Développements pour l'agrégation de mathématiques option informatique (2011)

Antoine MARNAT
antoine.marnat@ens-cachan.org
http://perso.eleves.bretagne.ens-cachan.fr/~amarn880/

Juillet 2011

Table des matières

Introduction

Ce document propose les références de développements pour l'agrégation de mathématiques utiles en option informatique (D). Il a donc pour but de faciliter la recherche de développements possibles pour les optionnaires d'informatique, et pourra bien sur être utile à tout les préparationnaires.

Vous trouverez dans chaque section une liste de développements - agrémentée d'une courte présentation, des références bibliographiques et des leçons correspondantes- suivi d'une table relatant mes propres choix pour chaque leçon. Mes choix sont bien évidemment personnels et non optimaux. J'attire votre attention sur le fait que votre choix de développements est très personnel, et qu'il vous faudra vous approprier chaque développement, en veillant le plus possible à ce qu'il vous plaise et corresponde à votre niveau mais aussi au cadre de la leçon. Volontairement, les leçon associées à un développement donné sont parfois très éloignées, pour renforcer l'esprit critique du lecteur : Certains développements sont capillotractés, et nécessitent un plan adapté pour les motiver, certains sont trop proches -et donc mauvais couplés entre eux, ou enfin peuvent devenir obsolètes avec le temps.

Même si certains développements deviennent inutiles en tant que développement, ils pourront surement agrémenter des plans de leçons.

Ce document utilise mes classeurs, fruits de mon année de préparation pour la partie informatique, et réutilise principalement et souvent outrageusement les très bons documents mis en ligne par Laurent PATER (`http://pagesperso-orange.fr/laurent.pater/`) pour la partie mathématiques.

Vous trouverez également sur mon site un fichier BibDesk qui s'avère très pratique pour faire son choix de développements (`http://perso.eleves.bretagne.ens-cachan.fr/~amarn880/`). Je vous invite à consulter la page de mon co-préparationnaire Simon BILLOUET (`http://perso.eleves.bretagne.ens-cachan.fr/~sbill404/`) qui contient également des bons documents. N'hésitez pas à me contacter si vous avez des questions, des remarques ou des suggestions d'ajouts : antoine.marnat@ens-cachan.org

Je remercie mes co-préparationnaires pour leur relecture assidue et leurs apports constructifs.

Chapitre 1

Informatique

1.1 Référence des développements d'informatique

1.1.1 Arbres Binaires de Recherche optimaux [901][907][921][925]

Résultat On construit les arbres binaires de recherche optimaux pour un texte donné connu (avec les fréquences des lettres) selon la méthode de Huffman.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.2 Additionneur n-bit [902][916]

Résultat : On utilise une méthode "diviser pour régner" pour construire un additionneur n-bit de hauteur (donc temps) logarithmique, alors que l'additionneur naïf est en hauteur linéaire. À noter que l'on perd sur le nombre de porte : on calcule double, le cas avec et sans propagation de retenue.

$$T(n) = 3(1 + \log_2 n), P(n) = 3n \log_2 n + 15n + 6$$

Attention à être clair dans les notations !

Référence :
- L. ALBERT, P.GASTIN, B.PETAZZONI *Cours et exercices d'informatique : classes préparatoires, 1er et 2nd cycles universitaires*

1.1.3 Algorithme Cocke Younger Kasami [906][910][923]

Résultat On donne un algorithme de programmation dynamique qui décide en temps $O(|w|^3)$ si un mot w appartient au langage engendré par une grammaire sous forme normale de Chomsky. Remarquez que la mise sous forme de Chomsky est coûteuse ...

Référence :
- R.FLOYD, C.BEIGEL *Le langage des machines* Broché (1995)

1.1.4 Algorithme de Bellman-Ford [907][925][926][927]

Résultat On expose l'algorithme de Bellman-Ford qui calcule de façon dynamique le plus court chemin à origine unique vers tout sommet d'un graphe orienté pondéré (même valué négativement), et détecte les cycles négatifs. Pour cela, on effectue des relâchements itérés sur toutes les arêtes, on obtient donc une complexité temporelle en $O(|S| \cdot |A|)$.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.5 Algorithme de coupure de Davis et Puttnam [916]

Résultat On expose l'algorithme de coupure de Davis et Puttnam qui résout SAT en temps exponentiel. On peut compléter ce développement un peu court par différents corollaires, comme le cas où une variable n'apparaît pas négativement.

Référence :
- M. DAVIS, R. SIGAL, E.J. WEYUKER *Computability, Complexity, and Languages : Fundamentals of Theoretical Computer Science*

1.1.6 Algorithme de Dijkstra [901][925][926][927]

Résultat On présente l'algorithme de Dijkstra -de type glouton- pour le calcul du plus court chemin vers chaque sommet à origine unique dans le cas d'un graphe valué positivement. La correction se fait par invariant de boucle. On peut selon la leçon discuter du choix de la structure de donnée et son influence sur la complexité. Attention à maîtriser les tas de Fibonnacci si vous les évoquez.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.7 Algorithme de Floyd-Warshall [906][925]

Résultat On expose l'algorithme de Floyd-Warshall qui calcule le plus court chemin entre toutes les paires de sommet d'un graphe orienté valué sans cycle négatif en complexité temporelle $O(|V|^3)$ avec une approche de programmation dynamique. On peut expliciter le plus court chemin, et donner une application au calcul de la fermeture transitive d'un graphe.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*
- C.FROIDEVAUX,M.-C. GAUDEL, M.SORIA *Types de données et algorithmes*, McGraw-Hill, Collection Informatique,1990, 575 pages.

1.1.8 Algorithme d'Hopcroft [902][908][926][927]

Résultat On donne l'algorithme d'Hopcroft qui calcule l'automate minimal d'un automate fini déterministe donné en temps $O(|Q||\Sigma|\log\Sigma)$. Pour cela on calcule l'équivalence de Nérode $p \sim q \Leftrightarrow L_p = L_q$, dont on utilise certaines propriétés, qui permettent entre autre d'utiliser une stratégie diviser pour régner. Attention ce développement est très long, il faudra choisir les parties que l'on compte exposer et celles qu'on admet selon la leçon.

Références :
- D.BEAUQUIER, J.BRESTEL, Ph. CHRÉTIENNE *Eléments d'algorithmique*
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert

1.1.9 Algorithme d'Unification [919][927]

Résultat : On expose l'algorithme naïf d'unification -exponentiel en temps et en espace- dont la terminