à $\mathbb{R}$ c'est un automorphisme de $\mathbb{R}$, qui est donc nécessairement l'identité.
- On utilise ensuite la caractérisation $q \in P \iff q^2 \in \mathbb{R}^-$ pour déduire que $u(q)^2 = u(q^2) \in \mathbb{R}^-$. Ainsi P est laissé stable par u.
- Mais pour $q \in P$, $N(q) = -q^2$, ainsi l'équation précédente dit que $N(u(q)) = N(q)$, et donc u préserve la norme. Ainsi $u_{|P} \in O(3,\mathbb{R})$.
- L'image de (i,j,k) par u est donc une base orthonormée, et quitte à poser $k' = -u(k)$ $(u(i),u(j),k')$ est orthonormée directe.
- En vertu du théorème démontré, il existe un quaternion q unitaire tel que $u(i) = s_q(i)$, $u(j) = s_q(j)$ et $k' = s_q(k)$.

  Or $u(k) = u(ij) = u(i)u(j) = s_q(i)s_q(j) = s_q(ij) = s_q(k)$ donc $u(k) = s_q(k)$. On constate alors $u_{|P}$ était déjà une rotation.
- Les deux applications $\mathbb{R}$ linéaires coïncident sur une base, donc $s_q = u$.

6.3.4 Annexe effectivité

Pourquoi "calculable" On peut exprimer effectivement ce morphisme de G vers $SO_3(\mathbb{R})$ au niveau matriciel. Si $h = a + bi + cj + dk$.

$$S_h(1) = h\bar{h} = N(h) = 1 \tag{6.44}$$

$$\begin{aligned} S_h(i) &= hi\bar{h} && (6.45)\\ &= (-b + ai + cji + dki)(a - bi - cj - dk) && (6.46)\\ &= (-b + ai + ck + dj)(a - bi - cj - dk) && (6.47)\\ &= (a^2 + b^2 - c^2 - d^2)i + 2(ad + bc)j + 2(bd - ac)k && (6.48) \end{aligned}$$

Cela permet d'expliciter comment construire la matrice associée. [7]

Pourquoi c'est "utile" Une fois donné un quaternion unitaire q et un vecteur (x, y, z) effectuer la rotation c'est simplement calculer $q(xi + yj + zk)\bar{q}$.

Cette description de $SO_3(R)$ qui est *beaucoup* plus stable numériquement que la manière matricielle. De plus elle est compacte : quatre nombres au lieu de 9. Cela donne de plus un nombre inférieur d'opérations élémentaires à effectuer pour le calcul de compostions de rotations !

Calcul effectif version plus plus Soit (x, y, z) un axe de rotation dans $\mathbb{R}^3$ et $\theta \in [0, 2\pi[$ un angle pour cette rotation.

Le quaternion pur q' suivant est associé à la rotation d'angle π de même axe : $xi + yj + zk$.

Pour obtenir une rotation d'angle θ, on ajoute une partie réelle, et pour conserver une norme 1 on normalise le vecteur précédent.

$$q = \cos\frac{\theta}{2} + \sin\frac{\theta}{2}\underbrace{(xi + yj + zk)}_{q'} \tag{6.49}$$

Montrons que ce q calcule bien la rotation désirée. Déjà, q est de norme 1, et correspond donc bien à une rotation.

$$S_q(p) = qp\bar{q} = \cos^2\frac{\theta}{2}p + \cos\frac{\theta}{2}\sin\frac{\theta}{2}(q'p - pq') - \sin^2\frac{\theta}{2}q'pq' \tag{6.50}$$

Elle possède le bon axe de rotation car $S_q(q') = q'$.

On remarque que $-q' = \bar{q'}$ car q' est un quaternion pur. Ainsi tout quaternion p représentant un vecteur orthogonal à l'axe de rotation vérifie : $-q'pq' = -p$ par définition de q'.

Un rapide calcul utilisant ce fait permet de déduire $pq' = -q'p$.

Ceci permet d'écrire pour un tel p

$$qp\bar{q} = \cos^2\frac{\theta}{2}p + 2\cos\frac{\theta}{2}\sin\frac{\theta}{2}q'p - \sin^2\frac{\theta}{2}p = \cos\theta p + \sin\theta q'p \tag{6.51}$$

Reste à remarquer que $q'p$ est un quaternion pur, et que $(q', p, q'p)$ correspond à une base orthonormée directe de l'espace pour conclure.

7. Le quotient par $\{\pm 1\}$ ne pose pas de souci précisément parce qu'il ne change pas le résultat de ce calcul

6.4 ■ SOUS GROUPES FINIS DE SO3(R)

Référence : H2G2, Rombaldi. Recasé 2 fois

■ **LEÇONS**

L104 GROUPES FINIS. EXEMPLES ET APPLICATIONS ⋆⋆⋆⋆⋆

L183 UTILISATION DES GROUPES EN GÉOMÉTRIE ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Rombaldi

H2G2

ON NE TRAITE QUE LES CAS CYCLIQUE, DIÉDRAL ET $\mathscr{A}_4$.

6.4.1 Préliminaires

Lemme 82 (Formule de Burnside)**.** *En notant r le nombre d'orbites pour l'action d'un groupe G sur un ensemble X on a*

$$|G|r = \sum_{g\in G} \operatorname{Fix} g \tag{6.52}$$

Démonstration. Il suffit de dénombrer $E = \{(g,x) \mid g\cdot x = x\}$ de deux manières différentes... □

Lemme 83. *L'unique sous groupe d'ordre* 12 *de $\mathscr{S}_4$ est $\mathscr{A}_4$.*

Démonstration. Tout sous groupe d'indice deux est distingué, il existe un unique morphisme non trivial de S_4 vers $\{\pm 1\}$ hop hop hop. □

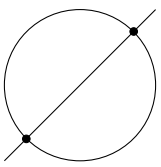
Lemme 84. *Les sous groupes finis de $SO_2(\mathbb{R})$ sont les groupes cycliques.*

Démonstration. C'est tout simplement parce que $SO_2(\mathbb{R})$ est isomorphe à $\mathbb{U}$, et on connaît les sous groupes de $\mathbb{U}$ via l'étude des sous groupes de $\mathbb{R}$.

Remarquons que la preuve de l'isomorphisme repose sur le théorème de réduction des matrices symétriques réelles, et qu'on peut se servir de la même réduction pour montrer que dans les dimensions supérieures, l'action de SO_n sur la sphère est transitive. □

Lemme 85. *Un élément $u \in SO_3(\mathbb{R}) - \{id\}$ possède exactement deux points fixes sur la sphère unité. On les appelles les pôles de u.*

Démonstration. On fait juste le dessin au tableau pour montrer les pôles sur une sphère



□

6.4.2 Développement

On fixe $G \subseteq \mathscr{O}^+(E)$, de cardinal $n \geq 2$ et on note P l'ensemble des pôles des éléments de G différents de l'identité.

Le décompte des points fixes donne alors

$$2 \leq |P| \leq 2(n-1) \tag{6.53}$$

On fait agir G sur P via l'action $g \cdot x = g(x)$. Il suffit de vérifier que $g(x) \in P$. Or si $x \in P$, il existe $g' \neq id$ tel que $\{\pm x\}$ soit l'ensemble des pôles de g'.

Mais $g \circ g' \circ g^{-1}(g(x)) = g(x)$, donc $g(x)$ est un point fixe de $g \circ g' \circ g^{-1}$ qui n'est pas l'identité (sans quoi $g' = id$).

On utilise la formule de Burnside en notant r le nombre d'orbites pour l'action de G sur P

$$r = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix} g| \tag{6.54}$$

Or, on sait que $\operatorname{Fix} id = P$, et que $\operatorname{Fix} g = \{\pm x_g\}$ si $g \neq id$, donc on a l'équation

$$r = \frac{1}{n}\left(|P| + 2(n-1)\right) \tag{6.55}$$

En utilisant les inégalités sur $|P|$ on peut alors déduire :

$$2 \leq r \leq 4\left(1 - \frac{1}{n}\right) \tag{6.56}$$

Il y a donc 2 ou 3 orbites

Si $r = 2$ alors la formule de Burnside donne $2n = |P| + 2(n-1)$ donc $|P| = 2$. Ainsi, toutes les rotations différentes de l'identité ont même axe.

Le groupe G est donc isomorphe[8] à un sous groupe fini de $SO_2(\mathbb{R})$ ce qui correspond à un groupe cyclique d'ordre n.

On peut donc obtenir les groupes cycliques d'ordre n

Si $r = 3$ on a l'équation suivante

$$3n = |P| + 2(n-1) \tag{6.57}$$

Et donc $|P| = n + 2$.

On note $\mathscr{O}_{x_k}$ les trois orbites avec $k \in \{1,2,3\}$, n_k leur cardinal respectif, et $m_k = n/n_k$ le cardinal du stabilisateur de x_k.

Comme chaque élément de P est point fixe de l'identité et d'une rotation alors $2 \leq m_k \leq n$.

En appliquant alors la formule des classes

$$n + 2 = |P| = \sum_{k=1}^{3} |\mathscr{O}_{x_k}| = \sum_{k=1}^{3} \frac{n}{m_k} \tag{6.58}$$

Ce qui se ré-écrit

$$\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} = 1 + \frac{2}{n} \tag{6.59}$$

8. Le plan orthogonal à l'axe commun est stable, ça donne une injection dans le bon truc

On peut ordonner les orbites de manière à ce que $m_1 \leq m_2 \leq m_3$.
Alors il est clair que

$$\frac{3}{m_3} \geq 1 + \frac{2}{n} > 1 \tag{6.60}$$

Ce qui montre que $m_1 < 3$, puis que $m_1 = 2$.

$$\boxed{\text{On sait que } m_1 = 2}$$

De la même manière, en ré-injectant on obtient

$$\frac{1}{m_2} + \frac{1}{m_3} = \frac{1}{2} + \frac{2}{n} \tag{6.61}$$

Puis

$$\frac{2}{m_2} \geq \frac{1}{2} + \frac{2}{n} > \frac{1}{2} \tag{6.62}$$

Donc $2 \leq m_2 < 4$.

$$\boxed{\text{On sait que } m_2 \in \{2,3\}}$$

Si $r = 3$**,** $m_1 = 2$ **et** $m_2 = 2$ **alors** on déduit rapidement que $m_3 = \frac{n}{2}$ et donc n est pair.
De plus le nombre d'éléments dans la troisième orbite est $n_3 = n/m_3 = 2$. Ce qui montre que $\mathcal{O}_{x_3} = \{\pm x_3\}$.
Ainsi, le stabilisateur de x_3 est composé de rotations avec les mêmes points fixes, donc par un argument similaire au cas $r = 2$ on déduit que $\mathrm{Stab}_{x_3} \simeq \mathbb{U}_{\frac{n}{2}}$, et est engendré par une rotation ρ.
Le groupe quotient de G par ce stabilisateur étant d'ordre 2, il existe donc $\sigma \notin \mathrm{Stab}_{x_3}$. On a alors

$$G = \left\{id, \rho, \ldots, \rho^{m_3-1}\right\} \uplus \left\{\sigma, \sigma\rho, \ldots, \sigma\rho^{m_3-1}\right\} \tag{6.63}$$

Reste à montrer que $\sigma^2 = id$ et $(\rho\sigma)^2 = id$ pour conclure que G est un groupe diédral.
Pour cela, on remarque que $\sigma(x_3) \in \mathcal{O}_{x_3} = \{\pm x_3\}$, mais comme σ n'est pas dans le stabilisateur, cela force $\sigma(x_3) = -x_3$. Alors σ^2 fixe $x_3, -x_3$ et les deux pôles de σ. C'est donc nécessairement l'identité.
D'autre part $\rho\sigma(x_3) = -x_3$, et donc on peut lui appliquer la même démonstration.

$$\boxed{G \text{ est le groupe } \mathscr{D}_n}$$

Si $r = 3$**,** $m_1 = 2$ **et** $m_2 = 3$ **alors**

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{m_3} = 1 + \frac{2}{n} \tag{6.64}$$

Cela montre que $\frac{1}{m_3} \geq \frac{1}{6}$ puis que $m_3 \in \{2,3,4,5\}$. Mais on avait supposé $m_3 \geq m_2 = 3$. Ainsi

$$\boxed{\text{On sait que } m_3 \in \{3,4,5\}}$$

On ne traite que le cas $m_3 = 3$. En injectant cela dans la formule précédente, on obtient $n = 12$.
(Au tableau il faut simplement écrire l'équation suivante)

$$\frac{5}{6} + \frac{1}{3} = 1 + \frac{n}{2} \tag{6.65}$$

On calcule donc par la suite $n_1 = \frac{12}{2} = 6$ et $n_2 = n_3 = \frac{12}{3} = 4$.
On va montrer que G est isomorphe à un sous groupe de $\mathscr{S}_4$, pour cela on regarde l'action de G sur $\mathcal{O}_{x_2}$ qui est de cardinal 4. Cela donne un morphisme de G dans $\mathscr{S}_4$, et ce morphisme est *injectif* car une rotation qui fixe $\mathcal{O}_{x_2}$ fixe plus de trois points, et est donc l'identité.
On a donc G d'ordre 12 isomorphe à un sous groupe de $\mathscr{S}_4$, mais c'est alors $\mathscr{A}_4$, l'unique sous groupe d'ordre 12.

On sait que $G \simeq \mathscr{A}_4$

STOP

Si on pose la question pour $r = 3$, $m_1 = 2$, $m_2 = 4$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{m_3} = 1 + \frac{2}{n} \tag{6.66}$$

Cela montre que $n = 24$. On déduit alors $n_1 = 12$, $n_2 = 8$, $n_3 = 6$.

On veut faire agir G sur une partie de cardinal 4. Pour cela on remarque que toutes les orbites ont des cardinaux différents et que $\mathrm{Stab}_x = \mathrm{Stab}_{-x}$. Ainsi, pour $y \in \mathscr{O}_{x_2}$, $\mathscr{O}_y = \mathscr{O}_{x_2}$ mais aussi $|\mathscr{O}_y| = |\mathscr{O}_{-y}|$ ce qui permet de conclure $\mathscr{O}_{-y} = \mathscr{O}_{x_2}$ (via l'unicité des cardinaux des orbites).

Ainsi, l'orbite de x_2, de cardinal 8, est stable par opposé. C'est pour cela qu'on fait agir G sur $E = \mathscr{O}_{x_2}/\{\pm 1\}$ qui est bien de cardinal 4.

Il reste alors à montrer que si g fixe E alors $g = id_G$. On sait déjà que $g(x) = \pm x$ pour $x \in E$. On fait une disjonction de cas sur l'image de x_2

Cas 1 $g \cdot x_2 = x_2$. Alors g stabilise x_2 et est donc dans Stab_{x_2} qui est d'ordre 3. Donc pour $y \in \mathscr{O}_{x_2}$ $y = g^3(y) = g(y)$. Ainsi $g = id$ car g a plus de trois points fixes distincts sur la sphère.

Cas 2 $g \cdot y = -y$ pour $y \in \mathscr{O}_{x_2}$ (c'est bien tout ce qu'il reste à tester !).

Mais alors on sait que g est une inversion sur une base de $\mathbb{R}^3$, ce qui force son déterminant à être négatif, c'est impossible car $g \in \mathscr{O}^+$.

En effet, $\mathrm{Vect}\mathscr{O}_{x_2} = \mathbb{R}^3$ car il est au moins de dimension 2 (vecteurs de même normes, non nuls distincts). S'il était de dimension deux, alors il serait stable par g, mais comme g est une isométrie, son orthogonal (une droite) serait aussi stable par g. La condition $g^3 = id$ force donc g à être l'identité sur cette droite. Mais alors g possède beaucoup de points fixes...

SO3 : preuve incertaine. Alors g^2 possède plus de trois points fixes sur la sphère, et donc $g^2 = id$, mais on sait aussi que $g^3 = id$, donc $g = id$ ce qui est absurde

On sait que $G \simeq \mathscr{S}_4$

Si on pose la question pour $r = 3$, $m_1 = 2$, $m_2 = 3$ **et** $m_3 = 5$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{m_3} = 1 + \frac{2}{n} \tag{6.67}$$

On déduit que $n = 60$. La taille des orbites est alors $n_1 = 30$, $n_2 = 20$, $n_3 = 10$. Comme pour le cas précédent, les cardinaux sont distincts, et donc on montre que $\mathscr{O}_{x_3}$ passe au quotient pour $\{\pm 1\}$. En faisant agir G sur le quotient, noté E, on a un morphisme injectif de G dans $\mathscr{S}_5$. Comme G est d'ordre 60 on déduit alors que $G = \mathscr{A}_5$ (même argument que pour $\mathscr{A}_4$).

Reste donc à montrer que ce morphisme est injectif. Les éléments dans Stab_{x_3} sont d'ordre 5, on peut donc faire exactement la même preuve que dans le cas précédent !

6.4.3 Réalisation des groupes associés

On peut se demander si les groupes évoqués sont les groupes d'isométries d'une figure spécifique.

Comment obtenir les groupes cycliques ?!

??? permet d'obtenir les groupes cycliques

Figures planes permet de construire les groupes diédraux

Tétraèdre permet de construire $\mathscr{A}_4$

Cube et octaèdre permet de construire $\mathscr{S}_4$

Dodécaèdre et icosaèdre permet de construite $\mathscr{A}_5$

Remarque. *Tous les sous groupes ne sont pas distingués, car SO_3 est simple !*

Remarque. *Si on arrive à montrer que deux solides de même groupe d'isométries sont duaux, on (re)découvre qu'il ne peut pas y avoir plus de solides platoniciens.*

6.5 ■ DÉNOMBREMENT POLYNÔMES IRRÉDUCTIBLES

Référence : Francinou agreg / perrin / Rombaldi page 422. Recasé 3 fois

■ **LEÇONS**

L123 CORPS FINIS. APPLICATIONS ★★★★★

L141 POLYNÔMES IRRÉDUCTIBLES À UNE INDÉTERMINÉE. CORPS DE RUPTURE. EXEMPLES ET APPLICATIONS ★★★★★

L190 MÉTHODES COMBINATOIRES ET DÉNOMBREMENT ★★★★

■ **RÉFÉRENCES**

Rombaldi page 422 (fait les trucs un peu à la main ...)

Demazure page 220 (fait mieux les choses ... j'ai l'impression)

Gourdon le fait aussi dans un "problème"

On fixe p premier et on veut étudier $I_n(p)$, le nombre de polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p$. On note $\mathscr{U}_n(p)$ l'ensemble des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p$.

6.5.1 Préliminaires

Pour $\lambda \in \mathbb{F}_p$ le polynôme $X-\lambda$ est irréductible unitaire de degré 1, on conclut alors $I_1(p) = p$.

Pour le polynômes de degré 2, il suffit de dénombrer les polynômes *réductibles* unitaires, qui ont nécessairement une racine dans $\mathbb{F}_p$. Soit celle-ci est double, soit il y en a deux distinctes. On déduit alors

$$I_2(p) = p^2 - \left(p + \frac{p(p-1)}{2}\right) = \frac{p(p-1)}{2} \tag{6.68}$$

6.5.2 Cas général

On va démontrer qu'il existe des polynômes irréductibles unitaires de tout degré supérieur à 1 dans $\mathbb{F}_p$, et préciser leur nombre.

On fixe n un entier naturel non nul et on note $P_n = X^{p^n} - X$.

Lemme 86. *Pour tout $P \in \mathscr{U}_d$, ce polynôme divise P_n si et seulement si son degré d divise n.*

Démonstration. Un polynôme P de degré d divise P_n dans $\mathbb{F}_p$ si et seulement si la classe de P_n dans le corps $\mathbb{F}_{p^d} = {}^{\mathbb{F}_p}\!/_{(P)}$ est 0. Ce qui équivaut à $X^{p^n} = X$ dans $\mathbb{F}_{p^d}$.

Mais on sait que pour les éléments de $\mathbb{F}_p$, $x^{p^n} = x$ (théorème de Fermat). Ainsi, on déduit que pour tout polynôme Q, la classe de Q^{p^n} est égale à la classe de Q dans $\mathbb{F}_{p^d}$. Cela reste une équivalence.

Sens implique En conséquence, pour tout $x \in \mathbb{F}_{p^d}^*$, on a $x^{p^n-1} = 1$. Or le groupe $\mathbb{F}_{p^d}^*$ est cyclique d'ordre p^d-1, et si on note ω un générateur, on trouve $\omega^{p^n-1} = 1$ et donc $p^d-1 | p^n-1$.

Cela force $d|n$.

Sens implique version 2 Supposons P irréductible de degré d qui divise $X^{p^n} - X$, alors en considérant x une racine de P dans une clôture algébrique on a $\mathbb{F}_q(x)$ qui est un corps, avec $[\mathbb{F}_q(x) : \mathbb{F}_q] = d$. Or, P divise $X^{p^n} - X$, donc cette racine x est une racine de $X^{p^n} - X$ ce qui prouve que $\mathbb{F}_q(x)$ est un sous corps de $\mathbb{F}_{q^n}$.

Mais alors

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = kd \tag{6.69}$$

Sens réciproque On sait que $n = qd$, et que $X^{p^d} = X$ dans $\mathbb{F}_{p^d}$, par récurrence immédiate on a $X^{p^{dk}} = X$ dans $\mathbb{F}_{p^d}$ puis $X^{p^n} = X$, ce qui permet de conclure.

□

Lemme 87. *Le polynôme P_n est sans facteur carré, dans $\mathbb{F}_p$, et on a la factorisation suivante :*

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathscr{U}_d(p)} P \tag{6.70}$$

Démonstration. On peut simplement calculer le polynôme dérivé de P_n $P_n'(X) = p^n X^{p^n-1} - 1 = -1$. Cela prouve $P_n' \wedge P_n = 1$ et donc P_n est sans facteur carré.

Le lemme précédent permet directement de conclure pour la formule en utilisant le fait qu'un polynôme irréductible n'apparaît qu'une unique fois dans P_n. □

On peut donc conclure

$$p^n = \sum_{d|n} \sum_{P \in \mathscr{U}_d(p)} \deg P = \sum_{d|n} d \times I_d(p) \tag{6.71}$$

On peut alors constater

$$I_n(p) \leq \frac{p^n}{n} \tag{6.72}$$

Et en ré-injectant dans l'équation en déduire

$$p^n - n I_n(p) \leq \sum_{d|n \text{ et } d<n} p^d \leq \frac{1 - p^{n/2+1}}{1-p} \leq p^{n/2+1} \tag{6.73}$$

Donc on peut conclure

$$\frac{p^n - p^{n/2+1}}{n} \leq I_n(p) \leq p^n/n \tag{6.74}$$

Cela permet non seulement de déduire qu'il existe des polynômes irréductibles de tout degrés, mais aussi l'équivalent suivant

$$I_n(p) \sim \frac{p^n}{n} \tag{6.75}$$

6.5.3 Commentaires

La formule permet de calculer $I_n(p)$ par récurrence, et en réalité on peut même utiliser la formule d'inversion de Möbius pour écrire directement

$$n I_n(p) = \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d \tag{6.76}$$

6.6 ■ INVARIANTS DE FROBENIUS

Référence : Gourdon ou Mneimné. Recasé 4 fois

■ **LEÇONS**

L150 EXEMPLES D'ACTIONS DE GROUPES SUR LES ESPACES DE MATRICES ★★★★

L151 DIMENSION D'UN ESPACE VECTORIEL. RANG. EXEMPLES ET APPLICATIONS ★★★

L153 POLYNÔMES D'ENDOMORPHISME EN DIMENSION FINIE. RÉDUCTION. APPLICATIONS ★★★★★

L159 FORMES LINÉAIRES ET DUALITÉ EN DIMENISON FINIE ★★★★

■ **RÉFÉRENCES**

Mansuy Mneimné page 125

Gourdon Algèbre page 290

On désire caractériser l'action du groupe $\mathrm{GL}(E)$ par conjugaison sur $\mathscr{L}(E)$.

Lemme 88 (Admis)**.** *Il pour tout endomorphisme u il existe un vecteur $x \in E$ tel que $\pi_{u,x} = \pi_u$.*

Démonstration. On procède en plusieurs étapes

(i) Si $\pi_u = P^\alpha$ avec P irréductible. Alors on a la suite strictement croissante

$$\{0\} \subsetneq \ker P(u) \subsetneq \cdots \subsetneq \ker P^\alpha(u) = E \tag{6.77}$$

On peut donc sélectionner $x \in E - \ker P^{\alpha-1}(u)$. Par construction $\pi_{u,x} | P^\alpha$, mais comme $P^{\alpha-1}(u)(x) \neq 0$, on a $\pi_{u,x} = \pi_u$.

(ii) Si $\pi_{u,x} \wedge \pi_{u,y} = 1$, alors $\langle x+y\rangle_u = \langle x\rangle_u \oplus \langle y\rangle_u$ et $\pi_{u,x+y} = \pi_{u,x}\pi_{u,y}$.
On commence par remarquer que $\langle x+y\rangle_u \subseteq \langle x\rangle_u + \langle y\rangle_u$.
De plus, la somme est directe car si z est un vecteur dans l'intersection, son polynôme minimal ponctuel doit diviser les deux polynômes et donc être constant égal à 1, ce qui force $z = 0$.
Enfin, l'astuce

$$0 = \pi_{u,x}\pi_{u,x+y}(u)(x+y) = \pi_{u,x+y}(u)(y) \tag{6.78}$$

Donc $\pi_{u,y} | \pi_{u,x+y}$, on a la même chose pour x, et on déduit donc que $\pi_{u,x+y} = \pi_{u,x}\pi_{u,y}$.
Cela donne donc la bonne dimension pour les espaces qui étaient inclus, et donc sont égaux.

(iii) Pour conclure dans le cas général il suffit de décomposer π_u en facteurs de type P^α, et de recombiner les résultats via le deuxième point.

□

6.6.1 Existence

On considère un vecteur x tel que $\pi_u = \pi_{u,x}$, on note $k = \deg\pi_u = \deg\pi_{u,x}$, et $E_x = \langle x\rangle_u$ l'espace vectoriel engendré par les $u^i(x)$.

On constate que E_x est de dimension k, qu'il est stable par u et que $\pi_{u_{|E_x}} = \pi_{u,x} = \pi_u$.

On recherche alors un supplémentaire stable à E_x. On complète la base $(x, u(x), \ldots, u^{k-1}(x))$ de E_x notée $(e_1, \ldots, e_k)$ en une base $(e_1, \ldots, e_n)$ de E.

On pose alors $G = \Gamma^\circ$ où $\Gamma = \{e_k^* \circ u^i \mid i \in \mathbb{N}\}$. De manière évidente, Γ est stable par ${}^t u$ et donc G est un sev stable par f.

Pourquoi a-t-on posé ceci ? Et bien en fait

$$\Gamma^\circ = \left(\langle e_k^*\rangle_{{}^t u}\right)^\circ \tag{6.79}$$

En effet,

$$\langle e_k^*\rangle_{{}^t u} = \left\{P\left({}^t u\right)\left(e_k^*\right) \mid P \in k[X]\right\} = \left\{e_k^* \circ P(u) \mid P \in k[X]\right\} \tag{6.80}$$

Montrons $F \cap G = \{0\}$ Soit $y \in F \cap G$, alors $e_j^*(y) = 0$ si $j > k$ car $y \in F$. De plus $e_k^*(y) = 0$ et par récurrence $e_j^*(y) = 0$ pour $j \leq k$. On a donc $y = 0$.

Montrons $\dim F + \dim G = n$ On sait que $\dim G = n - \dim \mathrm{Vect}\,\Gamma$. Il suffit de montrer que $\dim \mathrm{Vect}\,\Gamma = k$ pour conclure. Or on a montré que $\dim \mathrm{Vect}\,\Gamma = \dim \langle e_k^* \rangle_{{}^t u}$. C'est donc un espace vectoriel de dimension $\deg \pi_{{}^t u}$, mais le polynôme minimal de ${}^t u$ est le même que celui de u, donc les dimensions sont bonnes.

On a donc $E = F \oplus G$. On note P_1 le polynôme minimal de $u_{|F}$ et P_2 le polynôme minimal de $u_{|G}$. On a $P_2 | \pi_u = P_1$ et en appliquant l'hypothèse de récurrence à $u_{|G}$ on obtient la suite des espaces attendue.

6.6.2 Unicité

Supposons l'existence de deux suites de sous espaces $F_1 \dots F_r$ et $G_1 \dots G_s$ associées aux polynômes (P_i) et (Q_i).

On remarque que $P_1 = Q_1 = \pi_u$, car le polynôme minimal de u est le pgcd des polynômes minimaux des $u_{|F_i}$) qui se divisent tous (et de même pour Q_1).

On montre par récurrence que pour $j \leq \min(r, s)$ on a bien $P_i = Q_i$. L'initialisation a déjà été faite.

Considérons alors un $j \geq 2$.

On remarque

$$P_j(u)(E) = \oplus P_j(u)(F_i) = \oplus P_j(u)(G_i) \tag{6.81}$$

En passant aux dimensions on obtient

$$\sum_{i=1}^{j-1} \dim P_j(u)(F_i) = \sum_{i=1}^{s} \dim P_j(u)(G_i) \tag{6.82}$$

Préciser cette preuve

Mais on sait que [9].

$$\dim P_j(u)(F_i) = \deg \frac{P_i}{P_j \wedge P_i}$$

$$\dim P_j(u)(G_i) = \deg \frac{Q_i}{P_j \wedge Q_i}$$

On peut donc déduire par récurrence que $\dim P_j(u)(F_i) = \dim P_j(u)(G_i)$ pour $i < j$. Cela permet alors de déduire

$$\forall i \geq j, \dim P_j(u)(G_i) = 0 \tag{6.83}$$

En particulier on observe $Q_j | P_j$. Par symétrie dans la preuve, on déduit de même $P_j | Q_j$ et comme les polynômes sont unitaires $Q_j = P_j$.

CQFD.

6.6.3 Utilisations, résultats annexes

Résultat de classification Cela permet de totalement comprendre l'action de $GL(E)$ sur $L(E)$ par conjugaison.

Invariance par extension de corps TODO

Vers la réduction de Jordan

9. Considérer le morphisme de $K[u]$ vers l'espace associé et regarder son noyau

Endomorphismes cycliques Les endo cycliques sont très important, il y a pleins de résultats super cools et il faut les marquer.

6.7 ■ MÉTHODES ITÉRATIVES JACOBI/GAUSS-SEIDEL

Référence : Introduction à l'analyse numérique (CIA), Ciralet, page 96. Recasé 4 fois

■ **LEÇONS**

L157 ENDOMORPHISMES TRIGONALISABLES. ENDOMORPHISMES NILPOTENTS ★★★★★

L162 SYSTÈMES D'ÉQUATION LINÉAIRES ; OPÉRATIONS ÉLÉMENTAIRES, ASPECTS ALGORITHMIQUES ★★★★★

L226 SUITES VECTORIELLES ET RÉELLES DÉFINIES PAR UNE RELATION DE RÉCURRENCE UN+1 = F(UN). EXEMPLES. APPLICATIONS À LA RÉSOLUTION APPROCHÉE D'ÉQUATIONS. ★★★★★

L233 MÉTHODES ITÉRATIVES EN ANALYSE NUMÉRIQUE MATRICIELLE. ★★★★★

■ **RÉFÉRENCES**

Allaire Kaber

Ciralet p 95 / p 102

FGN Alèbre 3 page 169

6.7.1 Méthode itérative

On suppose $A \in GL_n(\mathbb{R})$ et on cherche à résoudre $Ax = b$.
L'idée est de découper $A = M - N$ avec M "facilement inversible".
Ainsi,

$$Ax = b \iff (M-N)x = b \iff x = M^{-1}(b + Nx) \tag{6.84}$$

On a donc transformé une équation "classique" en une recherche de point fixe.
Très naturellement, on s'intéresse alors à la suite

$$\begin{cases} x_0 = b \\ x_{k+1} = M^{-1}(b + Nx_k) \end{cases} \tag{6.85}$$

Si cette suite converge, c'est vers une solution du système. On se demande donc de manière très naturelle sous quelles conditions cette suite converge.

6.7.2 Householder et rayon spectral

Théorème 89 (Householder)**.** *Pour une matrice carrée A les trois quantités suivantes sont égales*

(i) $\rho(A)$

(ii) $\inf\{\|A\| \mid \|\cdot\| \textit{ norme matricielle}\}$

(iii) $\inf\{\|A\| \mid \|\cdot\| \textit{ norme subordonnée}\}$

Démonstration. Montrons dans un premier temps que $\rho(A)$ minore toute norme matricielle. Soit $\|A\|$ une norme matricielle, et v un vecteur propre associée à une valeur propre de module maximal de A. Alors on a

$$\|Av^t v\| \leq \|A\|\|v^t v\| \tag{6.86}$$

Or $Av = \lambda v$, donc $\|Av^t v\| = |\lambda|\|v^t v\|$.

Comme v est un vecteur propre, cette matrice est non nulle [10]. Elle est donc de norme non nulle, et on obtient bien

10. Pour qu'elle soit nulle, il faut que v soit nul

$$\rho(A) = |\lambda| \leq \|A\| \tag{6.87}$$

Reste à montrer que l'on peut obtenir $\rho(A) + \varepsilon$ pour une norme subordonnée.

Pour cela, on considère A comme une matrice à coefficients dans $\mathbb{C}$, elle est alors trigonalisable. On a donc $PAP^{-1} = T$.

On considère ensuite pour un $\delta > 0$ la matrice de changement de base suivante : $e_i \mapsto \delta^i e_i$. Alors on constate que

$$Te'_j = \sum_{i=1}^{j} \delta^{j-i} t_{i,j} e_i \tag{6.88}$$

$$D_\delta T D_\delta^{-1} = \begin{pmatrix} t_{1,1} & & \delta(*) \\ & \ddots & \\ (0) & & t_{n,n} \end{pmatrix} \tag{6.89}$$

En particulier, les coefficients de la matrice T dans la base $(e'_1, \dots, e'_n)$ sont multipliés par au moins δ sauf sur la diagonale.

On pose alors $\|x\| = \|D_\delta P x\|_\infty$. C'est une norme sur $\mathbb{C}^n$, mais aussi sur $\mathbb{R}^n$.

On considère $|||\cdot|||$ la norme subordonnée associée. Alors

$$|||A||| = \sup_{x \neq 0} \frac{\|Bx\|}{\|x\|} \tag{6.90}$$

$$= \sup_{x \neq 0} \frac{\|D_\delta PAx\|_\infty}{\|D_\delta Px\|_\infty} \tag{6.91}$$

$$= \sup_{y \neq 0} \frac{\|D\delta PAP^{-1} D_\delta^{-1} x\|_\infty}{\|y\|} \tag{6.92}$$

$$\leq \max_{1 \leq i \leq n} \sum_{j=1}^{n} |D_\delta T D_\delta^{-1}| \leq |t_{i,i}| + \varepsilon \tag{6.93}$$

Or $|t_{i,i}| \leq \rho(T) = \rho(A)$ car T est triangulaire. □

6.7.3 Application à l'étude de la convergence

L'étude de la suite va être simplifié par l'introduction du vecteur d'erreur $e_k = x_k - u$ avec u solution de l'équation $Ax = b$.

En effet, on obtient alors

$$e_{k+1} = x_{k+1} - u = M^{-1}(Nx_k + b) - u = M^{-1}(Nx_k + b) - M^{-1}(Nu + b) = M^{-1}Ne_k \tag{6.94}$$

On sait que notre méthode converge si et seulement si l'erreur tends vers 0.

Théorème 90. *La méthode converge pour tout b si et seulement si $\rho(M^{-1}N) < 1$.*

Démonstration. Si le rayon spectral est inférieur à 1, on possède une norme induite $|||\cdot|||$ telle que $|||A||| < 1$, alors il est aisé de vérifier que

$$\|e_k\| = \|(M^{-1}N)^k e_0\| \leq |||M^{-1}N|||^k \|e_0\| \longrightarrow 0 \tag{6.95}$$

En revanche, si le rayon spectral est supérieur ou égal à 1, il existe une valeur propre complexe λ de module supérieur ou égal à 1 et on note v un vecteur propre associé.

Alors par construction si $e_0 = v$ (c'est-à-dire $b = v + u$)

$$e_k = \lambda^k v \not\to 0 \tag{6.96}$$

Pour que ce soit tout à fait correct, il faut prendre b dans $\mathbb{R}^n$, par exemple en posant $v = v_1 + iv_2$ et en remarquant que comme A est réelle, $Av = Av_1 + iAv_2$, donc que v_1 est un vecteur propre *réel* associé à λ. □

Remarque. *L'erreur suit une décroissance exponentielle (dite "linéaire en le nombre de chiffres significatifs") de raison $\rho(M^{-1}N)$. Ainsi, plus le rayon spectral de cette matrice est faible, plus la vitesse va converger rapidement.*

6.7.4 Comment choisir sa décomposition ?

On considère par exemple la méthode de Jacobi, qui consiste, si la diagonale est non nulle, à prendre $M = D$ et $N = E + F$. **En faisant le dessin du Ciralet**.

Le schéma numérique est alors le suivant :

$$a_{i,i} \times x_{k+1}^i = -\sum_{j \neq i} a_{i,j} x_k^j + b_i \tag{6.97}$$

Les x_{k+1}^i se calculent donc assez simplement, Le nombre d'opérations pour passer de x_k à x_{k+1} est de $O(n^2)$ additions et multiplications, et n divisions.

Exemple 91. *Si le rayon spectral est* $1/2$*, afin d'avoir une précision en* $1/2^{10}$ *c'est à dire au millième près il faut faire* 10 *itérations.*

Globalement, pour une précision ε fixée, et un rayon spectral ρ il faut à peu près ce nombre de calcul :

$$(\log_\rho \varepsilon) n^2 \tag{6.98}$$

Dans les cas pratiques, c'est beaucoup plus efficace que le pivot de Gauss qui est en n^3.

Remarque. *Cette méthode bénéficie d'une parallélisation évidente, puisque toutes les coordonnées de x_{k+1} sont calculées de manière indépendantes ! En utilisant une machine avec beaucoup d'unités de calculs (par exemple un GPU) on peut donc obtenir pour des matrices de taille raisonnable des performances de l'ordre de n par itération !*

Remarque. *Une autre approche consiste à penser de manière séquentielle et utiliser le plus possible les informations déjà calculées, c'est à dire poser*

$$a_{i,i} \times x_{k+1}^i = -\sum_{j<i} a_{i,j} x_{k+1}^j - \sum_{j>i} a_{i,j} x_k^j + b_i \tag{6.99}$$

Cela ne nécessite alors plus qu'un seul segment mémoire pour le calcul de x_k, qui se fait en place. *C'est très très intéressant car on divise par deux l'utilisation de mémoire, mais aussi parce qu'on est beaucoup plus susceptible d'être dans le cache ....*

C'est la méthode de Gauss-Seidel. La décomposition est alors associée à la paire de matrices

$$\begin{cases} M = D - E \\ N = F \end{cases} \tag{6.100}$$

Avec D la diagonale de A, E qui vaut moins la partie inférieure, et F qui vaut moins la partie supérieure.

6.7.5 Une comparaison sur le cas tridiagonal

Remarque. *Le cas tridiagonal est très intéressant puisqu'il intervient dès qu'on essaie de discrétiser des équations différentielles avec des laplaciens. Ou bien en faisant des schémas numériques de type saute-mouton.*

Théorème 92 (Ciralet page 105)**.** *Pour une matrice tridiagonale, la méthode de Gauss-Seidel est deux fois plus rapide que celle de Jacobi. C'est-à-dire que le rayon spectral ρ_G pour Gauss-Seidel est le carré du rayon spectral ρ_J pour Jacobi.*

Démonstration. Soit A une matrice tridiagonale, alors on va montrer que les valeurs propres non nulles de $(D-E)^{-1}F$ sont les carrés des valeurs propres non nulles de $D^{-1}(E+F)$.

Pour cela on remarque que les valeurs propres des deux matrices sont les racines des polynômes suivants

$$\det(\lambda D - E - F) \qquad \det(\lambda D - \lambda E - F) \tag{6.101}$$

Or si λ est une racine non nulle du premier polynôme, alors

$$\begin{aligned}
\det(\lambda^2 D - \lambda^2 E - F) &= \lambda^n \det(\lambda D - \lambda E - \lambda^{-1} F) && (6.102)\\
&= \lambda^n \det(D_\lambda (\lambda D - E - F) D_\lambda^{-1}) && (6.103)\\
&= \lambda^n \det(\lambda D - E - F) && (6.104)\\
&= 0 && (6.105)
\end{aligned}$$

Où D_λ est la même matrice que dans la preuve de Householder.

En faisant le calcul à l'envers on a la réciproque, et donc le rayon spectral pour la méthode de Gauss-Seidel est le carré du rayon spectral pour la méthode de Jacobi, ce qui donne une vitesse de convergence doublée. □

6.7.6 Post requis

Conditionnement d'un système d'équation ?

Méthode de calcul de valeurs propres ?

Méthode de la relaxation ?

6.8 ■ RÉCIPROCITÉ QUADRATIQUE

Référence : Rombaldi page 435. Recasé 2 fois

■ **LEÇONS**

L121 NOMBRES PREMIERS. APPLICATIONS ★★★★★

L170 FORMES QUADRATIQUES SUR UN ESPACE VECTORIEL DE DIMENSION FINIE. ORTHOGONALITÉ, ISOTROPIE. APPLICATIONS ★★★★★

■ **RÉFÉRENCES**

Rombaldi page 435

6.8.1 Pré-requis

Définir le symbole de Legendre

Résidus quadratiques dans un corps finis et compagnie

6.8.2 Développement

On fixe p, q deux nombres premiers impairs distincts.

Lemme 93.

$$\left|\{x \in \mathbb{F}_q \mid px^2 = 1\}\right| = \left(\frac{p}{q}\right) + 1 \tag{6.106}$$

Démonstration. On distingue deux cas

Si p est un carré dans $\mathbb{F}_q$ alors $p = y^2$ puis $px^2 = (yx)^2 = 1$ si et seulement si $yx \in \{-1, +1\}$ si et seulement si $y \in \{-x^{-1}, x^{-1}\}$. Il y a donc bien deux solutions.

Sinon px^2 ne peut pas être un carré dans $\mathbb{F}_q$ et donc il n'y a pas de solutions car 1 est un carré.

□

On rappelle la loi de réciprocité quadratique

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{6.107}$$

On va la démontrer en dénombrant la sphère unité S pour la norme 2 de $\mathbb{F}_q^p$ de deux manières différentes.

$$S = \left\{x \in \mathbb{F}_q^p \mid \sum x_i^2 = 1\right\} \tag{6.108}$$

Premier dénombrement On fait agir à gauche $\mathbb{F}_p$ comme une permutation circulaire sur S via $k, (x_1, \dots, x_p) \mapsto (x_{1+k}, \dots, x_{k+p})$.

Les stabilisateurs pour cette action sont triviaux car p est premier. On veut calculer le cardinal des orbites pour cette action.

Si $\mathrm{Stab}_x = \{1\}$ alors $|\mathcal{O}_x| = p$

Sinon $\mathrm{Stab}_x = \mathbb{F}_p$, et donc l'orbite est l'ensemble des éléments de la forme $(x, \dots, x)$ vérifiant $p \times x^2 = 1$ Le lemme indique précisément que c'est $\left(\frac{p}{q}\right) + 1$.

On a donc via la formule des classes

$$|S| = \sum |\mathcal{O}_x| \equiv \left(\frac{p}{q}\right) + 1 [p] \tag{6.109}$$

Second dénombrement On considère la matrice A composée de $\frac{p-1}{2} = d$ blocs diagonaux de la forme $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ auquel on ajoute un dernier élément diagonal δ pour que la matrice soit dans $M_p(\mathbb{F}_q)$.

On constate les propriétés suivantes

(i) Le discriminant de A est la classe de $(-1)^d\delta$ modulo $\mathbb{F}_q^{2*}$

(ii) Le rang de A est n si δ est non nul

On pose donc $\delta = (-1)^d$, et via le théorème de caractérisation de la congruence des formes quadratiques sur les corps finis on a A congruente à I_p.

$$\exists P \in GL_p(\mathbb{F}_q), A = {}^tPP \tag{6.110}$$

Mais alors la sphère unité pour I_p est transportée par changement de variable via P vers la sphère unité pour A. En particulier ce changement de variable étant bijectif

$$|S| = \left|\{x \mid {}^txAx = 1\}\right| \tag{6.111}$$

On écrit $x = (y_1, z_1, \dots, y_d, z_d, t)$. L'équation que vérifie x se ré-écrit alors comme suit

$$2\sum_i y_i z_i + \delta t^2 = 1 \tag{6.112}$$

On compte le nombre de solutions dans $\mathbb{F}_q$

Si tous les y_i sont nuls Alors on peut choisir les z_i quelconques, et il y a exactement $\left(\frac{\delta}{q}\right) + 1$ choix pour t (adaptation du lemme).

Sinon il y a $q^d - 1$ choix pour les y_i. On fixe j le premier i tel que y_i est non nul. Les z_i pour $i \neq j$ sont pris arbirtairement (q^{d-1}) tout comme t. Il y a alors un unique z_j qui va bien, car $2 \neq 0$ dans $\mathbb{F}_q$.

Au total on a donc

$$|S| = q^d \times \left(\left(\frac{\delta}{q}\right) + 1\right) + q^d(q^d - 1) = q^d \times \left(\left(\frac{\delta}{q}\right) + q^d\right) \tag{6.113}$$

On peut conclure en regardant modulo p les deux dénombrements. En effet $q^d = \left(\frac{q}{p}\right)$ modulo p.

$$|S| \equiv \left(\frac{q}{p}\right)^2 + \left(\frac{q}{p}\right)\left(\frac{\delta}{q}\right) \equiv 1 + \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \quad [p] \tag{6.114}$$

On peut donc conclure en remarquant que le symbole de legendre est toujours inversible dans $\mathbb{F}_p$ et que comme $p \geq 3$ et que le symbole de legendre est toujours dans $\{-1, 1\}$ on a donc égalité des entiers.

6.8.3 Annexe utilisation

Utilisation du symbole de Legendre pour résoudre des équations du second degré dans les corps finis

Utilisation de la réciprocité quadratique pour un calcul plus rapide du symbole de Legendre

Symbole de Jacobi??

6.9 ■ DÉCOMPOSITION DUNFORD EFFECTIVE

Référence : Risler Boyer. Recasé 2 fois

■ **LEÇONS**

L153 POLYNÔMES D'ENDOMORPHISME EN DIMENSION FINIE. RÉDUCTION. APPLICATIONS ⋆⋆⋆⋆⋆

L157 ENDOMORPHISMES TRIGONALISABLES. ENDOMORPHISMES NILPOTENTS ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Rombaldi page 606

On suppose que $\mathbb{K}$ est algébriquement clos. On pose $u \in \mathscr{L}(E)$, avec E un $\mathbb{K}$-ev de dimension n. Comme $\mathbb{K}$ est algébriquement clos, le polynôme caractéristique de χ_u est scindé et s'écrit

$$\chi_u = \prod_{k=1}^{p} (X - \lambda_k)^{\alpha_k} \tag{6.115}$$

On pose $P = \prod_{k=1}^{p}(X - \lambda_k)$.

On note $u = d + v$ la décomposition de Dunford de l'endomorphisme u.

On sait que le polynôme minimal de d est P, et que d est un polynôme en u. L'idée est de rechercher d comme solution de l'équation $P(w) = 0$ avec w dans $\mathbb{K}[u]$. Pour cela on utilise la méthode de Newton

$$\begin{cases} w_0 = u \\ w_{k+1} = w_k - P(w_k)(P'(w_k))^{-1} \end{cases} \tag{6.116}$$

La question est de savoir si cette définiton a bien un sens. On montre par induction sur k les propriétés suivantes :

(i) w_k est un polynôme en u

(ii) $P'(w_k)$ est inversible dans $\mathbb{K}[u]$

(iii) $P(w_k)$ est nilpotent

6.9.1 Initialisation

(i) On remarque que u est un polynôme en u.

(ii) Comme P est scindé à racines simples, P et P' n'ont aucune racine commune, et donc il en va de même pour χ_u et P'. Les polynômes étant scindés, et non nuls ils sont donc premiers entre eux et par le théorème de Bézout il existe U, V tels que

$$U\chi_u + VP' = 1 \tag{6.117}$$

En appliquant cette relation à u on déduit que P' est inversible et que son inverse est un polynôme en u.

(iii) $P(u)^k = P^k(u)$, en particulier, pour k supérieur à tous les α_i on déduit $\chi_u | P^k$ puis $P(u)^k = P^k(u) = 0$.

6.9.2 Hérédité

(i) On constate que w_{k+1} est bien défini, et est dans $\mathbb{K}[u]$ comme somme de produits d'éléments de $\mathbb{K}[u]$.

(ii) En utilisant la formule de Taylor il existe un polynôme $Q \in \mathbb{K}[X,Y]$ vérifiant

$$P'(Y) - P'(X) = (Y-X)Q(X,Y) \tag{6.118}$$

En effet on a la formule suivante quand $p \geq 2$.

$$P'(Y) = \sum_{j=0}^{p-1} \frac{(P')^{(j)}}{j!}(X) \times (Y-X)^j \tag{6.119}$$

En appliquant la formule 6.118 à w_{k+1} et w_k on obtient alors

$$P'(w_{k+1}) - P'(w_k) \in P(w_k)(P'(w_k))^{-1}\mathbb{K}[u] \tag{6.120}$$

Par hypothèse de récurrence, on déduit que $R_k(u) = P'(w_{k+1}) - P'(w_k)$ est nilpotent. Ce qui prouve que $P'(w_{k+1}) = P'(w_k) + R_k(u)$ est inversible dans $\mathbb{K}[u]$ [11]

(iii) On utilise une fois de plus la formule de Taylor sur les polynômes

$$P(Y) = P(X) + P'(X)(Y-X) + (Y-X)^2 Q(X,Y) \tag{6.121}$$

On a donc $P(w_{k+1}) \in (P(w_k)(P'(w_k))^{-1})^2\mathbb{K}[u]$, ce qui permet de conclure sur sa nilpotence.

6.9.3 Convergence

Maintenant que la suite est bien définie, on veut montrer qu'elle converge vers la partie diagonalisable de la décomposition de Dunford.

La suite est stationnaire En étudiant l'équation de récurrence, on remarque que $P(w_{k+1}) \in P(w_k)^2\mathbb{K}[u]$. On constate donc que $P(w_k) \in P(u)^{2^k}\mathbb{K}[u]$ et donc que la suite stationne en un nombre d'étapes *logarithmique* par rapport à la taille du plus gros espace caractéristique.

La suite converge vers d Si la suite stationne à partir du rang n. On a w_n diagonalisable car annulé par un polynôme scindé à racines simples, et on a $u - w_n = w_0 - w_n = \sum_{j=0}^{n-1} w_j - w_{j+1}$. Or chacune des différences est un polynôme en u qui est nilpotent, en particulier cette somme est nilpotente, et donc on a une décomposition $u = w_n + w'$ ... C'est la décomposition de Dunford par unicité de celle-ci.

6.9.4 Annexe effectivité

Ordres de grandeurs du nombre d'opérations

Opération	Nombre d'opérations	
Somme de polynômes	$\mathcal{O}(k+k')$	
Dérivation de polynôme	$\mathcal{O}(k)$	
Produit de polynômes	$\mathcal{O}(k\log k)$	via FFT
Bézout	$\mathcal{O}(k\log^2 k)$	via euclide étendu
Somme de matrices	$\mathcal{O}(d^2)$	
Produit de matrices	$\mathcal{O}(d^3)$	
Calcul de déterminant	$\mathcal{O}(d^3)$	

(6.122)

11. $(a-b)^{-1} = (a(I-a^{-1}b))^{-1} = (I-a^{-1}b)^{-1}a^{-1} = \sum a^{-k-1}b^k$

Complexité globale de l'algorithme L'algorithme fait en gros $\log n$ itérations (degré de nilpotence), où l'on calcule $A_j - P(A_j)(P')^{-1}(A_j)$. Le calcul de $(P')^{-1}$ se fait en $\mathcal{O}(n^n)$ (oupsi ...).

On aurait pu remarquer dès le début que le U fournit par Bézout marche en fait pour inverer $P'(M)$ pour toute matrice M qui vérifie $P^d(M) = 0$ ... Ce qui évite d'avoir à faire le calcul compliqué

Pourquoi on demande scindé sur le corps ? On peut demander plus faible : les racines de P dans une clôture algébrique sont séparables sur $\mathbb{K}$, ou encore les fecteurs irréductibles de P dans $\mathbb{K}[X]$ sont de dérivée non nulle.

Cela permet de faire tous les calculs dans une extension où le polynôme est scindé à racines simples... Sinon on a le contre exemple suivant.

On pose $\mathbb{K} = \mathbb{F}_p(T)$ (le corps des fractions rationnelles) et $P = X^p - T$. On a bien P irréductible, mais dans une clôture algébrique, P ne possède qu'une seule racine de multiplicité p car $\alpha^p - T = 0$ et $\beta^p - T = 0$ implique $(\alpha - \beta)^p = 0$ et par injectivité de Frobenius [12] on déduit $\alpha = \beta$.

Terminer cette preuve chiante d'un contre exemple dans un corps non parfait

Que faire quand le polynôme n'est pas scindé mais le corps sympa ? C'est pas grave, ça marche quand même dans un surcorps, et donc on obtient une décomposition de type "diagonalisable dans un sucrorps" plus nilpotente. En fait on obtient semi-simple plus nilpotente du coup.

Doit-on scinder le polynôme ? NON ! Tous les calculs peuvent se faire via des calculs de divisions euclidienne et produits de polynômes. Le calcul du polynôme "sans facteurs carrés" se fait via $P/(P \wedge P')$ dans un corps de caractéristique nulle, et via un calcul un peu plus explicite dans un corps de caractéristique non nulle. (cf la première partie de Berlekamp).

12. Une puissance est nulle si et seulement si l'élément est nul

6.10 ■ ALGORITHME DE BERLEKAMP

Référence : Beck, Demazure. Recasé 4 fois

■ **LEÇONS**

L123 CORPS FINIS. APPLICATIONS ★★★★★

L141 POLYNÔMES IRRÉDUCTIBLES À UNE INDÉTERMINÉE. CORPS DE RUPTURE. EXEMPLES ET APPLICATIONS ★★★★★

L151 DIMENSION D'UN ESPACE VECTORIEL. RANG. EXEMPLES ET APPLICATIONS ★★★★

L162 SYSTÈMES D'ÉQUATION LINÉAIRES ; OPÉRATIONS ÉLÉMENTAIRES, ASPECTS ALGORITHMIQUES ★★★★

■ **RÉFÉRENCES**

Objectif Agrégation

Demazure

6.10.1 Polynômes dans les corps finis

Soit q une puissance d'un ombre premier p et $P \in \mathbb{F}_q[X]$.

Propriété 94. *Si $P' = 0$ alors il existe $Q \in \mathbb{F}_q[X]$ tel que $P = Q(X)^p$. Sinon, soit $P \wedge P' = 1$ et P est sans facteurs carré, soit $P \wedge P' \neq 1$ et P possède un facteur carré.*

Démonstration. Si $P' = 0$ il existe un R tel que $P = R(X^p)$ par identification des coefficients.

Par la suite, en calculant les racines p-èmes des puissances q-èmes des coefficients de R, on obtient un polynôme Q tel que $Q(X)^p = R(X^p)$, et on a conclu.

Sinon, le pgcd est un polynôme non nul, et donc il vaut soit 1 soit pas 1, et c'est le cas classique où tout se passe bien. □

Ainsi, on peut se limiter à étudier des polynômes sans facteurs carré, car on peut explicitement calculer Q dans le cas où la dérivée est nulle, et les pgcds dans les autres cas.

6.10.2 Développement

On suppose que P est un polynôme dans $\mathbb{F}_q[X]$ sans facteurs carré. On recherche un diviseur irréductible de P, on note $P_1, \dots, P_r$ les diviseurs irréductibles de P.

Pour cela on considère l'application

$$\begin{array}{rccc} \psi_P : & \mathbb{F}_q[X]/(P) & \longrightarrow & \mathbb{F}_q[X]/(P) \\ & Q & \mapsto & Q^q \end{array} \tag{6.123}$$

Cette application est $\mathbb{F}_q$-linéaire car c'est une itérée du morphisme de Frobénius sur $\mathbb{F}_q$.

D'un autre côté, le lemme Chinois fournit un isomorphisme

$$\mathbb{F}_q[X]/(P) \simeq \left(\mathbb{F}_q[X]/(P_1)\right) \times \cdots \times \left(\mathbb{F}_q[X]/(P_r)\right) \tag{6.124}$$

Cela permet d'étudier $\mathrm{Fix}\,\psi_P$.

Puisque les P_i sont irréductibles, les quotients à gauche sont des corps. Donc $Q^q - Q = 0$ dans $\mathbb{F}_q[X]/(P)$ si et seulement si $Q^q - Q = 0$ dans chacun de ces corps. Or ce sont des extensions de $\mathbb{F}_q$, dans lequel le polynôme $Y^q - Y$ possède exactement q racines.

Donc l'isomorphisme permet de déduire qu'il y a exactement q^r éléments dans $\mathrm{Fix}\,\psi_P$ qui est de dimension r.

On peut donc compter le nombre de diviseurs irréductibles de P

Si $r = 1$ alors P est irréductible et c'est terminé

Si $r \geq 2$ alors on va trouver explicitement un diviseur non-trivial de P, puis procéder par récurrence.

Pour cela on remarque que si Q est dans $\mathrm{Fix}\,\psi_P$ alors il existe des α_i dans $\mathbb{F}_q$ tels que $Q = \alpha_i$ dans $\mathbb{F}_q[X]/(P_i)$.

Mais alors pour $\alpha \in \mathbb{F}_q$, $Q-\alpha$ est nul seulement dans les corps où $\alpha_i = \alpha$. Ainsi $P \wedge Q-\alpha$ est précisément le produit de ces P_i. En faisant varier α dans $\mathbb{F}_q$ on a donc parcouru tous les diviseurs irréductibles de P une seule et unique fois, ce qui montre

$$P = \prod_{\alpha \in \mathbb{F}_q} P \wedge (Q-\alpha) \tag{6.125}$$

Seulement, si Q n'est pas un polynôme constant modulo P alors les α_i ne sont pas tous égaux, et donc un des pgcds permet d'obtenir un facteur non trivial de P.

Reste à trouver un polynôme Q dans $\mathrm{Fix}\,\psi_P$ qui n'est pas constant. Comme sa dimension est supérieure à deux, et que les polynômes constants sont fixés, il existe un polynôme non constant dans $\mathrm{Fix}\,\psi_P$. En calculant via l'algorithme du pivot de Gauss une base du noyau, on trouve donc automatiquement un polynôme non constant.

6.10.3 Question d'effectivité

Division euclidienne "Division euclidienne rapide par la méthode de Newton" Ça fait du temps linéaire par rapport à la multiplication de deux polynômes ... c'est drôlement bien !

Simplification du polynôme P Combien d'opérations faut-il faire pour rendre un polynôme sans facteurs
corps fini ?

Calcul de la matrice c'est facile, on prend la base canonique de l'espace vectoriel $1, X, \ldots, X^{n-1}$ et on calcule à la puissance q modulo P.

Cette opération prend n fois le temps d'une division euclidienne, qui se fait en n^2 en gros. Donc le précalcul est en n^3.

Détermination du noyau pour cela on utilise le pivot de Gauss. On échelonne en lignes pour déterminer une base où le noyau est directement visible. Cette base est effectivement calculée. Cela prend

$$\mathcal{O}(n^3) \tag{6.126}$$

Avec $n = \deg P$ bien entendu, puisque la matrice est de taille le degré de P.

La multiplication des polynômes se faisant aussi en gros en n^2, on fait donc le calcul d'une base du noyau en n^5.

Estimation de la complexité totale On sélectionne un polynôme dans le noyau, en temps linéaire.

On fait q choix pour pour α, puis pour chaque α on fait un calcul de pgcd de polynômes de taille n. Le calcul d'un pgcd demande en gros n divisions euclidiennes, donc on va dire qu'on fait n^{2q} opérations.

Remarque corps finis Il faut prendre en compte la taille des entiers ! Si q devient très grand c'est totalement irréaliste, et il faut ajouter du q^x partout...

En particulier, la dernière opération devient plutôt en q^q ! Et là c'est grave !

6.10.4 Amélioration probabiliste

Plutôt que de parcourir $\mathbb{F}_q$ pour et effectuer le calcul d'un pgcd pour chacun, on va fournir une factorisation de P avec 3 termes.

Si Q est fixé par ψ_P, alors Q correspond à un élément de $\mathbb{F}_q$ dans chacun des corps du lemme Chinois. En particulier, soit $Q = 0$, soit $Q^{\frac{q-1}{2}} = \pm 1$, les cas étant exactement ceux du symbole de Legendre.

Ainsi, on déduit que Q, $Q^{\frac{q-1}{2}} - 1$ et $Q^{fracq-12} + 1$ sont divisibles respectivement par ceux des P_i où c'est nul, un résidu quadratique ou un non-résidu quadratique.

On a donc l'écriture

$$P = (Q \wedge P) \times (Q^{\frac{q-1}{2}} - 1 \wedge P) \times (Q^{\frac{q-1}{2}} + 1 \wedge P) \tag{6.127}$$

En tirant aléatoirement un élément de $\mathrm{Fix}\,\psi_P$, ce qui est possible en tirant aléatoirement les coordonnées dans une base calculée par le pivot de Gauss, on doit ensuite simplement calculer 3 pgcds.

Le cas où les trois facteurs sont triviaux est précisément celui où tous les α_i sont de même nature.

Regarder le Demazure pour comprendre le truc

Cela arrive avec probabilité $2/2^r$ car un tirage uniforme dans $\mathrm{Fix}\,\psi_P$ donne un tirage uniforme dans les sous corps via la bijection, et il y a la moitié des gens qui sont des résidus quadratiques.

6.11 ■ LEMME DE MORSE

Référence : Rouvière. Recasé 4 fois

■ **LEÇONS**

L170 FORMES QUADRATIQUES SUR UN ESPACE VECTORIEL DE DIMENSION FINIE. ORTHOGONALITÉ, ISOTROPIE. APPLICATIONS ★★★★

L218 APPLICATION DES FORMULES DE TAYLOR ★★★★★

L214 THÉORÈME D'INVERSION LOCALE, THÉORÈME DES FONCTIONS IMPLICITES. EXEMPLES ET APPLICATIONS EN ANALYSE ET EN GÉOMÉTRIE. ★★★★★

L215 APPLICATIONS DIFFÉRENTIABLES DÉFINIES SUR UN OUVERT DE RN. EXEMPLES ET APPLICATIONS. ★★★★★

■ **RÉFÉRENCES**

Rouvière page 344, exercice 114

Rouvière page 201, exercice 66

Notations On considère $f : U \to \mathbb{R}$ de classe $\mathscr{C}^3$, qui vérifie $df_0 = 0$ et $d^2 f_0$ est non dégénérée de signature $(p, n-p)$.

Objectif Ramener l'étude de f en 0 à celle du polynôme $x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_n^2$ via un $\mathscr{C}^1$ difféomorphisme

Naturellement, on écrit la formule de Taylor avec reste intégral à l'origine :

$$f(x) - f(0) = \int_0^1 (1-t) d^2 f_{tx}(x,x)\, dt \tag{6.128}$$

Cette équation peut se ré-écrire

$$f(x) - f(0) = {}^t x Q(x) x \tag{6.129}$$

MORSE : Dérivable oui, mais pour quelle notion de variété ?

Où $Q(x)$ est la forme quadratique définie ci-dessous, qui varie de manière $\mathscr{C}^1$ en x.

$$Q(x) = \int_0^1 (1-t) D^2 f_{tx}\, dt \tag{6.130}$$

L'objectif est donc de réduire la forme $Q(x)$ au voisinage de $x = 0$.

Une première étape est d'écrire localement $Q(x) = {}^t M(x) Q(0) M(x)$ avec $M(x)$ assez régulière. Par la suite, une réduction de $Q(0)$ via le théorème d'inertie de Sylvester nous amènera au changement de variable désiré.

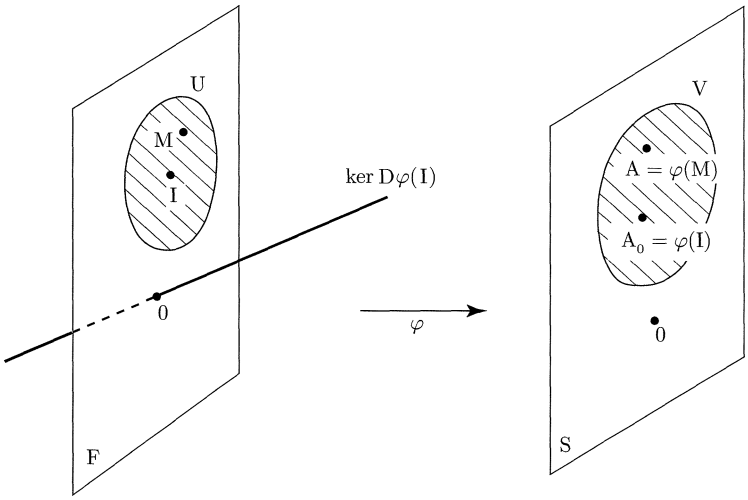
6.11.1 Existence de la fonction M

On pose pour simplifier les notations $A = Q(0) \in S_n \cap GL_n$. Naturellement, on considère l'application $\phi : M \mapsto {}^t MAM$, qui part de $\mathscr{M}_n$ vers S_n (deux espaces vectoriels, donc variétés). Cette application étant polynômiale, elle est en particulier $\mathscr{C}^1$.

De plus $\phi(I_n) = A$. On va donc rechercher un voisinage de l'identité où ϕ est un $\mathscr{C}^1$-difféomorphisme.

$$D\phi_{I_n}(H) = {}^t HA + AH = {}^t(AH) + AH \tag{6.131}$$

En effet A est symétrique. Comme A est inversible, on déduit directement $\ker D\phi_{I_n} = A^{-1} A_n(\mathbb{R})$.



Ainsi, il n'est pas possible d'utiliser directement le théorème d'inversion locale. Toutefois $\mathscr{M}_n = A^{-1}S_n \oplus A^{-1}A_n$, et donc en considérant ψ la restriction de ϕ à $A^{-1}S_n$, un sous espace vectoriel qui contient l'identité on a cette fois $D\psi_{I_n}$ injective par construction.

De plus, par un argument de dimension, $D\psi_{I_n}$ est surjective, et donc inversible.

On peut alors utiliser le théorème d'inversion locale pour trouver un voisinage V de I_n dans $A^{-1}S_n$ tel que $\psi_{|V}$ soit un $\mathscr{C}^1$-difféomorphisme sur son image (qui contient A).

Alors, quitte à supposer $V \subseteq GL_n$ (ce qui est possible car GL_n est un ouvert de $\mathscr{M}_n$) on a par construction

$$\forall B \in \psi(V), B = {}^t\psi^{-1}(B)A\psi^{-1}(B) \tag{6.132}$$

Avec ψ^{-1} un $\mathscr{C}^1$ difféomorphisme, et de plus $\psi^{-1}(B)$ inversible donc représentant un changement de base.

6.11.2 Application à la réduction de f

On peut alors réduire f comme souhaité. D'une part le théorème d'inertie de Sylvester donne une matrice $P \in GL_n$ telle que

$${}^tPQ(0)P = \begin{pmatrix} I_p & (0) \\ (0) & -I_{n-p} \end{pmatrix} \tag{6.133}$$

D'autre part comme $Q(x)$ est $\mathscr{C}^1$ en x, il existe un voisinage W de 0 dans $\mathbb{R}^n$ tel que $Q(W) \subseteq V$. Alors en utilisant ψ on peut écrire

$$\forall x \in W, Q(x) = {}^t(\psi^{-1}(Q(x)))Q(0)\psi^{-1}(Q(x)) \tag{6.134}$$

Ainsi, le "changement de variable dépendant de x" $M_x = \psi^{-1}(Q(x))P$ amène effectivement à la forme suivante

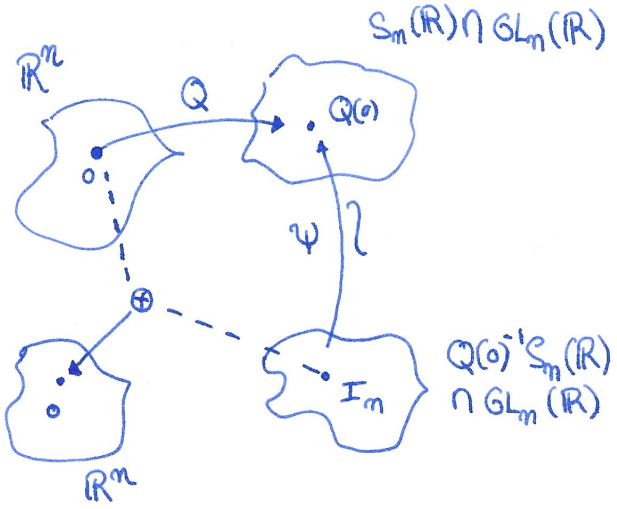
$$\forall x \in W, {}^txQ(x)x = {}^t(M_x x)\begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix}(M_x x) \tag{6.135}$$

Reste à vérifier que le changement de variable $x \mapsto M_x x$ est bien un $\mathscr{C}^1$ difféomorphisme.

Pour cela on constate déjà qu'il est $\mathscr{C}^1$ car M_x a la bonne régularité. De plus $M_0 = P$ donc $M_0 0 = 0$.

$$D(M_x x)_0 \cdot h = M_0 h + (D(M_x)_0 \cdot h)h = M_0 h + o(\|h\|) \tag{6.136}$$

Mais $M_0 = P$ et est donc inversible, donc quitte à utiliser le théorème d'inversion on peut supposer que $M_x x$ est un $\mathscr{C}^1$ difféomorphisme de W voisinage de 0 vers $(M_x x)(W)$ voisinage de 0.



6.11.3 Application en dimension deux

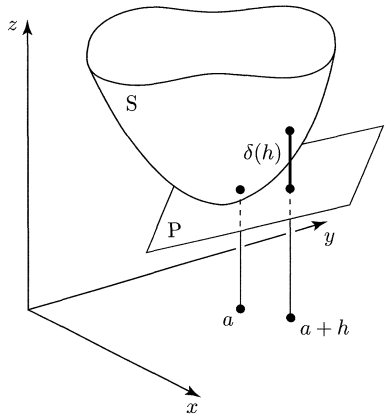
On peut appliquer ce lemme dans l'exercice 111 du Rouvière pour regarder la position par rapport au plan tangent.

On considère S la surface d'équation $f(x,y) = z$ avec f de classe $\mathscr{C}^3$ au voisinage d'un point a. On suppose que la forme $d^2 f_a$ est non dégénérée, et on veut discuter de la position relative de S par rapport à son plan tangent.

On commence par se ramener en $a = 0$ via une simple translation (qui ne change pas la Hessienne).

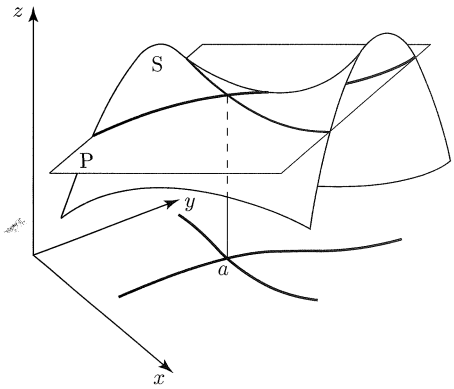
On déduit alors du lemme de morse qu'il existe un $\mathscr{C}^1$ difféomorphisme local $h = (x,y) \mapsto (u(x), v(y))$ tel que

$$\delta(h) = f(h) - (f(0) + Df_0(h)) = \varepsilon_1 u(x)^2 + \varepsilon_2 v(x)^2 \tag{6.137}$$



Ainsi, une signature $(+,+)$, $\delta(h) > 0$ localement, donc S est strictement au dessus de son plan tangent en a. Si la signature est $(-,-)$ par symétrie on a une surface strictement en dessous de son plan tangent en a.

Pour une signature $(+,-)$, on constate que localement $\delta(h)$ peut être strictement positif et strictement négatif, donc la sous variété intersecte de plan tangent (une partie est supérieure, l'autre inférieure).



6.11.4 Post requis

1. En fait ce théorème reste vrai pour f de classe seulement $\mathscr{C}^1$ et possédant une différentielle seconde non dégénérée en 0
2. Si $D^2 f$ est dégénérée, alors il faut aller plus loin dans le développement et on ne peut pas dire grand chose. Exemple $x^2 + x^3$ ne peut pas s'écrire de cette manière.

6.12 ■ ORDRE MOYEN $\phi(n)$

Référence : FGN Algèbre 1 p 156 / Rombaldi. Recasé 3 fois

■ **LEÇONS**

L120 ANNEAUX Z/nZ. APPLICATIONS ★★★

L121 NOMBRES PREMIERS. APPLICATIONS ★★★★★

L230 SÉRIES DE NOMBRES RÉELS OU COMPLEXES. COMPORTEMENT DES RESTES OU DES SOMMES PARTIELLES DES SÉRIES NUMÉRIQUES. EXEMPLES. ★★★★

■ **RÉFÉRENCES**

FGN Algèbre 1 page 156

Rombaldi dans arithmétique

6.12.1 Prérequis

Rappels basiques sur ϕ On a l'isomorphisme d'anneaux

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \simeq \prod \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)^\times \tag{6.138}$$

Ce qui donne la multiplicativité de ϕ et l'expression

$$\phi(n) = \prod \phi(p_i^{\alpha_i}) \tag{6.139}$$

De plus, $\phi(p^\alpha) = (p-1)p^{\alpha-1}$ pour $\alpha > 0$, car

$$\phi(p^\alpha) = \left|\left\{1 \le k \le p^\alpha \mid k \wedge p^\alpha = 1\right\}\right| = p^\alpha - \left|\left\{1 \le k \le p^\alpha \mid p|k\right\}\right| = p^\alpha - p^{\alpha-1} \tag{6.140}$$

Le petit truc qui fait plaisir sur ϕ ... et qui se prouve par un simple dénombrement

$$n = \sum_{d|n} \phi(d) \tag{6.141}$$

Expressions pratiques pour ϕ On en déduit les expressions suivantes

$$\phi(n) = \prod (p-1)p^{\alpha_i - 1} = n \prod \left(1 - \frac{1}{p}\right) \tag{6.142}$$

Encadrement Dans le Rombaldi, la propriété non-tirivale suivante est démontrée proprement :

$$\forall n \ge 2, \sqrt{n} - 1 < \phi(n) \le n - 1 \tag{6.143}$$

Limites De manière plus ou moins immédiate on a $\lim \phi(n) = +\infty$ [13].

On sait aussi que $\limsup \frac{\phi(n)}{n} = 1$ car il y a une infinité de nombres premiers. Un résultat tout aussi simple dit que de l'autre côté on a bien $\liminf \frac{\phi(n)}{n} = 0$.

Pour cela, on écrit :

$$\frac{\phi(n)}{n} = \prod \left(1 - \frac{1}{p}\right) \tag{6.144}$$

On trouve donc n nombres premiers supérieurs à 2 distincts tels que $1 - \frac{1}{p} < \frac{1}{2}$, et donc le produit est plus petit que $\frac{1}{2^n}$.

13. Sans avoir besoin de l'encadrement précédent, on peut simplement remarquer qu'avoir moins de k inversibles c'est plus possible quand on est trop grand

Formule du Crible / De Poincarré On considère un ensemble fini d'évènements A_k, alors on constate que

$$\mathbb{P}\left(\bigcup A_k\right) = \mathbb{E}\left(\mathbf{1}_{\bigcup A_k}\right) = \mathbb{E}\left(1 - \mathbf{1}_{\bigcap A_k^c}\right) = \mathbb{E}\left(1 - \prod(1 - \mathbf{1}_{A_k})\right) = 1 - \sum_{\emptyset \subseteq I \subseteq \{1,\dots n\}} (-1)^{|I|} \times \mathbb{P}\left(\bigcap A_k\right) \quad (6.145)$$

En simplifiant le terme en 1 on obtient alors

$$\mathbb{P}\left(\bigcup A_k\right) = \sum_{\emptyset \subsetneq I \subseteq \{1,\dots n\}} (-1)^{|I|+1} \times \mathbb{P}\left(\bigcap A_k\right) \quad (6.146)$$

Fonction de Möbius On note $\mu : \mathbb{N} \to \{-1, 0, 1\}$ la fonction qui à n associe 0 si n possède un facteur carré, 1 si $n = 1$, et $(-1)^r$ si n possède r facteurs premiers distincts.

On a alors la formule d'inversion dite « De Möbius »

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases} \quad (6.147)$$

Cette formule s'obtient simplement via un binôme de Newton de type $(1-1)^n$. En effet, cette somme est sur les choix des exposants qui valent ± 1 des nombres premiers p qui divisent n. On a donc pour $n > 1$.

$$\sum_{d|n} \mu(d) = \sum_{\emptyset \subseteq I \subseteq D_n} (-1)^{|I|} = \sum_{k=0}^{|D_n|} \binom{|D_n|}{k} (-1)^k = (1-1)^{|D_n|} = 0 \quad (6.148)$$

6.12.2 Développement

Objectif On introduit r_n la probabilité que deux entiers inférieurs à n soient premiers entre eux, et A_n l'ensemble associé à cet évènement. La relation entre les deux objets est bien évidemment

$$r_n = \frac{|A_n|}{n^2} \quad (6.149)$$

L'objectif est de calculer A_n, et de détermier un équivalent quand n devient grand.

Introduction des évènements plus simples Mais on peut écrire facilement A_n^c comme une union d'évènements plus simples :

$$A_n^c = \left\{(a,b) \leq n \mid \exists p \in P_{\leq n}, p|a \wedge p|b\right\}$$

On note $U_p = \{(a,b) \leq n \mid p|a \wedge p|b\}$.

Utilisation de la formule du Crible

$$\left|A_n^c\right| = n^2 - \sum_{\emptyset \subsetneq I \subseteq P_{\leq n}} (-1)^{|I|+1} \left|\bigcap_{p \in I} U_p\right|$$

Calcul des intersections Mais il est facile de remarquer que si on pose $\alpha_I = \prod_{i \in I} p_i$ alors :

$$\begin{aligned} \left|\bigcap_{p \in I} U_p\right| &= \left|\{(a,b) \leq n \mid \forall p \in I, p|a \wedge p|b\}\right| \\ &= |\{(\alpha_I k, \alpha_I l) \leq n \mid \alpha_I k = a \wedge \alpha_I l = b\}| \\ &= \left\lfloor \frac{n}{\alpha_I} \right\rfloor^2 \end{aligned}$$

Utilisation de la fonction de Möbius On peut alors conclure en reconnaissant la fonction μ cachée dans la somme :

$$\begin{aligned}|A_n| &= n^2 + \sum_{\emptyset \subsetneq I \subseteq P_{\leq n}} (-1)^{|I|} \left\lfloor \frac{n}{\alpha_I} \right\rfloor^2 \\ &= n^2 + \sum_{d=2}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2 \\ &= \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2\end{aligned}$$

Méthode d'estimation du développement asymptotique On veut un développmement asymptotique de r_n, pour cela on va simplement remarquer que le terme général est équivalent à $\mu(d)/d^2$.

On pose donc $s_n = \sum_{d=1}^{n} \mu(d)/d^2$. Cette somme converge absolument, tout comme r_n.

Comparaison des deux séries Or

$$\left\lfloor \frac{n}{d} \right\rfloor \geq \frac{n}{d} - 1$$

Ainsi

$$\left\lfloor \frac{n}{d} \right\rfloor^2 \geq (\frac{n}{d} - 1)^2$$

Et donc on peut majorer l'intérieur de la différence des sommes :

$$\begin{aligned}|r_n - s_n| &\leq \sum_{d=1}^{n} \left| \frac{1}{n^2} \left\lfloor \frac{n}{d} \right\rfloor^2 - \frac{1}{d^2} \right| \\ &\leq \sum_{d=1}^{n} \left| \frac{2}{dn} - \frac{1}{n^2} \right| \\ &\leq \frac{2}{n} \sum_{d=1}^{n} \frac{1}{d} + \frac{1}{n} \\ &\leq O\left(\frac{\ln n}{n} \right)\end{aligned}$$

On déduit donc, que r_n et s_n ont la même somme.

Calcul effectif Pour calculer la somme de s_n on procède comme suit

(i) Calculons le produit des sommes $\zeta(2)$ et s_∞. Ce sont deux sommes absolument convergentes c'est-à-dire que les familles $(\mu(d)/d^2)$ et $(1/n^2)$ sont sommables.

Ainsi, la famille $(\mu(d)/(dn)^2)$ est sommable, et on a en utilisant des sommations par paquets :

$$\left(\sum_{d\geq 1}\frac{\mu(d)}{d^2}\right)\left(\sum_{n\geq 1}\frac{1}{n^2}\right) = \sum_{n,d\geq 1}\frac{\mu(d)}{(dn)^2} \tag{6.150}$$

$$= \sum_{d\geq 1}\sum_{n\geq 1}\frac{\mu(d)}{(dn)^2} \tag{6.151}$$

$$= \sum_{d\geq 1}\sum_{d|p}\frac{\mu(d)}{p^2} \tag{6.152}$$

$$= \sum_{d\geq 1}\frac{1}{p^2}\sum_{d|p}\mu(d) \tag{6.153}$$

$$= 1 \tag{6.154}$$

Remarque. *On a prouvé par la même occasion que* $1/n^2$ *est l'inverse de* $\mu(d)/d^2$ *pour* $\star$. *Il serait amusant de généraliser cela ... (lien entre inverse classique pour les séries et inverse pour* $\star$*).*

(ii) Les deux sommes sont donc inverses, mais on sait que $\zeta(2) = \frac{\pi^2}{6}$, on a donc

$$\boxed{\sum_{d\geq 1}\frac{\mu(d)}{d^2} = \frac{6}{\pi^2}} \tag{6.155}$$

6.12.3 Lien avec l'ordre moyen

On constate que

$$|\{(a,b)\in[\![1,n]\!] \mid a\wedge b = 1\}| = 2|\{(a,b)\in[\![1,n]\!] \mid a\wedge b = 1 \text{ et } b<a\}| \tag{6.156}$$

$$= 2\sum_{a=1}^{n}|\{b\in[\![1,a]\!] \mid a\wedge b = 1\}| \tag{6.157}$$

$$= 2\sum_{k=1}^{n}\phi(k) \tag{6.158}$$

On déduit donc l'ordre moyen de $\phi(n)$

$$\boxed{\frac{1}{n}\sum_{k=1}^{n}\phi(k) \sim \frac{3}{\pi^2}n} \tag{6.159}$$

Remarque. *On a environ* $\frac{3}{\pi^2}\approx 0.31$*, ce qui veut dire qu'en moyenne il y a* 31% *d'inversibles dans un* Z/nZ.

6.12.4 Annexe Möbius

Formule d'inversion On munit l'espace des suites réelles (indicées à partir de 1) du produit $\star$ (de convolution)

$$(u\star v)(n) = \sum_{kl=n}u(k)v(l) = \sum_{d|n}u(d)v\left(\frac{n}{d}\right) \tag{6.160}$$

Ce produit est associatif, commutatif, et possède un neutre évident : la suite $(1,0,\dots)$.

La question est de trouver un inverse à la suite $\omega = (1,1,\dots)$. Son inverse est en fait μ ... C'est ce que dit la formule d'inversion de Möbius !

Cela permet d'inverser pleins de formules, puisque

$$u \star \omega = v \iff u = v \star \mu \tag{6.161}$$

En pratique, on écrit ça dans le sytle plus sommatoire (mais totalement équivalente)

$$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) \tag{6.162}$$

6.13 ■ SOUS ESPACES DE $\mathscr{C}(R,R)$ STABLES PAR TRANSLATION

Référence : Beck, FGN Algèbre 1 page 300. Recasé 2 fois

■ **LEÇONS**

L221 ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES. SYSTÈMES. ★★★★

L228 CONTINUITÉ ET DÉRIVABILITÉ DES FONCTIONS RÉELLES ★★

■ **RÉFÉRENCES**

FGN Algèbre 1 page 300

Objectif Agrégation page 144

Remarque. *Bien récupérer les différentes parties séparément du FGN et de Objectif Agrégation. La partie dualité est dans FGN, la partie convolution dans Beck, et la fin c'est perso.*

Théorème 95. *Soit F un sous espace de $\mathscr{C}(\mathbb{R},\mathbb{R})$, alors on a l'équivalence suivante*

$$\dim F < +\infty \wedge \forall a \in \mathbb{R}, \tau_a F \subseteq F \iff \exists P \in \mathbb{R}[X], F = \ker P(D) \tag{6.163}$$

Avec τ_a la translation par a, D l'endomorphisme de dérivation défini sur $\mathscr{C}^\infty(\mathbb{R},\mathbb{R})$, sous espace vectoriel de $\mathscr{C}(\mathbb{R},\mathbb{R})$.

Ce qui se lit

> Tout sous espace vectoriel de dimension finie des fonctions continues stable par translation est l'espace de solution d'une équation différentielle homogène (et réciproquement).

6.13.1 Sens réciproque

Il suffit de remarquer que l'espace de solutions est de dimension finie via Cauchy-Lipschitz, puis que la dérivation commute avec la translation, ce qui laisse donc F de dimension finie et stable par translation.

6.13.2 Sens implique, étape 1, F est stable par dérivation

On veut montrer que F est stable par dérivation, pour cela on considère une fonction f dans F, et l'espace vectoriel $E = \mathrm{Vect}(\tau_a f)_{a\in\mathbb{R}}$. Supposons le de dimension p.

Extraction d'une base On extrait de $(\tau_a f)$ une base $(f_1,\dots,f_n)$ correspondant aux points $(a_1,\dots,a_n)$.
Il est clair qu'il existe alors un unique n-uplet de fonctions $(\lambda_1,\dots,\lambda_n)$ vérifiant

$$\tau_a f = \sum_{i=1}^{n} \lambda_i(a) f_i \tag{6.164}$$

Montrons que les λ_i ont la régularité de f Pour cela, on va exprimer les λ_i comme des combinaisons linéaires des translatées de f, cela revient à inverser un système de type

$$\tau_\square f(x_j) = \sum_{i=1}^{n} \lambda_i(\square) f_i(x_j) \tag{6.165}$$

Pour un certain nombre de x_j.

Lemme 96. *Il existe des points (x_j) tels que la matrice M des $(f_i(x_j))$ soit inversible.*

Démonstration. La famille $ev_x : g \mapsto g(x)$ est génératrice de E^*, en effet en notant $G = \text{Vect}(ev_x)$ on a par construction :

$$G^\circ = \{0\} \tag{6.166}$$

En utilisant la dimension finie on peut donc conclure.

$$G = (G^\circ)^\perp = \{0\}^\perp = E^* \tag{6.167}$$

On a donc une base (ev_{x_j}) de E^*. Mais alors, considérons les colonnes de la matrice M, et une combinaison linéaire

$$\sum_{i=1}^{n} \alpha_i C_i = 0 \tag{6.168}$$

Cela se ré-écrit précisément

$$\forall j, ev_{x_j}(\sum_{i=1}^{n} \alpha_i f_i) = 0 \tag{6.169}$$

Ce qui, comme on a une base de E^* veut dire

$$\sum_{i=1}^{n} \alpha_i f_i = 0 \tag{6.170}$$

Puis que $\alpha_i = 0$ car (f_i) est libre. □

On peut donc écrire, pour tout $a \in \mathbb{R}$.

$$\begin{pmatrix} \vdots \\ \tau_a f(x_j) \\ \vdots \end{pmatrix} = \begin{pmatrix} \cdots & \cdots & \cdots \\ \vdots & f_i(x_j) & \vdots \\ \cdots & \cdots & \cdots \end{pmatrix} \begin{pmatrix} \vdots \\ \lambda_i(a) \\ \vdots \end{pmatrix} \tag{6.171}$$

Ce système s'inverse donc naturellement

$$\begin{pmatrix} \cdots & \cdots & \cdots \\ \vdots & f_i(x_j) & \vdots \\ \cdots & \cdots & \cdots \end{pmatrix}^{-1} \begin{pmatrix} \vdots \\ \tau_a f(x_j) \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ \lambda_i(a) \\ \vdots \end{pmatrix} \tag{6.172}$$

Or cela exprime $\lambda_i(a)$ comme une combinaison linéaire à coefficients indépendants de a de fonctions de type $\tau_a f(x_j)$ qui sont de même régularité que f.

Conclusion dans le cas où les λ_i sont dérivables Si les λ_i sont dérivables en a. Alors

$$\frac{\partial}{\partial a} \tau_a f(x) = \sum_{i=1}^{n} \lambda_i'(a) f_i(x) \tag{6.173}$$

En prenant $a = 0$, on obtient alors

$$f'(x) = \sum_{i=1}^{n} \lambda_i'(0) f_i(x) \in E \tag{6.174}$$

Si f est dérivable alors les λ_i aussi, donc E est stable par dérivation.

Dans le cas f continue montrons tout de même que les λ_i sont infiniment dérivables.

On considère θ_k une approximation de l'unité à support compact, et on convole en x l'équation 6.164 avec θ_k.

$$(\theta_k \star \tau_a f) = \sum_{i=1}^{n} \lambda_i(a)(\theta_k \star f_i) \tag{6.175}$$

Ainsi, on obtient une matrice $M_k = (\theta_k \star f_i(x_j))$ et le système d'équations

$$\begin{pmatrix} \vdots \\ (\theta_k \star \tau_a f)(x_j) \\ \vdots \end{pmatrix} = M_k \begin{pmatrix} \vdots \\ \lambda_i(a) \\ \vdots \end{pmatrix} \tag{6.176}$$

Mais les propriétés de la convolution montrent que $\theta_k \star \tau_a f \to \tau_a f$ simplement en x. Et donc la matrice M_k converge vers M. Or $\det M \neq 0$, et par continuité du déterminant, il existe un k_0 tel que M_{k_0} soit inversible.

On exprime alors les λ_i comme des combinaisons linéaires des convolées, qui sont toutes $\mathscr{C}^\infty$, ce qui permet de conclure.

6.13.3 Sens implique, étape 2, utiliser la stabilité

L'opérateur dérivation D laisse donc stable l'espace vectoriel F. On peut donc considérer π le polynôme minimal de $D_{|F}$ qui existe car c'est un espace de dimension finie.

On sait par Cayley-Hamilton que $\deg\pi \leq \dim F$, et par construction $\ker\pi(D_{|F}) = F$.

Mais alors, $F = \ker\pi(D_{|F}) \subseteq \ker\pi(D)$. Toutefois, $\ker\pi(D)$ est l'ensemble des solutions d'une équation différentielle linéaire à coefficients constant d'ordre $\deg\pi$, et donc par Cauchy-Lipschitz est de dimension $\deg\pi$.

Ainsi, par l'inclusion et les inégalités $\deg\pi \leq \dim F \leq \deg\pi$ on peut conclure $F = \ker\pi(D)$.

On remarque de plus que la dimension de F est précisément le degré de π, c'est-à-dire l'ordre de l'équation différentielle,

6.14 ■ BANACH STEINHAUS ET FOURIER

Référence : Gourdon Analyse, Brézis. Recasé 2 fois

■ **LEÇONS**

L208 ESPACES VECTORIELS NORMÉS, APPLICATIONS LINÉAIRES CONTINUES. EXEMPLES.★★★★★

L246 SÉRIES DE FOURIER ★★★★★

■ **RÉFÉRENCES**

Gourdon Analyse

6.14.1 Prérequis

Lemme de Baire Une intersection dénombrable d'ouverts dense dans EVN complet est dense.

Soit V un ouvert non vide de E. Pour chaque k, on construit une boule fermée de rayon plus petit que $1/2^k$ contenue dans $V \cap \cap_{\leq k} \Omega_k$, et la suite des boules est décroissante pour l'inclusion.

C'est possible via les hypothèses, mais alors clairement ce sont des fermés emboités non vides, donc leur intersection est non vide (evn complet).

Mais alors, par construction $x \in V \cap \cap_n \Omega_n$ donc l'ensemble $\cap \Omega_n$ rencontre V.

Fonctions continues périodiques norme infinie = Banach

6.14.2 Théorème de Banach-Steinhaus

On fixe E un espace de Banach et F un espace vectoriel normé. On considère H un ensemble d'applications linéaires continues de E dans F.

On a l'alternative suivante :

(i) L'ensemble des x tels que $\sup_{h\in H} \|h(x)\| = +\infty$ est un G_δ-dense

(ii) $\sup_{h\in H} |||h||| < +\infty$

En effet, considérons l'ensemble

$$\Omega_k = \left\{ x \in E \mid \sup_{h\in H} \|h(x)\| > k \right\} \tag{6.177}$$

Cet ensemble est clairement ouvert.

Si chaque Ω_k est dense Alors $\cap \Omega_k$ est un G_δ-dense via le lemme de Baire et on a le premier cas.

Si Ω_{k_0} n'est pas dense Alors il existe une boule *fermée* $B(x_0, r)$ qui n'intersecte pas Ω_{k_0}, et donc

$$\forall x \in B(0,1), \forall h \in H, \|h(x_0 + rx)\| \leq k_0 \tag{6.178}$$

En particulier, on déduit donc

$$\forall h \in H, \forall x \in B(0,1), \|h(x)\| \leq \frac{1}{r}(k_0 + \|h(x_0)\|) = C_0 \tag{6.179}$$

On déduit donc que $|||h||| \leq C_0$, et donc $\sup_{h\in H} |||h||| < +\infty$.

Remarque. *On en déduit en particulier les théorèmes suivants (Gourdon) : une limite simple d'applications linéaires continues est continue. Une application bilinéaire est continue si et seulement si elle est continue en chacun de ses arguments.*

6.14.3 Séries de Fourier qui divergent en zéro

On note $C_{2\pi}$ l'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{C}$ qui sont 2π périodiques, muni de la norme infinie.

On rappelle que

$$c_n(f) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-inx}dx \tag{6.180}$$

On construit la suite d'opérateurs linéaires continus suivante

$$L_n : f \mapsto \sum_{k=-n}^{n} c_k(f) \tag{6.181}$$

1. Les opérateurs sont bien linéaires et continus comme somme d'opérateurs linéaires continus.
2. Précisons la norme d'opérateur

$$2\pi L_n(f) = \sum_{k=-n}^{n}\int_{-\pi}^{\pi} f(x)e^{-ikx}dx = \int_{-\pi}^{\pi} f(x)\sum_{k=-n}^{n} e^{-ikx}dx \tag{6.182}$$

$$= \int_{-\pi}^{\pi} f(x)\frac{e^{inx}-e^{-i(n+1)x}}{1-e^{-ix}}dx \tag{6.183}$$

$$= \int_{-\pi}^{\pi} f(x)\frac{\sin(2n+1)/2x}{\sin x/2}dx \tag{6.184}$$

$$\tag{6.185}$$

Ainsi, $\|f\| = 1$ implique

$$\left|L_n(f)\right| \leq \frac{1}{2\pi}\int_{-\pi}^{\pi}\left|\frac{\sin(2n+1)/2x}{\sin x/2}\right|dx \tag{6.186}$$

Or la fonction intégrée est continue sur $[-\pi,\pi]$ (somme d'exponentielles ...) et donc cette intégrale existe et est en particulier finie.

Montrons que c'est précisément la norme d'opérateur de L_n. On pose $D_n(x) = \frac{\sin(2n+1)/2x}{\sin x/2}$

$$f_\varepsilon(x) = \frac{D_n(x)}{|D_n(x)|+\varepsilon} \tag{6.187}$$

On constate que f_ε est bien définie, continue et périodique si $\varepsilon > 0$. De plus, il est clair que $\|f_\varepsilon\| \leq 1$.

Par la suite

$$L_n(f_\varepsilon) = \frac{1}{2\pi}\int_{-\pi}^{\pi}\frac{D_n^2(x)}{|D_n(x)|+\varepsilon}dx \tag{6.188}$$

On peut alors utiliser le théorème de convergence monotone (les fonctions sont positives et la suite croissante) pour déduire

$$L_n(f_\varepsilon) \to \frac{1}{2\pi}\int_{-\pi}^{\pi}|D_n(x)|dx \qquad (\varepsilon \to 0) \tag{6.189}$$

Ainsi, on déduit

$$|||L_n||| \geq \frac{1}{2\pi}\int_{-\pi}^{\pi}|D_n(x)|dx \tag{6.190}$$

Ce qui permet de conclure.

3. Montrons que la suite $\|\|L_n\|\|$ tend vers $+\infty$.
   On constate que pour tout nombre réel t on a l'inégalité classique $|\sin(t/2)| \leq |t/2|$.
   Ainsi,

$$\|\|L_n\|\| \geq \frac{1}{\pi}\int_0^\pi \left|\frac{\sin(2n+1)/2x}{x/2}\right| dx = \frac{2}{\pi}\int_0^\pi \left|\frac{\sin(2n+1)/2x}{x}\right| dx = \frac{2}{\pi}\int_0^{(2n+1)\pi/2} \left|\frac{\sin u}{u}\right| du \quad (6.191)$$

   Cette dernière intégrale diverge en découpant sur les intervalles de type $[n\pi,(n+1)\pi]$, où l'intégrande est alors minoré par $\frac{1}{n\pi}|\sin u|$, et l'intégrale de ceci vaut alors $\frac{2}{n\pi}$. On peut donc la minorer par une série divergente H_n (la série harmonique) ce qui permet de conclure.

4. On peut alors conclure via le théorème de Banach Steinhaus qui indique que l'ensemble des fonctions continues 2π périodiques dont la série de Fourier diverge en zéro est un G_δ-dense.

6.14.4 Post-requis

Lemme 97 (Injectivité des Coefficients de Fourier)**.**

Exemple 98 (Construction explicite d'une telle fonction)**.**

6.15 ■ MÉTHODE DU GRADIENT À PAS OPTIMAL

Référence : Ciralet. Recasé 3 fois

■ **LEÇONS**

L219 EXTREMUMS : EXISTENCE, CARACTÉRISATION, RECHERCHE. ★★★★★

L229 FONCTIONS MONOTONES, FONCTIONS CONVEXES ★★★★★

L233 MÉTHODES ITÉRATIVES EN ANALYSE NUMÉRIQUE MATRICIELLE. ★★★★★

■ **RÉFÉRENCES**

Ciralet page 182, 189

Devillier

6.15.1 Préliminaires

Rappels sur la convexité Voir le Beck

Définition de α-convexité

Problèmes "elliptiques" ?

6.15.2 Développement

Considérons $J : \mathbb{R}^n \to \mathbb{R}$, C^1 et elliptique :

$$\langle \nabla J(x) - \nabla J(y) \mid x-y \rangle \geq \alpha \|x-y\|^2 \tag{6.192}$$

On cherche à trouver le minimum de J sur $\mathbb{R}$.

La fonction J est strictement convexe C'est clair puisque J est strictement convexe si et seulement si pour $x \neq y$

$$\langle \nabla J(x) - \nabla J(y) \mid x-y \rangle > 0 \tag{6.193}$$

Ce qui est le cas puisque $\alpha > 0$.

La fonction J est coercive Pour cela on utilise Taylor

$$J(x) - J(y) = \int_0^1 \langle \nabla J(y + t(x-y)) \mid x-y \rangle dt \tag{6.194}$$

Cela permet d'écrire ensuite

$$J(x) - J(y) = \langle \nabla J(y) \mid x-y \rangle + \int_0^1 \langle \nabla J(y + t(x-y)) - J(y) \mid x-y \rangle dt \tag{6.195}$$

En utilisant alors le caractère elliptique

$$J(x) - J(y) \geq \langle \nabla J(y) \mid x-y \rangle + \int_0^1 \frac{\alpha}{t} \|t(x-y)\|^2 dt \tag{6.196}$$

$$\boxed{J(x) - J(y) \geq \langle \nabla J(y) \mid x-y \rangle + \frac{\alpha}{2}\|x-y\|^2} \tag{6.197}$$

En particulier, en prenant $y = 0$ on déduit la coercivité

$$J(x) \geq \langle \nabla J(0) \mid x \rangle + \frac{\alpha}{2}\|x\|^2 \to +\infty \tag{6.198}$$

La fonction J possède un unique minimum local/minimum global Comme J est coercive, l'ensemble $K = \{x \in \mathbb{R}^n \mid J(x) \leq J(0)\}$ est compact (dimension finie !). Ainsi, J admet un minimum sur K par continuité, et par construction ce minimum est global. On le suppose atteint en $x^\star$.

Prenons x' un minimum global, alors $\nabla J(x') = 0$. Ainsi l'équation précédente permet de dire

$$J(x^\star) - J(x') \geq \frac{\alpha}{2}\|x^\star - x'\|^2 \tag{6.199}$$

Donc $x^\star = x'$ et le minimum global est unique [14]

La preuve permet de conclure même si x' est seulement un minimum local puisque :

$$0 \geq J(x^\star) - J(x') \geq \frac{\alpha}{2}\|x^\star - x'\|^2 \tag{6.200}$$

Donc le minimum $x^\star$ est *caractérisé* par $\nabla J(x^\star) = 0$.

Construction de la méthode itérative On pose $x_0 \in \mathbb{R}^n$ quelconque, et on prend l'équation

$$x_{n+1} = x_n - t_n \nabla J(x_n) \tag{6.201}$$

Avec t_n qui permet de minimiser la fonction réelle $g_n : t \mapsto J(x_n - t\nabla J(x_n))$.

(i) Intuitivement, on considère une direction de descente vers le minimum, et pour cela on considère l'information à l'ordre 1, c'est à dire le gradient, qui donne la direction de plus grande pente.

Une fois cette direction choisie, il faut savoir "jusqu'où aller", et quoi de plus naturel que de minimiser notre fonction sur la droite affine donnée par cette pente pour se rapprocher du minimum ?

(ii) La fonction g_n est C^1 par composition, et reste strictement convexe comme restriction d'une fonction convexe à une droite affine. De même, g_n est coercive. Elle a donc un unique minimum caractérisé par l'équation $g_n'(t) = 0$.

La suite x_n est donc bien définie.

Les pas sont orthogonaux En effet, par construction (développer ce calcul d'une ligne) :

$$g_n'(t_n) = 0 \iff \langle \nabla J(x_{n+1}) \mid \nabla J(x_n) \rangle = 0 \tag{6.202}$$

Cela permet non seulement de comprendre géométriquement la suite considérée, mais va permettre de prouver les propriétés de convergence.

La suite $J(x_n)$ On reprend l'équation encadrée au tout début et on l'applique à deux termes consécutifs de la suite :

$$J(x_n) - J(x_{n+1}) \geq \langle \nabla J(x_{n+1}) \mid x_n - x_{n+1} \rangle + \frac{\alpha}{2}\|x_n - x_{n+1}\|^2 \tag{6.203}$$

Or, $x_n - x_{n+1}$ est précisément un vecteur colinéaire à $\nabla J(x_n)$, donc le produit scalaire s'annule et

$$J(x_n) - J(x_{n+1}) \geq \frac{\alpha}{2}\|x_n - x_{n+1}\|^2 \tag{6.204}$$

Donc la suite $J(x_n)$ décroit strictement. Comme elle est minorée par $J(x^\star)$, elle converge.

14. C'est en réalité trivial puisque J était strictement convexe... Donc le barycentre de deux points minimaux distincts en donne un strictement inférieur ...

La suite x_n converge vers $x^\star$ De l'équation précédente on déduit déjà que $x_{n+1} - x_n \to 0$, donc que la suite x_n *s'essouffle*.

Sur le compact K considéré auparavant, la fonction ∇J est continue, donc uniformément continue (Heine).

Ainsi, il est clair que $\nabla J(x_{n+1}) - \nabla J(x_n) \to 0$ par uniforme continuité.

Enfin,

$$\|\nabla J(x_n)\|^2 = \langle \nabla J(x_n) \mid \nabla J(x_n) \rangle = \langle \nabla J(x_n) \mid \nabla J(x_n) - \nabla J(x_{n+1}) \rangle \leq \|\nabla J(x_n)\| \|\nabla J(x_n) - \nabla J(x_{n+1})\| \tag{6.205}$$

Donc $\nabla J(x_n) \to 0$!

Soit x_∞ une valeur d'adhérence de x_n qui existe car K est compact. Par continuité on déduit $\nabla J(x_\infty) = 0$, et donc $x_\infty = x^\star$ car on avait caractérisé le minimum.

Il y a donc une unique valeur d'adhérence, $x^\star$ et $x_n \to x^\star$.

6.15.3 Questions

Application à la résolution En minimisant $(Au, u) - (b, u)$ on trouve une solution du système $Ax = b$! (ciralet)

Comment trouver t_n ? Application pratique sur $(Au, u) - (b, u)$, on recherche une solution d'un trinôme du second degré ! Hop hop hop calcul explicite. (Ciralet page 191)

Comment savoir quand stopper la recherche ?

6.16 ■ PROCESSUS DE BRANCHEMENTS

Référence : COT exercices de probabilités, page 72. Recasé 3 fois

■ **LEÇONS**

L229 FONCTIONS MONOTONES, FONCTIONS CONVEXES ★★★

L260 ESPÉRANCE, VARIANCE ET MOMENTS D'UNE VARIABLE ALÉATOIRE. ★★★★★

L264 VARIABLES ALÉATOIRES DISCRÈTES. EXEMPLES ET APPLICATIONS ★★★★★

■ **RÉFÉRENCES**

COT exercices de probabilités, page 72

Probabilités pour les non-probabilistes, Walter Appel

6.16.1 Développement

On considère une suite Z_k de variables aléatoires définies par récurrence comme suit

$$\begin{cases} Z_0 = 1 \\ Z_{k+1} = \sum_{i=1}^{Z_k} X_{i,k} \end{cases} \tag{6.206}$$

Où les $X_{i,k}$ sont des variables aléatoires indépendantes identiquement distribuées selon la même loi qu'une certaine variable X.

Approche Modélisation On veut modéliser le caractère pérène d'un allèle dominant dans une population, en fonction de sa capacité de reproduction modélisée par la loi de X. On peut aussi penser à faire de l'épidémiologie avec ça.

L'objectif est de calculer la probabilité d'extinction.

Premières remarques De manière très naturelle, si $Z_k = 0$ pour un certain k, alors pour $n \geq k$, $Z_n = 0$.

Ainsi la probabilite d'extinction s'écrit

$$\mathbf{P}(ext) = \mathbf{P}\left(\bigcup_k \{Z_k = 0\}\right) \tag{6.207}$$

Par continuité décroissante de la limite, on déduit donc :

$$\mathbf{P}(ext) = \lim \mathbf{P}\left(\bigcup_{k \leq N} \{Z_k = 0\}\right) = \lim \alpha_k = \alpha \tag{6.208}$$

L'outil théorique On introduit l'outil théorique qui va faire marcher toute l'étude : la série génératrice.

$$G_{Z_n}(t) = \mathbf{E}(t^{Z_n}) = \sum_{k \in \mathbb{N}} \mathbf{P}(Z_n = k)\, t^k \tag{6.209}$$

C'est une série entière à termes positifs de rayon de convergence plus grand que 1. Et elle caractérise la loi de Z_n.

Son lien avec la suite α_n est le suivant :

$$G_{Z_n}(0) = \mathbf{P}(Z_n = 0) = \alpha_n \tag{6.210}$$

L'équation de récurrence

$$G_{Z_{n+1}}(t) = \mathbf{E}\left(t^{\sum_{i=1}^{Z_n} X_{i,n}}\right) \tag{6.211}$$
$$= \mathbf{E}\left(\sum_{N\in\mathbb{N}} t^{\sum_{i=1}^{N} X_{i,n}} \chi_{Z_n=N}\right) \tag{6.212}$$
$$= \sum_{N\in\mathbb{N}} \mathbf{E}\left(t^{\sum_{i=1}^{N} X_{i,n}} \chi_{Z_n=N}\right) \tag{6.213}$$
$$= \sum_{N\in\mathbb{N}} \prod_{i=1}^{N} \mathbf{E}\left(t^{X_{i,n}}\right) \mathbf{P}(Z_n = N) \tag{6.214}$$
$$= \sum_{N\in\mathbb{N}} (G_X(t))^N \mathbf{P}(Z_n = N) \tag{6.215}$$
$$= \left(G_{Z_n} \circ G\right)(t) \tag{6.216}$$

On a donc :

$$G_{Z_n}(t) = G_X^{\circ n}(t) \tag{6.217}$$

En particulier on déduit :

$$\begin{cases} \alpha_0 = 0 \\ \alpha_{n+1} = G(\alpha_n) \end{cases} \tag{6.218}$$

Quelques propriétés de G, et hypothèses sur X (i) On sait déjà que G est une série entière de rayon de convergence plus grand que 1, donc C^∞ sur $[0,1[$.

(ii) Comme la série G est à coefficients positifs et que $G(1) = 1$ on déduit que G est continue en 1. (permutation de sup)

La suite α_n converge donc vers un point fixe de G

(iii) Une autre permutation de suprema permet de déduire que G est croissante sur $[0,1]$.

La suite α_n converge donc vers le plus petit point fixe de G

(iv) On sait de plus que G est convexe comme supremum de fonctions convexes. On peut éviter le cas où G est une droite, et supposer que la série contient au moins un terme d'ordre ≥ 2. On constate alors que $G'' > 0$ sur $]0,1[$ et donc G est *strictement convexe.* [15]

(v) On sait par positivité que $\lim G'(t)$ existe et peut valoir $+\infty$. On remarque aisément que $G'(t) = \mathbf{E}(X)$ dans $\overline{\mathbb{R}_+}$.

En effet, on a d'une part

$$\sum_{n\leq N} \mathbf{P}(X=n)\frac{t^n-1}{t-1} \leq \sup_{t\in[0,1]} \sum_{n\leq N} \mathbf{P}(X=n)\frac{t^n-1}{t-1} = \sum_{n\leq N} \mathbf{P}(X=n)n \leq \mathbf{E}(X) \tag{6.219}$$

Et d'autre part les inégalités inverses

$$\sum_{n\leq N} \mathbf{P}(X=n)\frac{t^n-1}{t-1} \leq G'(t) \tag{6.220}$$

Traitons le cas $\mathbf{E}(X) \leq 1$. Dans ce cas, on sait que G est strictement croissante, et donc que G est strictement au dessus de sa tangente en 1 pour $t \neq 1$. C'est-à-dire :

15. Dans le cas où G donne une droite, on peut directement comprendre que soit le seul point fixe est 1, soit le plus petit point fixe est zéro.

$$\forall t \in [0,1[, G(t) > G'(1)(t-1) + G(1) \tag{6.221}$$

On obtient alors en faisant une soustraction par t :

$$G(t) - t > G'(1)(t-1) - (t-1) \tag{6.222}$$

Et donc

$$G(t) - t > (t-1)(G'(1) - 1) \geq 0 \tag{6.223}$$

Ainsi, on déduit qu'il n'y a pas de point fixe strictement plus petit que 1.

Traitons le cas $\mathbf{E}(X) > 1$. Au voisinage de 1, que l'espérance soit finie ou non, on a G qui est au dessous de sa corde, et donc au dessous de l'identité. Comme $G(0) \geq 0$ on déduit alors que G possède au moins un point fixe strictement plus petit que 1 via le théorème des valeurs intermédiaires.

Si jamais il y avait deux tels points fixes, s_1 et s_2, alors $G' - 1$ s'annule en ses deux points, mais comme G est strictement convexe, G' est strictement croissante sur $]0,1[$ et c'est absurde.

6.16.2 Remarques

Peut-on faire exactement la même chose avec des fonctions caractéristiques ?

6.17 ■ NOMBRES DE BELL

Référence : FGN Algèbre 1, page 14. Recasé 2 fois

■ **LEÇONS**

L190 MÉTHODES COMBINATOIRES ET DÉNOMBREMENT ★★★★★

L243 CONVERGENCE DES SÉRIES ENTIÈRES, PROPRIÉTÉS DE LA SOMME. EXEMPLES ET APPLICATIONS. ★★★★★

■ **RÉFÉRENCES**

FGN Algèbre 1 page 14

6.17.1 Développement

On définit B_n comme le nombre de partitions de $[\![1,n]\!]$. C'est-a-dire le cardinal de A_n où

$$A_n = \left\{ X \subseteq \mathscr{P}([\![1,n]\!]) \mid \bigsqcup_{x\in X} x = [\![1,n]\!] \right\} \tag{6.224}$$

On pose par convention $B_0 = 1$.

Calculs de premiers termes On calcule aisément $B_1 = 1$, et $B_2 = 2$.

On constate que $A_3 = \{\{\emptyset,\{1,2,3\}\},\{1,\{2,3\}\},\{2,\{1,3\}\},\{3,\{1,2\}\}\}$. Et donc $A_3 = 4$.

Formule de récurrence Soit $n \in \mathbb{N}^*$ et $k \in [\![1,n]\!]$. On note E_k l'ensemble des $X \in A_{n+1}$ tels que l'ensemble contenant $n+1$ est de taille k.

$$A_{n+1} = \bigsqcup_{k=1}^{n+1} E_k \tag{6.225}$$

Et donc

$$B_{n+1} = \sum_{k=1}^{n+1} |E_k| \tag{6.226}$$

Or, il est évident que $|E_k| = \binom{n}{k-1} \times B_{n+1-k}$ puisqu'on sélectionne les voisins de $n+1$, et une partition des éléments restants.

Ainsi

$$B_{n+1} = \sum_{k=1}^{n+1} \binom{n}{k-1} B_{n+1-k} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} = \sum_{k=0}^{n} \binom{n}{k} B_k \tag{6.227}$$

Construction de la série génératrice

$$f(x) = \sum_{n\geq 0} B_n \frac{x^n}{n!} \tag{6.228}$$

Montrons que cette fonction est bien définie sur $[0,1[$. Pour cela il suffit de remarquer que $B_n \leq n!$ et constater que c'est une série entière de rayon de convergence supérieur à 1.

En effet, on a l'injection suivante de A_n dans S_n qui à une partition X associe le produit de cycles à supports disjoints où chaque cycle est un cycle sur un élément de X.

Équation différentielle vérifiée par la série Sur l'intervalle $[0,1[$ la fonction f est C^∞ et on peut dériver terme à termes.

$$f'(x) = \sum_{n\geq 1} B_n n \frac{x^{n-1}}{n!} \tag{6.229}$$
$$= \sum_{n\geq 0} B_{n+1} \frac{x^n}{n!} \tag{6.230}$$
$$= \sum_{n\geq 0} \sum_{k=0}^{n} \binom{n}{k} B_k \frac{x^n}{n!} \tag{6.231}$$
$$= \sum_{n\geq 0} \sum_{k=0}^{n} B_k \frac{x^n}{k!(n-k)!} \tag{6.232}$$
$$= \sum_{n\geq 0} x^n \sum_{k=0}^{n} \frac{B_k}{k!} \frac{1}{(n-k)!} \tag{6.233}$$
$$= \left(\sum_{n\geq 0} \frac{B_n}{n!} x^n\right)\left(\sum_{n\geq 0} \frac{1}{n!} x^n\right) \qquad \text{Produit de Cauchy} \tag{6.234}$$
$$= f(x)e^x \tag{6.235}$$

Étude de la solution On résout facilement cette EDO linéaire d'ordre 1

$$f(x) = \frac{f(0)}{e} e^{e^x} = \frac{1}{e} e^{e^x} \tag{6.236}$$

On va donc étudier e^{e^x},

$$e^{e^x} = \sum_{n\geq 0} \frac{(e^x)^n}{n!} \tag{6.237}$$
$$= \sum_{n\geq 0} \frac{e^{nx}}{n!} \tag{6.238}$$
$$= \sum_{n\geq 0} \sum_{k\geq 0} \frac{(nx)^k}{n!} \tag{6.239}$$

On veut utiliser Fubini, et pour cela on étudie la somme suivante :

$$\sum_{n\geq 0} \sum_{k\geq 0} \left|\frac{(nx)^k}{n!}\right| = \sum_{n\geq 0} \frac{\left(e^{|x|}\right)^n}{n!} \tag{6.240}$$
$$= e^{e^{|x|}} < +\infty \tag{6.241}$$

Donc on peut continuer notre calcul

$$\sum_{n\geq 0} \sum_{k\geq 0} \frac{(nx)^k}{n!} = \sum_{k\geq 0} \sum_{n\geq 0} \frac{(nx)^k}{n!} \tag{6.242}$$
$$= \sum_{k\geq 0} \frac{x^k}{k!} \left(\sum_{n\geq 0} \frac{n^k}{n!}\right) \tag{6.243}$$
$$= \sum_{n\geq 0} \frac{x^n}{n!} \left(\sum_{k\geq 0} \frac{k^n}{k!}\right) \tag{6.244}$$
$$\tag{6.245}$$

Conclusion On peut alors conclure car $f(x) = \frac{1}{e}e^{e^x}$ sur $[0,1[$, par unicité du DSE on déduit que le rayon de convergence de f est en réalité $+\infty$ et que

$$\frac{B_n}{n!} = \frac{1}{en!}\sum_{k\geq 0}\frac{k^n}{k!} \tag{6.246}$$

$$B_n = \frac{1}{e}\sum_{k\geq 0}\frac{k^n}{k!} \tag{6.247}$$

6.17.2 Remarques

Donner un équivalent est difficile

On peut trouver en triffouillant $\ln B_n \sim n\ln n$ ce qui ne donne pas d'équivalent de B_n mais dit en gros que ça devrait pas être trop loin de n^n au final.

6.18 ■ SUITES À CONVERGENCE LENTE

Référence : FGN Analyse 1, page 99. Recasé 5 fois

■ **LEÇONS**

L218 APPLICATION DES FORMULES DE TAYLOR ★★★★★

L223 SUITES NUMÉRIQUES. CONVERGENCE, VALEURS D'ADHÉRENCE. EXEMPLES ET APPLICATIONS. ★★★★★

L224 EXEMPLES DE DÉVELOPPEMENTS ASYMPTOTIQUES DE SUITES ET DE FONCTIONS.★★★★★

L226 SUITES VECTORIELLES ET RÉELLES DÉFINIES PAR UNE RELATION DE RÉCURRENCE UN+1 = F(UN). EXEMPLES. APPLICATIONS À LA RÉSOLUTION APPROCHÉE D'ÉQUATIONS. ★★★★★

L230 SÉRIES DE NOMBRES RÉELS OU COMPLEXES. COMPORTEMENT DES RESTES OU DES SOMMES PARTIELLES DES SÉRIES NUMÉRIQUES. EXEMPLES. ★★★★★

■ **RÉFÉRENCES**

FGN Analyse 1 page 99

6.18.1 Prérequis

1. Savoir faire un DL d'une fonction classique

$$(1+x)^\alpha = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2}x^2 + \dots \tag{6.248}$$

$$\sin x = x - \frac{x^3}{3} + \frac{x^5}{120} - \frac{x^7}{7!}\dots \tag{6.249}$$

2. Sommation des relations de comparaison
3. Théorème de Cesaro

6.18.2 Développement

On fixe $c > 0$, on note $I = [0, c]$ et on considère $f : I \to I$ une fonction continue. On suppose de plus qu'au voisinage de zéro il existe un $\alpha > 1$ et $a > 0$ tels que

$$f(x) = x - ax^\alpha + o\left(x^\alpha\right) \tag{6.250}$$

On pose $u_0 \in I$ et $u_{n+1} = f(u_n)$.

Si u_0 est assez petit, la suite u_n converge vers zéro. En effet, on peut passer à la limite dans le développement asymptotique par continuité de f pour trouver

$$f(0) = 0 \tag{6.251}$$

Par la suite, on remarque que $f(x) - x$ est strictement négatif sur un voisinage épointé de zéro, car

$$f(x) - x = -ax^\alpha + o\left(x^\alpha\right) \tag{6.252}$$

Ainsi, il existe un $\eta > 0$ tel que

$$\forall 0 < x < \eta, f(x) < x \tag{6.253}$$

La suite u_n est alors décroissante si $u_0 < \eta$. Elle est de plus minorée par 0, elle converge donc. Par continuité de f elle converge vers un point fixe, qui est nécessairement 0 : c'est le seul point fixe de f sur $[0,\eta[$ (puisque sinon $f(x) < x$).

Déterminons un équivalent de u_n On essaie de savoir à quelle vitesse décroit u_n, pour cela on remarque que

$$u_{n+1} - u_n = -au_n^\alpha + o\left(u_n^\alpha\right) \tag{6.254}$$

Cette décroissance est donc d'autant plus lente que u_n devient petit car $a > 0$ et $\alpha > 1$.
Pour se ramener à un pas presque constant on décide de renormaliser l'échelle : on pose $v_n = u_n^\beta$, et on recherche un β tel que $v_{n+1} - v_n$ soit constant.

$$\begin{aligned} v_{n+1} - v_n &= \left(u_n - au_n^\alpha + o\left(u_n^\alpha\right)\right)^\beta - u_n^\beta && (6.255)\\ &= u_n^\beta\left(\left(1 - au_n^{\alpha-1} + o\left(u_n^{\alpha-1}\right)\right) - 1\right) && (6.256)\\ &= u_n^\beta\left(-a\beta u_n^{\alpha-1} + o\left(u_n^{\alpha-1}\right)\right) && (6.257)\\ &\sim -a\beta u_n^{\alpha+\beta-1} && (6.258) \end{aligned}$$

On considère donc $\beta = 1 - \alpha$, ce qui était plus ou moins logique, vu que la décroissance était à la puissance α.
On a alors :

$$v_{n+1} - v_n \longrightarrow a(\alpha - 1) > 0 \tag{6.259}$$

On utilise le théorème de sommation des équivalents positifs (ou le théorème de Cesaro) pour déduire

$$\sum_{k<n} v_{k+1} - v_k \sim na(\alpha - 1) \tag{6.260}$$

Ce qui montre alors que

$$u_n^\beta - u_0^\beta \sim na(\alpha - 1) \tag{6.261}$$

Comme les suites tendent vers $+\infty$, il est clair que le terme constant u_0^β ne joue pas, et donc

$$u_n^\beta \sim na(\alpha - 1) \tag{6.262}$$

Cela montre alors

$$\boxed{u_n \sim (na(\alpha - 1))^{\frac{1}{1-\alpha}}} \tag{6.263}$$

Considérons un cas particulier On se place sur $I = \left[0, \frac{\pi}{2}\right]$ qui est stable par la fonction sin, le développement en zéro de cette fonction est

$$\sin x = x - \frac{x^3}{6} + o\left(x^3\right) \tag{6.264}$$

C'est-à-dire $a = \frac{1}{6} > 0$ et $\alpha = 3 > 1$. De plus, si $x > 0$, $\sin x < x$, donc la suite converge pour $u_0 \in I$ vers zéro.
Enfin, en appliquant notre théorème :

$$u_n \sim \left(n\frac{1}{6}(3-1)\right)^{\frac{1}{1-3}} = \sqrt{\left(\frac{3}{n}\right)} \tag{6.265}$$

Si on veut un terme de plus ... On peut itérer la méthode ! On écrit alors

$$\sin x = x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^5) \tag{6.266}$$

Et on considère de nouveau

$$\frac{1}{u_{n+1}^2} - \frac{1}{u_n^2} \tag{6.267}$$

On trouve alors :

$$\sin u_n = u_n \left(1 - \frac{u_n^2}{6} + \frac{u_n^4}{120} + o(u_n^4)\right) \tag{6.268}$$

D'où après calcul :

$$\frac{1}{u_{n+1}^2} = \frac{1}{(\sin u_n)^2} = \frac{1}{u_n^2} \frac{1}{\left(1 - \frac{u_n^2}{6} + \frac{u_n^4}{120} + o(u_n^4)\right)^2} \tag{6.269}$$

$$= \frac{1}{u_n^2}\left(1 - 2\left(\frac{-u_n^2}{6} + \frac{u_n^4}{120}\right) + 3\left(\frac{-u_n^2}{6} + \frac{u_n^4}{120}\right)^2 + o(u_n^4)\right) \tag{6.270}$$

$$= \frac{1}{u_n^2}\left(1 + \frac{u_n^2}{3} + \frac{u_n^4}{15} + o\left(u_n^4\right)\right) \tag{6.271}$$

On déduit alors directement

$$u_{n+1}^\beta - u_n^\beta - \frac{1}{3} \sim \frac{u_n^2}{15} \tag{6.272}$$

Et en injectant l'équivalent de u_n on déduit

$$u_{n+1}^\beta - u_n^\beta - \frac{1}{3} \sim \frac{1}{5n} \tag{6.273}$$

Ce qui en utilisant le théorème de sommation des équivalents (positifs) donne alors (en utiliant H_n)

$$u_n^\beta - \frac{n}{3} \sim \frac{1}{5}\log n \tag{6.274}$$

De là on déduit

$$u_n = \left(\frac{n}{3} + \frac{\log n}{5} + o(\log n)\right)^{-\frac{1}{2}} \tag{6.275}$$

$$= \sqrt{\frac{3}{n}}\left(1 + \frac{3\log n}{5n} + o\left(\frac{\log n}{n}\right)\right)^{-\frac{1}{2}} \tag{6.276}$$

$$\sim \sqrt{\frac{3}{n}} - \sqrt{\frac{3}{n}}\frac{1}{2}\frac{3\log n}{5n} + o\left(\frac{\log n}{n\sqrt{n}}\right) \tag{6.277}$$

$$\tag{6.278}$$

6.18.3 Remarques

La vision "accroissements finis" du FGN Quand on écrit $u_{n+1} - u_n \sim -a u_n^{\alpha}$ on écrit

$$(u_{n+1} - u_n)\, u_n^{-\alpha} \sim -a \tag{6.279}$$

Or $g' : x \mapsto x^{-\alpha}$ est la dérivée à une constante près de $g : x \mapsto x^{1-\alpha}$. On a donc approximativement en utilisant le théorème des accroissements finis :

$$-a \sim (u_{n+1} - u_n)\, g'(u_n) \approx g(u_{n+1}) - g(u_n) \tag{6.280}$$

Il devient alors naturel d'étudier $g(u_n)$...

Il est beaucoup plus simple de prendre comme exemple $f(x) = \log(1+x)$ puisque les développements font intervenir beaucoup moins de fractions ...

6.19 ■ MÉTHODE DE LAPLACE

Référence : Rouvière , ZQ , Faraut. Recasé 4 fois

■ **LEÇONS**

L224 EXEMPLES DE DÉVELOPPEMENTS ASYMPTOTIQUES DE SUITES ET DE FONCTIONS. ★★★★

L228 CONTINUITÉ ET DÉRIVABILITÉ DES FONCTIONS RÉELLES ★

L236 ILLUSTER DES MÉTHODES DE CALCUL D'INTÉGRALES (PLUSIEURS VARIABLES) ★★★

L239 INTÉGRALES À PARAMÈTRE ★★★★★

■ **RÉFÉRENCES**

ZQ

Rouvière page 344

6.19.1 Développement

On considère $I = [a, b[$ un intervalle de $\mathbb{R}$, $\phi : I \to \mathbb{R}$ et $f : I \to \mathbb{C}$.
On pose

$$F(\lambda) = \int_I e^{-\lambda\phi(x)} f(x)\,dx \tag{6.281}$$

On suppose que pour $\lambda \geq \lambda_0$ on a $F(\lambda)$ qui converge absolument, c'est-à-dire que $e^{-\lambda\phi(x)f(x)}$ est intégrable.

L'objectif est d'étudier le comportement de F quand $\lambda \to +\infty$.

Trouvons la masse Le terme exponentiel écrase tout assez vite quand $\lambda \to +\infty$. La contribution majoritaire va donc se faire quand $\phi(x)$ est minimale. Ce qui justifie le bloc suivant.

> Supposons que ϕ vérifie les hypothèses suivantes : $\phi' > 0$ sur $I - \{a\}$, $\phi'(a) = 0$ et $\phi''(a) > 0$. On ajoute que f est continue en a et $f(a) \neq 0$.

Étude de ϕ Alors localement ϕ s'écrit

$$\phi(x) = \phi(a) + 0 + \frac{1}{2}\phi''(a)(x-a)^2 + o\left((x-a)^2\right) \tag{6.282}$$

On a donc un terme en $e^{-\lambda\phi(a)}$, et un terme qui se comporte au voisinage de a comme $(x-a)^2$.
Cela justifie d'étudier dans un premier temps le terme en $(x-a)^2$, et pour simplifier encore de considérer $a = 0$...

Le cas particulier On considère donc $\boxed{\phi(x) = x^2}$. Les précédentes remarques invitent à découper l'intégrale au voisinage de zéro, et en dehors.

On se sert de la continuité de f au voisinage de 0 pour obtenir $\eta > 0$ et $M > 0$ tels que

$$\forall x \in I, x \leq \eta \implies |f(x)| \leq M \tag{6.283}$$

On a alors

$$\int_0^\eta e^{-\lambda x^2} f(x)\,dx = \frac{1}{\sqrt{\lambda}} \int_0^\eta e^{-u^2} f\left(\frac{u}{\sqrt{\lambda}}\right) du \tag{6.284}$$

Par convergence dominée, on déduit alors

$$\int_0^{\eta\sqrt{\lambda}} e^{-u^2} f\left(\frac{u}{\sqrt{\lambda}}\right) du \longrightarrow \int_0^{+\infty} e^{-u^2} f(0)\,du \tag{6.285}$$

En utilisant la valeur de l'intégale de Gauss on déduit donc

$$\int_0^\eta e^{-\lambda x^2} f(x)dx \sim \frac{f(0)}{2}\sqrt{\frac{\pi}{\lambda}} \tag{6.286}$$

Dans le cas général On veut se ramener au cas particulier, et au vu du développement limité, il est très naturel de poser le changement de variable suivant

$$\phi(x) = \phi(a) + 0 + \frac{1}{2}\phi''(a)(x-a)^2 + o\left((x-a)^2\right) \tag{6.287}$$

$$\Phi(x) = \sqrt{\phi(x) - \phi(a)} \tag{6.288}$$

(i) On constate que Φ est bien C^1 sur $I - \{a\}$ par simple composition et que

$$\Phi'(x) = \frac{\phi'(x)}{2\sqrt{\phi(x) - \phi(a)}} > 0 \tag{6.289}$$

(ii) En utilisant le développement limité, on considère la limite comme suit

$$\frac{\phi'(x)}{\sqrt{2}\sqrt{(x-a)^2(\phi''(a) + o(1))}} = \frac{\phi'(x)}{\sqrt{2}(x-a)\sqrt{\phi''(a) + o(1))}} \tag{6.290}$$

Comme $\phi'(x) = 0 + \phi''(a)\frac{(x-a)}{2} + o(x-a)$
On en déduit que

$$\Phi'(x) \longrightarrow \sqrt{\frac{\phi''(a)}{2}} > 0 \qquad (x \to 0) \tag{6.291}$$

On a donc Φ qui est C^1 sur I et de différentielle inversible. C'est donc un C^1-difféomorphisme (inversion locale) et on conclut donc à un "lemme de Morse en une variable" :

$$\phi(x) = \phi(a) + \Phi(x)^2 \tag{6.292}$$

On note ψ l'application réciproque, en posant $x = \psi(u)$ on a le changement de variables

$$F(\lambda) = \int_a^b e^{-\lambda(\phi(a)+\Phi(x)^2} f(x)dx = e^{-\lambda\phi(a)} \int_{\Phi(I)} e^{-tu^2} f(\psi(u))|\psi'(u)|du \tag{6.293}$$

On déduit alors qu'il existe $c > 0$ tel que

$$F(\lambda) = e^{-\lambda\phi(a)} \int_0^c e^{-tu^2} f(\psi(u))\psi'(u)du \tag{6.294}$$

En appliquant le théorème démontré pour le cas particulier, on a alors

$$F(\lambda) \sim e^{-\lambda\phi(a)} \frac{f(\psi(0))\psi'(0)}{2}\sqrt{\frac{\pi}{\lambda}} = e^{-\lambda\phi(a)} f(a)\sqrt{\frac{1}{2\phi''(a)}}\sqrt{\frac{\pi}{\lambda}} \tag{6.295}$$

Application à Γ

$$\Gamma(t+1) = \int_0^\infty x^t e^{-x} dx = \int_0^\infty \exp\left(-[x - t\ln(x)]\right) \tag{6.296}$$

Ce n'est pas une intégrale sous la bonne forme pour appliquer notre théorème. Toutefois, on peut essayer de calculer le minimum de la fonction pour effectuer un changement de variable qui "suit" ce minimum.

On pose $g_t(x) = x - t\ln x$ on calcule $g_t'(x) = 1 - t/x$. Cela montre que g_t est strictement convexe sur $\mathbb{R}^+$ avec un minimum en 1, c'est-à-dire quand $x = t$.
On pose donc $u = x/t$, avec $dx = tdu$, ce qui donne

$$\Gamma(t+1) = \int_0^\infty \exp\left(-[tu - t\ln(tu)]\right) tdu = t^{t+1}\int_0^\infty \exp\left(-t[u - \ln(u)]\right) du \tag{6.297}$$

Il suffit alors de couper l'intégrale au niveau de 1, et d'utiliser deux fois le théorème pour obtenir :

$$\Gamma(t+1) \sim t^{t+1} \times 2 \times e^{-t\phi(1)} \sqrt{\frac{1}{2\phi''(1)}} \sqrt{\frac{\pi}{t}} \tag{6.298}$$

Or il est clair que $\phi(1) = 1$ et $\phi''(1) = 1$, donc

$$\Gamma(t+1) \sim t^t e^{-t}\sqrt{2\pi t} \tag{6.299}$$

Ce qui donne la formule de Stirling

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n} \tag{6.300}$$

6.19.2 Annexes

Améliorations On peut se ramener à ϕ admettant un minimum local strict en a et avoir le même équivalent

6.20 ■ INVERSION DE FOURIER L1

Référence : Faraut + Zuily Quéffelec. Recasé 3 fois

■ **LEÇONS**

L236 ILLUSTER DES MÉTHODES DE CALCUL D'INTÉGRALES (PLUSIEURS VARIABLES) ★★★★★

L239 INTÉGRALES À PARAMÈTRE ★★★★★

L250 TRANSFORMATIONS DE FOURIER ★★★★★

■ **RÉFÉRENCES**

Faraut qui fait le côté inversion de Fourier, mais avec des noyaux de poisson (ce qui revient au même)

ZQ pour le calcul du noyau gaussien via l'holomorphie

6.20.1 Prérequis

Intégrale de Gauss Se calcule via l'intégrale $\int e^{-x^2-y^2}\,dxdy$ plus fubini plus changement de variables polaires.

Holomorphie sous signe intégral

6.20.2 Développement

Transformée de Fourier d'une Gaussienne

$$g_\sigma(x) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{x^2}{2\sigma}\right) \tag{6.301}$$

Et $g = g_1$. On pose alors $G : \mathbb{C} \to \mathbb{R}$ comme suit :

$$G(z) = \int_{\mathbb{R}} e^{-x^2} e^{zx}\,dx \tag{6.302}$$

La fonction G est holomorphe sur $\mathbb{C}$ et en particulier elle est bien définie.

En effet, l'intégrande est un produit de fonctions holomorphes sur $\mathbb{C}$.

Considérons maintenant un compact K de $\mathbb{C}$ de diamètre R. On sait que

$$|e^{zx-x^2}| = \exp\left(x\Re z - x^2\right) \tag{6.303}$$

Mais alors

Pour $|x| \leq 2R$ On peut majorer la fonction par une constnate car elle est holomorphe et donc continue sur un compact

Pour $|x| > 2R$ On remarque que

$$\begin{aligned} x\Re(z) - x^2 &\leq |x\Re z| - |x|^2 && (6.304)\\ &\leq |x|R - x^2 && (6.305)\\ &\leq -\frac{|x|^2}{2} && (6.306) \end{aligned}$$

On peut donc majorer la valeur absolue de l'intégrande par une fonction intégrable sur $\mathbb{R}$ et appliquer le théorème d'holomorphie sous signe somme.

Pour $z \in \mathbb{R}$ on a un calcul explicite En effet, on utilise la valeur de l'intégrale de Gauss

$$G(z) = \int_{\mathbb{R}} e^{zx-x^2} dx = \int_{\mathbb{R}} e^{-(x-z/2)^2+z^2/4} dx = \sqrt{\pi} e^{z^2/4} \tag{6.307}$$

Par prolongement analytique on déduit une expression de G Les deux fonctions étant clairement holomorphes, et coincidant sur $\mathbb{R}$ qui possède un point d'accumulation on déduit qu'elles sont égales sur $\mathbb{C}$.

On en déduit une expression de la transformée de Fourier

$$\widehat{e^{-x^2}}(t) = G(-it) = \sqrt{\pi} e^{-t^2/4} \tag{6.308}$$

On généralise pour g_σ

$$\widehat{g_\sigma}(t) = \int_{\mathbb{R}} \frac{1}{\sqrt{2\pi\sigma}} e^{-x^2/(2\sigma)-itx} dx = \frac{1}{\sqrt{\pi}} \int_{\mathbb{R}} e^{-u^2-iu2\sigma t} du = \exp\left(-\frac{\sigma t}{2}\right) \tag{6.309}$$

Application à l'inversion de Fourier L^1

Pourquoi définir k_σ ? C'est inutile...

On définit le noyau de convolution gaussien On pose $k_\sigma = g_{\sigma^2}$.

On constate qu'il vérifie

$$\widehat{k_\sigma}(t) = \sqrt{2\pi\sigma^2} k_{1/\sigma} \tag{6.310}$$

Cela prouve directement que

$$\widehat{\widehat{k_\sigma}}(t) = 2\pi k_\sigma(-t) \tag{6.311}$$

On a donc bien la formule d'inversion L^1 sur les gaussiennes.

Si $f \in L^1$ et $\hat{f} \in L^1$ alors On peut convoler par k_σ, utiliser l'inversion de Fourier sur les gaussiennes, puis fubini pour conclure :

$$(k_\sigma \star f)(x) = \frac{1}{2\pi} \int_{\mathbb{R}} \widehat{k_\sigma}(t) \hat{f}(t) e^{itx} dt \tag{6.312}$$

On applique le théorème de convolution car k_σ est une approximation de l'unité (convergence dominée) On a donc $k_\sigma \star f \to f$ en convergence L^1

On peut donc conclure par convergence dominée car $\widehat{k_\sigma}(t) = \widehat{k}(\sigma t)$ donc

$$k_\sigma \star f \to \frac{1}{2\pi} \int_{\mathbb{R}} \hat{f}(t) e^{itx} dt \tag{6.313}$$

En effet il est possible d'utiliser la convergence dominée car $\hat{f}$ est intégrable !

On peut alors conclure en utilisant le théorème de Reiz-Fréchet qui démontre l'existence d'une sous-suite qui converge vers f presque partout. Il y a alors égalité pour l'inversion de Fourier presque partout.

6.20.3 Annexes

6.21 ■ THÉORÈME D'HADAMARD LÉVY

Référence : ZQ page 399. Recasé 4 fois

■ **LEÇONS**

L203 UTILISATION DE LA NOTION DE COMPACITÉ. ★★★★

L214 THÉORÈME D'INVERSION LOCALE, THÉORÈME DES FONCTIONS IMPLICITES. EXEMPLES ET APPLICATIONS EN ANALYSE ET EN GÉOMÉTRIE. ★★★★

L215 APPLICATIONS DIFFÉRENTIABLES DÉFINIES SUR UN OUVERT DE RN. EXEMPLES ET APPLICATIONS. ★★★★

L220 ÉQUATIONS DIFFÉRENTIELLES GÉNÉNRALES. EXEMPLES DIM 1 ET 2 ★★★★

■ **RÉFÉRENCES**

Zavidovique

Zuily Queffélec page 399

6.21.1 Prérequis

Lemme 99 (Gronwall)**.** *Si ϕ et ψ sont des fonctions positives sur $I=[a,b]$ qui vérifient*

$$\phi(t) \leq A + B\int_a^t \psi(s)\phi(s)ds \tag{6.314}$$

Alors

$$\phi(t) \leq A\exp\left(B\int_a^t \psi(s)ds\right) \tag{6.315}$$

Démonstration. Considérer le quotient des deux majorations, c'est une fonction dérivable strictement décroissante, et donc la majoration déduite est toujours au dessus de la majoration supposée ... □

Théorème 100 (Cauchy-Lipschitz)**.** *Le système $X' = F(t,X)$ où F est localement-lip en la seconde variable admet une unique solution vérifiant $X(t_0) = x_0$ et cette solution est C^1.*

Théorème 101 (Sortie de tout compact)**.** *Sortie de tout compact ZQ*

Théorème 102 (Inégalité des Accroissements Finis)**.** *Si $f : I \to E$ et $g : I \to \mathbb{R}$ vérifient $\|f'(t)\| \leq g'(t)$, alors*

$$\|f(b) - f(a)\| \leq g(b) - g(a) \tag{6.316}$$

Remarque. *On déduit le cas vectoriel vers vectoriel en appliquant ce théorème à $F : I \to E$ $F(t) = f(tx + (1-t)y)$ en fixant x et y.*

Lemme 103 (Fonction propres)**.** *Une fonction f vérifie que la pré-imaa pré-imagee de tout compact est compacte si et seulement si $|f(x)| \to +\infty$ quand $x \to +\infty$.*

6.21.2 Développement

On considère $f \in \mathscr{C}^2(\mathbb{R}^n)$. On montre l'équivalence entre les deux propriétés suivantes

(i) f est un $\mathscr{C}^1$ difféomorphisme global

(ii) df_x est inversible pour tout x et f est propre, c'est-à-dire que la pré-image de tout compact est compacte

On commence par remarquer qu'un sens est évident. En effet si f est un difféomorphisme global, alors df_x est inversible pour tout x, et comme f^{-1} est continue, l'image de tout compact par f^{-1} est donc compacte, ce qui permet de conclure.

Pour le sens réciproque, on suppose $f(0) = 0$. Il suffit de construire g surjective de $\mathbb{R}^n$ dans $\mathbb{R}^n$ telle que $f \circ g = id$ pour déduire que f est un difféomorphisme global (puisqu'injectif et global).

Construction d'un flot On fixe $y \in \mathbb{R}^n$ et on pose

$$\begin{cases} \dot{x}(t) = (df_{x(t)})^{-1} y = F(x,t) \\ x(0) = 0 \end{cases} \tag{6.317}$$

L'application $F(x,t)$ est C1 par composition d'applications C^1 !

L'application $t \mapsto x(t,y)$ est bien définie En effet, on peut utiliser Cauchy-Lipschitz car $F(x,t)$ est C^1 et donc à y fixé il existe une solution maximale sur $I = [0, T^*[$.

La solution était en réalité globale De plus, pour $t \in I$ on a

$$\frac{d}{dt} f(x(t,y)) = df_{x(t,y)} \dot{x}(t,y) = df_{x(t,y)} (df_{x(t,y)})^{-1} y = y \tag{6.318}$$

Ainsi, comme $f(x(0,y)) = 0$, on déduit en résolvant une équation différentielle linéaire d'ordre 1 que

$$\forall t \in [0, T^*[, f(x(t,y)) = ty \tag{6.319}$$

En particulier $x(t,y) \in f^{-1}(B(0, T^* y)$.

Supposons par l'absurde que $T^* < +\infty$, on a alors contrôlé $x(t,y)$ dans un compact, ce qui est absurde au vu du théorème de sortie de tout compact !

Ainsi $T^* = +\infty$.

Définition de la fonction g On pose $g(y) = x(1,y)$ ce qui est possible au vu des résultats précédents.

On sait de plus que $f \circ g = id$ sur $\mathbb{R}^n$, mais il reste à montrer que g est surjective ! Pour cela on va d'abord montrer que g est continue.

La fonction g est en réalité continue C'est la partie dure de ce développement.

Déjà, on remarque que si $0 \leq t \leq 1$ alors $x(t,y) \in f^{-1}(B(0, |y|))$ (via les magouilles d'avant).

Fixons y_0. Supposons alors $|y - y_0| \leq 1$, et posons $K_0 = f^{-1}(B(0, |y_0| + 1))$. Il est clair que les $x(t,y)$ et $x(t,y_0)$ sont dans K_0, mais on va poser B_0 une boule contentant K_0 afin d'avoir un compact *connexe*.

$$\dot{x}(t,y_0) - \dot{x}(t,y) = (df_{x(t,y_0)})^{-1} y_0 - (df_{x(t,y)})^{-1} y \tag{6.320}$$

$$= (df_{x(t,y_0)})^{-1} (y_0 - y) + \left(df^{-1}_{x(t,y_0)} df^{-1}_{x(t,y)} \right) y \tag{6.321}$$

L'application $x \mapsto df_x$ est continue par hypothèse, et la fonction inverse aussi, donc $x \mapsto (df_x)^{-1}$ est continue, donc de norme triple bornée par un M_{y_0} sur le compact B_0.

Pour le second terme, on remarque que cela se ré-écrit $F(x(s,y_0)) - F(x(s,y))$. Mais comme F est C^1, on peut utiliser l'inégalité des accroissements finis sur le compact *convexe* B_0

$$\| F(x(t,y_0)) - F(x(t,y)) \| \leq C(y_0) \| x(t,y_0) - x(t,y) \| \tag{6.322}$$

On a alors montré :

$$\left\| \int_0^s \dot{x}(t,y_0) - \dot{x}(t,y) dt \right\| \leq \int_0^s M_{y_0} \| y - y_0 \| dt + \int_0^s C(y_0) \| x(t,y_0) - x(t,y) \| dt \tag{6.323}$$

On déduit donc

$$\|x(t,y_0)-x(t,y)\| \leq M_{y_0}\|y-y_0\| + C(y_0)\int_0^s \|x(t,y_0)-x(t,y)\|\,dt \tag{6.324}$$

On peut alors utiliser le lemme de Gronwall à y fixé sur la fonction $\phi(t) = \|x(t,y_0)-x(t,y)\|$ pour déduire

$$\|x(t,y_0)-x(t,y)\| \leq M_{y_0}\|y-y_0\| \exp\big(C(y_0)t\big) \tag{6.325}$$

Ce qui permet de conclure vu que la fonction g est continue.

La fonction g est donc surjective Pour cela on montre que $g(\mathbb{R}^n)$ est ouvert et fermé (car il est clairement non vide).

(i) On a l'égalité $g(\mathbb{R}^n) = g(f(g(\mathbb{R}^n)))$ ce qui montre qu'une suite dans $g(\mathbb{R}^n)$ qui converge converge bien dans $g(f(\mathbb{R}^n))$ c'est à dire dans $g(\mathbb{R}^n)$ via la continuité de f et g.

(ii) Soit $x_0 \in g(\mathbb{R}^n)$, alors on a $g(y_0) = x_0$ pour un certain y_0.

FAIRE UN PUTAIN DE DESSIN ICI

En particulier $f(x_0) = y_0$, et par le théorème d'inversion locale, on a des voisinages ouverts de x_0 et de y_0 où f est un C^1-difféo.

Or, g étant continue, on peut restreindre le voisinage autour de y_0 afin que g l'envoie dans le voisinage de x_0.

Les fonctions g et f^{-1} définies sur ces domaines et co-domaines sont deux inverses de f, et donc coïncident.

En particulier, l'image par g est l'image par un C^1-difféo et est donc ouverte.

Ainsi il existe un voisinage ouvert de x_0 inclus dans $g(\mathbb{R}^n)$.

On a donc $g(\mathbb{R}^n) = \mathbb{R}^n$.

On peut alors conclure Exactement comme dit avant.

6.21.3 Questions subsidiaires

Exemple 104. *Un exemple d'application*

Definition 105 (Flot)**.**

Théorème 106 (Théorèmes sur le flot)**.**

6.22 ■ THÉORÈME DE STURM LIOUVILLE

Référence : Bonne question. Recasé 2 fois

■ **LEÇONS**

L220 ÉQUATIONS DIFFÉRENTIELLES GÉNÉNRALES. EXEMPLES DIM 1 ET 2 ★★★★★

L221 ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES. SYSTÈMES. ★★★★★

■ **RÉFÉRENCES**

ZQ

Gourdon

6.22.1 Pré-requis

On veut étudier les équations de la forme

$$y'' + py' + qy = 0 \tag{6.326}$$

Le cas particulier Le cas particulier c'est quand p et q sont constants. On retrouve alors les phénomènes d'oscillateur harmonique amorti, ou bien hyperbolique amorti.

Résolution théorique Si p et q sont continues, alors on a affaire à un Cauchy-Lipschitz linéaire à coefficients continus, qui admet donc une unique solution *globale* sur l'intervalle de définition pour toute paire de conditions initiales.

Principe des zéros isolés Les zéros d'une solution non nulle d'une telle équation sont nécessairement isolés, car si α est un zéro de y qui n'est pas isolé, alors on a une suite α_k de zéros avec $\alpha_k \to \alpha$.

Mais alors les taux d'accroissements pris en les α_k montrent que $(y(\alpha_k) - y(\alpha))/(\alpha_k - \alpha) = 0$ et donc $y'(\alpha) = 0$. Or il existe une unique solution au problème de cauchy $y(\alpha) = 0$, $y'(\alpha) = 0$, et c'est la solution nulle.

Application des zéros isolés Si y non nulle possède une infinité de zéros. L'ensemble des zéros de y étant *fermé, discret,* dans chaque compact il ne peut y en avoir qu'un nombre fini. Donc on peut les ordonner (il sont dénombrables), et il y a des zéros à des distances arbitrairement grandes.

Wronsiken Le wronskien de deux solutions, noté $w(y_1, y_2)$ est le déterminant des deux vecteurs (y_1, y_1') et (y_2, y_2'). S'il est nul en un point, les deux solutions sont proportionnelles globalement (CL) et réciproquement, si les deux sont proportionnelle alors il est nul tout le temps.

Lemme des pentes Si $y > 0$ sur $]x_1, x_2[$ avec $y(x_1) = y(x_2) = 0$ alors on a nécessairement $y'(x_1) > 0$ et $y'(x_2) < 0$.

En effet, l'étude du taux d'accroissement nous indique que $y'(x_1) \geq 0$ et $y'(x_2) \leq 0$, et s'ils étaient nuls alors y serait nulle, et c'est absurde.

Prouver qu'on peut se ramener à étudier le cas $y'' + qy = 0$ dans STURM ...

6.22.2 Développement

Le théorème d'entrelacement de Sturm On pose $I = [a, b]$ un intervalle de $\mathbb{R}$ (possiblement $\mathbb{R}$ entier). On considère deux fonctions $q \leq r$ continues sur I.

$$y'' + qy = 0 \tag{E_1}$$

$$y'' + ry = 0 \tag{E_2}$$

On considère y une solution non nulle de (E_1) et z une solution non nulle de (E_2). Montrons qu'entre deux zéros de y il y a un zéro de z.

Démonstration. Soient $x_1 < x_2$ deux zéros consécutifs de y dans I, supposons par l'absurde que z n'ait pas de zéro dans $[x_1, x_2]$, on peut par sans restriction de généralité prendre $z > 0$ sur cet intervalle.
Alors, comme ce sont deux zéros consécutifs de y, on peut supposer sans restriction de généralité que $y > 0$ sur $]x_1, x_2[$.
En utilisant le lemme des pentes on déduit alors

$$y'(x_1) > 0 > y'(x_2) \tag{6.327}$$

Considérons alors le Wronskien mixte de y et z

$$w = yz' - zy' \tag{6.328}$$

C'est une application dérivable, et on remarque que

$$\begin{aligned} w'(x) &= y'z' + yz'' - z'y' - y''z \\ &= -yrz + rqy \\ &= yz(q - r) \end{aligned}$$

Donc le wronskien est négatif sur $[x_1, x_2]$. Toutefois, on remarque que $w(x_1) = -z(x_1)y'(x_1)$ est strictement négatif, et que $w(x_2) = -z(x_2)y'(x_2)$ est strictement positif. C'est absurde !
On a donc bien un zéro entre x_1 et x_2 pour z. □

Amélioration Supposons de plus que $z(x_1) = 0$, alors on peut appliquer le même raisonnement pour déduire qu'il existe un *autre* zéro dans $[x_1, x_2]$!

Conséquence On peut appliquer ce théorème à une unique équation par exemple (E_1) en prenant deux solutions non nulles y_1 et y_2.
On déduit alors qu'entre deux zéros de y_1 il y a un zéro de y_2. Mais en étudiant le wronskien de y_1 et y_2, si elles ne sont pas colinéaires, il est non nul, et donc les zéros sont *strictement entrelacés* car il s'annule sur un zéro commun à y_1 et y_2.

Théorème de Sturm périodique On suppose désormais q continue et périodique de période $\omega > 0$.
On va montrer qu'il n'y a que deux comportements possibles :

(i) Toute solution réelle possède au plus un zéro (hyperbolique)

(ii) Toute solution réelle possède une infinité de zéros (sinusoïdal)

Démonstration. Soit y une solution de (E_1) qui possède deux zéros $x_1 < x_2$. On pose $z(x) = y(x + n\omega)$ avec $n\omega > x_2 - x_1$.
La fonction $z(x)$ est clairement une solution de (E_1) puisque

$$z''(x) = y''(x + n\omega) = -q(x + n\omega)y(x + n\omega) = -q(x)z(x) \tag{6.329}$$

Par le théorème d'entrelacement, on déduit qu'il existe $x_1 \leq x_3 \leq x_2$ zéro de z.
Or, ce zéro pour z dit que $x_3 + n\omega$ est un zéro pour y. Mais

$$x_3 + n\omega > x_3 + x_2 - x_1 \geq x_2 \tag{6.330}$$

Donc on a trouvé un zéro strictement au dessus de x_1 et x_2 pour y.

L'ensemble des zéros de y n'étant pas majoré, on déduit qu'il est infini.

Enfin, si y_2 est une autre solution de (E_1), le principe des zéros entrelacés permet de déduire que y_2 possède aussi une infinité de zéros ! On est donc bien dans le cas (ii). □

Le cas particulier où $q \leq 0$ Dans ce cas là, même sans supposer q périodique, on peut montrer que les solutions possèdent un unique zéro, comme le montre le modèle $y'' - y = 0$.

Supposons par l'absurde que y ait au moins deux zéros, entre ces deux zéros on a $y'' = -qy$ qui est de signe constant, et sans restriction de généralité on peut supposer $y > 0$ donc $y'' > 0$ entre ces deux zéros.

On déduit donc que y' est strictement croissante sur cet intervalle. Toutefois, par le lemme des pentes, on déduit que $y'(x_1) > 0$ et $y'(x_2) < 0$, ce qui est absurde !

Le cas particulier où $q \geq 0$ et $q \neq 0$ Il suffit de fabriquer une solution avec 2 zéros pour conclure qu'on est dans le deuxième cas des équations périodiques.

On possède a tel que $q(a) > 0$ car il n'est pas nul. On prend y solution du problème de cauchy (E_1) $y(a) = 1$, $y'(a) = 0$.

Alors on a $y''(a) = -q(a)y(a) = -q(a) < 0$ et donc $y''(a) < 0$ sur un voisinage de a, donc y' strictement décroissante sur un voisinage de a. Or on sait que $y'(a) = 0$, donc il existe $a_1 < a < a_2$ tels que

$$y'(a_2) < 0 = y'(a) < y'(a_1) \tag{6.331}$$

Supposons par l'absurde qu'il n'y ait pas de zéros dans $[a, +\infty[$. On sait alors que y y est de signe constant, mais comme $y(a) > 0$, on déduit que $y > 0$ sur $[a, +\infty[$. Ainsi, on déduit que $y'(x)$ est décroissante sur $[a, +\infty[$.

$$0 < y(x) = y(a_2) + \int_{a_2}^{x} y'(t)\,dt \leq y(a_2) + (x - a_2)y'(a_2) \to +\infty \qquad (x \to \infty) \tag{6.332}$$

Ce qui est totalement absurde. En procédant de même pour $]+\infty, a]$ on déduit qu'il y a au moins deux zéros pour y.

6.23 ■ MARCHE ALÉATOIRE ZD

Référence : Fourier Series and Integrals, Mc Kean. Recasé 2 fois

■ **LEÇONS**

L260 ESPÉRANCE, VARIANCE ET MOMENTS D'UNE VARIABLE ALÉATOIRE. ★★★★★

L264 VARIABLES ALÉATOIRES DISCRÈTES. EXEMPLES ET APPLICATIONS ★★★★★

■ **RÉFÉRENCES**

Fourier Series and integrals , Dym Mc Kean

6.23.1 Développement

On note (e_i) la base canonique de $\mathbb{R}^d$.
On considère sur $\mathbb{Z}^d$ une marche aléatoire définie par

$$\begin{cases} X_0 = 0 \\ X_{n+1} = X_n + \theta_n \end{cases} \tag{6.333}$$

En notant θ_n une suite iid de variables aléatoires avec la loi uniforme sur l'ensemble $A = \{\pm e_i\}$ de cardinal $2d$.

Lien avec la transformée de Fourier

$$f_n(x) = \phi_{X_n}(2\pi x) = \mathbf{E}\left(e^{2i\pi\langle X_n \mid x\rangle}\right) \tag{6.334}$$

On a

$$f_n(x) = \sum_{k\in\mathbb{Z}^d} \mathbf{P}(X_n = k) e^{2i\pi\langle k \mid x\rangle} \tag{6.335}$$

Ce qu'on veut c'est retrouver le terme $\mathbf{P}(X_n = k)$ en faisant des calculs sur f_n, puis de passer à la limite.

Calcul de f_n On commence par remarquer que par indépendance des θ_i et comme ils sont identiquement distribués on a :

$$\phi_{X_n}(x) = \left(\phi_{\theta_1}(x)\right)^n \tag{6.336}$$

Reste donc à calculer ϕ_{θ_1}.
Pour cela, on constate que

$$\phi_{\theta_1}(x) = \frac{1}{2d}\sum_{k\in A} e^{i\langle k \mid x\rangle} \tag{6.337}$$

$$= \frac{1}{2d}\sum_{j=1}^{d} e^{i\langle e_j \mid x\rangle} + e^{-i\langle e_j \mid x\rangle} \tag{6.338}$$

$$= \frac{1}{d}\sum_{j=1}^{d} \cos x_j \tag{6.339}$$

On peut donc conclure

$$\boxed{f_n(x) = \left(\frac{1}{d}\sum_{j=1}^{d} \cos 2\pi x_j\right)^n} \tag{6.340}$$

Comme barycentre d'éléments dans $[-1,1]$, la somme est dans $[-1,1]$ puis sa puissance n-ème reste dans cet intervalle. On a donc $|f_n(x)| \leq 1$.

On notera $f(x) = \frac{1}{d}\sum_{j=1}^{d} \cos 2\pi x_j$ par la suite. On remarque que $|f(x)| \leq 1$ mais mieux, presque pour tout x on a $|f(x)| < 1$. **IMPORTANT, NE PAS L'OUBLIER !**.

Série de Fourier de f_n Par injectivité des coefficients de Fourier, on déduit que $c_k(f_n) = \mathbf{P}(X_n = k)$.

En particulier

$$\mathbf{P}(X_n = 0) = \int_{[0,1]^d} f_n(x)\,dx = \int_{[0,1]^d} f(x)^n\,dx \tag{6.341}$$

Écriture intégrale du problème On pose $N = \mathbf{E}\left(\sum_{n\in\mathbb{N}} \chi_{X_n=0}\right)$. C'est l'espérance du nombre de retours en zéro.

On constate que $N = \sum_{n\in\mathbb{N}} \mathbf{P}(X_n = 0)$ mais est aussi égal à $\sum_{n\in\mathbb{N}} \mathbf{P}(X_{2n} = 0)$ puisque pour atteindre zéro, il faut un nombre pair de pas.

On veut donc étudier les nombres suivants (qui sont des réels potentiellement égaux à $+\infty$).

$$N = \sum_{n\in\mathbb{N}} \int_{[0,1]^d} f(x)^{2n}\,dx \tag{6.342}$$

Toutes les fonctions étant positives, on peut appliquer Fubini-Tonelli pour obtenir

$$N = \int_{[0,1]^d} \sum_{n\in\mathbb{N}} f(x)^{2n}\,dx = \int_{[0,1]^d} \frac{1}{1-f^2(x)}\,dx \tag{6.343}$$

En effet, presque pour tout x on a $|f(x)| < 1$, donc on peut utiliser l'expression sous forme de fraction.

Nombre de retours en zéro Pour déduire quelque chose sur N il suffit alors d'étudier l'intégrabilité de la fonction.

Le défaut d'intégrabilité est sur tous les points à coordonnées dans $\{0,1\}$ ainsi qu'en $(1/2,\dots,1/2)$.

On étudie seulement le cas $(0,\dots,0)$ qui se transporte à tous les autres points.

Au voisinage de zéro, on peut faire un développement limité de $f^2(x)$:

$$f^2(x) = \left(\frac{1}{d}\sum_{j=1}^{d} 1 - \frac{x_j^2}{2} + o(t_j^2)\right)^2 = \left(1 - \frac{\|t\|^2}{2d} + o(\|t\|^2)\right)^2 = 1 - \frac{\|t\|^2}{d} + o(\|t\|^2) \tag{6.344}$$

Ainsi

$$\frac{1}{1-f^2(x)} \sim \frac{d}{\|t\|^2} \tag{6.345}$$

Or cette fonction est intégrable en zéro si et seulement si $d > 2$ [16].

Donc N **est fini si et seulement si** $d > 2$.

Conclusion À corriger niveau probas ...

(i) Si $d > 2$ alors $N < \infty$, mais alors la probabilité que N retourne une infinité de fois en 0 est nulle. Le même arguent s'appliquant à toute position, on déduit que X_n sort presque sûrement de tout compact.

Ainsi $|X_n| \to +\infty$ presque sûrement, par continuité croissante de la mesure de proba.

16. Changement de coordonnées polaires

(ii) Si $d \leq 2$, alors $N = +\infty$. On pose alors $B_1 = \{\exists n, X_n = 0\}$, l'évènement où il y a au moins un retour en zéro.

On pose alors B_k l'évènement où il y a au moins k retours en zéro. Comme la chaine vérifie une propriété d'oubli, on a

$$\mathbf{P}(B_k) = \mathbf{P}(B_1)\mathbf{P}(B_{k-1}) \tag{6.346}$$

En notant $p = \mathbf{P}(B_1)$ on déduit alors que la probabilité d'avoir k visites suit une loi géométrique de paramètre p. Supposons alors $p < 1$, l'espérance de cette loi est nécessairement finie, et donc c'est absurde.

Ainsi, $p = 1$ et presque sûrement il y a un retour en zéro, mais par le calcul précédent, on déduit que presque sûrement il y a k retours en zéro, et par continuité croissante de la proba on déduit qu'il y a presque sûrement une infinité de retours en zéro.

6.24 ■ EXTREMA LIÉS ET APPLICATION ...

Référence : Gourdon, Rouvière. Recasé 4 fois

■ **LEÇONS**

L151 DIMENSION D'UN ESPACE VECTORIEL. RANG. EXEMPLES ET APPLICATIONS ★★★★★

L159 FORMES LINÉAIRES ET DUALITÉ EN DIMENISON FINIE ★★★★★

L214 THÉORÈME D'INVERSION LOCALE, THÉORÈME DES FONCTIONS IMPLICITES. EXEMPLES ET APPLICATIONS EN ANALYSE ET EN GÉOMÉTRIE. ★★★★★

L219 EXTREMUMS : EXISTENCE, CARACTÉRISATION, RECHERCHE. ★★★★★

■ **RÉFÉRENCES**

Gourdon Analyse

Rouvière

Beck

Lafontaine pour les preuves des théorèmes utiles

6.24.1 Prérequis

Théorème 107 (Submersion)**.** *Soit $f : U \to \mathbb{R}^p$ avec U un ouvert de $\mathbb{R}^q$ contenant* 0*. On suppose que df_0 est surjective.*

Il existe un voisinage W de zéro inclus et un C^1 difféo $\psi : W \to \psi(W)$ tel que $0 \in \psi(W) \subseteq U$ et

$$f(\psi(x_1, \dots, x_q)) = (x_1, \dots, x_p) \tag{6.347}$$

Démonstration. On constate que $p \geq q$ car sinon la différentielle ne peut pas être surjective.

Quitte à faire un changement de base, on peut supposer que la différentielle de $f = (f_1, \dots, f_p)$ en zéro s'écrit comme suit

$$Df_0 = \begin{pmatrix} A & \star \\ \star & \star \end{pmatrix} \tag{6.348}$$

Avec $A \in GL_p(\mathbb{R})$.

On pose alors la fonction h comme suit où $\pi_i(x)$ est la i-ème coordonnée de x.

$$h(x) = (f_1(x), \dots, f_p(x), \pi_{p+1}(x), \dots, \pi_q(x)) \tag{6.349}$$

La différentielle de h en zéro s'écrit alors

$$Dh_0 = \begin{pmatrix} A & \star \\ 0 & I_{p-q} \end{pmatrix} \tag{6.350}$$

Ainsi, dh_0 est inversible, et par théorème d'inversion locale h est un C^1 difféomorphisme sur un ouvert V de 0 vers $h(V)$. On pose $\psi = h^{-1}$ sur cet ouvert.

Alors comme $h(\psi(x)) = x$, et que $h(u) = (f(u), u_{p+1}, \dots, u_q)$ on déduit que pour les x dans le voisinage $W = h(V)$ on a :

$$f(\psi(x)) = (x_1, \dots, x_p) \tag{6.351}$$

□

Lemme 108 (Inverse local à droite)**.** *Soit f une submersion, il existe g une application C^1 telle que $f \circ g = id$.*

Pour cela, il suffit de poser $g(x_1,\dots,x_p) = \psi(x_1,\dots,x_p,0,\dots,0)$.

On a alors

$$f(g(x_1,\dots,x_p)) = f(\psi(x_1,\dots,x_p,0,\dots,0)) = (x_1,\dots,x_p) \tag{6.352}$$

Definition 109 (Sous variété)**.** Une partie M de $\mathbb{R}^n$ est une sous variété de dimension p de $\mathbb{R}^n$ si et seulement s'il existe pour tout point $x \in M$ un voisinage U_x et un C^1 difféomorphisme $\phi_x : U_x \to V$, avec V voisinage de zéro. Le tout vérifiant l'équation suivante

$$\phi_x(U \cap M) = (\mathbb{R}^p \times \{0\}^{n-p}) \cap V \tag{6.353}$$

Théorème 110 (Des sous variétés)**.** *Soit M une partie de $\mathbb{R}^n$, les propriétés suivantes sont équivalentes :*

(i) M est une sous-variété de dimension p

(ii) Pour tout point a de M il existe un ouvert U_a et une submersion $f_a : U_a \to \mathbb{R}^{n-p}$ telle que $M \cap U_a = (f_a)^{-1}(\{0\})$.

Démonstration. **Prouvons d'abord le sens facile** , c'est-à-dire $(i) \implies (ii)$. Soit $a \in M$, on dispose de U_a un voisinage de a et $\phi_a : U_a \to V$ voisinage de zéro vérifiant

$$\phi_a(U_a \cap M) = (\mathbb{R}^p \times \{0\}^{n-p}) \cap V \tag{6.354}$$

On pose alors $f_a(x) = (\phi_a^{p+1}(x),\dots,\phi_a^n(x))$. Par construction, on sait que df_a est surjective puisque les colonnes sont linéairement indépendantes (puisque $d\phi_a$ est inversible).

De plus, on a une fois de plus par construction,

$$f_a(U_a \cap M) = \{0\}^{n-p} \cap V = \{0\} \tag{6.355}$$

Donc $f_a^{-1}(\{0\}) = U_a \cap M$.

Pour le sens réciproque Soit $a \in M$, on dispose de U_a un voisinage de a et d'une submersion $f_a : U_a \to \mathbb{R}^{n-p}$ telle que $M \cap U_a = (f_a)^{-1}(\{0\})$.

Par le théorème de submersion, il existe un voisinage W_a et un C^1-difféo ψ tels que

$$f_a(\psi(x_1,\dots,x_n)) = (x_{p+1},\dots,x_n) \tag{6.356}$$

$$\psi^{-1}(M \cap U_a) = \psi^{-1}\left((f_a)^{-1}\left(\{0\}^{n-p}\right)\right) = (f_a \circ \psi)^{-1}\left(\{0\}^{n-p}\right) = W_a \cap \left(\mathbb{R}^p \times \{0\}^{n-p}\right) \tag{6.357}$$

□

Definition 111 (Espace Tangent)**.** Si M est une sous-variété de dimension p dans $\mathbb{R}^n$ et $x \in M$ on note T_xM l'espace tangent à M en x qui est

$$T_xM = \left\{\gamma'(0) \mid \gamma : I \to M, C^1, \gamma(0) = x\right\} \tag{6.358}$$

Lemme 112 (Espace tangent)**.** *L'espace tangent est un espace vectoriel de dimension identique à la sous-variété.*

Démonstration. On considère ϕ telle que $\phi(U\cap M) = (R^p\times\{0\}^{n-p})\cap V$ donnée par la définition d'une sous variété.

Alors si $v\in T_xM$, on a $\gamma : I\to M$ et on peut considérer $\phi\circ\gamma$. Cette application est C^1 par composition, et on peut alors écrire :

$$(\phi\circ\gamma)'(0) = d\phi_x\cdot v\in\mathbb{R}^p\times\{0\}^{n-p} \tag{6.359}$$

Réciproquement, si $v\in\mathbb{R}^p\times\{0\}^{n-p}$ alors on peut trouver ε tel que $\forall|t|<\varepsilon, tw\in\phi(U)$. On pose alors

$$\gamma : t\mapsto\phi^{-1}(tw) \tag{6.360}$$

Par construction, $\gamma(0)=\phi^{-1}(0)=x$, et $\gamma'(0) = (d\phi_x)^{-1}\cdot w$. Donc $(d\phi_x)^{-1}w\in T_xM$.

Donc

$$T_xM = (df_a)^{-1}\left(\mathbb{R}^p\times\{0\}^{n-p}\right) \tag{6.361}$$

□

Lemme 113 (Espace tangent et submersion)**.** *Si M est définie implicitement par la submersion f au point a, alors $T_aM = \ker df_a$.*

Démonstration. Il est clair que $T_aM\subseteq\ker df_a$ puisqu'en composant par f n'importe quel chemin, on est constant égal à zéro, donc $(f\circ\gamma)'(0)=0$ et donc $df_a\cdot v=0$ pour $v\in T_aM$.

Mais comme df_a est surjective (submersion) il est clair que les deux espaces ont même dimension ! □

6.24.2 Théorème des extrema liés

Soit U un ouvert de $\mathbb{R}^n$, $g_1,\dots,g_k$ des fonctions C^1 de U dans $\mathbb{R}$ telles que $dg_1,\dots,dg_k$ soit une famille libre. On pose $M=\{x\in U\mid g_1(x)=\cdots=g_k(x)=0\}$.

On considère $f : U\to\mathbb{R}$, et on veut trouver les éventuels extrema de $f_{|M}$.

L'ensemble M est une sous variété En effet, en notant $G : x\mapsto(g_1(x),\dots,g_k(x))$ on obtient une submersion de $\mathbb{R}^n$ dans $\mathbb{R}^k$.

Ainsi M est une sous variété dont le plan tangent en x est $T_xM = \ker dG_x = \cap_{i=1}^k \ker dg_i(x)$

Si f possède un extremum en $x^\star$ alors considérons $v\in T_{x^\star}M$. On possède $\gamma : I\to M$ tel que $\gamma(0) = x^\star$ et $\gamma'(0)=v$.

La fonction $f\circ\gamma$ possède par construction un extremum en 0, et donc

$$\frac{d}{dt}(f(\gamma(t))) = 0 \tag{6.362}$$

Or cela veut précisément dire que

$$df_{x^\star}v = 0 \tag{6.363}$$

On déduit donc $T_{x^\star}M\subseteq\ker df_{x^\star}$.

On en déduit une condition sur $df_{x^\star}$ En effet, comme on est en dimension finie on peut utiliser la dualité sans problèmes

$$\bigcap\ker dg_i(x^\star)\subseteq\ker df_{x^\star} \iff \left(\ker df_{x^\star}\right)^\perp\subseteq\left(\bigcap\ker dg_i(x^\star)\right)^\perp \tag{6.364}$$

$$\iff \mathrm{Vect}\left(df_{x^\star}\right)\subseteq\bigoplus\mathrm{Vect}\left(dg_i(x^\star)\right) \tag{6.365}$$

$$\tag{6.366}$$

On peut donc déduire qu'il existe un unique ensemble de réels $\lambda_1, \dots, \lambda_k$ vérifiant

$$df_{x^\star} = \sum_{i=1}^{k} \lambda_i dg_i(x^\star) \tag{6.367}$$

C'est le théorème des extrema liés.

6.24.3 Application

On va démontrer que si $A \in \mathscr{L}(\mathbb{R}^n)$ est symétrique alors il est diagonalisable dans une base orthonormée.

Pour cela on considère l'application $f : x \mapsto \langle A(x) \mid x \rangle$ et on recherche un maximum sur la sphère S^{n-1} définie comme $S^{n-1} = \{x \in \mathbb{R}^n \mid g(x) = \|x\|^2 - 1 = 0\}$.

Comme la sphère est compacte en dimension finie, on déduit que f admet bien un maximum en un certain point y.

On a bien g qui est une application C^1 de différentielle non nulle, car $dg_x(h) = 2\langle x \mid h \rangle$. Et en appliquant le théorème des extrema liés on déduit

$$\exists \lambda \in \mathbb{R}, \forall h \in \mathbb{R}^n, df_y(h) = \lambda dg_y(h) = 2\lambda \langle y \mid h \rangle \tag{6.368}$$

D'un autre côté on peut calculer facilement la différentielle de f

$$df_y(h) = \langle h \mid A(y) \rangle + \langle y \mid Ah \rangle \tag{6.369}$$

Par symétrie on déduit alors

$$\forall h \in \mathbb{R}^n, \langle A(y) - \lambda y \mid h \rangle = 0 \tag{6.370}$$

Cela montre donc que $A(y) = \lambda y$, et comme $y^\perp$ est stable par A, on peut utiliser une récurrence pour diagonaliser A en base orthonormée.

6.25 ■ THÉORÈME DE BERNSTEIN SUR LES SÉRIES ENTIÈRES

Référence : Gourdon Analyse. Recasé 1 fois

■ **LEÇONS**

L243 CONVERGENCE DES SÉRIES ENTIÈRES, PROPRIÉTÉS DE LA SOMME. EXEMPLES ET APPLICATIONS. ★★★★★

6.26 ■ CONTINUITÉ DES RACINES D'UN POLYNÔME

Référence : Gourdon. Recasé 1 fois

■ **LEÇONS**

L223 SUITES NUMÉRIQUES. CONVERGENCE, VALEURS D'ADHÉRENCE. EXEMPLES ET APPLICATIONS. ★★★★★

6.27 ■ FORMULE SOMMATOIRE DE POISSON

Référence : Gourdon, Zuily. Recasé 2 fois

■ **LEÇONS**

L246 SÉRIES DE FOURIER ★★★★★

L250 TRANSFORMATIONS DE FOURIER ★★★★★

■ **RÉFÉRENCES**

ZQ page 93

FGN Analyse 2

6.27.1 Démonstration de la formule sommatoire

On veut démontrer la formule de Poisson, c'est-à-dire

$$\sum_{-\infty}^{+\infty} F(x+2n\pi) = 2\pi \sum_{-\infty}^{+\infty} \hat{F}(2\pi n) e^{inx} \tag{6.371}$$

Énoncé des hypothèses On suppose $F \in L^1 \cap C^0$ afin de pouvoir définir $\hat{F}$ et d'avoir assez de régularité sur les coefficients de Fourier de F.

On suppose de plus

$$\sum_{-\infty}^{+\infty} |\hat{F}(n)| < +\infty \tag{6.372}$$

$$\exists M > 0, \alpha > 1, \forall x \in \mathbb{R}, |F(x)| \leq M(1+|x|)^{-\alpha} \tag{6.373}$$

Ce qui donne une garantie sur la décroissance de la fonction suffisante pour pouvoir sommer.

Introduction du périodisé Afin de faire le lien entre les coefficients de Fourier de F et sa transformée de Fourier, on périodise la fonction. Pour cela on considère

$$f(x) = \sum_{-\infty}^{+\infty} F(x+2\pi n) \tag{6.374}$$

Cette série est normalement convergente car F décroit suffisamment vite. En effet si $|x| \leq A$, on a convergence normale car $\alpha > 1$, via une comparaison avec une série de Riemann :

$$|F(x+2\pi n)| \leq M(1+|x+2\pi n|)^{-\alpha} \leq M\left(\frac{1}{1+(2\pi n - A)}\right)^{\alpha} \tag{6.375}$$

On a donc f qui est bien définie, et comme il y a convergence uniforme sur tout compact, f est aussi continue.

De plus, on a par définition $f(x+2\pi) = f(x)$ donc f est 2π-périodique !

Calcul des coefficients de Fourier de f

$$c_m(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-imt}dt \tag{6.376}$$

$$= \frac{1}{2\pi}\int_0^{2\pi} \sum_{-\infty}^{+\infty} F(t+2\pi n)e^{-imt}dt \tag{6.377}$$

$$= \frac{1}{2\pi}\sum_{-\infty}^{+\infty}\int_0^{2\pi} F(t+2\pi n)e^{-imt}dt \qquad \text{Via Fubini car il y a convergence normale} \tag{6.378}$$

$$= \frac{1}{2\pi}\sum_{-\infty}^{+\infty}\int_0^{2\pi} F(t+2\pi n)e^{-mi(t+2\pi n)}dt \qquad \text{Par } 2\pi \text{ périodicité} \tag{6.379}$$

$$= \frac{1}{2\pi}\sum_{-\infty}^{+\infty}\int_{2\pi n}^{2\pi(n+1)} F(t)e^{-imt}dt \qquad \text{Changement de variable} \tag{6.380}$$

$$= \frac{1}{2\pi}\int_{-\infty}^{+\infty} F(t)e^{-mit}dt \tag{6.381}$$

$$= \frac{1}{2\pi}\hat{F}(m) \tag{6.382}$$

On a donc bien un lien entre les coefficients de Fourier du périodisé de F et sa transformée de Fourier ... C'est logique !

Conclusion On sait que $\sum|\hat{F}(n)| < +\infty$, et donc via l'égalité précédente $\sum|c_n(f)| < +\infty$.

Comme la fonction est *continue* et que sa série de Fourier converge absolument, on l'égalité

$$f(x) = \sum_{m\in\mathbb{Z}} c_m(f)e^{imx} = \frac{1}{2\pi}\sum_{m\in\mathbb{Z}}\hat{F}(m)e^{imx} \tag{6.383}$$

Par construction de f, on déduit alors l'égalité attendue

$$2\pi\sum_{m\in\mathbb{Z}} F(x+2m\pi) = \sum_{m\in\mathbb{Z}}\hat{F}(m)e^{imx} \tag{6.384}$$

Dans la classe de Schwartz, tout se passe bien En effet, automatiquement f et $\hat{f}$ sont à décroissance rapide, et les hypothèses sont vérifiées.

Application à une Gaussienne Si on pose $f(x) = e^{-x^2/(4\alpha t)}$ avec $\alpha, t > 0$ (la Gaussienne centrée d'écart type $2\alpha t$) qui est vérifie clairement les hypothèses de l'énoncé, on trouve alors pour $x \in \mathbb{R}$

$$2\pi\sum_{n\in\mathbb{Z}}\exp\left(-\frac{(x-2n\pi)^2}{4\alpha t}\right) = \sum_{n\in\mathbb{Z}}\hat{f}e^{inx} \tag{6.385}$$

Or la transformée de Fourier d'une Gaussienne est connue, c'est

$$\hat{f}(\xi) = \frac{1}{\sqrt{2\pi(2\alpha t)}}\exp\left(-\frac{\xi^2 2\alpha t}{2}\right) \tag{6.386}$$

Ce qui prouve que

$$\sqrt{\frac{\pi}{\alpha t}}\sum_{n\in\mathbb{Z}}\exp\left(-\frac{(x-2n\pi)^2}{4\alpha t}\right)=\sum_{n\in\mathbb{Z}}e^{-\alpha n^2 t}e^{inx} \tag{6.387}$$

Conclusion sur la fonction Θ de Jacobi en posant $\alpha=\pi$ et $x=0$, on déduit immédiatement

$$\frac{1}{\sqrt{t}}\Theta\left(\frac{1}{t}\right)=\Theta(t) \tag{6.388}$$

Avec $\Theta(x)=\sum_{n\in\mathbb{Z}}e^{-\pi n^2 x}$.

Résolution de l'équation de la Chaleur Pour $t>0$ on pose sur le Tore

$$p_t(x)=\sum_{n\in\mathbb{Z}}e^{-n^2 t}e^{inx} \tag{6.389}$$

En utilisant la formule de Poisson sur les gaussiennes avec $\alpha=1$ on déduit

$$p_t(x)=\sqrt{\frac{\pi}{t}}\sum_{n\in\mathbb{Z}}\exp\left(-\frac{(x-2n\pi)^2}{4t}\right) \tag{6.390}$$

C'est une fonction de classe C^∞ (convergence normale et dérivation terme à terme) sur $\mathbb{R}_+^*\times\mathbb{T}$. Si on se donne une condition initiale $f\in\mathscr{C}(\mathbb{T})$ alors la convolée $f\star p_t(x)$ est de classe C^∞ sur le même ensemble.

De plus, on constate que p_t vérifie (sur son domaine de définition) l'équation (via une dérivation terme à terme)

$$\frac{\partial p_t}{\partial t}=\frac{\partial^2 p_t}{\partial x^2} \tag{6.391}$$

Ainsi, en posant u comme suit

$$\begin{cases}u(0,x)=f(x)\\ u(t,x)=(f\star p_t)(x)\end{cases} \tag{6.392}$$

On construit une solution de l'équation de la Chaleur sur $\mathbb{R}_+^*\times\mathbb{T}$ (car la convolution passe bien à la dérivation).

Il suffirait que p_t est une approximation de l'unité pour pouvoir conclure que cette solution est continue sur $\mathbb{R}_+\times\mathbb{T}$ via les théorèmes généraux sur la convolution.

Or, on peut utiliser l'expression sous forme de somme de gaussiennes :

$$\begin{aligned}f\star p_t(x)&=\frac{1}{2\pi}\int_0^{2\pi}f(y)\sqrt{\frac{\pi}{t}}\sum_{n\in\mathbb{Z}}\exp\left(-\frac{(x-2n\pi)^2}{4t}\right) &(6.393)\\ &=\frac{1}{\sqrt{4\pi t}}\sum_{n\in\mathbb{Z}}\int_0^{2\pi}f(y)\exp\left(-\frac{(x-y-2n\pi)^2}{4t}\right) &(6.394)\\ &=\frac{1}{\sqrt{4\pi t}}\sum_{n\in\mathbb{Z}}\int_{2n\pi}^{2(n+1)\pi}f(y-2n\pi)\exp\left(-\frac{(x-y)^2}{4t}\right) &(6.395)\\ &=\frac{1}{\sqrt{4\pi t}}\sum_{n\in\mathbb{Z}}\int_{2n\pi}^{2(n+1)\pi}f(y)\exp\left(-\frac{(x-y)^2}{4t}\right) &(6.396)\\ &=\frac{1}{\sqrt{4\pi t}}\int_{-\infty}^{+\infty}f(y)\exp\left(-\frac{(x-y)^2}{4t}\right) &(6.397)\\ &=f\star_{\mathbb{R}}g_{4t} &(6.398)\end{aligned}$$

On a donc bien une convolution avec un noyau gaussien, qui est une approximation de l'unité, et donc on a la continuité de u !
Mieux, on retrouve un principe du maximum puisque pour $t > 0$ (de diffusion de la chaleur)

$$\|u(t,\cdot)\|_\infty \leq \|f \star_{\mathbb{R}} g_{4t}\|_\infty \leq \|f\|_\infty \|g_{4t}\|_1 = \|f\|_\infty \tag{6.399}$$

6.28 ■ CONIQUE ET DÉTERMINANT

Référence : Eiden. Recasé 2 fois

■ **LEÇONS**

L152 DÉTERMINANT. EXEMPLES ET APPLICATIONS ★★★★★

L181 BARYCENTRES DANS UN ESPACE AFFINE RÉEL DE DIMENSION FINIE, CONVEXITÉ ,APPLICATIONS ★★★★★

■ **RÉFÉRENCES**

Eiden page 94

FGN Algèbre 2 Pour les déterminants par blocs

6.28.1 Mise en place

On se donne 3 points dans le plan P_1, P_2, P_3 qui forment un repère barycentrique. On peut former un triangle non plat avec ces trois points.

On fixe $M = (x, y, z)$ et $N = (x', y', z')$ deux points qui ne sont pas confondus et différents des P_i.

On construit par la suite les points M_i et N_i en regardant les droites MP_i et en faisant l'intersection avec le côté opposé.

6.28.2 Énoncé du théorème

Il existe une unique conique qui passe par ces points.

6.28.3 Équation d'une conique

L'équation d'une conique dans un repère affine est de la forme

$$au^2 + buv + cu^2 + du + ev + f = 0 \tag{6.400}$$

Avec $(a, b, c) \neq (0, 0, 0)$. Par la suite on passe aux aux coordonnées barycentriques.

$$X\overrightarrow{MP_1} + Y\overrightarrow{MP_2} + Z\overrightarrow{MP_3} + = \overrightarrow{0} \tag{6.401}$$

$$(X + Y + Z)\overrightarrow{P_1M} = Y\overrightarrow{P_1P_2} + Z\overrightarrow{P_1P_3} \tag{6.402}$$

Donc on déduit $u = \frac{Y}{X+Y+Z}$ et $v = \frac{Z}{X+Y+Z}$.
En injectant dans l'équation on trouve

$$\alpha X^2 + \beta Y^2 + \gamma Z^2 + \delta XY + \varepsilon YZ + \zeta XZ = 0 \tag{6.403}$$

Avec $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta) \neq 0$. Il suffit donc de trouver un tel uplet.

6.28.4 Expression des points M_i

Le point M_1 est sur la droite (P_1M) et (P_2P_3). La première droite nous permet de déduire que $M_1 = (0, y_1, z_1)$. La deuxième nous permet d'écrire

$$\begin{vmatrix} 1 & 0 & 0 \\ x & y & z \\ 0 & y' & z' \end{vmatrix} = 0 \tag{6.404}$$

Cela prouve en développant par rapport à la première ligne que (y, z) est colinéaire à (y_1, z_1).

Comme les coordonnées barycentriques sont invariantes par multiplication, et que la première coordonnée de M_1 est nulle, on peut donc écrire

$$M_1 = (0, y, z) \tag{6.405}$$

Par symétrie, on obtient ainsi M_2, et M_3 comme ayant chacun les coordonnées de M sauf en i où ils ont un zéro.

Les points N_i se traitent exactement de la même manière avec des x', y', z'.

6.28.5 Injection dans la conique

En injectant ceci dans l'équation de la conique recherchée, on trouve

$$\begin{pmatrix} 0 & y^2 & z^2 & yz & 0 & 0 \\ x^2 & y^2 & 0 & 0 & xy & 0 \\ x^2 & 0 & z^2 & 0 & 0 & xz \\ 0 & y'^2 & z'^2 & y'z' & 0 & 0 \\ x'^2 & y'^2 & 0 & 0 & x'y' & 0 \\ x'^2 & 0 & z'^2 & 0 & 0 & x'z' \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \\ \varepsilon \\ \zeta \end{pmatrix} = 0 \tag{6.406}$$

On reconnait des blocs de la forme A, A', B et B' ce qui ramène à calculer le déterminant suivant

$$\begin{vmatrix} A & B \\ A' & B' \end{vmatrix} \tag{6.407}$$

6.28.6 Déterminant par blocs

On remarque que B et B' sont diagonales, donc commutent. On applique la méthode de Eiden qui marche bien ... Ou celle du FGN.

On déduit que le déterminant recherché est égal à

$$\begin{aligned} \det B'A - BA' &= \begin{vmatrix} 0 & yy'(yz' - zy') & zz'(zy' - yz') \\ xx'(xy' - yx') & 0 & zz'(zx' - xz') \\ xx'(xz' - zx') & yy'(yx' - xy') & 0 \end{vmatrix} \\ &= xx'yy'zz' \begin{vmatrix} 0 & (yz' - zy') & (zy' - yz') \\ (xy' - yx') & 0 & (zx' - xz') \\ (xz' - zx') & (yx' - xy') & 0 \end{vmatrix} \end{aligned}$$

Or la somme des colonnes fait 0 donc le déterminant est nul.

6.28.7 Conclusion

Comme le déterminant est nul, le système possède une solution non nulle, et par construction cette solution est une conique. Comme les coordonnées barycentriques sont définies avec homogénéité, on obtient une *droite vectorielle* qui définit une unique conique.

On peut montrer que cette conique est unique. En effet, 5 points donc quatre d'entre eux ne sont pas alignés définissent une unique conique. [EID p52/43]

CHAPITRE 7

LEÇONS

■ **LEÇONS** **2XX**

L203 UTILISATION DE LA NOTION DE COMPACITÉ. 2D

L208 ESPACES VECTORIELS NORMÉS, APPLICATIONS LINÉAIRES CONTINUES. EXEMPLES. 2D

L214 THÉORÈME D'INVERSION LOCALE, THÉORÈME DES FONCTIONS IMPLICITES. EXEMPLES ET APPLICATIONS EN ANALYSE ET EN GÉOMÉTRIE. 3D

L215 APPLICATIONS DIFFÉRENTIABLES DÉFINIES SUR UN OUVERT DE RN. EXEMPLES ET APPLICATIONS. 2D

L218 APPLICATION DES FORMULES DE TAYLOR 2D

L219 EXTREMUMS : EXISTENCE, CARACTÉRISATION, RECHERCHE. 2D

L220 ÉQUATIONS DIFFÉRENTIELLES GÉNÉNRALES. EXEMPLES DIM 1 ET 2 2D

L221 ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES. SYSTÈMES. 2D

L223 SUITES NUMÉRIQUES. CONVERGENCE, VALEURS D'ADHÉRENCE. EXEMPLES ET APPLICATIONS. 2D

L224 EXEMPLES DE DÉVELOPPEMENTS ASYMPTOTIQUES DE SUITES ET DE FONCTIONS. 2D

L226 SUITES VECTORIELLES ET RÉELLES DÉFINIES PAR UNE RELATION DE RÉCURRENCE UN+1 = F(UN). EXEMPLES. APPLICATIONS À LA RÉSOLUTION APPROCHÉE D'ÉQUATIONS. 2D

L228 CONTINUITÉ ET DÉRIVABILITÉ DES FONCTIONS RÉELLES 2D

L229 FONCTIONS MONOTONES, FONCTIONS CONVEXES 2D

L230 SÉRIES DE NOMBRES RÉELS OU COMPLEXES. COMPORTEMENT DES RESTES OU DES SOMMES PARTIELLES DES SÉRIES NUMÉRIQUES. EXEMPLES. 2D

L233 MÉTHODES ITÉRATIVES EN ANALYSE NUMÉRIQUE MATRICIELLE. 2D

L236 ILLUSTER DES MÉTHODES DE CALCUL D'INTÉGRALES (PLUSIEURS VARIABLES) 2D

L239 INTÉGRALES À PARAMÈTRE 2D

L243 CONVERGENCE DES SÉRIES ENTIÈRES, PROPRIÉTÉS DE LA SOMME. EXEMPLES ET APPLICATIONS. 2D

L246 SÉRIES DE FOURIER 2D

L250 TRANSFORMATIONS DE FOURIER 2D

L260 ESPÉRANCE, VARIANCE ET MOMENTS D'UNE VARIABLE ALÉATOIRE. 2D

L264 VARIABLES ALÉATOIRES DISCRÈTES. EXEMPLES ET APPLICATIONS 2D

L104 GROUPES FINIS. EXEMPLES ET APPLICATIONS
- ✓ Théorème de Brauer en car qcq
- ✓ Sous groupes finis de SO3(R)

L105 GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI. APPLICATIONS
- ✓ Frobénius-Zolotarev
- ✓ Théorème de Brauer en car qcq

L106 GROUPE LINÉAIRE D'UN ESPACE VECTORIEL DE DIMENSION FINIE, SOUS GROUPES. APPLICATIONS
- ✓ Frobénius-Zolotarev
- ✓ Sous groupes compacts de GLn(R)

L108 EXEMPLE DE PARTIES GÉNÉRATRICES D'UN GROUPE. APPLICATIONS
- ✓ Théorème de Brauer en car qcq
- ✓ SO3(R) et les quaternions

L120 ANNEAUX Z/nZ. APPLICATIONS
- ✓ Frobénius-Zolotarev
- ✓ Ordre moyen $\phi(n)$

L121 NOMBRES PREMIERS. APPLICATIONS
- ✓ Frobénius-Zolotarev
- ✓ Réciprocité quadratique
- ✓ Ordre moyen $\phi(n)$

L123 CORPS FINIS. APPLICATIONS
- ✓ Dénombrement polynômes irréductibles
- ✓ Algorithme de Berlekamp

L141 POLYNÔMES IRRÉDUCTIBLES À UNE INDÉTERMINÉE. CORPS DE RUPTURE. EXEMPLES ET APPLICATIONS
- ✓ Dénombrement polynômes irréductibles
- ✓ Algorithme de Berlekamp

L150 EXEMPLES D'ACTIONS DE GROUPES SUR LES ESPACES DE MATRICES
- ✓ Sous groupes compacts de GLn(R)
- ✓ Invariants de Frobenius

L151 DIMENSION D'UN ESPACE VECTORIEL. RANG. EXEMPLES ET APPLICATIONS
- ✓ Invariants de Frobenius
- ✓ Algorithme de Berlekamp
- ✓ Extrema liés et application ...

L152 DÉTERMINANT. EXEMPLES ET APPLICATIONS
- ✓ Frobénius-Zolotarev
- ✓ Conique et déterminant

L153 POLYNÔMES D'ENDOMORPHISME EN DIMENSION FINIE. RÉDUCTION. APPLICATIONS
- ✓ Invariants de Frobenius
- ✓ Décomposition Dunford Effective

L157 ENDOMORPHISMES TRIGONALISABLES. ENDOMORPHISMES NILPOTENTS
- ✓ Méthodes itératives Jacobi/Gauss-seidel
- ✓ Décomposition Dunford Effective

L159 FORMES LINÉAIRES ET DUALITÉ EN DIMENISON FINIE
- ✓ Invariants de Frobenius
- ✓ Extrema liés et application ...

L162 SYSTÈMES D'ÉQUATION LINÉAIRES ; OPÉRATIONS ÉLÉMENTAIRES, ASPECTS ALGORITHMIQUES
- ✓ Méthodes itératives Jacobi/Gauss-seidel
- ✓ Algorithme de Berlekamp

L170 FORMES QUADRATIQUES SUR UN ESPACE VECTORIEL DE DIMENSION FINIE. ORTHOGONALITÉ, ISOTROPIE. APPLICATIONS
- ✓ Réciprocité quadratique
- ✓ Lemme de Morse

L181 BARYCENTRES DANS UN ESPACE AFFINE RÉEL DE DIMENSION FINIE, CONVEXITÉ ,APPLICATIONS
- ✓ Sous groupes compacts de GLn(R)
- ✓ Conique et déterminant

L182 APPLICATIONS DES NOMBRES COMPLEXES À LA GÉOMÉTRIE
- ✓ SO3(R) et les quaternions

L183 UTILISATION DES GROUPES EN GÉOMÉTRIE
- ✓ SO3(R) et les quaternions
- ✓ Sous groupes finis de SO3(R)

L190 MÉTHODES COMBINATOIRES ET DÉNOMBREMENT
- ✓ Dénombrement polynômes irréductibles
- ✓ Nombres de Bell

L203 UTILISATION DE LA NOTION DE COMPACITÉ.
- ✓ Sous groupes compacts de GLn(R)
- ✓ Théorème d'Hadamard Lévy

L208 Espaces vectoriels normés, applications linéaires continues. Exemples.
- ✓ Sous groupes compacts de GLn(R)
- ✓ Banach Steinhaus et fourier

L214 Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie.
- ✓ Lemme de Morse
- ✓ Théorème d'Hadamard Lévy
- ✓ Extrema liés et application ...

L215 Applications différentiables définies sur un ouvert de Rn. Exemples et applications.
- ✓ Lemme de Morse
- ✓ Théorème d'Hadamard Lévy

L218 Application des formules de Taylor
- ✓ Lemme de Morse
- ✓ Suites à convergence lente

L219 Extremums : existence, caractérisation, recherche.
- ✓ Méthode du gradient à pas optimal
- ✓ Extrema liés et application ...

L220 Équations différentielles génénrales. Exemples dim 1 et 2
- ✓ Théorème d'Hadamard Lévy
- ✓ Théorème de Sturm Liouville

L221 Équations différentielles linéaires. Systèmes.
- ✓ Sous espaces de $\mathscr{C}(R,R)$ stables par translation
- ✓ Théorème de Sturm Liouville

L223 Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.
- ✓ Suites à convergence lente
- ✗ Continuité des racines d'un polynôme

L224 Exemples de développements asymptotiques de suites et de fonctions.
- ✓ Suites à convergence lente
- ✓ Méthode de Laplace

L226 Suites vectorielles et réelles définies par une relation de récurrence un+1 = f(un). Exemples. Applications à la résolution approchée d'équations.
- ✓ Méthodes itératives Jacobi/Gauss-seidel
- ✓ Suites à convergence lente

L228 Continuité et dérivabilité des fonctions réelles
- ✓ Sous espaces de $\mathscr{C}(R,R)$ stables par translation
- ✓ Méthode de Laplace

L229 Fonctions monotones, fonctions convexes
- ✓ Méthode du gradient à pas optimal
- ✓ Processus de branchements

L230 Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.
- ✓ Ordre moyen $\phi(n)$
- ✓ Suites à convergence lente

L233 Méthodes itératives en analyse numérique matricielle.
- ✓ Méthodes itératives Jacobi/Gauss-seidel
- ✓ Méthode du gradient à pas optimal

L236 Illuster des méthodes de calcul d'intégrales (plusieurs variables)
- ✓ Méthode de Laplace
- ✓ Inversion de Fourier L1

L239 Intégrales à paramètre
- ✓ Méthode de Laplace
- ✓ Inversion de Fourier L1

L243 Convergence des séries entières, propriétés de la somme. Exemples et applications.
- ✓ Nombres de Bell
- ✗ Théorème de Bernstein sur les séries entières

L246 Séries de Fourier
- ✓ Banach Steinhaus et fourier
- ✓ Formule Sommatoire de Poisson

L250 Transformations de Fourier
- ✓ Inversion de Fourier L1
- ✓ Formule Sommatoire de Poisson

L260 Espérance, variance et moments d'une variable aléatoire.
- ✓ Processus de branchements
- ✓ Marche aléatoire Zd

L264 Variables aléatoires discrètes. Exemples et applications
- ✓ Processus de branchements
- ✓ Marche aléatoire Zd

7.104 ■ GROUPES FINIS. EXEMPLES ET APPLICATIONS

■ **DÉVELOPPEMENTS** **5.0**

D02 THÉORÈME DE BRAUER EN CAR QCQ ⋆⋆⋆⋆⋆

D04 SOUS GROUPES FINIS DE SO3(R) ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

X-ENS Algèbre 1/2

Rombaldi

Perrin / Ortiz

■ **RAPPORT DE JURY**

Dans cette leon il faut savoir manipuler correctement les éléments de différentes structures usuelles (Z/nZ, S_n,etc.) comme, par exemple, en proposer un générateur ou une famille de générateurs, savoir calculer un produit de deux permutations, savoir décomposer une permutation en produit de cycles à supports disjoints. Il est importantque la notion d'ordre d'un élément soit mentionnée et comprise dans des cas simples. Le théorème de structure des groupes abéliens finis doit être connu. Les exemples doivent figurer en bonne place dans cette leçon. Les gorupes d'automorphismes fournissent des exemples très naturels. On peut aussi étudier les groupes de symétries A_4, S_4 et A_5 et relier sur ces exemples géométrie et algèbre ; es représentations ayant ici toute leur place ; il est utile de connaître les groupes diédraux. S'ils le désirent les candidats peuvent ensuite mettre en avant les spécificités de groupes comme le groupe des quaternions, les sous-groupse finis de $SU(2)$ ou les groupes de $GL_n(F_q)$.

7.104.1 Outils sur les groupes finis

■ **PREMIÈRES DÉFINITIONS**

Defs Cardinal, indice d'un sous groupe, théorème de Lagrange

EX Z/nZ, S_n

EX Formule "du rang"

Def Ordre d'un élément, propriétés du Rombaldi sur les ordres, exposant d'un groupe.

Def Exposant, $(Z/2Z)^{\mathbb{N}}$

DEV Burnside $GL_n(\mathbb{C})$

EX Sous groupe des racines de l'unité dans un corps

■ **ACTION DE GROUPE ET DÉNOMBREMENT**

Def Action de groupe, formule des classes, lien orbite stabilisateur

EX Intérieur, à gauche. Action du groupe des permutations.

EX D'indice deux implique distingué (Per)

Def Noyau de l'action/Stabilisateurs

EX Wedderburn

Def Formule de Burnside

EX Nombre moyen de point fixe par une permutation aléatoire

7.104.2 Le cas des groupes abéliens

■ **RETOUR SUR LES GROUPES CYCLIQUES**

EX Sous groupe fini multiplicatif d'un corps est cyclique, sous groupe des racines de l'unité

Def Tous isomorphes à Z/nZ

Def Générateurs de Z/nZ, $\phi(n)$, sous groupes, formule $n, \phi(n)$

EX Tout groupe d'ordre p est un Z/pZ

Def Lemme chinois sur Z/nZ

Def Morphismes et automorphismes de Z/nZ

EX Groupe *abélien* d'ordre pq avec p,q premiers distincts est cyclique

EX Ordre premier ssi cyclique et simple.

■ **EXEMPLES ET CLASSIFICATION**

EX Théorème de Cauchy abélien

EX Groupe d'ordre p ou p^2 implique abélien.

EX Exposant 2 implique abélien

EX Quotient cyclique implique abélien

Thm Classification des groupes abéliens finis.

7.104.3 Le groupe symétrique

■ **LE GROUPE SYMÉTRIQUE**

coucou Support, cycles, transpositions. Générateurs. Classes de conjugaison. A_n et simplicité. Conséquences pour certains morphismes. La signature.

DEV Brauer en caractéristique qcq

7.104.4 Tentative de classification

■ **LE CAS DES p-GROUPES**

Def p-groupe, p-sylow

EX Le théorème de Cauchy général

Def p-groupe centre non trivial

Lem Per 5.5 sur les Sylow, puis existence par récurrence

Thm Sylow général

Lem Abélien est produit direct de ses p-sylow

■ **APPLICATION À LA CLASSIFICATION**

Def Produit semi-direct, direct, groupe simple

EX Ordre 63 implique non simple, voir **ortiz** p57

EX $GL_n(\mathbb{F}_q)$ et sylow

EX Groupes d'ordre pq (Perrin)

EX Un sous groupe d'ordre 6 est S_3 ou $Z/6Z$

EX Sous groupes finis d'ordre inférieur à 15 (Où ...)

EX Groupe d'ordre $45 = 3*3*5$

EX A_5 est le seul groupe simple d'ordre 60.

7.104.5 Quelques groupes remaquables

■ **LE GROUPE LINÉAIRE**

Def $GL_n(K)$ et $GL_m(K)$ sont isomorphes ssi $n = m$.

Def Dénombrement de $GL_n(F_q), SL_n(F_q)$

Def Groupes dérivés

EX Tout sous groupe fini de $GL_n(R)$ est conjugué à $O_n(R)$.

Def Isomorphismes exceptionnels

DEV Frobenius Zolotarev

EX Dénombrement des endomorphismes nilpotents d'indice max dans $M_n(F_q)$.

■ **LES GROUPES D'ISOMÉTRIES**

EX Groupes d'isométries dans $\mathbb{R}^2$ c'est $\mathbb{U}$.

Def Groupes diédraux

Def Groupes d'isométries du cube, tétraèdre etc...

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

7.105 ■ GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI. APPLICATIONS

■ **DÉVELOPPEMENTS** **5.0**

D00 FROBÉNIUS-ZOLOTAREV ⋆⋆⋆⋆⋆

D02 THÉORÈME DE BRAUER EN CAR QCQ ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Perrin / Ortiz

Rombaldi

Gourdon Algèbre (pour les polynômes symétriques)

■ **RAPPORT DE JURY**

Parmi les attendus, il faut savoir relier la leçon avec les notions d'orbites et d'action de gorupes. Il faut aussi savoir décomposer une permutation en cycles à supports disjoints, tant sur le plan théorique (preuve du théorème de décomposition) que pratique (sur un exemple). Il est important de savoir déterminer les classes de conjugaisons du groupe symétrique par la décomposition en cycles, d'être capable de donner des systèmes de générateurs. L'existence du morphisme signature est un résultat non trivial mais ne peut pas constituer à elle seule l'object d'un développement. Les applications sont nombreuses, il est tèrs naturel de parler du déterminant, des polynômes symétriques ou des fonctions symétriques des racines d'un polynôme. S'ils le désient, les candidats peuvent aller plus loin en s'intéressant aux automorphismes du groupe symétrique, à des problèmes de dénombrement, aux représentations des groupes des permutations ou encore aux permutations aléatoires.

7.105.1 Groupe symétrique $S(X)$ et action sur X

■ **GROUPE DES PERMUTATIONS**

Def $S(X)$, isomorphisme avec S_n, cardinal (par récurrence) (ROM)

EX S_3, non-commutatif, ordres des éléments etc ...(ROM)

EX Complexité moyenne du tri par comparaison

Not notation des permutations (ROM)

■ **ACTION DE $S(X)$ SUR X**

Def Action de $S(X)$ sur X, transitivité, pas libre, fidèle. Mieux, $|X|$-transitive (PER)

Def Action de groupe via morphisme

Def Cayley (PER)

EX $GL_n(\mathbb{F}_q)$ agit comme un sous groupe de S_{q^n}

EX G infini avec un sous groupe propre d'indice fini n'est pas simple (PER)

Def Stabilisateur d'un point isom à S_{n-1} (PER)

■ **CYCLES ET TRANSPOSITIONS**

Def Orbite d'un élément (ROM)

Def Support, cycle, transposition (ROM)

Def Commutativité à support disjoints (ROM)

AP $Z(S_n) = \{id\}$ si $n \geq 3$ (PER)

Thm Décomposition en cycles (ROM)

AP Calcul de l'ordre d'une permutation (ROM)

Thm Décomposition en transpositions (systèmes de générateurs) (ROM)

EX Algorithmes de tri (bulle)

7.105.2 Structure de S_n et A_n

■ **CLASSES DE CONJUGAISON**

Def Type d'une permutation

Def Conjugaison d'un cycle

Thm Caractérisation de la conjugaison

DEV Brauer en caractéristique qcq

■ **SIGNATURE**

Def Signature comme unique morphisme

EX Signature d'un cycle, d'une transposition, d'un truc avec r orbites

Def Inversion, et version alternative de la signature

EX Exemple de calcul

DEV Frobenius Zolotarev et applications

■ **GROUPE ALTERNÉ**

Def A_n, unique sous groupe d'indice $n/2$

EX A_3

Def 3-cycles et 2-transpositions

Thm A_n engendré par les 3-cycles, et les $(1\,2\,k)$ et les $(k\,k+1\,k+2)$ (ROM)

Thm L'unique sous groupe distingué non trivial de S_n est A_n pour $n \geq 5$ (ROM)

EX A_4 calcul explicite, A_4 n'a pas de sous groupe d'ordre 6

Thm A_n est simple pour $n \geq 5$

Thm Classes de conjugaison de A_n en fonction de celles de S_n (??)

■ **RÉSULTATS STRUCTURELS**

Thm Groupe dérivés et centres

Thm Les automorphismes de S_n sont intérieurs pour $n \neq 6$

EX Il existe des automorphismes de S_6 qui ne sont pas intérieurs

EX Injections de S_n dans A_{n+2} mais pas de S_n dans A_{n+1}

7.105.3 Applications

■ **DÉNOMBREMENT**

Def Inversion de Pascal

EX Nombre de dérrangements

Def Coefficient binômial via l'action de S_n sur les parties de X et l'orbite d'une partie à k éléments

Def Formule de Burnside

EX Nombre moyen de points fixes, application aux enfants

EX Complexité moyenne du tri rapide (uniformité)

■ **DÉTERMINANT**

Def Forme linéaire altenée/etc

Thm Formule du déterminant d'une matrice

AP Généralisation à un anneau

■ **POLYNÔME SYMÉTRIQUES**

Def Action de S_n sur $K[X_1,\dots,X_n]$

Def Polynômes symétriques élémentaires, relations coefficients racines

Thm Des polynômes symétriques

App Résolution par radicaux des équations de degré 3 par la méthode de Lagrange (GOU)

■ **GROUPES D'ISOMÉTRIE**

EX Interprétation de S_3 comme le groupe d'isométries du triangle équilatéral dans le plan

ROM Tout ce qui est sur les groupes d'isométries en général et truc conservant une partie

ROM Groupes d'isométrie du cube, etc..

DEV Sous groupes d'isométrie.

■ **PEUT-ÊTRE**

PER les isomorphismes exceptionnels ?

7.106 ■ GROUPE LINÉAIRE D'UN ESPACE VECTORIEL DE DIMENSION FINIE, SOUS GROUPES. APPLICATIONS

■ **DÉVELOPPEMENTS** **4.5**

D00 FROBÉNIUS-ZOLOTAREV ⋆⋆⋆⋆

D01 SOUS GROUPES COMPACTS DE GLN(R) ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon algèbre

Objectif Agrégation

H2G2

Perrin

Rombaldi

FGN

Seguin Invitations aux formes quadratiques

■ **RAPPORT DE JURY**

> Cette leçon ne doit pas se résumer à un catalogue de résultats épars sur $GL(E)$. Il est important de savoir faire correspondre les sous-groupes du groupe linéaire avec les stabilisateurs de certaines actions naturelles (sur des formes quadratiques, symplectiques, sur des drapeaux, sur une décomposition en somme directe, etc.). On doit présenter des systèmes de générateurs, étudier la topologie et préciser pourquoi le choix du corps de base est important. Les liens avec le pivot de Gauss sont à détailler. Il faut aussi savoir réaliser S_n dans $GL(n,K)$ et faire le lien entre signature et déterminant. S'ils le désirent, les candidats peuvent aller plus loin en remarquant que la théorie des représentations permet d'illustrer l'importance de $GL(n,\mathbb{C})$et de son sous-groupe unitaire.

■ **IDÉE DU PLAN :** Il faut centrer la leçon sur les groupes, et surtout pas sur les *actions*. On doit évoquer celles-ci (équivalence, conguruence) quand on présente un système de générateur (pivot de gauss) ou quand on introduit un sous groupe (orthogonal).

Ne pas oublier la décomposition polaire, QR, cholesky, LU, qui permettent d'agrémenter la leçon de considérations pratiques. La partie corps finis

Un plan séparant finitude/topologie en deux dernières parties est sympathique car découple Frobenius des sous groupes compacts.

I. GROUPE LINÉAIRE ET SPÉCIAL LINÉAIRE
- A) Définitions
- B) Gauss et générateurs
- C) Groupe dérivés

II. GROUPES ET CORPS FINIS
- A) S_n, Brauer, Burnside
- B) Dénombrements
- C) Frobenius

III. TOPOLOGIE
- (a) Topologie sur GL
- (b) Groupe orthogonal
- (c) Isométries en dim 2/3

■ **MISC**

FGN $GL_n(k) \simeq GL_m(k)$ ssi $n = m$

FGN Drapeaux et actions sur les drapeaux

■ **DÉTERMINANT**

Def Déterminant

Def SL_n

Thm $GL(n,k) \simeq SL(n,k) \rtimes k^\times$

■ **DIAGONALISABLE, TRIGONALISABLE**

Def Drapeau

Thm Trigonalisable ssi stabilise un drapeau

Def Diagonalisable ssi stabilise tout espace

■ **GÉNÉRATEURS**

Def Transvection, dilatation, permutations

Thm Conjugaison et transvections

Thm Génération de GL

Thm Génération de SL

■ **PIVOT DE GAUSS ET ACTIONS DE GL**

Def $M \mapsto PM$

Def $M \mapsto MP^{-1}$

Def $M \mapsto PMQ^{-1}$

Alg Pivot de Gauss

Thm Forme réduite pour l'équivalence

Thm Forme réduite pour la translation

■ **CENTRES ET GROUPES DÉRIVÉS**

Def Z, D

Thm Centres homothéties

Thm Groupes dérivés

Thm $GL_n(\mathbb{F}_2) \simeq SL_n(\mathbb{F}_2)$

EX $GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2) \simeq S_3$ et son groupe dérivé est A_3

EX $SL_2(\mathbb{F}_3) \neq S_4$ et $SL_2(\mathbb{F}_3) \simeq \mathbb{H}_8 \rtimes Z/3Z$

■ **SUR LES CORPS FINIS**

Thm Cardinaux de $GL_n(\mathbb{F}_q)$ etc...

Cor p-sylows

■ **TOPOLOGIE**

Thm GL_n est ouvert dense

APP ... multiples !

APP Base de M_n composée d'éléments de GL_n

■ **GROUPE SYMÉTRIQUE**

Def Réalisation du groupe symétrique

Thm Brauer

APP Théorèmes de Sylow

Thm Burnside

EX $(Z/2Z)^N$

Def Réalisation de GL_n dans S_k

Thm Frobenius-Zolotarev

EX Symbole de Legendre

EX Signature de Frobenius

■ **ACTION PAR CONJUGAISON**

Def $M \mapsto PMP^{-1}$

Def Interprétation géométrique

Thm Invariants de Frobenius

■ **GROUPE ORTHOGONAL**

Def Forme quadratique

Def Forme simplecique

Def Groupe orthogonal/d'isométries

Def Groupe spécial orthogonal

Rem $1 \to SO_n \to O_n \to 1$

Thm Produit semi-direct si n pair

Thm Générateurs de O_n et SO_n (réflexions)

Thm Centre du groupe othogonal

Thm Groupe dérivé du groupe orthogonal

Thm Cardinal du groupe orthogonal sur un corps fini (TODO ?)

Thm Théorie de Witt ??

Thm Classification des formes quadratiques

DEV Réciprocité quadratique

Thm Réduction simultanée

■ **Groupe Orthogonal $\mathbb{R}$ et $\mathbb{C}$**

Thm Fome réduite des éléments de $SO_n(\mathbb{R})$

DEV Sous groupes compacts

Csq Ellipsoïde de John et compagnie

Def S_n, S_n^+, S_n^{++}

Thm Racines carrées dans S_n etc ...

Thm Décomposition d'Iwasawa

Thm Décomposition polaire

■ **Exponentielle**

Def Définition de l'expo

Thm C'est une application continue

Rem $\det\circ\exp = \exp\circ\mathrm{tr}$ (sur tout corps parfait ??)

Thm Surjectivité de l'exp via dunford

APP Racines p-èmes

APP Décomposition de dunford multiplicative

Thm Petits sous groupes de GL_n

Thm $GL(n,\mathbb{R}) \simeq O_n \times S_n$ un groupe compact et un espace vectoriel

Thm $\exp(A_n) = SO_n$ dans $\mathbb{R}$

EX $X' = AX$ avec A antisymétrique

■ **Isométries en dimension 2 et 3**

Def Polyèdre régulier

EX Groupe du tétraèdre, etc ...

Thm Sous groupes de SO_2

DEV Sous groupes finis SO_3

DEV SO_3 et les quaternions

7.108 ■ EXEMPLE DE PARTIES GÉNÉRATRICES D'UN GROUPE. APPLICATIONS

■ **DÉVELOPPEMENTS** **4.0**

D02 THÉORÈME DE BRAUER EN CAR QCQ ⋆⋆⋆⋆⋆

D03 SO3(R) ET LES QUATERNIONS ⋆⋆⋆

7.120 ■ ANNEAUX Z/NZ. APPLICATIONS

■ **DÉVELOPPEMENTS** **3.5**

D00 FROBÉNIUS-ZOLOTAREV ⋆⋆⋆⋆

D12 ORDRE MOYEN $\phi(n)$ ⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon algèbre

FGN Algèbre 1

Objectif Agrégation

Demazure

Perrin

Rombaldi Regarder les exercices et les trucs sur les anneaux avant

■ **RAPPORT DE JURY**

Dans cette leçon, l'entier n n'est pas frcément un nombre premier. Il serait bon de connaître les idéaux de Z/nZ et plus généralement, les morphismes de groupes te Z/nZ dans Z/mZ. Il est nécessaire de bien maîtriser le théorème chinois et sa réciproque. S'ils le désirent les candidats peuvent poursuivre en donnant ue généralisation du théorème chinois lorsque les deux éléments ne sont pas premiers entre eux, ceci en faisant apparaître le pgcd et le ppcm des deux éléments. Il faut bien sûr savoir appliquer le théorème chinois à l'étude du groupe des inversibles et ainsi, retrouver la multiplicativité de l'indicatrice d'Euler. Toujours dans le cadre du théorème chinois, il est bon de distinguer clairement les propriétés de groupes additifs et d'anneaux, de connaître les automorphismes, les nilpotents et les idempotents. Enfin, il est indispensabe de présenter quelques applications arithmétiques des propriétés de Z/nZ telles que l'étude de quelques équations diophantiennes bien choisies. De même les applications cryptographiques telles que l'algorithme RSA sont naturelles dans cette leçon. S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant au calcul effectif des racines carrées dans Z/nZ.

7.120.1 Premiers résultats de structure

■ **PROPRIÉTÉS ARITHMÉTIQUES DE Z**

Def Anneau euclidien, division euclidienne

Def Structure des idéaux, des sous-groupes, etc.

Thm Gauss, divisibilité pgcd ppcm et compagnie

Def Théorème de bézout, et calcul pratique via euclide étendu

Def Nombre premier, quelques propriétés

Thm Théorème de factorisation en nombre premiers

■ **LE GROUPE Z/nZ**

Def Définition du groupe, notion de congruence (version additive)

Def Cyclicité, générateurs

Def Morphismes de Z/nZ

Thm Automorphismes de Z/nZ (groupes)

Thm Théorème chinois (V1)

EX Structure des groupes abéliens finis

■ **L'ANNEAU Z/nZ**

Def Définition de l'anneau, congruence

EX Calcul modulaire numérique

Thm Des chinois pour les anneaux, réciproque et calcul pratique

EX Synchronisation de processus

EX $(0,2)$ dans $Z/3Z \times Z/5Z$

Def Morphismes de Z/nZ

Thm Nilpotents, idempotents, inversibles

EX Calcul effectif d'inversibles via Bézout

Thm Structure des inversibles

EX Cyclicité des inversibles

Thm Structure des automorphismes

7.120.2 Polynômes et corps

■ **LES CORPS $(Z/pZ)^\alpha$**

Def Z/pZ est un corps, caractéristique d'un corps fini

Thm Caractérisation des corps finis

Thm Schwartz-Zippel

Def Test de nullité (PIT)

■ **POLYNÔMES DANS Z ET Q**

Def Contenu d'un polynôme

Def Réduction modulo p

Def Critère d'Eisenstein

Def Irréductibilité sur Z entraine celle sur Q sous quelques hypothèses (PER)

■ **POLYNÔMES CYCLOTOMIQUE**

Def Polynôme cyclotomique en général

Def Équation de récurrence

Def À coefs dans Z (resp corps de base)

Def Irréductibilité, lien avec les F_p

APP Progression de dirichlet faible

7.120.3 Résolution d'équations

■ **Équations diophantiennes linéaires**

Def Définition générale

EX Diophantiennes droites, avec Bézout

Thm Invariants de Smith ?

EX Un exemple ?

Thm Sophie Germain ?

Thm Triplets pythagoriciens ?

■ **Résidus quadratiques**

Def Résidus quadratiques

EX Utilisation du symbole de Legendre pour résoudre un polynôme de degré 2

Def Forme quadratique sur les corps finis ?

Thm Loi de réciprocité quadratique

DEV Frobenius Zolotarev

Def Test de primalité Solovay-Strassen ?

Thm p premier impair, p est somme de deux carrés ssi $p \equiv 1\,[4]$.

AP Entiers de Gauss

AP Structure des solutions de $x^2 + y^2 = pz^2$

Thm Classification des formes quadratiques sur corps finis

Thm Les carrés dans les Z/nZ en général, le symbole de Jacobi ! (Demazure)

■ **Théorème de Fermat**

Def $x^n + y^n = z^n$

Def Triplets pythagoriciens

Def Sophie Germain

7.120.4 Applications à l'arithmétique

■ **Fonctions arithmétiques**

Def Indicatrice d'Euler, propriétés sur l'indicatrice

Def Nombre moyen de diviseurs

Pro Formule d'inversion de Möbius

DEV Proba que deux entiers...

Thm Dirichlet Faible

Thm Divergence de $\sum 1/p$

Thm Répartition des nombres premiers

■ **Cryptosystème RSA**

Def Cryptosystème, clef publique clef privée, etc.

Thm Le RSA marche bien

■ **Tests de primalité (ROM p 324)**

Def Euler $a^{\phi(n)} = 1$

Def Fermat $a^{n-1} = 1$

Def Théorème de Wilson

Thm Nombres de Carmichael (GOU)

Def Miller-Rabin

Def AKS

Def PIT + Frobenius (ROM + Arora Barack)

7.121 ■ NOMBRES PREMIERS. APPLICATIONS

■ **DÉVELOPPEMENTS** **5.0**

D00 FROBÉNIUS-ZOLOTAREV ⋆⋆⋆⋆

D08 RÉCIPROCITÉ QUADRATIQUE ⋆⋆⋆⋆⋆

D12 ORDRE MOYEN $\phi(n)$ ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon algèbre

FGN Algèbre 1

Objectif Agrégation

Demazure

Perrin

Rombaldi Regarder les exercices et les trucs sur les anneaux avant

■ **RAPPORT DE JURY**

Le sujet de cette leçon est vaste. Aussi les choix devront être clairement motivés. La réduction modulo p n'est pas hors-sujet et constitue un outil puissant pour résoudre des problèmes arithmétiques simples. La répartition des nombres premiers est un résultat historique qu'il faudrait citer. Sa démonstration n'est bien sûr pas exigible au niveau de l'agrégation. Quelques résultats sur les corps finis et leur géométrie sont les bienvenus, ainsi que des applications en cryptographie.

7.121.1 Nombres premiers et arithmétique

■ **PROPRIÉTÉS ARITHMÉTIQUES DE Z**

Def Anneau euclidien, division euclidienne

Def Structure des idéaux, des sous-groupes, etc.

Thm Gauss, divisibilité pgcd ppcm et compagnie

Def Théorème de bézout, et calcul pratique via euclide étendu

Def Nombre premier, infinité de nombres premiers etc.

Thm Théorème de factorisation en nombre premiers

Def Valuation p-adique, applications pgcd ppcm et compagnie

Def Crible d'eratosthène et compagnie

■ **FONCTIONS ARITHMÉTIQUES**

Def Indicatrice d'Euler, propriétés sur l'indicatrice

Def Nombre moyen de diviseurs

Pro Formule d'inversion de Möbius

DEV Proba que deux entiers...

Def Généralisation à $r \geq 2$ entiers

7.121.2 Dans les structures algébriques

■ **ÉQUATIONS DIOPHANTIENNES LINÉAIRES**

Def Définition générale

EX Diophantiennes droites, avec Bézout

Thm Invariants de Smith ?

EX Un exemple ?

Thm Sophie Germain ?

Thm Triplets pythagoriciens ?

■ **APPLICATIONS AUX GROUPES**

Def p-groupes

Def toutes les propriétés triviales sur les p-groupes

Thm Théorèmes de Sylow

APP exemples et applications

EX Groupes d'ordre pq

Thm Classification des groupes abéliens finis

■ **LES CORPS $(Z/pZ)^\alpha$**

Def Z/pZ est un corps, caractéristique d'un corps fini

Thm Caractérisation des corps finis

Thm Schwartz-Zippel

Def Test de nullité (PIT)

■ **POLYNÔMES DANS Z ET Q**

Def Contenu d'un polynôme

Def Réduction modulo p

Def Critère d'Eisenstein

Def Irréductibilité sur Z entraine celle sur Q sous quelques hypothèses (PER)

■ **RÉSIDUS QUADRATIQUES**

Def Résidus quadratiques

EX Utilisation du symbole de Legendre pour résoudre un polynôme de degré 2

Def Forme quadratique sur les corps finis ?

Thm Loi de réciprocité quadratique

DEV Frobenius Zolotarev

Def Test de primalité Solovay-Strassen ?

Thm p premier impair, p est somme de deux carrés ssi $p \equiv 1\,[4]$.

AP Entiers de Gauss

AP Structure des solutions de $x^2 + y^2 = pz^2$

Thm Classification des formes quadratiques sur corps finis

Thm Les carrés dans les Z/nZ en général, le symbole de Jacobi ! (Demazure)

7.121.3 Critères et répartition (CRUCIAL)

■ **RÉPARTITION**

Thm Dirichlet Faible

Thm Divergence de $\sum 1/p$

Thm Répartition des nombres premiers

■ **CLASSES DE NOMBRES PREMIERS**

Def Nombres de Mersennes

Def Nombres de Carmichael

Def Sophie-Germain

■ **TESTS DE PRIMALITÉ (ROM P 324)**

Def Euler $a^{\phi(n)} = 1$

Def Fermat $a^{n-1} = 1$

Def Théorème de Wilson

Thm Nombres de Carmichael (GOU)

Def Miller-Rabin

Def AKS

Def PIT + Frobenius (ROM + Arora Barack)

■ **CRYPTOSYSTÈME RSA**

Def Cryptosystème, clef publique clef privée, etc.

Thm Le RSA marche bien

7.123 ■ CORPS FINIS. APPLICATIONS

■ **DÉVELOPPEMENTS** **5.0**

D05 DÉNOMBREMENT POLYNÔMES IRRÉDUCTIBLES ⋆⋆⋆⋆⋆

D10 ALGORITHME DE BERLEKAMP ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon algèbre

FGN Algèbre 1

Objectif Agrégation

Demazure

Rombaldi

Perrin

■ **RAPPORT DE JURY**

Une construction des corps finis doit être connue et une bonne maîtrise des calculs dans les corps finis est indispensable. Les injections des divers $\mathbb{F}_q$ doivent être connues et les applications des corps finis (y compris pour $\mathbb{F}_q$ avec q non premier !) ne doivent pas être oubliées, par exemple l'étude de polynômes à coefficients entiers et de leur irréductibilité peut figurer dans cette leçon. La structure du groupe multiplicatif doit aussi être connue. Le calcul des degrés des extensions et le théorème de la base téléscopique sont incontournables. L'étude des carrés dans un corps fini et la résolution d'équations de degré 2 sont envisageables. S'ils le désirent, les candidats peuvent aller plus loin en détaillant des codes correcteurs ou en étudiant l'irréductiblilité des polynômes à coefficients dans un corps fini.

7.123.1 Construction et étude des corps finis

■ **CARACTÉRISTIQUE** **[ROM]**
SOUS CORPS PREMIER

Def $\phi : \mathbb{Z} \to A$

Def Caractéristique

Thm Première ou 0

EX $\mathbb{F}_2$

Def Sous corps premier

EX Corps des fractions rationnelles sur $\mathbb{F}_2$.

Def Morphisme de Frobenius

EX $\mathbb{F}_2$ pour BPP ?

■ **EXTENSIONS DE CORPS** **[PER]**

Def Extension de rupture d'un polynôme irréductible

Thm Isomorphisme

EX Construction de $\mathbb{F}_{16}$

Def Extension de décomposition

EX Construction de $\mathbb{F}_{16}$

Thm De la base télescopique

Def $\mathbb{F}_q$ n'est jamais algébriquement clos

■ **ÉTUDE THÉORIQUE** **[ROM]**
DES CORPS FINIS

Def Cardinaux possibles

Def Ce sont tous des corps de décomposition du truc qui va bien

Thm Existence, $\mathbb{F}_{p^n}$ est bien un corps

DEV Wedderburn

Def Anneau integre fini est un corps

Def Construction de la clôture algébrique

Def Inclusions des $\mathbb{F}_p$ si et seulement si division

7.123.2 Polynômes et corps finis

■ **CONSTRUCTION "EXPLICITE" DES** **[ROM]**
CORPS FINIS

REM Toute application de $\mathbb{F}_q$ dans $\mathbb{F}_q$ est polynômiale ...

DEV Dénombrement des polynômes

Thm Corps finis = corps rupture

Csq Élément primitif

Csq Automorphismes de $\mathbb{F}_q$

Rem Le sous groupe multiplicatif est cyclique

EX Dans $\mathbb{F}_{16}$ on a un élément "de rupture" qui n'est pas génératrice du groupe multiplicatif

■ **POLYNÔMES** **[PER]**

Def Réduction modulo p

Def Degré des extensions pour irréductibilité

Def Eisenstein

Def Racines simples et dérivées

Def Corps parfait et compagnie

DEV Berlekamp

Thm Schwartz-Zippel, PIT

APP Test de primalité

■ **POLYNÔMES CYCLOTOMIQUES** **[PER]**

Def Définition abstraite

Def Équation de récurrence

Def Formule de Möbius

Thm Irréductibles et coefs entiers sur Z

Thm $\Phi_{n,p} = \phi(\Phi_{n,Q})$

APP Progression de dirichlet faible [ROM]

7.123.3 Algèbre linéaire et bilinéaire

■ **ALGÈBRE LINÉAIRE** **[PER]**

Def Cardinaux des GL_n, SL_n

Thm Dénombrement des nilpotents d'indice max (facile)

Def Trouver des p-sylow

Thm Frobenius Zolotarev ?

Rem f diagonalisable si et seulement si $f^q = f$ [GOU]

Rem Contre exemple pour l'union d'espaces vectoriels [GOU]

Thm Groupes dérivés et compagnie

■ **CARRÉS DANS $\mathbb{F}_q$** **[ROM]**

Def Le sous groupe des carrés, des puissances r-èmes

Def Dénombrement via les polynômes

Thm Caractérisations

APP Infinité de $4m+1$

APP Polynômes de degré 2

Def Symbole de Legendre

DEV Frobenius Zolotarev

APP Legendre 2, p

APP Signature du morphisme de Frobenius

■ **FORMES QUADRATIQUES** **[ROM]**

APP Équations de degré 2 dans $\mathbb{F}_q$

Thm Caractérisation des formes quadratiques

DEV Réciprocité quadratique

Def Symbole de Jacobi

Thm Des trucs du demazure sur pourquoi c'est bien utile ?

7.123.4 Possibilités d'ouverture

■ **CRYPTOGRAPHIE** **[DEM]**

Def elliptiques etc ...

EX El-Gamal

EX Partage de secret via polynômes...

Def Logarithme discret toussa

■ **TESTS DE PRIMALITÉ** **[DEM]**

EX AKS bordel !!!

■ **CODES CORRECTEURS** **[DEM]**

Def Codes linéaires sur les corps finis

Def Codes cycliques sur les corps finis

7.141 ■ POLYNÔMES IRRÉDUCTIBLES À UNE INDÉTERMINÉE. CORPS DE RUPTURE. EXEMPLES ET APPLICATIONS

■ **DÉVELOPPEMENTS** **5.0**

D05 DÉNOMBREMENT POLYNÔMES IRRÉDUCTIBLES ⋆⋆⋆⋆⋆

D10 ALGORITHME DE BERLEKAMP ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon algèbre

FGN Algèbre 1

Objectif Agrégation

Demazure

Rombaldi

Perrin

■ **RAPPORT DE JURY**

La présentation du bagage théorique permettant de définir corps de rupture, corps de décomposition, ainsi que des illustrations dans différents types de corps (réel, rationnel, corps finis) sont inévitables. Les corps finis peuvent être illustrés par des exemples de polynômes irréductibles de degré 2, 3, 4 sur $\mathbb{F}_2$ ou $\mathbb{F}_3$. Il est nécessaire de présenter des critères d'irréductibilité de polynômes et des polynômes minimaux de quelques nombres algébriques. Il faut savoir qu'il existe des corps algébriquement clos de caractéristique nulle autres que $\mathbb{C}$; il est bon de savoir montrer que l'ensemble des nombres algébriques sur le corps $\mathbb{Q}$ des rationnels est un corps algébriquement clos. Le théorème de la base téléscopique, ainsi que les utilisations arithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes, est incontournable.

Trouver un plan qui premet de ne pas isoler les corps finis, tout en ayant un nombre de parties raisonnable

7.141.1 Polynômes irréductibles

■ **GÉNÉRALITÉS**

Def Irréductibilté dans un anneau

Def $A[X]$ et ses propriétés

Def Degré et trucs évidents

Thm Irréductibilité pour les petits degrés

■ **PROPRIÉTÉS DE STRUCTURE**

Def Division euclidienne

Def Factorialité et compagnie

Def Quotient par un polynôme

Def Corps si poly irred

■ **CRITÈRES D'IRRÉDUCTIBILITÉ**

Def Polynômes primitifs

Def Contenu

Def Les éléments de Frac(A)

Thm Eisenstein

Thm Irréductibilité modulo un idéal premier

DEV Algorithme de Berlekamp

7.141.2 Extensions de corps

■ **EXTENSIONS DE CORPS**

Def Extension de corps

Def Base télescopique

Def Élément algébrique

Def Degré des extensions pour irréductibilité

■ **EXTENSION DE RUPTURE**

Def Existence, unicité

THM Élément primitif

■ **EXTENSION DE DÉCOMPOSITION**

Def Existence, unicité

■ **CLÔTURE ALGÉBRIQUE**

Def Existence, unicité

7.141.3 Construction de corps

■ **CORPS FINIS**

Def Cardinaux possibles

Def Ce sont tous des corps de décomposition du truc qui va bien

Thm Existence, $\mathbb{F}_{p^n}$ est bien un corps

Def Anneau integre fini est un corps

Def Construction de la clôture algébrique

Def Inclusions des $\mathbb{F}_p$ si et seulement si division

REM Toute application de $\mathbb{F}_q$ dans $\mathbb{F}_q$ est polynômiale ...

DEV Dénombrement des polynômes

Thm Corps finis = corps rupture

Csq Élément primitif

Csq Automorphismes de $\mathbb{F}_q$

Rem Le sous groupe multiplicatif est cyclique

EX Dans $\mathbb{F}_{16}$ on a un élément "de rupture" qui n'est pas génératrice du groupe multiplicatif

Thm Schwartz-Zippel, PIT

■ **EXTENSIONS CYCLOTOMIQUES**

Def Équation de récurrence

Def Formule de Möbius

Thm Irréductibles et coefs entiers sur Z

Thm $\Phi_{n,p} = \phi(\Phi_{n,Q})$

APP Progression de dirichlet faible [ROM]

EX AKS

Thm Wedderburn

7.150 ■ EXEMPLES D'ACTIONS DE GROUPES SUR LES ESPACES DE MATRICES

■ **DÉVELOPPEMENTS** **4.5**

D01 SOUS GROUPES COMPACTS DE GLN(R) ⋆⋆⋆⋆⋆

D06 INVARIANTS DE FROBENIUS ⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon algèbre

Objectif Agrégation

H2G2 pour tous les tableaux !

Perrin

Rombaldi

FGN

Seguin Invitations aux formes quadratiques

■ **RAPPORT DE JURY**

> Dans cette leçon il faut présenter différentes actions (congruence, similitude, équivalence, ...) et dans chaque cas on pourra dégager d'une part des invariants (rang, matrices échelonnées réduites...) et d'autre part des algorithmes, comme le pivot de Gauss, méritent aussi d'être présentés dans cette leçon. Si l'on veut aborder un aspect plus théorique, il est pertinent de faire apparaître à travers ces actions quelques décompositions célèbres ; on peut décrire les orbites lorsque la topologie s'y prête. S'ils le désirent, les candidats peuvent travailler sur des corps finis et utiliser le dénombrement dans ce contexte.

■ **IDÉE DU PLAN :** On procède en construisant un plan thématique. D'abord les actions faciles, sur $M_{n,1}$, à gauche et à droite. Ensuite la similitude et en fin la congruence.

Chaque partie fait intervenir *invariants*, *formes normales*, *factorisations*[1], et *topologie*. On ne manquera pas d'en souligner les applications (connexité, résolution de systèmes...).

On évitera de se lancer dans une description trop lourde des actions, par exemple l'action par congruence se fait directement de manière matricielle, et il n'y a pas besoin de traiter autre chose que les corps usuels.

I. ACTIONS PAR PRODUIT
- A) À droite
- B) À gauche
- C) Steinitz

II. CONJUGAISON
- A) Invariants
- B) Topologie
- C) Combinatoire

III. CONGRUENCE
- (a) $\mathbb{R}$ et $\mathbb{C}$
- (b) Corps finis

1. Décomposition polaire !

150 : Étudier la décomposition en valeurs singulières

■ **Actions sur $M_{n,1}(k)$**

Def Action du groupe symétrique

DEV Brauer

Pro Décomposition de Bruhat

Def Action linéaire veut dire injection dans GL_n

Pro Burnside

Pro Sous groupes compacts de GL_n

■ **Action de GL_n par translation**

Def

Alg Pivot de Gauss

Thm Forme réduite

EX Exemples du FGN

■ **Action de GL_n par équivalence**

Def

Thm Forme réduite

EX Exemples du FGN

Thm Topologie des orbites via le rang

??? Dénombrement des matrices de rang r ?

■ **Action par conjugaison (I)**

Def $M \mapsto PMP^{-1}$

Def π_u, χ_u

DEV Invariants de Frobenius

Def Endomorphisme cyclique

EX Théorème de Kronecker

■ **Action par conjugaison (II)**

Def Aspects topologiques

Thm topologie des classes de similitude

Thm Continuité de χ_u mais pas de π_u

Thm Adhérence des diago, etc ...

■ **Action par conjugaison (III)**

Def Aspects combinatoires

Thm Critère de diagonalisabilité

EX Dénombrement des nilpotents d'indice max

EX Dénombrement des diagonalisables

■ **Action par conjugaison (IV)**

Def Aspects algébriques

Thm Lemme des noyaux, dunford

Thm Réduction des nilpotents

Thm Décomposition de Jordan

APP Tableau de Young et combinatoire

■ **Action par congruence (I)**

Def

Thm Classification des formes quadratiques

Thm Réduction simultanée

DEV Réciprocité quadratique

■ **Action par congruence (II)**

Thm Fome réduite des éléments de $SO_n(\mathbb{R})$

DEV Sous groupes compacts

Csq Ellipsoïde de John et compagnie

Def S_n, S_n^+, S_n^{++}

Thm Racines carrées dans S_n etc ...

Thm Décomposition d'Iwasawa

Thm Décomposition polaire

■ **Action par congruence (III)**

Def Action de $O_p \times O_q$ sur $M_{p,q}$

Thm Décomposition en valeurs singulières

APP Compression d'images

APP Pseudo-inverse

7.151 ■ DIMENSION D'UN ESPACE VECTORIEL. RANG. EXEMPLES ET APPLICATIONS

■ **DÉVELOPPEMENTS** **4.5**

D06 INVARIANTS DE FROBENIUS ⋆⋆⋆

D10 ALGORITHME DE BERLEKAMP ⋆⋆⋆⋆

D24 EXTREMA LIÉS ET APPLICATION ... ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon algèbre

FGN Algèbre 1

Rombaldi

Objectif Agrégation

Tauvel Pour toute la partie "cours"

Demazure

Mneimné

Ciralet

Allaire Kaber

■ **RAPPORT DE JURY**

> Dans cette leçon, il est important de présenter les résultats fondateurs de la théorie des espaces vectoriels de dimension finie en ayant une idée de leurs preuves. Ces théorèmes semblent simples car ils ont été très souvent pratiqués, mais leur preuve demande un soin particulier. Il est important de savoir justifier pourquoi un sous-espace vectoriel d'un espace vectoriel de dimension finie est aussi de dimension finie. Le pivot de Gauss ainsi que les diverses notions et caractérisations du rang trouvent leur place dans cette leçon. Les applications sont nombreuses, on peut par exemple évoquer l'existence de polynômes annulateurs ou alors décomposer les isométries en produits de réflexions. S'ils le désirent, les candidats peuvent déterminer des degrés d'extensions dans la théorie des corps ou s'intéresser aux nombres algébriques. Dans un autre registre, il est pertinent d'évoquer la méthode des moindre carrés dans cette leçon, par exemple en faisant ressortir la condition de rang maximal pour garantir l'unicité de la solution et s'orienter vers les techniques de décomposition en valeurs singulières pour le cas général. On peut alors naturellement explorer l'approximation d'une matrice par une suite de matrices de faible rang.

■ **IDÉE DU PLAN :**

On suit l'intitulé du cours en commençant par la dimension pour aller vers le rang. On utilise ensuite ces notions en algèbre et en analyse.

Il ne faut pas oublier toutes les définitions préalables à la notion même de dimension finie. La dualité par exemple fonctionne particulièrement bien au niveau des espaces. Tout ce qui est réduction rentre parfaitement dans endomorphismes. Les applications aux extensions de corps et à l'analyse (équations différentielles, extrema liés) sont inévitables.

Ne surtout pas négliger les apports de la topologie en dimension finie, ou plutôt de la dimension finie en topologie...

I. DIMENSION
   A) Notion de dimension
   B) Sous espaces
   C) Dimension et dualité
   D) Topologie de la dimension finie

II. RANG
   A) Applications linéaires
   B) Action par équivalence
   C) Action par conjugaison

III. APPLICATIONS
   (a) Extensions de corps
   (b) Extrema liés, rang constant etc...
   (c) Équations différentielles

■ **PSEUDO-SOLUTIONS ET RANG**

Def Méthode des moindres carrés

Thm Décomposition en valeurs singulières

APP Pseudo-inverse

Thm Approximation par des matrices de rang faible ?

■ **THÉORIE DE LA DIMENSION ET DU RANG**

Def Matroïde des familles libres

Thm Toutes les bases ont même cardinal

Thm De la base incomplète

EX Bases dans $\mathbb{F}_q^n$

Def Caractérisations de sommes directes avec le rang

Thm Théorème du rang

Def Dimension d'un produit, d'une somme

Thm Caractérisation d'injectivité en dimension finie

EX Même dimension ssi isomorphes

EX Même dimension implique supplémentaire commun

■ **DIMENSION ET TOPOLOGIE**

Thm La sphère unité est compacte ssi dimension finie

Thm Fermé-borné $\Longleftrightarrow$ compact

■ **DIMENSION ET FORMES QUADRATIQUES**

Def Isotrope, anisotrope

Def Orthogonal

Thm Si anisotrope alors $\dim F + \dim F^\perp = \dim E$

ETC...

■ **APPLICATIONS LINÉAIRES ET RANG**

Alg Pivot de Gauss

Thm Forme normale réduite

APP Calcul de noyau

DEV Algorithme de Berlekamp

Def Propriétés topologiques du rang

Def Propriétés combinatoires du rang

■ **DÉTERMINANT ET RANG**

Def Déterminant

Thm Inversible ssi det inversible

Thm Rang ssi det d'une sous matrice

■ **SYSTÈMES ET RANG**

Def Système linéaire

Thm Résolution via Cramer

Def Sur-conditionné, sous-conditionné, etc ...

Met Moindre carrés

■ **DUALITÉ EN DIMENSION FINIE**

Def Espace dual, isomorphe

Pro Propriétés sur les dimensions etc...

Thm Sous espaces de $\mathscr{C}(\mathbb{R})$

■ **CHANGEMENT DE COORDONNÉES**

Thm "base incomplète pour les changements de coordonnées".

Thm Forme normale des submersions

EX det est une submersion

Thm Forme normale des immersions

Thm Du rang constant

■ **SOUS-VARIÉTÉS**

Def Définition par redressement

Thm des sous variétés

EX La sphère est une sous var

EX Le tore est une sous-var

EX $O_n(\mathbb{R})$ est une sous-var

EX SL_n est une sous-var

Thm Cartan-Von Neumann

EX Matrices de rang r sous var est une sous-var ?

Def espace tangent

EX $T_x S^{n-1} = x^\perp$

EX $T_M O_n(\mathbb{R}) = MA_n(\mathbb{R})$

EX $T_M SL_n(\mathbb{R}) = M\{X \mid \operatorname{tr} X = 0\}$

DEV Extrema liés

APP Diagonalisation des matrices symétriques

APP Loi d'entropie maximale

APP Trajectoire sur un billard elliptique

■ **POLYNÔMES D'ENDOMORPHISME**

Def π_u

Thm Dimension de $k[u]$ etc ...

Thm Invariants de Frobenius

Thm Dimension du bicommutant

■ **DIMENSION ET GROUPES**

Thm Base de Burnside

Def Injection de S_n dans GL_n

Thm Brauer

Thm Burnside

■ **EXTENSIONS DE CORPS**

Def Ext

Thm Base télescopique

Def Élément algébrique etc ...

Thm Gauss-Wantzel

7.152 ■ DÉTERMINANT. EXEMPLES ET APPLICATIONS

■ **DÉVELOPPEMENTS** **5.0**

D00 FROBÉNIUS-ZOLOTAREV ⋆⋆⋆⋆⋆

D28 CONIQUE ET DÉTERMINANT ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon algèbre

FGN Algèbre 1

Rombaldi

Objectif Agrégation

Tauvel Pour toute la partie "cours"

Demazure

Mneimné

Ciralet

Allaire Kaber

■ **RAPPORT DE JURY**

> Dans cette leçon, il faut commencer par définir correctement le déterminant. Il est possible d'entamer la leçon en disant que le sous-espace des formes n-linéaires alternées sur un espace de dimension n est de dimension 1 et, dans ce cas, il est essentiel de savoir le montrer. Le plan doit être cohérent ; si le déterminant n'est défini que sur R ou C, il est délicat de définir $\det(A - XI_n)$ avec A une matrice carrée. L'interprétation du déterminant comme volume est essentielle. On peut rappeler son rôle dans les formules de changement de variables, par exemple pour des transformations de variables aléatoires. Le calcul explicite est important, mais le jury ne peut se contenter d'un déterminant de Vandermonde ou d'un déterminant circulant. Les opérations élémentaires permettant de calculer des déterminants, avec des illustrations sur des exemples, doivent être présentées. Il est bienvenu d'illustrer la continuité du déterminant par une application, ainsi que son caractère polynomial. Pour les utilisations des propriétés topologiques, on n'ommetra pas de préciser le corps de base sur lequel on se place. S'ils le désirent, les candidats peuvent s'intéresser aux calculs de déterminants sur Z avec des méthodes multimodulaires. Le résultant et les applications simples à l'intersection ensembliste de deux courbes algébriques planes peuvent aussi trouver leur place dans cette leçon pour des candidats ayant une pratique de ces notions.

■ **IDÉE DU PLAN :** Commencer par une définition minutieuse, puis s'attaquer aux calculs. Ensuite seulement faire des parties totalement disjointes d'applications, permettant une écriture facile du plan.

I. DÉTERMINANT
- A) D'une famille
- B) D'une application
- C) D'une matrice
- D) Application aux corps finis

II. CALCULS
- A) EXEMPLES

III. SYSTÈMES
- A) Système linéaire
- B) Rouché, Comatrice

IV. ALGÈBRE
- (a) SL_n
- (b) Volumes
- (c) Affine

V. ANALYSE
- (a) C^1-diffeo
- (b) Brouwer
- (c) Wronskien

■ **FORME MULTILINÉAIRES**

Def Forme n-linéaire

Def Alternée, antisymétrique, symétrique

Thm Formule du déterminant dans une base

Thm Dimension 1 de l'espace des déterminants

Thm Dimension des formes linéaires p alternées

■ **DÉTERMINANT D'UN ENDO**

Thm Formule ed changement de base

Def Déterminant d'un endomorphisme

Thm Indepandant de la base

Thm Propriétés du déterminant ...

Thm Inversible ssi det $\neq 0$

■ **DÉTERMINANT D'UNE MATRICE**

Def De l'application linéaire associée

Thm Formule avec des produits sur S_n

Def Généralisation à un anneau

Pro $1 \to SL \to GL \to k^* \to 1$

■ **SYSTÈMES LINÉAIRES**

Def Comatrice

Thm Formule de la comatrice

APP $f(Z^n) = Z^n$ ssi entier et déterminant entier

Thm Inversible ssi det inversible

Def Système de Cramer

Thm Formules de Cramer

■ **MÉTHODES DE CALCUL**

Def Développement par rapport à une ligne

Def Formule de Cauchy-binet (?)

Def Opérations élémentaires

ALG Pivot de Gauss !

ALG Invariants de Smith dans un anneau euclidien

■ **RÉDUCTION**

Def Polynôme caractéristique

Thm Lien valeur-propre/racine

Def Matrice compagnon

Thm Cayley-Hamilton

Thm De réduction ...

Thm Dans $\mathbb{C}$ les compagnons sont un ouvert connexe dense

Thm π_u n'est pas continu

■ **CORPS FINIS**

Thm $D(GL) = SL = \ker \det$ dans une majorité des cas

Thm Frobenius Zolotarev

APP Réciprocité quadratique

APP Signature de Frobenius

APP Legendre de $2/p$

■ **SYSTÈMES DE COORDONNÉES**

Def Topologie du rang

Thm De l'immersion

Thm De submersion

Thm Du rang constant

■ **DÉTERMINANTS CLASSIQUES**

Def Vandermonde

Def Déterminant circulant

Def Déterminant de Smith (arithmétique)

APP Brauer en dim qcq

Def Dédetrimant de Cauchy

APP Müntz

■ **GÉOMÉTRIE**

Def Volume

Thm Formule du changement de variables

Def Déterminant de Gram

Def Ellipsoïde

DEV Ellipsoïde de John

DEV Brouwer via Milnor

Def Déterminant et produit scalaire

Def Produit vectoriel $\mathbb{R}^3$

Def O_n et SO_n (directes vs indirectes)

■ ÉQUATIONS DIFFÉRENTIELLES

Def Wronskien

Thm Régularité du déterminant

Pro $w'(t) = \operatorname{tr} A(t)\, w(t)$

APP Sturm Liouville

APP Solutions particulières degré 2 déterminant de Cramer

7.153 ■ POLYNÔMES D'ENDOMORPHISME EN DIMENSION FINIE. RÉDUCTION. APPLICATIONS

■ **DÉVELOPPEMENTS** **5.0**

D06 INVARIANTS DE FROBENIUS ⋆⋆⋆⋆⋆

D09 DÉCOMPOSITION DUNFORD EFFECTIVE ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Mneimné Linéaires et compagnie

Gourdon Algèbre

Rombaldi

FGN Algèbre

■ **RAPPORT DE JURY**

Cette leçon ne doit pas être un catalogue de résultats autour de la réduction qui est ici un moyen pour démontrer des théorèmes ; les polynômes d'endomorphismes doivent y occuper une place importante. Il faut consacrer une courte partie de la leçon à l'algèbre $K[u]$ et connaître sa dimension sans hésitation. Il est ensuite possible de s'intéresser aux propriétés globales de cette algèbre. Les liens entre réduction d'un endomorphisme u et la structure de l'algèbre $K[u]$ sont importants, tout comme ceux entre les idempotents et la décomposition en somme de sous-espaces caractéristiques. Il faut bien préciser que, dans la réduction de Dunford, les composantes sont des polynômes en l'endomorphisme, et en connaître les conséquences théoriques et pratiques. L'aspect applications est trop souvent négligé. Il est possible, par exemple, de mener l'analyse spectrale de matrices stochastiques. On attend d'un candidat qu'il soit en mesure, pour une matrice simple de justifier la diagonalisabilité et de déterminer un polynôme annulateur (voire minimal). Il est bien sûr important de ne pas faire de confusion entre diverses notions de multiplicité pour une valeur propre λ donnée (algébrique ou géométrique). Enfin, calculer A^k ne nécessite pas, en général, de réduire A (la donnée d'un polynôme annulateur de A suffit souvent).

■ **IDÉE DU PLAN :** Encore une fois, suivre le plan du jury et ajouter une partie supplémentaire à la fin. On prend Rombaldi, Mansuy et Gourdon pour tout. Pas besoin de chercher la généralité : on fait de la réduction "abstraite" au début, en donnant des exemples dans tout. Puis on revient sur R/C où la topologie ajoute une structure intéressante. On fait du dénombrement quand bon nous chante, ce n'est pas une partie à part entière.

I. POLYNÔMES
- A) Polynôme caractéristique
- B) Algèbre $k[u]$
- C) Compagnons et cayley

II. RÉDUCTION
- (a) En scindant des polynômes
- (b) Via les cycliques
- (c) Quelques applications

III. DANS $\mathbb{R}/\mathbb{C}$
- (a) Topologie conjugaison
- (b) Continuité et densité
- (c) Exponentielle

153 : Le rombaldi fait *très très* bien les choses dans les exercices !

Idéal Annulateur

Def $\phi_u : k[X] \to k[u]$

Def π_u

Thm $\dim k[u] = \deg \pi_u$

Espaces cycliques

Def $\phi_{u,x} : k[X] \to \langle x \rangle_u$

Def $\pi_{u,x}$

Thm $\exists x, \pi_{u,x} = \pi_u$

Def Matrice compagnon

Pro Compagnon et cyclicité

Thm Théorème de Kronecker sur les polynômes entiers

Valeurs propres

Def Valeur propre, espace propre

Def χ_u

Thm $\pi_u | \chi_u$

Def Multiplicité algébrique, géométrique

Thm Algébrique et degrés, géométriques idem

Suite des noyau itérés

Def Suite des noyaux

Thm Décomposition de Fitting

Thm Réduction des nilpotents

Thm Réduction de Jordan

Lemme des noyaux

Def Lemme des noyaux

APP Décomposiiton de l'espace

Thm Diagonalisabilité, $k[u] \simeq k^r$

EX $u^q - u = 0$ dans $\mathbb{F}_q$

Thm Trigonalisablitié, $k[u]$ est un produit d'anneaux

Thm Décomposition de Dunford

DEV Dunford Effectif

Thm Idempotents de $k[u]$ si u trigonalisable

Commutant

Def Commutant

Thm Diagonalisation, trigonalisation simultanée

Def $k[u] = C(u)$ ssi cyclique

EX réduction des matrices circulantes

Thm $C(C(u)) = k[u]$

Systèmes dynamiques

Def Structure de l'espace des solutions d'une suite récurrente linéaire

Def Structure de l'espace des solutions d'une EDO linéaire d'ordre n

Def Structure de l'espace des solutions d'une EDO linéaire en dimension n

Def Étude asymptotique des EDOL

Thm Lyapunov

Exponentielle

Def Unipotent/inversible

Def Exponentielle

Thm $\exp : k[u] \twoheadrightarrow (k[u])^\times$

APP Détermination d'une racine

Def Résolution système linéaire

APP $X' = AX$ avec A antisymétrique, ou symétrique

Invariants de Frobenius

DEV Invariants de Frobenius

REM Calcul effectif via Smith

Endomorphismes semi-simples

Def Définition

Pro Réduction des endo semi-simples

Thm Décomposition de Dunford pour les semi-simples

Topologie

Thm Topologie des classes de similitude

Thm Densité des inversibles, ouvert connexe etc ...

Thm Densité des compagnons, ouvert connexe etc ...

Thm χ_u est continu

Thm π_u n'est pas continu

Thm Disques de Gershgorin

■ **MISC**

Def Fonction invariante $f(PMP^{-1}) = f(M)$

Thm Toute fonction f invariante de $M_n(\mathbb{C})$ dans X, X topologique et f continue se factorise par les coefficients du polynôme caractéristique

7.157 ■ ENDOMORPHISMES TRIGONALISABLES. ENDOMORPHISMES NILPOTENTS

■ **DÉVELOPPEMENTS** **5.0**

D07 MÉTHODES ITÉRATIVES JACOBI/GAUSS-SEIDEL ⋆⋆⋆⋆⋆

D09 DÉCOMPOSITION DUNFORD EFFECTIVE ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Mneimné Linéaires et compagnie

Gourdon Algèbre

Rombaldi

FGN Algèbre

■ **RAPPORT DE JURY**

L'utilisation des noyaux itérés est fondamentale dans cette leçon, par exemple pour déterminer si deux matrices nilpotentes sont semblables. Il est intéressant de présenter des conditions suffisantes de trigonalisation simultanée ; l'étude des endomorphismes cycliques a toute sa place dans cette leçon. L'étude des nilpotents en dimension 2 débouche naturellement sur des problèmes de quadriques et l'étude sur un corps fini donne lieu à de jolis problèmes de dénombrement. S'ils le désirent, les candidats peuvent aussi présenter la décomposition de Frobenius.

■ **IDÉE DU PLAN :** On suit le titre une fois de plus. Il faudra bien justifier la partie jacobi/gauss-seidel, en la liant par exemple à la partie exponentielle. Jordan/Dunford/Young est à maîtriser. Parler de dénombrement, de commutant, de burnside et de toutes les petites propriétés de GL/SL et autres remplissent bien cette leçon.

I. TRIGONALISABLES
- A) Définitions
- B) Caractérisations
- C) Conséquences (Jacobi)

II. NILPOTENTS
- (a) Définitions
- (b) Noyaux itérés
- (c) Propriétés

III. RÉDUCTION
- (a) Dunford/Jordan
- (b) Exponentielle

157 : C'est clairement pas suffisant pour une leçon ...

■ **TRIGONALISATION**

Def Dans une base

Car π_u, χ_u

Thm Co-trigonalisable

Def Espaces caractéristiques

Thm Stabilise un drapeau

■ **TRIGONALISATION ET SPECTRE**

Def det via trigo

Def Spectre sur la diagonale

Def Calcul polynômial sur le spectre

■ **NILPOTENCE**

Def definition

Car Caractérisation via π, χ

Thm Nilpotence d'indice maximal et cyclicité

Thm Dénombrement des nilpotents

DEV Burnside

■ **DÉCOMPOSITION DE JORDAN**

Thm Décomposition de Dunford

APP Surjectivité de exp

DEV Dunford Effectif

Def Suite des noyaux

Thm Lemme de fitting

Def Réduction des nilpotents

Thm Réduction de Jordan

Def Tableau de Young

EX Dénombrements

■ **TOPOLOGIE**

Thm Topologie des classes de similitude

Thm Densité des inversibles, ouvert connexe etc ...

Thm Densité des compagnons, ouvert connexe etc ...

Thm χ_u est continu

Thm π_u n'est pas continu

Thm Disques de Gershgorin

■ **FROBENIUS**

Def $\phi_{u,x} : k[X] \to \langle x \rangle_u$

Def $\pi_{u,x}$

Thm $\exists x, \pi_{u,x} = \pi_u$

Def Matrice compagnon

Pro Compagnon et cyclicité

Thm Théorème de Kronecker sur les polynômes entiers

DEV Invariants de Frobenius

REM Calcul effectif via Smith

■ **SYSTÈMES DYNAMIQUES**

Def Structure de l'espace des solutions d'une suite récurrente linéaire

Def Structure de l'espace des solutions d'une EDO linéaire d'ordre n

Def Structure de l'espace des solutions d'une EDO linéaire en dimension n

Def Étude asymptotique des EDOL

Thm Lyapunov

7.159 ■ FORMES LINÉAIRES ET DUALITÉ EN DIMENISON FINIE

■ **DÉVELOPPEMENTS** **4.5**

D06 INVARIANTS DE FROBENIUS ⋆⋆⋆⋆

D24 EXTREMA LIÉS ET APPLICATION ... ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Mneimné Linéaires et compagnie

Gourdon Algèbre

Rombaldi

FGN Algèbre

■ **RAPPORT DE JURY**

Il est important de bien placer la thématique de la dualité dans cette leçon ; celle-ci permet de mettre en évidence des correspondances entre un morphisme et son morphisme transposé, entre un sous-espace et son orthogonal (canonique), entre les noyaux et les images ou entre les sommes et les intersections. Bon nombre de résultats d'algèbre linéaire se voient dédoublés par cette correspondance. Les liens entre base duale et fonctions de coordonnées doivent être parfaitement connus. Savoir calculer la dimension d'une intersection d'hyperplans via la dualité est important dans cette leçon. L'utilisation des opérations élémentaires sur les lignes et les colonnes permet facilement d'obtenir les équations d'un sous-espace vectoriel ou d'exhiber une base d'une intersection d'hyperplans. Cette leçon peut être traitée sous différents aspects : géométrique, algébrique, topologique ou analytique. Il faut que les développements proposés soient en lien direct avec la leçon. Enfin rappeler que la différentielle d'une fonction à valeurs réelles est une forme linéaire semble incontournable. Il est possible d'illustrer la leçon avec un point de vue probabiliste, en rappelant que la loi d'un vecteur aléatoire X est déterminée par les lois unidimensionnelles de $X \cdot u$ pour tout vecteur u.

■ **IDÉE DU PLAN :** Un plan didactique s'impose, d'abord l'espace dual, le bidual et les propriétés élémentaires. Ensuite transposition et orthogonalité. Enfin des applications en algèbre et analyse.

I. ESPACE DUAL
- A) Définitions
- B) Caractérisations
- C) Conséquences (Jacobi)

II. ORTHOGONALITÉ ET TRANSPOSITION
- (a) Définitions
- (b) Noyaux itérés
- (c) Propriétés

III. APPLICATIONS
- (a) Réduction
- (b) Optimisation
- (c) Interpolation
- (d) Géométrie (hyperplans ?)

7.162 ■ SYSTÈMES D'ÉQUATION LINÉAIRES ; OPÉRATIONS ÉLÉMENTAIRES, ASPECTS ALGORITHMIQUES

■ **DÉVELOPPEMENTS** **4.5**

D07 MÉTHODES ITÉRATIVES JACOBI/GAUSS-SEIDEL ★★★★★

D10 ALGORITHME DE BERLEKAMP ★★★★

■ **RÉFÉRENCES**

Allaire Kaber

Allaire

Ciralet

Gourdon (rouché fontené)

■ **RAPPORT DE JURY**

Dans cette leçon, les techniques liées au simple pivot de Gauss constituent l'essentiel des attendus. Il est impératif de présenter la notion de système échelonné, avec une définition précise et correcte, et de situer l'ensemble dans le contexte de l'algèbre linéaire (sans oublier la dualité). Un point de vue opératoire doit accompagner l'étude théorique et l'intérêt pratique (algorithmique) des méthodes présentées doit être expliqué y compris sur des exemples simples où l'on attend parfois une résolution explicite. S'ils le désirent, les candidats peuvent aussi présenter les relations de dépendance linéaire sur les colonnes d'une matrice échelonnée qui permettent de décrire simplement les orbites de l'action à gauche de GL_n sur M_n donnée par $(P,A) \mapsto PA$. De même, des discussions sur la résolution de systèmes sur Z et la forme normale de Hermite peuvent trouver leur place dans cette leçon. Enfin, il est possible de présenter les décompostions LU et de Choleski, en évaluant le coût de ces méthodes ou encore d'étudier la résolution de l'équation normale associée aux problèmes des moindres carrés et la détermination de la solution de norme minimale par la méthode de décomposition en valeurs singulières.

■ **IDÉE DU PLAN :** On doit commencer par tout ce qui est généralités sur un système linéaire, sa forme, l'existence de solutions, les propriétés théoriques. Ensuite on fait une partie entière sur Gauss, les factorisations et les méthodes de résolution explicites. Enfin, on termine par des méthodes itératives.

S'il y a assez de temps, la décomposition en valeurs singulières est intéressante, car elle obtient via le pseudo-inverse la minimisation de la norme quadratique à l'image de la matrice ... C'est-à-dire la régression linéaire !

Ne négligons pas le côté "conséquences théoriques" qui peut s'avérer très vaste ...

I. SYSTÈMES LINÉAIRES
   A) Définitions
   B) Caractérisations
   C) Conséquences (Jacobi)

II. RÉSOLUTIONS ALGORITHMIQUES
   (a) Pivot de Gauss
   (b) Factorisations

III. MÉTHODES ITÉRATIVES
   (a) Convergence
   (b) Jacobi/Gauss seidel
   (c) Gradient ...

7.162.1 Systèmes d'équations

■ **DÉFINITIONS**

Def Système linéaire

Def Sur-déterminé/sous-déterminé

Def Système homogène

Def Conditionnement

■ **INTERPRÉTATION VECTORIELLE**

Def Application linéaire, rang etc ...

Def Interprétation géométrique via les hyperplans

Def Déterminant et injectivité

APP Conique et déterminant

■ **RÉSOLUTION THÉORIQUE**

Def Comatrice

Def Formules de Cramer

APP EDO avec second membre ordre 2

Thm Rouché

Thm Décomposition en valeurs singulières

Def Pseudo-inverse

7.162.2 Résolution explicitie

■ **PIVOT DE GAUSS**

Def Matrices élémentaires

Algo Algorithme de Gauss

Thm $O(n^3)$ opérations, complexité polynômiale

CSQ Générateurs de GL_n et SL_n

CSQ Connexité

APP Calcul explicite du noyau

DEV Berlekamp

REM Gauss et stabilité numérique

■ **DÉCOMPOSITION LU**

Def Existence via Gauss

Thm Unicité

APP Résolutions multiples

EX Sur une tridiagonale

Def Cholesky

■ **DÉCOMPOSITION QR**

Def Existence et unicité

Alg Par Gram-Schmidt

Rem Instabilité numérique

Alg Par Householder

■ **MOINDRES CARRÉS**

Def Problème des moindres carrés

Rem Équivalence avec l'inverse dans le cas inversible

APP Régression linéaire etc ...

MET Lire le Kaber-Allaire pour les résolutions numériques

■ **DANS LE CAS D'UN ANNEAU**

Def Matrice dans un anneau

Thm Invariants de Smith

Alg Algo des invariants

Csq Permet de décrire l'espace des solutions

7.162.3 Résolution itérative

■ **MÉTHODES ITÉRATIVES**

Def Convergence

Thm Householder

DEV Jacobi Gauss-Seidel

APP Au cas tridiagonal

Rem Complexité VS précision

Rem Conditionnement

Def Méthode de la relaxation

■ **MÉTHODES ISSUES DE L'OPTIMISATION**

Def Optimisation "convexe"

Met Descente de gradient

Thm Le gradient à pas optimal

APP $(Ax,x)-(b,x)$ et résolution

7.170 ■ FORMES QUADRATIQUES SUR UN ESPACE VECTORIEL DE DIMENSION FINIE. ORTHOGONALITÉ, ISOTROPIE. APPLICATIONS

■ **DÉVELOPPEMENTS** **4.5**

D08 RÉCIPROCITÉ QUADRATIQUE ⋆⋆⋆⋆⋆

D11 LEMME DE MORSE ⋆⋆⋆⋆

■ **RÉFÉRENCES**

Invitation aux formes quadratiques

Perrin

Rombaldi

Rouviere Morse/géométrie

■ **RAPPORT DE JURY**

Il faut tout d'abord noter que l'intitulé implique implicitement que le candidat ne doit pas se contenter de travailler sur R. Le candidat pourra parler de la classification des formes quadratiques sur le corps des complexes et sur les corps finis. L'algorithme de Gauss doit être énoncé et pouvoir être mis en œuvre sur une forme quadratique simple. Les notions d'isotropie et de cône isotrope sont un aspect important de cette leçon. On pourra rattacher cette notion à la géométrie différentielle.

7.170.1 Formalisme des formes quadratiques

■ **Forme bilinéaire symétrique**

Def L'espace vectoriel

EX produit-scalaire etc ...

Rem Construction via $E \to E^\star$

Def Morphismes de FBS

Def Action de GL sur cet espace

EX La hessienne, des traces etc...

■ **Forme quadratique**

Def Forme quadratique

EX ...

Def Forme polaire

Thm Unique forme FBS

Def Noyau, rang

Def Morphismes, action de GL

EX ...

■ **Représentation matricielle**

Def Représentation de q via sa FBS

Rem La matrice est symétrique

Pro Changement de base via transposition

Pro Action de GL via transposition

Thm Rang, discriminant et trucs sont des invariants

7.170.2 Orthogonalité et isotropie

■ **Orthogonal**

Def Orthogonal d'un vecteur

Def Orthogonal d'un espace

REM $\ker q = E^\perp$

Pro Décroissance, dimensions

REM Lien entre $F^\perp$ et la dualité

Pro $\dim F + \dim F^\perp = \dim E - \dim E^\perp \cap F$ via la dualité

Def Non-dégénérée

EX Les contre-exemples classiques

Pro Théorèmes dans les cas non-dégénérés

■ **Isotropie**

Def Vecteur isotrope

Def Cône isotrope

REM $\ker q \subsetneq C(q)$

Def $q_{|F}$

Def F isotrope si possède un vecteur isotrope, anisotrope sinon

Def SETI

■ **Base orthogonale**

Def Base orthogonale

Def Sous espace régulier

Thm Diagonalisation

Thm Complétion de bases orthogonales

■ **Groupe orthogonal**

Def Le groupe d'isométries pour q

Thm Cartan-Dieudonné

Thm $q \sim q'$ ssi $O(q)$ conjugué à $O(q')$

Pro Connexité de $O_n^+(\mathbb{R})$ etc ...

Thm Sous groupes compacts de O_n

Thm Sous groupes finis de SO_3

7.170.3 Études de cas dans différents corps

■ **Réduction de Gauss et matricielle**

Def Méthode de Gauss de réduction

Def Opérations élémentaires symétriques

APP Forme "normale" avec des espaces hyperboliques

APP En caractéristique $\neq 2$

Pro Lien entre le nombre de classes et les carrés dans dans k

■ **Dans $\mathbb{C}$**

Thm Tout est facile !

■ **Dans $\mathbb{R}$**

Def Signature

Thm Invariant total

Thm Réduction des endomorphismes orthogonaux

APP Conditions d'extremum local

Pro Topologies etc ...

Thm Rang constant etc ...

DEV Lemme de Morse

APP Géométrie différentielle

■ **DANS $\mathbb{F}_q$**

Thm Dénombrement des carrés

Thm Réduction dans $\mathbb{F}_q$

DEV Réciprocité quadratique

APP Étude des équations de degré 2 sur $\mathbb{F}_q$

7.170.4 Espaces hyperboliques

■ **DÉFINITIONS**

Def Espace hyperbolique

EX L'exemple caractéristique

■ **PLANS HYPERBOLIQUES**

Thm Sur un plan que peut-il se passer ?

Thm Décomposition en plans

■ **APPLICATIONS**

Thm Gonflement hyperbolique

7.181 ■ BARYCENTRES DANS UN ESPACE AFFINE RÉEL DE DIMENSION FINIE, CONVEXITÉ ,APPLICATIONS

■ **DÉVELOPPEMENTS** **5.0**

D01 SOUS GROUPES COMPACTS DE GLN(R) ⋆⋆⋆⋆⋆

D28 CONIQUE ET DÉTERMINANT ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Eiden

Mercier

Rombaldi

■ **RAPPORT DE JURY**

Dans cette leçon, la notion de coordonnées barycentriques est incontournable ; des illustrations dans le triangle (coordonnées barycentriques de certains points remarquables) sont envisageables. Il est important de parler d'enveloppe convexe, de points extrémaux, ainsi que des applications qui en résultent. S'ils le désirent, les candidats peuvent aller plus loin en présentant le lemme de Farkas, le théorème de séparation de Hahn-Banach, ou les théorèmes de Helly et de Caratheodory.

7.181.1 Barycentres et espaces affines

■ **Définition du barycentre**

Def Point pondéré

Thm La fonction $M \mapsto \sum \alpha_k \overrightarrow{MA_k}$ est constante ou bijective

Def Barycentre pondéré

Pro Homogénéité

Pro Associativité

Def Isobarycentre

APP Médianes d'un triangle

■ **Espaces affines**

Def Base affine

Def Application affine

Thm Caractérisation via barycentre

Def Coordonnées barycentriques

Thm Homogénéité

7.181.2 Dans le plan affine

■ **Équations affines**

Def Équation d'une droite

EX ...

Thm Caractérisation de l'intersection

Thm Concourrantes droites etc ...

Thm Menelaïus et ceva

EX Convergence vers l'isobarycentre ...

■ **Coniques**

Def Conique dans le plan

Thm Coniques circonscrites

Thm Par cinq pts passe une conique

DEV Conique et déterminant

■ **Volumes et angles**

Thm Angle et barycentre

Thm Aire et barycentre

EX ...

7.181.3 En dimension plus grande

■ **Convexité**

Def Convexité

EX Ensembles de matrices

EX Intérieur d'un triangle

Thm Gauss-Lucas

■ **Enveloppe convexe**

Def Enveloppe convexe

Thm Via les barycentres

Thm Carathéodory

Thm Enveloppe d'un compact etc ...

DEV Sous groupes compacts

Thm Hann-Banach

Thm Kreill-Millman

Thm Enveloppe convexe de O_n

7.182 ■ APPLICATIONS DES NOMBRES COMPLEXES À LA GÉOMÉTRIE

■ **DÉVELOPPEMENTS** **5.0**

D03 SO3(R) ET LES QUATERNIONS ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Eiden

Mercier

Perrin

Rombaldi

Audin

■ **RAPPORT DE JURY**

Cette leçon ne doit pas rester au niveau de la classe de Terminale. L'étude des inversions est tout à fait appropriée, en particulier la possibilité de ramener un cercle à une droite et inversement ; la formule de Ptolémée illustre bien l'utilisation de cet outil. On peut parler des suites définies par récurrence par une homographie et leur lien avec la réduction dans $SL_2(C)$. S'ils le désirent, les candidats peuvent aussi étudier l'exponentielle complexe et les homographies de la sphère de Riemann. La réalisation du groupe SU_2 dans le corps des quaternions et ses applications peuvent trouver leur place dans la leçon. Il est possible de présenter les similitudes, les homographies et le birapport.

7.183 ■ UTILISATION DES GROUPES EN GÉOMÉTRIE

■ **DÉVELOPPEMENTS** **5.0**

D03 SO3(R) ET LES QUATERNIONS ⋆⋆⋆⋆⋆

D04 SOUS GROUPES FINIS DE SO3(R) ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Rombaldi (un peu court)

Perrin (pour les quaternions)

Audin

H2G2

■ **RAPPORT DE JURY**

C'est une leçon dans laquelle on s'attend à trouver des utilisations variées. On s'attend à ce que soient définis différents groupes de transformations (isométries, déplacements, similitudes, translations) et à voir résolus des problèmes géométriques par des méthodes consistant à composer des transformations. De plus, les actions de groupes sur la géométrie permettent aussi de dégager des invariants essentiels (angle, birapport, excentricité d'une conique). Les groupes d'isométries d'une figure sont incontournables.

7.190 ■ MÉTHODES COMBINATOIRES ET DÉNOMBREMENT

■ **DÉVELOPPEMENTS** **4.5**

D05 DÉNOMBREMENT POLYNÔMES IRRÉDUCTIBLES ⋆⋆⋆⋆

D17 NOMBRES DE BELL ⋆⋆⋆⋆⋆

7.203 ■ UTILISATION DE LA NOTION DE COMPACITÉ.

■ **DÉVELOPPEMENTS** **4.5**

D01 SOUS GROUPES COMPACTS DE GLN(R) ⋆⋆⋆⋆⋆

D21 THÉORÈME D'HADAMARD LÉVY ⋆⋆⋆⋆

■ **RÉFÉRENCES**

Brezis

Gourdon Analyse

ZQ

FGN

Queffelec Topologie

■ **RAPPORT DE JURY**

Il est important de ne pas concentrer la leçon sur la compacité en général (confusion entre utilisation de la notion compacité et notion de compacité), et de se concentrer en priorité sur le cadre métrique. Néanmoins, on attend des candidats d'avoir une vision synthétique de la compacité. Des exemples d'applications comme le théorème de Heine et le théorème de Rolle doivent y figurer et leur démonstration être connue. Par ailleurs, le candidat doit savoir quand la boule unité d'un espace vectoriel normé est compacte. Des exemples significatifs d'utilisation comme le théorème de Stone-Weierstrass (version qui utilise pertinemment la compacité), des théorèmes de point fixe, voire l'étude qualitative d'équations différentielles, sont tout-à fait envisageables. Le rôle de la compacité pour des problèmes d'existence d'extrema mériterait d'être davantage étudié. On peut penser comme application à la diagonalisation des matrices symétriques à coefficients réels. Pour aller plus loin, les familles normales de fonctions holomorphes fournissent des exemples fondamentaux d'utilisation de la compacité. Les opérateurs auto-adjoints compacts sur l'espace de Hilbert relèvent également de cette leçon, et on pourra développer l'analyse de leurs propriétés spectrales.

203 : En parler avec Théo et Gaëtan...

Définitions

Def Compacité Borel

Thm Caractérisation séquentielle

Def Pré-compact, relativement compact

Pro Fermé dans un compact, etc ...

Thm Lien entre complet et compact

Met Extraction diagonale

Thm Tychonoff dénombrable

Thm Tychonoff

Thm L'image d'un compact par C^0 est compact

Thm Si f C^0 et bijective alors homéo

Analyse réelle

Thm Continue implique bornée et atteint ses bornes

Thm Des valeurs intermédiaires

Thm De Rolle

Thm Des accroissements finis

Thm De Heine

Compacité en dim finie

Thm Fermés bornés et compacts

Thm Riez boule compact ssi dim finie

Compacité en dim infinie

Thm De Dini (?)

Def Équi-continuité

Def Équi-continuité uniforme

Pro "Heine" pour l'équi

Thm Arzela-Ascoli

APP Opérateurs à Noyau (?)

APP Théorème de Montel

Densité et compacité

Thm Stone Weierstrass Réel

Thm Stone Weierstrass Complexe

APP Densité des polynômes

APP Densité des polynômes trigo

APP Séparabilité de $\mathscr{C}(K)$

APP Séries de Fourier ?

Équations différentielles

Thm Cauchy-Lipschitz

Thm Cauchy-Peano-Arzela

Thm Sortie de tout compact

DEV Hadamard Lévy

Théorèmes de point fixe

Thm Point fixe dans un compact

Thm Brouwer

Thm Schauder

Problèmes d'extrema

Def Fonction coercive

Thm Existence de minimum

DEV Ellipsoïde de John

DEV Sgpes compacts

7.208 ■ ESPACES VECTORIELS NORMÉS, APPLICATIONS LINÉAIRES CONTINUES. EXEMPLES.

■ **DÉVELOPPEMENTS** **5.0**

D01 SOUS GROUPES COMPACTS DE GLN(R) ⋆⋆⋆⋆⋆

D14 BANACH STEINHAUS ET FOURIER ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon Analyse

ZQ

Brezis

■ **RAPPORT DE JURY**

Une telle leçon doit bien sûr contenir beaucoup d'illustrations et d'exemples, notamment avec quelques calculs élémentaires de normes subordonnées (notion qui met en difficulté un trop grand nombre de candidats). Le lien avec la convergence des suites du type $X_{n+1} = AX_n$ doit être connu. Lors du choix de ceux-ci (le jury n'attend pas une liste encyclopédique), le candidat veillera à ne pas mentionner des exemples pour lesquels il n'a aucune idée de leur pertinence et à ne pas se lancer dans des développements trop sophistiqués. La justification de la compacité de la boule unité en dimension finie doit être maîtrisée. Il faut savoir énoncer le théorème de Riesz sur la compacité de la boule unité fermée d'un espace vectoriel normé. Le théorème d'équivalence des normes en dimension finie, ou le caractère fermé de tout sous-espace de dimension finie d'un espace normé, sont des résultats fondamentaux à propos desquels les candidats doivent se garder des cercles vicieux. A contrario, des exemples d'espaces vectoriels normés de dimension infinie ont leur place dans cette leçon et il faut connaître quelques exemples de normes usuelles non équivalentes, notamment sur des espaces de suites ou des espaces de fonctions et également d'applications linéaires qui ne sont pas continues.

■ **DÉFINITIONS**

Def Espace normé

Def Topologie induite

Def Normes équivalentes

Thm Équivalentes ssi même topologie

Def Continuité d'une APPLIN

Def Norme d'opérateur

■ **ANALYSE NUMÉRIQUE MATRICIELLE**

Def Conditionnement

Def Rayon spectral

Thm Householder

DEV Méthodes numériques

■ **NORMES ET DIMENSION**

Thm Équivalence des normes en dim finie

Thm Fermés bornés = compact

Thm Dim finie $\Longrightarrow$ complet

CSQ Les applications linéaires sont continues

Thm Riez, compact ssi dim finie

■ **ESPACE DE BANACH**

Def Complet

EX L^p et compagnie

Def Normalement convergente

Thm Implique convergente (équivalence)

Thm Picard-Banach

APP Cauchy-Lipschitz

■ **LEMME DE BAIRE**

Def Espaces de Baire

Thm Banach $\Longrightarrow$ Baire

APP dim finie ou indénombrable

APP Densité de truc much

Thm Banach Steinhaus

Csq Stabilité par limite simple

DEV Banach Steinhaus et Fourier

■ **LINÉAIRES SUR UN BANACH**

Thm Application ouverte

Thm Graphe fermé

APP Isomorphisme de Banach

APP Opérateurs adjoints automatiquement continus etc...

■ **ESPACES PRÉHILBERTIENS**

Def produit scalaire hermitien

Def Norme induite

Thm Identités de polarisation

Pro Identité du parallélograme et norme hermitienne

■ **ESPACES EUCLIDIENS**

Def produit scalaire

Def O_n, S_n etc...

Thm Ellipsoïide de John

DEV Sous groupes compacts

APP Une norme dont le groupe d'isométrie agit transitivement sur la sphère est euclidienne

■ **ESPACES HILBERTIENS**

Def préhilbertien complet

EX L^2 etc ...

Def Orthogonalité

Thm Pythagore dans un hilbert

APP Parseval et Fourier (!)

APP $\zeta(2) = \frac{\pi^2}{6}$

■ **APPLICATIONS DANS UN HILBERT**

Thm Projection sur un convexe fermé

Thm Elle est 1-lip

Thm Somme directe et orthogonalité

Thm Représentation de Riez

■ **DUALITÉ DANS UN HILBERT**

Thm Riez-Fréchet dans un hilbert

Thm Lax-Milgram

APP Solutions faibles d'une edo

Def Convergence faible

Thm Fermé-borné ssi faiblement compact

APP Minimisation dans un hilbert

7.214 ■ THÉORÈME D'INVERSION LOCALE, THÉORÈME DES FONCTIONS IMPLICITES. EXEMPLES ET APPLICATIONS EN ANALYSE ET EN GÉOMÉTRIE.

■ **DÉVELOPPEMENTS** **5.0**

D11 LEMME DE MORSE ★★★★★

D21 THÉORÈME D'HADAMARD LÉVY ★★★★

D24 EXTREMA LIÉS ET APPLICATION ... ★★★★★

■ **RÉFÉRENCES**

Rouvière

Lafontaine (au début)

Objectif Agrégation

Gourdon

■ **RAPPORT DE JURY**

Il s'agit d'une leçon qui exige une bonne maîtrise du calcul diférentiel. Même si le candidat ne propose pas ces thèmes en développement, on est en droit d'attendre de lui des idées de démonstration des deux théorèmes fondamenteux qui donnent son intitulé à la leçon. Il est indispensable de savoir mettre en pratique le théorème des fonctions implicites au moins dans le cas de deux variables réelles. On attend des applications en géométrie différentielle notamment dans la formulation des multiplicateurs de Lagrange. Plusieurs inégalités classiques de l'analyse peuvent se démontrer avec ce point de vue : Hölder, Carleman, Hadamard,...En ce qui concerne la preuve des extrema liés, la présentation de la preuve par raisonnement « sous matriciel est souvent obscure ; on privilégiera si possible une présentation géométrique s'appuyant sur l'espace tangent. Pour aller plus loin, l'introduction des sous-variétés est naturelle dans cette leçon. Il s'agit aussi d'agrémenter cette leçon d'exemples et d'applications en géométrie, sur les courbes et les surfaces.

7.214.1 Théorèmes d'inversion

■ **INVERSION LOCALE**

Def C^k-difféo

Thm d'inversion locale

EX exp sur M_n et sa surjectivité

EX Racine p-ème

EX $(x,y) \mapsto (x+y, xy)$ (racines)

EX Résolution d'une EDP ? (Rouvière)

■ **INVERSION GLOBALE**

Thm D'inversion globale

DEV Hadamard Lévy

??? Pour les fonctions holo ???

Thm Non rétraction C^1

APP Théorème de Brouwer

7.214.2 Fonctions implicites et coordonnées

■ **CHANGEMENT DE COORDONNÉES**

Thm Changement de variable

EX Calcul de l'intégrale de Gauss

Thm "base incomplète pour les changements de coordonnées".

Thm Forme normale des submersions

EX det est une submersion

Thm Forme normale des immersions

Thm Du rang constant

DEV Lemme de morse

EX Surfaces dans $\mathbb{R}^2$

■ **FONCTIONS IMPLICITES**

Thm Des fonctions implicites

Def Équivalence avec l'inversion

EX Suivi des racines d'un polynôme

EX Folium de Descartes

EX x^2+y^2 et fonctions implicites

EX Équation de Burgers

7.214.3 Sous variétés

■ **SOUS-VARIÉTÉS**

Def Définition par redressement

Thm des sous variétés

EX La sphère est une sous var

EX Le tore est une sous-var

EX $O_n(\mathbb{R})$ est une sous-var

EX SL_n est une sous-var

Thm Cartan-Von Neumann

EX Matrices de rang r sous var est une sous-var ?

■ **ESPACE TANGENT**

Def espace tangent

EX $T_x S^{n-1} = x^\perp$

EX $T_M O_n(\mathbb{R}) = MA_n(\mathbb{R})$

EX $T_M SL_n(\mathbb{R}) = M\{X \mid \operatorname{tr} X = 0\}$

DEV Extrema liés

APP Diagonalisation des matrices symétriques

APP Loi d'entropie maximale

APP Trajectoire sur un billard elliptique

7.215 ■ APPLICATIONS DIFFÉRENTIABLES DÉFINIES SUR UN OUVERT DE RN. EXEMPLES ET APPLICATIONS.

■ **DÉVELOPPEMENTS** **4.5**

D11 LEMME DE MORSE ⋆⋆⋆⋆⋆

D21 THÉORÈME D'HADAMARD LÉVY ⋆⋆⋆⋆

■ **RÉFÉRENCES**

Rouvière

Lafontaine (au début)

Objectif Agrégation

Gourdon

■ **RAPPORT DE JURY**

Cette leçon requiert une bonne maîtrise de la notion de différentielle première et de son lien avec les dérivées partielles, mais aussi de ce qui les distingue. On doit pouvoir mettre en pratique le théorème de différentiation composée pour calculer des dérivées partielles de fonctions composées dans des situations simples (par exemple le laplacien en coordonnées polaires). La différentiation à l'ordre 2 est attendue, notamment pour les applications classiques quant à l'existence d'extrema locaux. On peut aussi faire figurer dans cette leçon la différentielle d'applications issues de l'algèbre linéaire (ou multilinéaire). La méthode du gradient pour la minimisaiton de la fonctionnelle $1/2(Ax|x) - (b|x)$ où A est une matrice symétrique définie positive, conduit à des calculs de différentielles qui doivent être acquis par tout candidat. Pour aller plus loin, l'exponentielle matricielle est une ouverture pertinente. D'autres thèmes issus de la leçon 214 trouvent aussi toute leur place ici.

215 : Faire un plan plus simple (I) Différentielles (II) Application aux extremums (III) Difféomorphismes

7.215.1 Étude locale des fonctions

■ Notion de différentielle

Def En dimension finie/infinie

EX différentiable/dérivable dans $\mathbb{R}$ et $\mathbb{C}$

EX Différentielle d'une application linéaire

Def Stabilité par somme, produit, formule de leibnitz

Def Pour la composition

EX Différentielle de det

Def Fonctions de classe C^1

EX La norme $\|\|$

■ Dérivées partielles

Def Dérivées directionnelles

Thm Si C^1 tout va bien

EX Les contres exemples classiques

Def Matrice jacobienne

Def Gradient !

EX Résolution d'une EDP (rouvière)

7.215.2 Théorèmes locaux

■ Inversion locale

Def C^k-difféo

Thm d'inversion locale

EX exp sur M_n et sa surjectivité

EX Racine p-ème

EX $(x,y) \mapsto (x+y, xy)$ (racines)

Les fonctions implicites c'est pas si bien...

■ Fonctions implicites

Thm Des fonctions implicites

Def Équivalence avec l'inversion

EX Suivi des racines d'un polynôme

EX Folium de Descartes

EX x^2+y^2 et fonctions implicites

EX Équation de Burgers

■ Changement de coordonnées

Thm Changement de variable

EX Calcul de l'intégrale de Gauss

Thm "base incomplète pour les changements de coordonnées".

Thm Forme normale des submersions

EX det est une submersion

Thm Forme normale des immersions

Thm Du rang constant

7.215.3 Différentielles d'ordre supérieur

■ Définitions

Def

Thm Schwartz

Def Formules de Taylor

■ Conditions d'extremum

Def Local

DEV Lemme de morse

EX Surfaces dans $\mathbb{R}^2$

7.215.4 Contrôle global

■ **ÉTUDE GLOBALE**

Def Inégalité de la moyenne

Thm D'inversion globale

DEV Hadamard Lévy

Thm Pour les fonctions holo ???

Thm Non rétraction C^1

APP Théorème de Brouwer

Def Inversion globale

■ **FONCTIONS CONVEXES**

Def Définition de la convexité

Thm Caractérisation des fonctions convexes via les machins

Thm Minimum est global truc much

??? Existence de dérivées un peu partout si la fonction est convexe ?

DEV Gradient à pas optimal

7.215.5 Sous variétés

■ **SOUS-VARIÉTÉS**

Def Définition par redressement

Thm des sous variétés

EX La sphère est une sous var

EX Le tore est une sous-var

EX $O_n(\mathbb{R})$ est une sous-var

EX SL_n est une sous-var

Thm Cartan-Von Neumann

EX Matrices de rang r sous var est une sous-var ?

■ **ESPACE TANGENT**

Def espace tangent

EX $T_x S^{n-1} = x^\perp$

EX $T_M O_n(\mathbb{R}) = MA_n(\mathbb{R})$

EX $T_M SL_n(\mathbb{R}) = M\{X \mid \operatorname{tr} X = 0\}$

DEV Extrema liés

APP Diagonalisation des matrices symétriques

APP Loi d'entropie maximale

APP Trajectoire sur un billard elliptique

7.218 ■ APPLICATION DES FORMULES DE TAYLOR

■ **DÉVELOPPEMENTS** **5.0**

D11 LEMME DE MORSE ⋆⋆⋆⋆⋆

D18 SUITES À CONVERGENCE LENTE ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon Analyse

ZQ

Demailly

Faraut

FGN Analyse

Rouvière

■ **RAPPORT DE JURY**

> Il faut connaître les formules de Taylor et certains développements très classiques et surtout être capable de faire la différence entre les formules et de maîtriser leurs champs d'application. En général, le développement de Taylor d'une fonction comprend un terme de reste qu'il est crucial de savoir analyser. Le candidat doit pouvoir justifier les différentes formules de Taylor proposées ainsi que leur intérêt. Le jury s'inquiète des trop nombreux candidats qui ne savent pas expliquer clairement ce que signifient les notations o ou O qu'ils utilisent. De plus la différence entre l'existence d'un développement limité à l'ordre deux et l'existence de dérivée seconde doit être connue. On peut aussi montrer comment les formules de Taylor permettent d'établir le caractère développable en série entière (ou analytique) d'une fonction dont on contrôle les dérivées successives. Pour aller plus loin, on peut mentionner des applications en algèbre bilinéaire (lemme de Morse), en géométrie (étude locale au voisinage des points stationnaires pour les courbes et des points critiques pour la recherche d'extrema) et, même si c'est plus anecdotique, en probabilités (théorème central limite). On peut aussi penser à la méthode de Laplace, du col, de la phase stationnaire ou aux inégalités contrôlant les dérivées intermédiaires lorsque f et sa dérivée n-ième sont bornées, ou encore à l'analyse de méthodes d'intégration numérique ou l'étude de consistance de l'approximation de d^2x/dx^2 par différences finies. On soignera particulièrement le choix des développements.

■ **IDÉE DU PLAN :** On commence par la variable réelle, puisque c'est là où on est le plus à l'aise. Seulement ensuite viennent les fonctions de pluisueurs variables. Si le temps le permet, on peut alors s'attaquer à des problèmes numériques.

Les applications sont clairement marquées dans le rapport de jury, et il faut simplement saupoudrer intelligement.

I. FONCTIONS RÉELLES D'UNE VARIABLE RÉELLE
   A) Généralités
   B) Développements limités
   C) Séries
   D) Développements asymptotiques
   E) Probabilités

II. FONCTIONS DE PLUSIEURS VARIABLES
   A) Définitions
   B) Optimisation
   C) Sous variétés

III. NUMÉRIQUE
   (a) Intégration
   (b) Équations différentielles
   (c) EDP (Laurent Di Menza)

■ **FONCTIONS RÉELLES D'UNE VARIABLE RÉELLE**

Thm De Rolle

Thm TAF

Thm Taylor-Lagrange avec TAF

APP Régularité de $\frac{1}{x^{n+1}} f(x) - DL_n(x)$

Thm IAF

Thm Taylor-Lagrange avec majoration

Thm Taylor-Young

Thm Taylor-Reste-Intégral

■ **DÉVELOPPEMENTS LIMITÉS**

Def DL

Thm Unicité du DL

Rem $DL_1 \implies D^1$ mais pas aux ordres supérieurs!!

EX $x^3 \sin(1/x^2)$ et compagnie

EX BEAUCOUP D'EXEMPLES

Thm Hadamard factorisation (idéal)

■ **DÉVELOPPEMENT EN SÉRIE ENTIÈRE**

Def Série entière

Thm $f^{(2n)} \geq 0$ analytique

Thm Borel

EX DL mais pas entière

■ **MISC**

Thm Darboux

Pro $f(0) = 0$ et $\lim f(x) = 0$ alors une suite croissante $f^{(n)}(x_n) = 0$

■ **TAYLOR ET SCHÉMA NUMÉRIQUES**

Def Schéma numérique

Def Consistence, stabilité etc ..

Thm Schéma équation de la chaleur

■ **MÉTHODE D'INTÉGRATION NUMÉRIQUE**

Thm Vitesse de convergence de Simpson

■ **TAYLOR ET PROBABILITÉS**

Def Fonction génératrice des moments

Def Fonction caractéristique

Thm Génération des moments!

Thm Théorème central limite

■ **TAYLOR ET EXTREMUM**

Def Condition à l'ordre 1

Def Condition à l'ordre 2

EX Exemples

Thm Principe du maximum

■ **ÉTUDE ASYMPTOTIQUE**

Def Suite récurrente

Thm Suites à convergence lente

Thm Méthode de Newton

Thm Méthode de Laplace

Thm Développements limités de fonctions implicites

Thm Racines troisième degré

■ **TAYLOR EN PLUSIEURS VARIABLES**

Thm Taylor en plusieurs variables

Thm Adaptation des conditions d'extrema

Thm Lemme de division

■ **CHANGEMENT DE VARIABLE**

Thm Forme globale des immersions, submersions, rang constant

Thm Lemme de Morse

EX Étude autour des points singuliers

7.219 ■ EXTREMUMS : EXISTENCE, CARACTÉRISATION, RECHERCHE.

■ **DÉVELOPPEMENTS** **5.0**

D15 MÉTHODE DU GRADIENT À PAS OPTIMAL ⋆⋆⋆⋆⋆

D24 EXTREMA LIÉS ET APPLICATION ... ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon Analyse

ZQ

Demailly

Faraut

FGN Analyse

Rouvière

■ **RAPPORT DE JURY**

> Comme souvent en analyse, il est tout à fait opportun d'illustrer dans cette leçon un exemple ou un raisonnement à l'aide d'un dessin. Il faut savoir faire la distinction entre propriétés locales (caractérisation d'un extremum) et globales (existence par compacité, par exemple). Dans le cas important des fonctions convexes, un minimum local est également global. Les applications de la minimisation des fonctions convexes sont nombreuses et elles peuvent illustrer cette leçon. L'étude des algorithmes de recherche d'extremums y a toute sa place : méthode du gradient et analyse de sa convergence, méthode à pas optimal,... Le cas particulier des fonctionnelles sur $\mathbb{R}^n$ de la forme $1/2(Ax,x)-(b,x)$ où A est une matrice symétrique définie positive, ne devrait pas poser de difficultés (la coercivité de la fonctionnelle pose problème à de nombreux candidats). Les problèmes de minimisation sous contrainte amènent à faire le lien avec les extrema liés et la notion de multiplicateur de Lagrange. À ce sujet, une preuve géométrique des extrema liés sera fortement valorisée par rapport à une preuve algébrique, formelle et souvent mal maîtrisée. Enfin, la question de la résolution de l'équation d'Euler-Lagrange peut donner l'opportunité de mentionner la méthode de Newton. Les candidats pourraient aussi être amenés à évoquer les problèmes de type moindres carrés, ou, dans un autre registre, le principe du maximum et ses applications.

■ **IDÉE DU PLAN :** On commence par l'aspect topologique (global), ensuite on attaque l'aspect différentiel (local), pour terminer sur une étude de cas concret (convexe).

Bien penser à parler de hilberts (pour l'existence de minimums), l'étude des fonctions holomorphes peut aussi faire une petite partie. La partie numérique ne saurait être négligée, surtout qu'on a tout ce qu'il faut dans le ciralet/allaire.

Le beck développe bien les fonctions convexes.

I. FONCTIONS RÉELLES D'UNE VARIABLE RÉELLE
- A) Généralités
- B) Développements limités
- C) Séries
- D) Développements asymptotiques
- E) Probabilités

II. FONCTIONS DE PLUSIEURS VARIABLES
- A) Définitions
- B) Optimisation
- C) Sous variétés

III. NUMÉRIQUE
(a) Intégration
(b) Équations différentielles
(c) EDP (Laurent Di Menza)

■ **EXTREMUM ET TOPOLOGIE**

Def Compact

Def Coercive

Def ...

■ **EXTREMUM ET CALCUL DIFF**

Def Caractérisation minimum local ordre 1

Def Caractérisation minimum local ordre 2

Thm Lemme de Morse

EX Forme des points critiques

■ **EXTREMUM SUR VARIÉTÉ (I)**

Def Sous variété

Def Définition par redressement

Thm des sous variétés

EX La sphère est une sous var

EX Le tore est une sous-var

■ **EXTREMUM SUR VARIÉTÉ (II)**

Def espace tangent

EX $T_x S^{n-1} = x^\perp$

EX $T_M O_n(\mathbb{R}) = MA_n(\mathbb{R})$

EX $T_M SL_n(\mathbb{R}) = M\{X \mid \operatorname{tr} X = 0\}$

DEV Extrema liés

APP Diagonalisation des matrices symétriques

APP Loi d'entropie maximale

APP Trajectoire sur un billard elliptique

■ **EXTREMUM ET FONCTION HOLOMORPHE**

Thm Principe du maximum

EX etc. ..

■ **FONCTIONS CONVEXES RÉELLES**

Def Fonction convexe

Thm Lemme des pentes, croissance des taux d'acroissements

Thm Dérivabilité sauf sur un dénombrable

Thm Caractérisations via les dérivées

APP Optimisation convexe, unicité du minimum/maximum et globalité

■ **FONCTIONS CONVEXES VECTORIELLES**

Def Fonction convexe

Thm Caractérisations via les dérivées

APP Optimisation convexe, unicité du minimum/maximum et globalité

Def α-convexité

Def Convexité et normes euclidiennes

Thm Ellipsoïde de John

■ **ANALYSE HILBERTIENNE**

Def Projection sur un convexe fermé

APP minimisation etc ...

Thm Caractérisation des projections

EX Beaucoup d'exemples !

■ **MÉTHODES NUMÉRIQUES**

Thm Méthode de Gradient

Thm Algorithme du Simplexe

Thm Méthode de Newton

DEV Gradient a pas optimal

EX Programmation linéaire...

■ **RÉSOLUTION APPROCHÉE**

Thm Singular Value Decomposition

Thm Calcul des moindres carrés

7.220 ■ ÉQUATIONS DIFFÉRENTIELLES GÉNÉNRALES. EXEMPLES DIM 1 ET 2

■ **DÉVELOPPEMENTS** **4.5**

D21 THÉORÈME D'HADAMARD LÉVY ⋆⋆⋆⋆

D22 THÉORÈME DE STURM LIOUVILLE ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon Analyse pour la théorie de base

Zuily Queffelec pour la théorie de base

Demailly pour ce qui est plutôt numérique

Rouvière pour le wronskien et les études locales

FGN Analyse 4 pour les exemples

Hubbard et West pour tous les systèmes autonomes

■ **RAPPORT DE JURY**

C'est l'occasion de rappeler une nouvelle fois que le jury s'alarme des nombreux défauts de maîtrise du théorème de Cauchy-Lipschitz. Il est regrettable de voir des candidats ne connaître qu'un énoncé pour les fonctions globalement lipschitziennes ou plus, grave, mélanger les conditions sur la variable de temps et d'état. La notion de solution maximale et le théorème de sortie de tout compact sont nécessaires. Bien évidemment, le jury attend des exemples d'équations différentielles non linéaires. Le lemme de Grönwall semble trouver toute sa place dans cette leçon mais est trop rarement énoncé. L'utilisation du théorème de Cauchy-Lipschitz doit pouvoir être mise en œuvre sur des exemples concrets. Les études qualitatives doivent être préparées et soignées. Pour les équations autonomes, la notion de point d'équilibre permet des illustrations de bon goût come par exemple les petites oscillations du pendule. Trop epeu de candidats pensent à tracer et discuter des portraits de phase alors que le sujet y invite clairement. Il est possible d'évoquer les problématiques de l'approximation numérique dans cette leçon en présentant le point de vue du schéma d'Eular. On peut aller jusqu'à aborder la notion de problèmes raides et la conception de schémas implicites pour autant que le candidait ait une maîtrise convenable de ces questions.

7.220.1 Théorie générale

■ **Vocabulaire**

Def Vocabulaire sur $X' = F(t, X)$,

Def Problème de Cauchy

Def Solution, régularité

EX Encoder des équations d'ordre supérieur

EX EDO ordre 1 sans C.L.

Thm Gronwall

■ **Théorie locale**

Def Localement lip

Def Problème intégral équivalent

DEV Cauchy-Lipschitz

Def Prolongement des solutions

Def Solutions maximales

EX $y' = y^2$ maximal pas global

Def Cauchy-Peano-Arzela

EX $y' = 2\sqrt{|y|}$

Def Récapitulatif avec f continue, C^1 etc ...

EX Les systèmes linéaires avec $A(t)$ continue ça marche bien

Faire effectivement les dessins un jour

■ **Étude qualitative dans $\mathbb{R}^2$**

Def $x' = Ax$

■ **Théorie globale**

Def Solution globale

Thm Sortie de tout compact si $U = \mathbb{R}^n$.

AP f continue et bornée alors globale

EX $\frac{x^2}{1+x^2}$

AP $|F(t,x)| \leq C|x| + D$ alors globale

EX Les systèmes linéaires !

Thm Sortie de tout compact version dure

DEV Hadamard Levy

7.220.2 Études en dimension 1 et 2

■ **Cas linéaire**

Thm Rappel existence unicité

Thm Sous espace affine et dim

Def Système fondamental de solutions

Def Wronskien

Def Props du wronskien

Thm Solution exponentielle si A cst

Def Abaissement de l'ordre

Fig Nœuds stables, instables, selle, col, foyer, centre

Regarder les FGN

Def Variation des constantes

EX des exemples du Gourdon

Def Résolvante (GOU)

■ **Quelques équations particulières**

EX Ricatti, euler, etc ...

■ **Équation "d'oscillateurs"**

Def $y'' + q(t)y = 0$

DEV Sturm

Def Oscillation (GOU)

Def Estimation du nombre de zéros

7.220.3 Systèmes autonomes

■ **Étude de systèmes autonomes**

Def Système autonome

Def Trajectoire

Def Tracé des champs de vecteurs

Def Point d'équilibre

Def Stabilité

Thm Lyapunov

Thm Linéarisation ZQ

■ **Système Proie-Prédateur**

FGN faire les dessins

■ **Étude du pendule simple**

FGN faire les dessins

7.220.4 Approximation numérique

Recopier du Demailly ?

7.221 ■ ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES. SYSTÈMES.

■ **DÉVELOPPEMENTS** **4.5**

D13 SOUS ESPACES DE $\mathscr{C}(R,R)$ STABLES PAR TRANSLATION ⋆⋆⋆⋆

D22 THÉORÈME DE STURM LIOUVILLE ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Rouvière

Gourdon Analyse

ZQ

Demailly

Hubbard et West pour tous les systèmes autonomes

FGN Analyse 4 pour les exemples

■ **RAPPORT DE JURY**

Le jury attend d'un candidat qu'il sache déterminer rigoureusement la dimension de l'espace vectoriel des solutions. Le cas des systèmes à coefficients constants fait appel à la réduction des matrices qui doit être connue et pratiquée. Le jury attend qu'un candidat puisse mettre en œuvre la méthode de variation des constantes pour résourde une équation différentielle d'ordre 2 simple (à coefficients constants par exemple) avec second membre. L'utilisation des exponentielles de matrices a toute sa place ici. Les problématiques de stabilité des solutions et le lien avec l'analyse spectrale devraient être exploitées. Le théorème de Cauchy-Lipschitz linéaire constitue un exemple de développement pertinent pour cette leçon. Les résultats autour du comportement des solutions ou de leurs zéros, de certaines équations linéaires d'ordre 2 (Sturm, Hill-Mathieu,...) sont d'autres possibilités.

7.221.1 Généralités

■ **Existence et unicité**

Def Équation homogène, avec second membre

Def Encodage dans $X' = F(t, X)$

Def Cauchy linéaire

■ **Structure de l'espace des solutions**

Def Espace vectoriel de dim

Thm Les trucs du gourdon sur l'espace

DEV Sous espaces stables par translation

Def Wronskien, résolvante

7.221.2 Résolutions explicites

■ **Coefficients constants**

Def Exponentielle de matrice

Thm Structure des solutions d'une EDO linéaire

Thm Sturcture des solutions d'une EDO linéaire dim 1

EX Si la matrice est antisymétrique, si elle est symétrique ...

EX Si la matrice est de rang 2

■ **Systèmes avec second membre**

Met Abaissement de l'ordre

Met Variation des constantes

■ **Quelques cas particuliers**

EX Les trucs du gourdon (ricatti et co.)

7.221.3 Études qualitatives

■ **Systèmes dans $\mathbb{R}^2$**

Thm Stabilité ?

Def Portrait de phase ...

■ **Équation "d'oscillateurs"**

Def $y'' + q(t)y = 0$

DEV Sturm

Def Oscillation (GOU)

Def Estimation du nombre de zéros

■ **Linéarisation**

Thm Lyapunov ?

7.223 ■ SUITES NUMÉRIQUES. CONVERGENCE, VALEURS D'ADHÉRENCE. EXEMPLES ET APPLICATIONS.

■ **DÉVELOPPEMENTS** **5.0**

D18 SUITES À CONVERGENCE LENTE ★★★★★

D26 CONTINUITÉ DES RACINES D'UN POLYNÔME ★★★★★

■ **RÉFÉRENCES**

Gourdon Analyse

FGN Analyse 1

■ **RAPPORT DE JURY**

Cette leçon permet souvent aux candidats de s'exprimer. Il ne faut pas négliger les suites de nombres complexes. Le théorème de Bolzano-Weierstrass doit être cité et le candidat doit être capable d'en donner une démonstration. On attend des candidats qu'ils parlent des limites inférieure et supérieure d'une suite réelle bornée, et qu'ils en maîtrisent le concept. Les procédés de sommation peuvent être éventuellement évoqués mais le théorème de Cesàro doit être mentionné et sa preuve maîtrisée par tout candidat à l'agrégation. Les résultats autour des sous-groupes additifs de R permettent d'exhiber des suites denses remarquables et l'ensemble constitue un joli thème. Des thèmes de la leçon 226 peuvent également se retrouver dans cette leçon. Pour aller plus loin, un développement autour de l'équirépartition est tout à fait envisageable. La méthode de Newton peut aussi illustrer la notion de vitesse de convergence.

223 : TROUVER DES PUTAINS DE RÉFÉRENCES

223 : Trouver un plan correct ...

Suites

Def Construction de l'espace des suites

Def Période, croissance, etc ...

Def Propriétés "APCR"

Def Produit, somme

Def Produit de convolution et polynômes

Def Produit de convolution möbius et fonctions arithmétiques

Limites de suites V1

Def Limite d'une suite

Thm Produit, somme etc ...

Thm Des gendarmes

Suites et topologie

Def Caractérisation des fermés

Def Caractérisation des ouverts (que l'on observe "en temps fini")

Def Propriété de la borne sup

Def $\mathbb{R}$ est archimédien

Def Suites minimisantes

APP Sous groupes de $\mathbb{R}$

CSQ Sous groupes de $\mathbb{U}$ puis sous groupes finis de $SO_2(\mathbb{R})$.

Thm Suite croissante majorée converge et compagnie

Thm Des segments emboités

Thm Bolzano-Weierstrass

Def Compacité, recouvrement

Thm De baire (dans $\mathbb{C}$)

Limites de suite V2

Def Limite sup, Limite inf

Def Suite de Cauchy, complétude

Def Valeur d'adhérence

Thm Suites $u_{n+1} - u_n \to 0$ et convexité

EX Suites sous additives

Définitions "directes"

Def $u_n = f(n)$, avec f sympathique

Def Caractérisation séquentielle de la continuité

Thm Théorème de Heine pour les fonctions via les suites

Définitions par récurrence

Def $u_{n+1} = f(u_n)$

REM Analogie avec les champs de vecteurs et la dynamique continue

Thm Suites récurrentes linéaires (analogue des équadiffs)

Définitions implicites

Def Suites des zéros d'une fonction

EX $\tan x = x$

EX Ré-injection des développements asymptotiques

Comparaison asymptotique

Def Équivalent

Def Petit o

Def Système de comparaison asymptotique

Suites et approximation

Def Sommes de Riemann pour intégrales

MOR Moralité du calcul de point fixe par itération

Thm Méthode de Newton

EX Méthode de dichotomie

HS Numérique Matriciel, Cauchy-Lip, Inversion locale etc ...

DEV Équirépartition

Liens suites/séries

Def Traduction de l'un vers l'autre

Def Ré-écriture de la complétude version séries

Def Sommation des relations de comparaison

Def Séries génératrices de suites

EX Nombres de Bell

Thm Moyenne de Cesaro

DEV Ordre moyen de $\phi(n)$

DEV Suites à convergence lente

7.224 ■ EXEMPLES DE DÉVELOPPEMENTS ASYMPTOTIQUES DE SUITES ET DE FONCTIONS.

■ **DÉVELOPPEMENTS** **4.5**

D18 SUITES À CONVERGENCE LENTE ⋆⋆⋆⋆⋆

D19 MÉTHODE DE LAPLACE ⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon Analyse

Rouvière

Ciralet

Allaire Kaber

■ **RAPPORT DE JURY**

Cette leçon doit permettre aux candidats d'exprimer leur savoir-faire sur les techniques d'analyse élémentaire que ce soit sur les suites, les séries ou les intégrales. On peut par exemple établir un développement asymptotique à quelques termes des sommes partielles de la série harmonique, ou bien la formule de Stirling que ce soit dans sa version factorielle ou pour la fonction Γ. On peut également s'intéresser aux comportements autour des singularités de fonctions spéciales célèbres. Du côté de l'intégration, on peut évaluer la vitesse de divergence de l'intégrale de la valeur absolue du sinus cardinal, avec des applications pour les séries de Fourier, voire présenter la méthode de Laplace. Par ailleurs, le thème de la leçon permet l'étude de suites récurrentes (autres que le poncif[2] $u_{n+1} = \sin u_n$), plus généralement de suites ou de fonctions définies implicitement, ou encore des études asymptotiques de solutions d'équations différentielles (sans résolution explicite).

2. NDLR : poncif = Formule rabâchée, qui a perdu toute originalité ; cliché.

224 : Réfléchir à la leçon avec d'autres gens

■ Échelle asymptotique

Def Gourdon

■ Définitions implicites

Def Suites des zéros d'une fonction

EX $\tan x = x$

EX Ré-injection des développements asymptotiques

DEV Équation de degré 3

■ Intégrales à paramètres

Def Intégrales à paramètres

DEV Méthode de Laplace

■ Intégrales

Def Intégrales impropres

Def Intégrabilité et développement limité

■ Équations différentielles

Def Définitions

Thm Lyapunov

Thm Nombre de zéros d'une équadiff

■ Séries

Def Séries de Riemann

Def Comparaison série-intégrale

Def Formule d'Euler McLaurin

Def Sommation des relations de comparaison

Def Séries génératrices de suites

EX Nombres de Bell

Thm Moyenne de Cesaro

DEV Ordre moyen de $\phi(n)$

DEV Suites à convergence lente

MET Roabe-Duhame

■ Suites récurrentes

Def

Thm Formes des suites récurrentes linéaires d'ordre n et asymptotique

DEV Suites à convergence lente

Thm Méthode de newton

Thm Newton pour les polynômes ?!

7.226 ■ SUITES VECTORIELLES ET RÉELLES DÉFINIES PAR UNE RELATION DE RÉCURRENCE UN+1 = F(UN). EXEMPLES. APPLICATIONS À LA RÉSOLUTION APPROCHÉE D'ÉQUATIONS.

■ **DÉVELOPPEMENTS** **5.0**

D07 MÉTHODES ITÉRATIVES JACOBI/GAUSS-SEIDEL ⋆⋆⋆⋆⋆

D18 SUITES À CONVERGENCE LENTE ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Rouvière

Ciralet

Allaire Kaber

Gourdon

FGN Analyse

■ **RAPPORT DE JURY**

Citer au moins un théorème de point fixe dans cette leçon est pertinent. Le jury attend d'autres exemples que la sempiternelle suite récurrente $u_{n+1} = f(u_n)$ (dont il est souhaitable de savoir expliquer les techniques sous-jacentes). La notion de points attractifs ou répulsifs peut illustrer cette leçon. L'étude des suites linéaires récurrentes d'ordre p est souvent mal connu, notamment le lien avec l'aspect vectoriel, d'ailleurs ce dernier point est trop souvent négligé. Le comportement des suites vectorielles définies par une relation linéaire $X_{n+1} = AX_n$ fournit pourtant un matériel d'étude conséquent. La formulation de cette leçon invite résolument à évoquer les problématiques de convergence d'algorithmes (notamment savoir estimer la vitesse) d'approximation de solutions de problèmes linéaires et non linéaires : dichotomie, méthode de Newton (avec sa généralisation au moins dans $\mathbb{R}^2$), algorithme du gradient, méthode de la puissance, méthodes itératives de résolution de systèmes linéaires, schéma d'Euler,...

■ Suites réelles

Def Suite récurrente réelle

EX Suite géométrique, arithmétique, combinaison

EX Croissance, décroissance, convergence en fonction de f

MET Méthodes pour récupérer des équivalents, reconnaître une dérivée

EX λ tel que pour tout n n^λ est entier (FGN)

■ Vitesses de convergence

Def Convergence linéaire

Def Convergence quadratique

EX newton, etc ...

■ Dynamique discrète

Def Notion de point fixe, analogie avec point singulier

REM Analogie avec les équa-diffs

Thm Points fixes et dérivées de f dans le cas réel

EX $x_{n+1} = 1 - \lambda x_n^2$

DEV Suites à convergence lente

Thm Points fixes et dérivées de f dans le cas vectoriel

EX $z_{n+1} = z_n^2 + c$

EX $X_{n+1} = AX_n$ avec A symétrique, A antisymétrique, A orthogonale etc...

■ Suites récurrentes linéaires

Def d'une suite récurrente

Pro Encodage dans $X_{n+1} = AX_n$

Thm Forme des solutions via espaces vectoriels

EX Fibonnaci

■ Construction de points fixes

Thm De point fixe dans un compact

Thm De point fixe dans de Picard

APP Cauchy-Lipschitz

APP Inversion locale

HS Sémantique et points fixes

■ Recherche de solutions

Def Itératives matricielles

DEV Jacobi-Gauss Seidel

Def Méthodes de householder pour les valeurs propres

Def Méthode de la puissance

Thm Méthode de newton

Thm Méthode de Newton-Raphson

■ Recherche de minimum

Def Problème d'optimisation

EX Encodage de $Ax = b$

MET Algorithme du gradient

DEV Gradient à pas optimal

APP Méthode de newton pour l'optimisation convexe

Bosser les schémas numériques !!

■ Équations différentielles

Def Schéma numérique

Def Consistant, convergent, stable

Def Schéma d'Euler

EX Schéma pour l'équation de la chaleur

Thm Cauchy-Arzela-Peano

7.228 ■ CONTINUITÉ ET DÉRIVABILITÉ DES FONCTIONS RÉELLES

■ **DÉVELOPPEMENTS** **1.5**

D13 SOUS ESPACES DE $\mathscr{C}(R,R)$ STABLES PAR TRANSLATION ⋆⋆

D19 MÉTHODE DE LAPLACE ⋆

■ **RÉFÉRENCES**

Pommelet ?

Testard ?

Gourdon

FGN Analyse 1

■ **RAPPORT DE JURY**

Cette leçon permet des exposés de niveaux très variés. Les théorèmes de base doivent être maîtrisés et illustrés par des exemples intéressants, par exemple le théorème des valeurs intermédiaires pour la dérivée. Le jury s'attend évidemment à ce que le candidat connaisse et puisse calculer la dérivée des fonctions usuelles. Les candidats doivent disposer d'un exemple de fonction dérivable de la variable réelle qui ne soit pas continûment dérivable. La stabilité par passage à la limite des notions de continuité et de dérivabilité doit être comprise par les candidats. De façon plus fine, on peut s'intéresser aux fonctions continues nulle part dérivables. Pour aller plus loin, la dérivabilité presque partout des fonctions lipschitziennes ou des fonctions monotones relève de cette leçon. L'étude de la dérivée au sens des distributions de $x \in [a,b] \mapsto \int_a^x f(t)dt$ pour une fonction intégrable $f \in L^1([a,b])$ est un résultat intéressant qui peut trouver sa place dans cette leçon.

7.228.1 Propriétés locales de régularité

■ **CONTINUITÉ**

Def Continuité en un point

Def Continuité en tout point

EX $\chi_{\mathbb{Q}}$

Thm Stabilité par composition, produit, somme

Thm "Commute à la limite"

APP Étude de système $u_{n+1} = f(u_n)$

Def Continuité à gauche, à droite

EX ?

Def Semi-continuité inférieure, supérieure

Thm Continue ssi à droite et à gauche de même valeur

EX Préservation des sup/inf

■ **DÉRIVABILITÉ**

Def Taux d'accroissement

Def Tangente en un point

EX Avec des dessins

Def Dérivabilité en un point, à gauche, à droite

EX Contres exemples, les $|x|^\alpha$

Thm Stabilité par somme, produit etc ...

APP Comportement local d'une fonction (croissante, etc ...)

Thm Condition nécessaire de minimum local

APP Points fixes attractifs, répulsifs, hyperattractifs dans $u_{n+1} = f(u_n)$

■ **FORMULES DE TAYLOR**

Def Classes C^k, D^k et inclusions

APP Application des formules de Taylor

Thm Formules T-Y, T-L etc...

EX sin, exp, etc ...

APP Résolution des formes indéterminées

APP Schémas numériques et consistence [TODO]

APP Estimation des erreurs des estimations d'intégrales (Simpson, etc...)

7.228.2 Propriétés globales

■ **CONTINUITÉ GLOBALE**

Thm Caractérisation via pré-images

Thm Des valeurs intermédiaires

Thm Continue sur un compact bornée et atteint ses bornes

APP Toute fonction continue de K dans K admet un point fixe

Def Uniforme continuité

Thm Heine

Def homéomorphisme

Thm Image d'un connexe est connexe

■ **DÉRIVABILITÉ GLOBALE**

Thm De Rolle

Thm De rolle généralisé

Thm Des accroissements finis

Thm De Darboux

APP Tableaux de variation

Thm De la limite de la dérivée

Thm Inégalité des accroissements finis

Def difféomorphisme

APP Changement de variable

MET Méthode de Newton

■ **APPROXIMATIONS RÉGULIÈRES**

APP on se sert du DL et d'un segment pour majorer une différence de fonctions

Thm Weierstrass polynomial

Def Développement en série entière

Thm Bernstein

7.228.3 Étude de classes de fonctions

■ **FONCTIONS MONOTONES**

Def Monotonie

Thm Points de discontinuité

Thm Points de discontinuité au plus dénombrables

Thm Monotone implique semi-continue inférieurement ?

EX Monotone dans $[0,1]$ admet un point fixe

Thm Monotonie et dynamique des $u_{n+1} = f(u_n)$

Def Inverse généralisé d'une fonction croissante

APP Simulation de variables aléatoires ? [TODO]

Thm Une fonction strictement croissante est injective

Thm Une fonction continue et injective est strictement monotone

■ **FONCTIONS LIPSCHITZIENNES**

Def Fonctions Lip

REM Si f est k-lip alors $f + kid$ est croissante

Thm Continuité et dérivabilité sauf sur un ensemble dénombrable

■ **FONCTIONS CONVEXES**

Def Fonction convexe

Thm Lemme des pentes, croissance des taux d'acroissements

Thm Dérivabilité sauf sur un dénombrable

Thm Caractérisations via les dérivées

APP Optimisation convexe, unicité du minimum/maximum et globalité

■ **FONCTIONS RÉGLÉES**

Def Fonction réglée

Def Variation totale

Thm Variation totale différence de monotones

7.228.4 Structure des espaces de fonctions

■ **RÉPARTITION DES PROPRIÉTÉS**

Thm Baire/Banach steinhaus

Thm Continues/dérivables

Thm

■ **PASSAGE À LA LIMITE**

Def Convergence simple

Def Convergence uniforme

Thm Limite simple, limite uniforme de fonctions continues etc ...

APP Construction d'une fonction continue partout dérivable nulle part

Thm Fonctions lip etc ...

Thm Arzela-Ascoli

Thm De sélection de Helly

Thm De Dini

TODO Théorèmes de sommation ?

■ **INTÉGRATION**

Def Intégrale, primitive d'une fonction continue

Def Somme de Riemann, convergence si uniformément continue

Thm Linéarité, positivité, etc...

Thm Continuité des intégrales dépendant d'un paramètre

DEV Méthode de Laplace

7.229 ■ FONCTIONS MONOTONES, FONCTIONS CONVEXES

■ **DÉVELOPPEMENTS** **4.0**

D15 MÉTHODE DU GRADIENT À PAS OPTIMAL ⋆⋆⋆⋆⋆

D16 PROCESSUS DE BRANCHEMENTS ⋆⋆⋆

■ **RÉFÉRENCES**

Pommelet ?

Testard ?

Gourdon

FGN Analyse 1

Ciralet

■ **RAPPORT DE JURY**

L'énoncé et la connaissance de la preuve de l'existence de limites à gauche et à droite pour les fonctions monotones sont attendues. Ainsi on doit parler des propriétés de continuité et de dérivabilité à gauche et à droite des fonctions convexes de la variable réelle. Il est souhaitable d'illustrer la présentation de la convexité par des dessins clairs. On notera que la monotonie concerne les fonctions réelles d'une seule variable réelle, mais que la convexité concerne également les fonctions définies sur une partie convexe de $\mathbb{R}^n$, qui fournissent de beaux exemples d'utilisation. L'étude de la fonctionnelle quadratique ou la minimisation de $\|Ax-b\|^2$ pourront illustrer agréablement cette leçon. Pour aller plus loin, la dérivabilité presque partout des fonctions monotones est un résultat remarquable (dont la preuve peut être éventuellement admise). L'espace vectoriel engendré par les fonctions monotones (les fonctions à variation bornée) relève de cette leçon. Enfin, la dérivation au sens des distributions fournit les caractérisations les plus générales de la monotonie et de la convexité ; les candidats maîtrisant ces notions peuvent s'aventurer utilement dans cette direction.

229 : C'est une leçon de merde

7.229.1 Pour les fonctions réelles

■ **FONCTIONS MONOTONES**

Def Monotonie

Thm Points de discontinuité

Thm Points de discontinuité au plus dénombrables

Thm Monotone implique semi-continue inférieurement ?

EX Monotone dans $[0,1]$ admet un point fixe

Thm Monotonie et dynamique des $u_{n+1} = f(u_n)$

Def Inverse généralisé d'une fonction croissante

APP Simulation de variables aléatoires ? [TODO]

Thm Une fonction strictement croissante est injective

Thm Une fonction continue et injective est strictement monotone

■ **FONCTIONS CONVEXES**

Def Fonction convexe

Thm Lemme des pentes, croissance des taux d'acroissements

Thm Dérivabilité sauf sur un dénombrable

Thm Caractérisations via les dérivées

APP Optimisation convexe, unicité du minimum/maximum et globalité

■ **FONCTIONS RÉGLÉES**

Thm Fonctions à variations bornées

7.229.2 Fonctions vectorielles

■ **FONCTIONS CONVEXES**

Def Fonction convexe

Thm Caractérisations via les dérivées

APP Optimisation convexe, unicité du minimum/maximum et globalité

Def α-convexité

DEV Gradient a pas optimal

Def Convexité et normes euclidiennes

7.230 ■ SÉRIES DE NOMBRES RÉELS OU COMPLEXES. COMPORTEMENT DES RESTES OU DES SOMMES PARTIELLES DES SÉRIES NUMÉRIQUES. EXEMPLES.

■ **DÉVELOPPEMENTS** **4.5**

D12 ORDRE MOYEN $\phi(n)$ ⋆⋆⋆⋆

D18 SUITES À CONVERGENCE LENTE ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon

ZQ

FGN

■ **RAPPORT DE JURY**

De nombreux candidats commencent leur plan par une longue exposition des conditions classiques assurant la convergence ou la divergence des séries numériques. Sans être hors sujet, cette exposition ne doit pas former l'essentiel de la matière de la leçon. Un thème important de la leçon est en effet le comportement asymptotique des restes et sommes partielles (équivalents, développements asymptotiques — par exemple pour certaines suites récurrentes — cas des séries de Riemann, comparaison séries et intégrales,...). Le manque d'exemples est à déplorer. On peut aussi s'intéresser à certaines sommes particulières, que ce soit pour exhiber des nombres irrationnels (voire transcendants), ou mettre en valeur des techniques de calculs non triviales (par exemple en faisant appel aux séries de Fourier ou aux séries entières). Enfin le jury apprécie que le théorème des séries alternées (avec sa version sur le contrôle du reste) soit maîtrisé, mais il rappelle aussi que la transformation d'Abel trouve toute sa place dans cette leçon.

■ THÉORIE ÉLÉMENTAIRE

Def Définition de séries réelles, complexes

Def Somme partielle, reste

EX Somme télescopique (lien suite série)

EX Somme arithmétique

EX Somem géométrique

■ FAMILLES SOMMABLES

Def Lien suite croissante, famille positive

Def Sommabilité

Def Majorée $\Longrightarrow$ converge

Thm De sommation par paquets, convergence commutative

Thm Fubini

AP Formule des probas avec $P(X > n)$

AP Produit de Cauchy de séries

AP $\Sigma 1/(p^2q^2) = \pi^4/36$

■ COMPARAISON SÉRIE-INTÉGRALE

CSI Dans le cas décroissant

EX Séries de Riemann

EX Séries de Bertrand

CSI Avec la dérivée

EX ??

APP Équivalent de la série harmonique

■ CRITÈRES DE CONVERGENCE

Cri Comparaison dans $\overline{\mathbb{R}_+}$

Cri Critère de d'Alembert

Cri Critère de Cauchy

Cri Critère de Raabe-Duhamel

APP $n!/n^n$, $2^{(-1)^n-n}$, $1/\sqrt{n}$, $1/n^2$

APP Nombres sans 9

■ CALCULS EXPLICITES DE SÉRIES

EX à trouver

Thm Produit de Cauchy

DEV Ordre moyen ϕ

Thm Sommation en utilisant des séries entières

Thm Décompositon en éléments simples

■ SÉRIES ENTIÈRES ET SÉRIES

Thm Abel

EX ...

Thm Hardy-Littlewood

EX ...

DEV Nombres de Bell

■ FOURIER ET SÉRIES

Thm Parseval

EX $\pi^2/6$

DEV Formule de Poisson

■ ASYMPTOTIQUE DE SÉRIES

Thm Comparaison série-intégrale quantitative

APP $H_n = \ln n + \gamma + o(1)$.

Thm Sommation des relations de comparaison

APP DA de H_n

■ APPLICATION AUX SUITES

Thm Cesaro

Thm $u_{n+1} = \arctan u_n$

Thm $u_{n+1} = u_n + e^{-u_n}$

■ SÉRIES ABSOLUMENT CONVERGENTES

Thm De convergence absolue

Thm Critère de Cauchy

Thm Condensation de Cauchy

Thm Sommation par tranches

EX $(-1)^n/(n+z)$ et sommation par tranches

■ SÉRIES SEMI-CONVERGENTES

Thm Des séries alternées

Thm Accélération de convergence

Thm Transformation d'Abel

Thm Critère d'Abel

Thm Convergence commutative

■ IRRATIONALITÉ ET TRANSCENDANCE

Thm Liouville

Thm e est irrationnel

Thm e est transcendant

Thm π est irrationnel

Thm π est transcendant

■ **PROLONGEMENTS**

Thm Prolongement de ζ au plan complexe

■ **SÉRIES DE FOURIER**

Thm ...

7.233 ■ MÉTHODES ITÉRATIVES EN ANALYSE NUMÉRIQUE MATRICIELLE.

■ **DÉVELOPPEMENTS** **5.0**

D07 MÉTHODES ITÉRATIVES JACOBI/GAUSS-SEIDEL ⋆⋆⋆⋆⋆

D15 MÉTHODE DU GRADIENT À PAS OPTIMAL ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Allaire Kaber

Allaire tout court pour l'équation de la chaleur

Ciralet

Objectif Agrégation

Rouvière

Demailly

■ **RAPPORT DE JURY**

Dans cette leçon de synthèse, les notions de norme matricielle et de rayon spectral sont centrales, en lien avec le conditionnement et avec la convergence des méthodes itératives ; elles doivent être développées. Le résultat général de convergence, relié au théorème du point fixe de Banach, doit être enrichi de considérations sur la vitesse de convergence. Le jury invite les candidats à étudier diverses méthodes issues de contextes variés : résolution de systèmes linéaires, optimisation de fonctionnelles quadratiques (du type $(Ax,x)-(b,x)$), recherche de valeurs propres,... Parmi les points intéressants à développer, on peut citer les méthodes de type Jacobi pour la résolution de systèmes linéaires, les méthodes de gradient dans le cadre quadratique, les méthodes de puissance pour la recherche de valeurs propres. Les candidats pourront également envisager les schémas numériques pour les équations différentielles ou aux dérivées partielles linéaires.

7.233.1 Suites de matrices

■ **NORMES MATRICIELLES**

Def Norme matricielle

Thm Équivalence des normes

Def Rayon spectral

Thm Householder

7.233.2 Résolution d'équation

■ **DÉCOMPOSITION DE DUNFORD EFFECTIVE**

Def Décomposition de Dunford

MET Méthode de newton

Thm Convergence

Rem Nombre d'étapes

Rem stabilité numérique

■ **ÉQUATION ET CONDITIONNEMENT**

Def Conditionnement

EX Cas normal, symétrique, unitaire ...

Thm Majoration d'erreur via conditionnement

■ **ÉQUATION ET POINT FIXE**

MET passer de $f(x) = b$ à $\phi(x) = x$

Def $A = E + F + D$

Def Méthode de Jacobi

Def Méthode de Gauss-Seidel

Thm Méthode matricielle converge ssi erreur tends vers zéro ssi rayon spectral

Thm Stabilité de la méthode (ajout d'une erreur numérique)

Def Méthode de la relaxation

EX Comparaison sur le cas tridiagonal

7.233.3 Optimisation convexe

■ **MÉTHODE DE GRADIENTS**

Def Méthode de gradient

Thm Convergence ?

Def α-convexité

DEV Gradient a pas optimal

Thm Kantorovitch

APP Gradient à pas optimal et $(Ax, x) - (b, x)$ majoration erreur

Def Méthode du gradient conjugué

■ **MÉTHODES GÉNÉRALES**

Thm Méthode de Newton-Raphson

APP Méthodes intérieures ?

Thm Méthode de l'ellipsoïde ?

Thm Méthode du simplexe ?

7.233.4 Résolution numérique

■ **DISCRÉTISATION DU LAPLACIEN**

BLOC À trouver dans le Kaber-Allaire

■ **RÉSOLUTION DE L'ÉQUATION DE LA CHALEUR**

BLOC À trouver dans XX ??

7.236 ■ ILLUSTER DES MÉTHODES DE CALCUL D'INTÉGRALES (PLUSIEURS VARIABLES)

■ **DÉVELOPPEMENTS** **4.0**

D19 MÉTHODE DE LAPLACE ⋆⋆⋆

D20 INVERSION DE FOURIER L1 ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon

Beck

Faraut

Barbe et Ledoux

Zuily Quéffelec

Hauchecorne

Méléard Monte-Carlo

Demailly Analyse numérique

■ **RAPPORT DE JURY**

Cette leçon doit être très riche en exemples, que ce soit l'intégrale $\int \sin(t)/t$ ou bien d'autres encore. Il est tout à fait pertinent de commencer par les différentes techniques élémentaires (intégration par parties, changement de variables, décomposition en éléments simples, intégrale à paramètres,...). On peut également présenter des utilisations du théorème des résidus, ainsi que des exemples faisant intervenir les intégrales multiples comme le calcul de l'intégrale d'une gaussienne. Le calcul du volume de la boule unité de $\mathbb{R}^n$ ne doit pas poser de problèmes insurmontables. Le calcul de la transformation de Fourier d'une gaussienne a sa place dans cette leçon. On peut aussi penser à l'utilisation du théorème d'inversion de Fourier ou du théorème de Plancherel. Certains éléments de la leçon précédente, comme par exemple l'utilisation des théorèmes de convergence monotone, de convergence dominée et/ou de Fubini, sont aussi des outils ermettant le calcul de certaines intégrales. Enfin, il est aussi possible d'évoquer les méthodes de calcul approché d'intégrales (méthodes des rectangles, méthode de Monte-Carlo, etc.).

Les développements ne rentrent pas L236

7.236.1 Méthodes élémentaires

■ **Calcul de primitives**

Thm Fondamental du calcul intégral

LST Les primitives des fonctions usuelles!!

EX Des exemples du Gourdon

Thm Décomposition en éléments simples

LST Méthodes pour les fractions rationnelles

■ **Intégration par parties**

Thm Intégration par parties

EX WALLIS

EX Des suites d'intégrales

EX La fonction Γ

EX Des exemples classiques avec IPP

■ **Changement de variable**

Thm Changement de variable

LST Règles de Bioche

LST Règles de Bioche hyperbolique

LST Règles pour les racines

■ **En dimension supérieure**

Thm Fubini

Thm Changement de variables

APP Coordonnées porlaires, volume de la boule unité

APP Intégrale de Fresnel

7.236.2 Méthodes numériques

■ **Sommes de Riemann** **[DEM]**

Def Sommes de Riemann

Def Méthodes des rectangles

Thm Convergence pour le cas uniforme, décroissance pour le cas lip

Def Méthode des trapèzes

Def Méthode de Simpson [GOU]

■ **Interpolation** **[DEM]**

Def Interpolation de Lagrange

Def Méthode de l'interpolation

■ **Méthode de Monte-Carlo** **[OUV]**

Thm Loi forte des grands nombres

Thm Théorème Central Limite

Met Méthode de monte-carlo

7.236.3 Méthodes extérieures

■ **Passage à la limite**

Thm Convergence monotone, Convergence dominée

APP Bonne question

Def Développement en série entière

EX Des exemples du Gourdon

■ **Analyse complexe**

Thm Des résidus etc ...

APP Du Gourdon

■ **Intégrales à paramètres**

Thm Régularité etc ...

APP Du gourdon, Gamma etc...

APP l'intégrale sin t/t via laplace

Def Transformée de Fourier

DEV Inversion de Fourier L1

APP Calcul d'intégrales ?!?!?!

7.239 ■ INTÉGRALES À PARAMÈTRE

■ **DÉVELOPPEMENTS** **5.0**

D19 MÉTHODE DE LAPLACE ⋆⋆⋆⋆⋆

D20 INVERSION DE FOURIER L1 ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Gourdon

Beck

Faraut

Barbe et Ledoux

Zuily Quéffelec

Hauchecorne

■ **RAPPORT DE JURY**

> Souvent les candidats incluent les théorèmes de régularité (version segment — a minima — mais aussi version « convergence dominée ») ce qui est pertinent. Cette leçon peut être enrichie par des études et méthodes de comportements asymptotiques. Les propriétés de la fonction Γ d'Euler fournissent un développement standard (on pourra y inclure le comportement asymptotique, voire son prolongement analytique). Les différentes transformations classiques (Fourier, Laplace,...) relèvent aussi naturellement de cette leçon. On peut en donner des applications pour obtenir la valeur d'intégrales classiques (celle de l'intégrale de Dirichlet par exemple). Le théorème d'holomorphie sous le signe intégrale est trop peu souvent cité. Pour aller encore plus loin, on peut par exemple développer les propriétés des transformations mentionnées (notamment la transformée de Fourier, par exemple en s'attardant sur le lien entre régularité de la fonction et décroissance de sa transformée de Fourier), ainsi que de la convolution.

7.239.1 Définitions et régularité

On note $(X, \mathcal{T}, \mu)$ un espace mesuré et E un espace métrique. On considère les fonctions de la forme

$$F(t) = \int_X f(t,x)d\mu(x)$$

Exemple 114 (La fonction log)**.**

$$\log(x) = \int_0^{+\infty} \chi_{[1,x]}(t)dt$$

Exemple 115 (La fonction Γ d'Euler)**.** *Pour $x > 0$ on pose*

$$\Gamma(x) = \int_0^{+\infty} t^{x-1}e^{-t}dt$$

On a alors $\Gamma(1) = 1, \Gamma(n+1) = n!$ *et* $\Gamma(1/2) = \sqrt{\pi}$

Continuité et dérivabilité

Théorème 116 (Continuité sous signe intégral)**.** *Si les conditions suivantes sont vérifiées, alors F est continue au point t_0.*

(i) Pour tout $t \in E$, la fonction $x \mapsto f(t,x)$ est intégrable

(ii) Pour presque tout $x \in X$, la fonction $t \mapsto f(t,x)$ est continue en t_0

(iii) Il existe une fonction g intégrable positive indépendante de t telle que pour tout $t \in E$, presque pour tout x on ait :

$$|f(t,x)| \leq g(x)$$

Remarque. *On adapte le théoèrme pour vérifier la continuité sur E entier en vérifiant les hypothèses sur tout compact K inclus dans E.*

Exemple 117. *On pose $f : (x,t) \mapsto (x \in \mathbb{Q})$, alors $x \mapsto \int_{[0,1]} f(x,t)dt$ est discontinue en tout point de $\mathbb{R}$*

Exemple 118. *On pose $f : (x,t) \mapsto xe^{-xt}$, et on regarde x,t dans $[0,+\infty[$. Cette fois l'intégrande est continue, mais il n'y a pas de domination intégrable et l'intégrale en t est discontinue en $x = 0$.*

Théorème 119 (Dérivation sous signe intégral)**.** *On suppose que $E = I$ un intervalle ouvert de $\mathbb{R}$, et que les conditions suivantes sont vérifiées*

(i) Pour tout $t \in I$ la fonction $x \mapsto f(t,x)$ est intégrable

(ii) Presque pour tout $x \in X$ la fonction $t \mapsto f(t,x)$ est dérivable sur I

(iii) Pour tout compact K de I il existe une fonction g positive intégrable indépendante de t qui majore la dérivée sur K presque pour tout x.

Alors F est dérivable, et sa dérivée est (bien) définie par l'équation suivante :

$$F'(t) = \int_X \frac{\partial f}{\partial t}(t,x)d\mu(x)$$

Remarque. *On adapte aisément les hypothèses du théorème pour démontrer que F est C^k sur I.*

Application 120. *La fonction Γ est C^∞ sur $]0,+\infty[$*

Application 121 (Gourdon p163)**.** *Calcul de $\int e^{-t^2} = \sqrt{\pi/2}$ via l'expression*

$$F(x) = \int_0^1 \frac{e^{-x^2(t^2+1)}}{t^2+1}dt$$

Application 122 (Gourdon p164)**.**

$$\forall x \in \mathbb{R}_+^*, \int_0^{+\infty} \frac{\sin(xt)}{t}e^{-t}dt = \arctan(x)$$

Application 123 (Intégrale de Dirichlet)**.** *La fonction suivante est continue sur $[0,+\infty[$ et vérifie $F'(t) = \frac{-1}{1+t^2}$ sur $]0,+\infty[$ et $F(t) \to 0$ si $t \to +\infty$.*

$$F(t) = \int_0^{+\infty} \frac{\sin x}{x}e^{-tx}dx \qquad \text{On déduit alors} \qquad \int_0^{+\infty} \frac{\sin x}{x}dx = \frac{\pi}{2}$$

Remarque. *La continuité en zéro dans l'application précédente ne découle pas des théorèmes généraux !*

Holomorphie

Théorème 124. *Si f est une fonction méromorphe sur Ω ouvert connexe de $\mathbb{C}$ et γ est un lacet dans Ω alors*

$$\int_\gamma f(z)\,dz = 2i\pi \sum_{\alpha\in\mathbb{C}} \mathrm{Res}(f,\alpha)\,\mathrm{Ind}_\gamma(\alpha)$$

Application 125 (Gourdon p185)**.**

$$\forall \alpha>1, \int_0^{+\infty} \frac{dt}{1+t^\alpha} = \frac{\pi}{\alpha \sin(\pi/\alpha)} \qquad \forall 0<\beta<1, \int_0^{+\infty} \frac{dt}{t^\beta(1+t)} = \frac{\pi}{\sin \beta\pi}$$

Théorème 126 (Holomorphie sous signe intégral)**.** *On suppose que $E=\Omega$ un ouvert de $\mathbb{C}$, et que les conditions suivantes sont vérifiées*

(i) Pour tout $z\in\Omega$ la fonction $x\mapsto f(z,x)$ est intégrable et dominée presque partout par une fonction $g(x)$ indépendante de z

(ii) Presque pour tout $x\in X$ la fonction $z\mapsto f(z,x)$ est holomorphe sur Ω

Alors F est holomorphe sur Ω et ses dérivées s'obtiennent de la même manière que pour le théorème de dérivation sous signe intégral.

Propriété 127. *La fonction Γ généralisée à $z\in\mathbb{C}$ avec $\Re(z)>0$ est holomorphe.*

Propriété 128 (Formule des compléments)**.** *Pour z tel que $0<\Re z<1$ on a*

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

On peut donc prolonger Γ à $\mathbb{C}\setminus(-\mathbb{N})$ de manière holomorphe.

7.239.2 Convolution

Sur $\mathbb{R}^d$

Definition 129 (Convolution sur $\mathbb{R}^d$)**.** Quand cette définition a un sens on pose

$$f\star g(x) = \int_{\mathbb{R}^d} f(t)g(x-t)\,dt$$

Propriété 130. *Si f est dans $L^1(\mathbb{R}^d)$ et g est dans $L^p(\mathbb{R}^d)$ alors $f\star g$ est bien définie et dans $L^p(\mathbb{R}^d)$ avec*

$$\|f\star g\|_p \le \|f\|_1 \|g\|_p$$

Propriété 131. *Si p et q sont conjugués avec $f\in L^p, g\in L^q$ alors $f\star g$ définit une fonction dans L^∞ qui est de plus $f\star g$ uniformément continue. Si $1<p<+\infty$ alors $f\star g$ tend vers 0 en $+\infty$. Enfin on a la majoration :*

$$\|f\star g\|_\infty \le \|f\|_p \|g\|_p$$

Application 132. *Si $A\subseteq\mathbb{R}$ vérifie $0<\mu(A)<+\infty$ alors $A-A$ contient un voisinage de zéro.*

Exemple 133. *Si $f:\mathbb{R}\to\mathbb{R}$ est mesurable et vérifie $f(x+y)=f(x)+f(y)$ alors f est linéaire.*

Théorème 134. *Si $f:\mathbb{R}^d\to\mathbb{C}$ est localement intégrable et $\alpha:\mathbb{R}^d\to\mathbb{R}$ est de classe C^k à support compact alors :*

(i) $f\star\alpha$ est définie partout et de classe C^k

(ii) $\partial^j(f\star\alpha) = f\star\partial^j\alpha$ pour un multi-indice j de poids inférieur à k

Definition 135 (Approximation de l'unité)**.** C'est une suite (α_n) de fonctions mesurables positives d'intégrale 1 qui vérifient

$$\forall \delta > 0, \int_{|x|>\delta} \alpha_n(x)dx \underset{n\to\infty}{\longrightarrow} 0$$

Propriété 136. *Il existe des approximations de l'unité C^∞ à support compact*

Propriété 137. *Si $f \in C_b(\mathbb{R})$ alors $f \star \alpha_n \underset{n\to\infty}{\longrightarrow} f$ uniformément sur les compacts*

Propriété 138. *Si $f \in L^p(\mathbb{R})$ et $p < +\infty$ alors $f \star \alpha_n \underset{n\to\infty}{\longrightarrow} f$ dans L^p.*

Application 139. *Si $\Omega \subseteq \mathbb{R}^d$ est ouvert et $p < +\infty$ alors $C_c^\infty(\Omega)$ est dense dans $L^p(\Omega)$*

Application 140 (Weierstrass)**.** *Si K est un compact de $\mathbb{R}^d$ alors toute fonction continue de K dans $\mathbb{R}$ est limite uniforme de fonctions polynômiales.*

Sur $\mathbb{T}$

Definition 141. On pose, quand cela a un sens la convolution comme suit

$$f \star g(x) = \int_{\mathbb{T}} f(t)g(x-t)dt = \frac{1}{2\pi}\int_0^{2\pi} f(t)g(x-t)dt$$

Propriété 142. *La convolution sur $\mathbb{T}$ possède les propriétés de régularité de la convolution sur $\mathbb{R}^d$. De plus, on a pour $1 \le p \le +\infty$ les inclusions $\mathscr{C}(\mathbb{T}) \subseteq L^p(\mathbb{T}) \subseteq L^1(\mathbb{T})$.*

Definition 143 (Approximation de l'unité)**.** Une suite (α_n) de fonctions mesurables positives sur $\mathbb{T}$ est une approximation de l'unité si et seulement si elles sont d'intégrale 1 et vérifient

$$\forall \delta > 0, \int_{[-\pi,\pi]-[-\delta,\delta]} \alpha_n d_\mu \underset{n\to\infty}{\longrightarrow} 0$$

Propriété 144. *Les propriétés des approximations de l'unité s'adaptent à $\mathbb{T}$.*

Definition 145 (Coefficient de fourier)**.** Soit $f \in L^1(\mathbb{T})$ on pose $e_n(t) = e^{int}$ puis :

$$c_n(f) = \frac{1}{2\pi}\int_0^{2\pi} f(x)e^{-inx}dx = \int_{\mathbb{T}} f\overline{e_n}d\mu$$

Definition 146 (Noyaux de convolution)**.** On pose $D_N(t) = \sum_{-N\le k\le N} e_k(t)$ le noyau de Dirichlet et $K_N(t) = \frac{1}{N+1}\sum_{n=0}^N D_n(t)$. le noyau de Féjer.

Propriété 147. *La suite K_n est une approximation de l'unité sur $\mathbb{T}$. Si f est continue alors $\sigma_N f \to f$ uniformément, si f est L^p avec $1 \le p < +\infty$ alors $\sigma_N f \to f$ dans L^p.*

Dans les deux cas, la norme de $\sigma_N f$ est inférieure à celle de f.

Application 148. *(a) Les polynômes trigonométriques sont denses dans L^p pour $p < +\infty$. (b) Le développement en série de Fourier est injectif (c) La famille e^{inx} est une base hilbertienne de $L^2(\mathbb{T})$.*

7.239.3 Transformées de fonctions

Transformée de Fourier

Definition 149. Si $f \in L^1(\mathbb{R})$ on pose

$$\hat{f}(\xi) = \int_{\mathbb{R}} f(x)e^{-i\xi x}dx$$

Propriété 150 (Riemann-Lebesgue)**.** *On sait que $\hat{f}$ est continue bornée par $\|f\|_1$ et tend vers zéro quand $|x| \to +\infty$.*

Propriété 151 (Lien avec la convolution)**.** *Si f et g dans $L^1\left(\mathbb{R}^d\right)$ alors $\widehat{f \star g} = \hat{f}\hat{g}$.*

Propriété 152 (Lien avec la dérivation)**.** *On pose f une fonction intégrable et $\hat{f}$ sa transformée de Fourier :*

1. *Si xf est intégrable alors $\hat{f}$ est dérivable et $(\hat{f})'$ est la transformée de Fourier de $-ixf$.*
2. *Si f est de classe C^1 et si sa dérivée f' est intégrable alors $\hat{f}' = it\hat{f}$*

Remarque. *Ce résultat se généralise aux dérivées k-èmes*

Definition 153 (Noyau Gaussien)**.** Pour $\sigma > 0$ on pose $k_\sigma(t) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{t^2}{2\sigma^2}\right)$. La suite des k_σ est une approximation de l'unité pour $\sigma \to 0$.

Definition 154 (Inversion de Fourier L^1)**.** Si $f \in L^1(\mathbb{R})$ avec $\hat{f} \in L^1(\mathbb{R})$ alors presque pour tout x :

$$f(x) = \frac{1}{2\pi} \int_{\mathbb{R}} \hat{f}(t) e^{itx} dt$$

On calcule dans un premier temps $\widehat{k_\sigma}(t) = \sqrt{\frac{2\pi}{\sigma^2}} k_{1/\sigma}$ puis on convole f avec k_σ pour obtenir la formule d'inversion générale.

Application 155. *L'application $f \mapsto \hat{f}$ est injective de $L^1(\mathbb{R})$ dans $C_0(\mathbb{R})$.*

Théorème 156 (Densité des polynômes orthogonaux)**.** *Soit I un intervalle de $\mathbb{R}$ et $\rho : I \to \mathbb{R}$ mesurable strictement positive, telle que*

$$\exists \alpha \in \mathbb{R}_+^*, \int_I e^{\alpha|x|} \rho(x) dx < +\infty$$

Alors les polynômes orthogonaux associés à ρ forment une base hilbertienne de $L^2(I, \rho)$.

Application 157. *Soit $f : \mathbb{R} \to \mathbb{C}$ continue et bornée. On pose $k_t(x) = \frac{1}{\sqrt{4\pi t}} e^{-|x|^2/(4t)}$ le noyau de la chaleur. Alors $u(t,x) = k_t \star f(x)$ est continue sur $\mathbb{R}_+ \times \mathbb{R}$ et $\mathscr{C}^\infty$ sur $\mathbb{R}_+^* \times \mathbb{R}$. De plus u vérifie les équations suivantes*

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2} \text{ sur } \mathbb{R}_+^* \times \mathbb{R} \qquad u(0,x) = f(x) \forall x \in \mathbb{R}$$

Exemple 158 (Quelques transformées de Fourier)**.**

$$\widehat{\frac{1}{2a}\chi_{[-a,a]}} = \frac{\sin at}{at} \qquad \widehat{\text{sinc}} = \pi\chi_{[-1,1]}$$

$$\widehat{e^{-a|x|}} = \frac{2a}{a^2+t^2} \qquad \widehat{\frac{2a}{a^2+t^2}} = 2\pi e^{-a|x|}$$

7.239.4 Analyse asymptotique

Exemple 159 (Gourdon)**.**

$$\int_1^{+\infty} \frac{e^{-tx}}{\sqrt[3]{x^3+1}} dt \sim -\log t \qquad (t \to 0^+)$$

Méthode de Laplace

On étudie le comportement asymptotique d'intégrales du type

$$F(t) = \int_a^b f(x)e^{-t\phi(x)}dx$$

Avec f continue en a et $f(a) \neq 0$.

On a plusieurs résultats, qui dépendent du type de fonction ϕ. On étudie deux catégories : les fonctions qui se comportent comme x, et celles qui se comportent comme x^2.

Théorème 160. *Supposons ϕ de classe C^1 sur $[a,b[$, $\phi'(x) > 0$ sur $[a,b[$. Alors*

$$F(t) \sim \frac{f(a)}{\phi'(a)}\frac{1}{t}e^{-t\phi(a)} \qquad (t \to \infty)$$

Definition 161. Supposons ϕ de classe C^2 sur $[a,b[$, $\phi'(x) > 0$ sur $]a,b[$, $\phi'(a) = 0$ et $\phi''(a) > 0$. Alors

$$F(t) \sim \sqrt{\frac{\pi}{2}}\frac{f(a)}{\sqrt{\phi''(a)}}\frac{1}{\sqrt{t}}e^{-t\phi(a)} \qquad (t \to \infty)$$

Application 162 (Formule de Stirling)**.**

$$\Gamma(x+1) \sim x^{x+1}\Gamma\left(\frac{1}{2}\right)e^{-x}\sqrt{\frac{2}{x}} = \sqrt{2\pi}x^{x+1/2}e^{-x}$$

Exemple 163 (Gourdon p167)**.**

$$\int_0^\pi (\sin x)x^t dt \sim \frac{\pi^{t+2}}{t^2} \qquad (t \to +\infty)$$

7.243 ■ CONVERGENCE DES SÉRIES ENTIÈRES, PROPRIÉTÉS DE LA SOMME. EXEMPLES ET APPLICATIONS.

■ **DÉVELOPPEMENTS** **5.0**

D17 NOMBRES DE BELL ⋆⋆⋆⋆⋆

D25 THÉORÈME DE BERNSTEIN SUR LES SÉRIES ENTIÈRES ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

FGN

Gourdon Analyse

Zuilly Queffelec

Hauchecorne

■ **RAPPORT DE JURY**

Les candidats évoquent souvent des critères (Cauchy, D'Alembert) permettant d'estimer le rayon de convergence mais oublient souvent la formule de Cauchy-Hadamard. Le jury attend bien sûr que le candidat puisse donner des arguments justifiant qu'une série entière en 0 dont le rayon de convergence est R est développable en série entière en un point z_0 intérieur au disque de convergence et de minorer le rayon de convergence de cette série. Sans tomber dans un catalogue excessif, on peut indiquer les formules de développement de fonctions usuelles importantes (exp , log , $1/(1-z)$, sin ,...). S'agissant d'exemples fondamentaux et classiques, le jury attend que le candidat puisse les donner sans consulter ses notes. En ce qui concerne la fonction exponentielle, le candidat doit avoir réfléchi au point de vue adopté sur sa définition et donc sur l'articulation entre l'obtention du développement en série entière et les propriétés de la fonction. À ce propos, les résultats sur l'existence du développement en série entière pour les fonctions dont on contrôle toutes les dérivées successives sur un voisinage de 0 sont souvent méconnus. Le comportement de la série entière dans le disque de convergence vis à vis des différents modes de convergence (convergence absolue, convergence uniforme, convergence normale) doit être maîtrisé. Le théorème d'Abel (radial ou sectoriel) trouve toute sa place mais doit être agrémenté d'exercices pertinents. Réciproquement, les théorèmes taubériens offrent aussi de jolis développements. On pourra aller plus loin en abordant quelques propriétés importantes liées à l'analyticité de la somme d'une série entière.

7.243.1 Premières propriétés

■ **SÉRIE ENTIÈRE**

Def Série entière

EX $a_n = 1$

Pro Abel

Thm Convergence absolue dans un disque

Def Rayon de convergence

Def Convergence absolue, semi-convergence, divergence

EX $1/n$, $1/n^2$, $1/n!$

■ **CALCUL DE R_{CV}**

Def Critère d'Alembert

Def Critère de Cauchy

Def Formule d'Hadamard

EX Gourdon

■ **PROPRIÉTÉS DE STRUCTURE**

Def Somme de séries

Def Produit de Cauchy

Def Inverse d'une série entière

Def Composition

7.243.2 Comme séries de fonctions

■ **RÉGULARITÉ SOUS SIGNE SOMME**

Thm Convergence normale, donc uniforme

Pro Multiplication par n ne change pas R_{CV}

Thm Dérivation sous signe somme

Thm Série entière C^∞

■ **CONVERGENCE PONCTUELLE**

Thm Théorème d'Abel radial

Thm Théorème taubérien faible

Thm (ADMIS) Taubérien fort

APP Gourdon

CSQ Si on ne converge pas uniformément sur le disque, alors on diverge en un point.

■ **LIEN AVEC TAYLOR**

Thm $a_n = f^{(n)}(0)/n!$

CSQ Unicité du développement

Pro Si f est C^∞ et le reste converge uniformément vers zéro alors nickel

DEV Bernstein

EX Les contre-exemples classiques

■ **LIEN AVEC L'HOLOMORPHIE**

Thm Formule de Cauchy analytique

Thm $2\pi r^n a_n = \int_C f(re^{it})e^{-int}dt$

APP Liouville

Thm (ADMIS) Dérivable au sens complexe ssi analytique sur un ouvert

Thm Toute série entière est analytique sur son disque de convergence et réciproque

Thm Des zéros isolés

Thm Égalité de Parseval

Thm Principe du maximum

7.243.3 Méthodes de calcul & Utilisation

■ **CALCUL DE SÉRIES**

Def Convergence au sens d'Abel

EX Calculs en passant à la limite

■ **EDO**

Def EDO à coefs entiers

Thm Il existe une unique solution entière qui se calcule par récurrence

EX Dérivation plus équation fonctionnelle

■ **MÉTHODES DE CALCUL**

Thm Primitive d'un DSE

MET $(1-x)f(x)$ permet de faire la dérivée discrète de a_n

MET $(1-x)^{-1}$ fait la primitive discrète de a_n

■ **SÉRIES GÉNÉRATRICES**

EX Nombres de catalan

DEV Nombes de Bell

Def Série génératrice pour $\mathbb{N}$

Thm Toutes les propriétés des séries génératrices

Thm Galton-Watson

Thm Caractérisation de la loi

7.246 ■ SÉRIES DE FOURIER

■ **DÉVELOPPEMENTS** **5.0**

D14 BANACH STEINHAUS ET FOURIER ⋆⋆⋆⋆⋆

D27 FORMULE SOMMATOIRE DE POISSON ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Dyn Mc Kean

Fourier series and integrals Princeton

Faraut

Gourdon Analyse

ZQ

Objectif Agrégation

■ **RAPPORT DE JURY**

Les différents résultats autour de la convergence (L^2, Féjer, Dirichlet, ...) doivent être connus. On prendra garde au sens de la notation $\sum_{n\in\mathbb{Z}}$ (qu'il peut être plus prudent d'éviter en général). Il faut avoir les idées claires sur la notion de fonctions de classe C^1 par morceaux (elles ne sont pas forcément continues). Dans le cas d'une fonction continue et C^1 par morceaux on peut conclure sur la convergence normale de la série Fourier sans utiliser le théorème de Dirichlet. Il est classique d'obtenir des sommes de séries remarquables comme conséquence de ces théorèmes. On peut aussi s'intéresser à la formule de Poisson et à ses conséquences. L'existence d'exemples de séries de Fourier divergentes, associées à des fonctions continues (qu'ils soient explicites ou obtenus par des techniques d'analyse fonctionnelle) peuvent aussi compléter le contenu. Il est souhaitable que cette leçon ne se réduise pas à un cours abstrait sur les cœfficients de Fourier. La résolution d'équations aux dérivées partielles (par exemple l'équation de la chaleur ou l'équation des ondes avec une estimation de la vitesse de convergence) peuvent illustrer de manière pertinente cette leçon, mais on peut penser à bien d'autres applications (inégalité isopérimétrique, comportements remarquables des fonctions à spectre lacunaire,...).

7.250 ■ TRANSFORMATIONS DE FOURIER

■ **DÉVELOPPEMENTS** **5.0**

D20 INVERSION DE FOURIER L1 ⋆⋆⋆⋆⋆

D27 FORMULE SOMMATOIRE DE POISSON ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Dyn Mc Kean

Fourier series and integrals Princeton

Faraut

Gourdon Analyse

ZQ

Objectif Agrégation

■ **RAPPORT DE JURY**

Cette leçon offre de multiples facettes. Les candidats peuvent adopter différents points de vue : L^1, L^2 et/ou distributions. L'aspect « séries de Fourier» n'est toutefois pas dans l'esprit de cette leçon ; il ne s'agit pas de faire de l'analyse de Fourier sur n'importe quel groupe localement compact mais sur R ou R^d. La leçon nécessite une bonne maîtrise de questions de base telle que la définition du produit de convolution de deux fonctions de L^1. En ce qui concerne la transformation de Fourier, elle ne doit pas se limiter à une analyse algébrique de la transformation de Fourier. C'est bien une leçon d'analyse, qui nécessite une étude soigneuse des hypothèses, des définitions et de la nature des objets manipulés. Le lien entre la régularité de la fonction et la décroissance de sa transformée de Fourier doit être fait, même sous des hypothèses qui ne sont pas minimales. Les candidats doivent savoir montrer le lemme de Riemann-Lebesgue pour une fonction intégrable. La formule d'inversion de Fourier pour une fonction L^1 dont la transformée de Fourier est aussi L^1 est attendue ainsi que l'extension de la transformée de Fourier à l'espace L^2 par Fourier-Plancherel. Des exemples explicites de calcul de transformations de Fourier, classiques comme la gaussienne ou $(1+x^2)^{-1}$, paraissent nécessaires. Pour aller plus loin, la transformation de Fourier des distributions tempérées ainsi que la convolution dans le cadre des distributions tempérées peuvent être abordées. Rappelons une fois de plus que les attentes du jury sur ces questions restent modestes, au niveau de ce qu'un cours de première année de master sur le sujet peut contenir. Le fait que la transformée de Fourier envoie $S(R^d)$ dans lui même avec de bonnes estimations des semi-normes doit alors être compris et la formule d'inversion de Fourier maîtrisée dans ce cadre. Des exemples de calcul de transformée de Fourier peuvent être données dans des contextes liés à la théorie des distributions comme par exemple la transformée de Fourier de la valeur principale. La résolution de certaines équations aux dérivées partielles telle que, par exemple, l'équation de la chaleur sur R, peut être abordée, avec une discussion sur les propriétés qualitatives des solutions. Dans un autre registre, il est aussi possible d'orienter la leçon vers l'étude de propriétés de fonctions caractéristiques de variables aléatoires.

7.260 ■ ESPÉRANCE, VARIANCE ET MOMENTS D'UNE VARIABLE ALÉATOIRE.

■ **DÉVELOPPEMENTS** **5.0**

D16 PROCESSUS DE BRANCHEMENTS ⋆⋆⋆⋆⋆

D23 MARCHE ALÉATOIRE ZD ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Fourier Series and Integrals Mc Kean

Barbe et Ledoux

Probabilités pour les non-probabilistes

Ouvrard

Hauchecorne

CGCDM (COT) plein d'exemples!!!

Méléard Monte-Carlo

■ **RAPPORT DE JURY**

Le jury attend des candidats qu'ils donnent la définition des moments centrés, qu'ils rappellent les implications d'existence de moments (décroissance des L^p). Le candidat peut citer — mais doit surtout savoir retrouver rapidement — les espérances et variances de lois usuelles, notamment Bernoulli, binomiale, géométrique, Poisson, exponentielle, normale. La variance de la somme de variables aléatoires indépendantes suscite souvent des hésitations. Les inégalités classiques (de Markov, de Bienaymé-Chebyshev, de Jensen et de Cauchy-Schwarz) pourront être données, ainsi que les théorèmes de convergence (lois des grands nombres et théorème central limite). La notion de fonction génératrice des moments pourra être présentée ainsi que les liens entre moments et fonction caractéristique. Pour aller plus loin, le comportement des moyennes empiriques pour une suite de variables aléatoires indépendantes et identiquement distribuées n'admettant pas d'espérance pourra être étudié. Pour les candidats suffisamment à l'aise avec ce sujet, l'espérance conditionnelle pourra aussi être abordée.

7.260.1 Espérance et variance

■ **ESPÉRANCE**

Def Espérance

Def Centrée-réduite etc.

Thm Linéarité, etc...

Def Liste de formules

■ **PROPRIÉTÉS DE L'ESPÉRANCE**

Thm Jensen

Thm Indépendance

Thm De transfert

EX Inégalité de Markov

Thm Espérance et indépendance (def-prop)

APP Polynômes de Bernstein

■ **VARIANCE**

Def Variance

REM Caractérisation via norme L^2

Pro Variance $\Longrightarrow$ Espérance

Def Écart-type

Def Centrée-réduite

Def Liste de formules

■ **PROPRIÉTÉS DE LA VARIANCE**

Thm Quadratique etc ...

Def Covariance et produit scalaire L^2

Thm Minimise $\mathbf{E}((X-a)^2)$

Pro Indépendance somme des variances

EX Bernouilli et Binomiale

Thm Variance et indépendance

EX $Cov(X,Y)=0$ mais X non indép de Y

Thm Inégalité de Tchebychev

Thm Inégalité de Cauchy-Schwartz

7.260.2 Moments et fonctions

■ **DÉFINITIONS**

Def Moment d'ordre k

Thm Inclusion des L^p

Def Moment centré d'ordre p

Pro Théorème de transfert pour les moments

Thm Inégalité de Hölder

Thm Inégalité de Minkowski

■ **SÉRIE GÉNÉRATRICE**

Def Série génératrice pour $\mathbb{N}$

Thm Toutes les propriétés des séries génératrices

DEV Galton-Watson

Thm Caractérisation de la loi

Def Généralisation via la transformée de Laplace

EX Inégalité de Hoeffding

EX Bornes de Chernoff

■ **FONCTION CARACTÉRISTIQUE**

Def Fonction caractéristique

REM Lien avec la transformée de Fourier

Thm Inversion de Fourier L^1

Thm Caractérisation de la loi

DEV Marche aléatoire sur Z^d

■ **INÉGALITÉS DE CONCENTRATION**

Thm Transformée de Laplace pour avoir es bornes ... ?

7.260.3 Méthodes d'estimation

■ **CONVERGENCE EN PROBABILITÉ**

Def Définition

Thm Loi faible des grands nombres

■ **CONVERGENCE PRESQUE-SÛRE**

Def Définition

Thm Loi forte des grands nombres

■ **CONVERGENCE L^p**

Def Définition

APP Méthodes de Monte-Carlo (I)

■ **CONVERGENCE EN LOI**

Def Définition

Thm Équivalences avec ϕ_X

Thm Théorème Central Limite

APP Méthodes de Monte-Carlo (II)

Thm Slutsky

7.260.4 En informatique

■ **RP ET CORP**

Def Algorithme probabiliste

Def RP/coRP

Thm Réduciton d'erreur avec markov

EX Tests de primalité ! (Rabin-Miller, Solovay-Strassen)

■ **ZPP**

Def ZPP

Thm coRP ∩ RP = ZPP

■ **BPP**

Def BPP

Thm Réduction d'erreur BPP via Chernoff

7.264 ■ VARIABLES ALÉATOIRES DISCRÈTES. EXEMPLES ET APPLICATIONS

■ **DÉVELOPPEMENTS** **5.0**

D16 PROCESSUS DE BRANCHEMENTS ⋆⋆⋆⋆⋆

D23 MARCHE ALÉATOIRE ZD ⋆⋆⋆⋆⋆

■ **RÉFÉRENCES**

Fourier Series and Integrals Mc Kean

Barbe et Ledoux

Probabilités pour les non-probabilistes

Ouvrard tome 1

Hauchecorne

Méléard Monte-Carlo

CGCDM (COT) plein d'exemples!!!

■ **RAPPORT DE JURY**

Le jury attend des candidats qu'ils rappellent la définition d'une variable aléatoire discrète et que des lois usuelles soient présentées, en lien avec des exemples classiques de modélisation. Le lien entre variables aléatoires de Bernoulli, binomiale et de Poisson doit être discuté. Il peut être d'ailleurs intéressant de mettre en avant le rôle central joué par les variables aléatoires de Bernoulli. Les techniques spécifiques aux variables discrètes, notamment à valeurs entières, devront être mises en évidence, comme par exemple la caractérisation de la convergence en loi, la notion de fonction génératrice. Pour aller plus loin, le processus de Galton-Watson peut se traiter intégralement à l'aide des fonctions génératrices et cette voie a été choisie par plusieurs candidats : cela donne un développement de très bon niveau pour ceux qui savent justifier les étapes délicates. Pour aller beaucoup plus loin, les candidats pourront étudier les marches aléatoires, les chaînes de Markov à espaces d'états finis ou dénombrables, les sommes ou séries de variables aléatoires indépendantes.

7.264.1 Définitions et exemples

■ **LOI DISCRÈTE** **[OUV]**

Def Espace discret ssi E est dénombrable et $A = P(E)$

Rem La mesure de proba est alors carctérisée par la mesure des singletons

Def VA-discrète

Pro Stable par opérations élémentaires

Def Germe de probabilité

■ **LOIS USUELLES ET MODÉLISATION**

Def Loi uniforme

Def Loi de Bernouilli

Def Loi Binômiale

Def Loi Géométrique

Def Loi de Poisson

Def Loi hypergéométrique ?

■ **À CLASSER**

Def Indépendance de variables aléatoires

Thm Simplification dans le cas discret

Thm Dénombrement, formule de poincarre etc ...

Def Conditionnement

Def Probabilité conditionnelle

Def Formule des probabilités totales

Def Formule de Bayes

Def Espérance conditionnelle discrète....

■ **ESPÉRANCE**

Def Espérance

Thm Linéarité etc ...

EX Calculs sur les lois usuelles

Thm De transfert

Thm Inégalité de Markov

APP $ZPP = RP \cap coRP$

APP Polynômes de Bernstein

7.264.2 Moments et fonctions

■ **VARIANCE**

Thm Quadratique etc ...

Def Covariance et produit scalaire L^2

Thm Minimise $\mathbf{E}((X-a)^2)$

Pro Indépendance somme des variances

EX Bernouilli et Binomiale

EX $Cov(X,Y) = 0$ mais X non indép de Y

Thm Inégalité de Tchebychev

Thm Inégalité de Cauchy-Schwartz

■ **DÉFINITIONS**

Def Moment d'ordre p

Thm Inclusion des L^p

Def Moment centré d'ordre p

Pro Théorème de transfert pour les moments

Thm Inégalité de Hölder

Thm Inégalité de Minkowski

Thm Inégalités de Markov "Améliorées"

■ **SÉRIE GÉNÉRATRICE**

Def Série génératrice pour $\mathbb{N}$

Thm Toutes les propriétés des séries génératrices

Pro Somme, produit, CL etc ...

DEV Galton-Watson

Thm Caractérisation de la loi

EX Inégalité de Hoeffding

EX Bornes de Chernoff

■ **FONCTION CARACTÉRISTIQUE**

Def Fonction caractéristique

REM Lien avec la transformée de Fourier

Pro Somme, produit, CL etc ...

Thm Inversion de Fourier L^1

Thm Caractérisation de la loi

DEV Marche aléatoire sur Z^d

7.264.3 Convergence(s)

■ **CONVERGENCE EN PROBABILITÉ**

Def Définition

Thm Loi faible des grands nombres

■ **CONVERGENCE PRESQUE-SÛRE**

Def Définition

Thm Loi forte des grands nombres

■ **CONVERGENCE EN LOI**

Def Définition

Thm Caractérisation pour les va à valeurs dans $\mathbb{N}$

EX Contre exemple avec $\{1/n\}$

Thm Limite Poissonnien

APP $np_n \to \lambda$ la binômiale est comme un poisson

CHAPITRE 8

RÉSULTATS À RECASER

■ **ALGÈBRE**

Cardinal groupe linéaire sur corps fini

Dénombrement des endomorphismes nilpotents

1. Gourdon Analyse
2. Gourdon Algèbre
3. Perrin
4. Invitation aux formes quadratiques
5. H2G2
6. Rouvière
7. Beck
8. Zuily Quéffélec
9. Ciralet
10. Allaire Kaber
11. J.D. Eiden Géométrie
12. Gonnord Tosel
13. Audin
14. Rombaldi
15. Cours de géométrie Mercier
16. Introduction à la calculabilité
17. Éléments d'algorithmique
18. Introduction à l'algorithmique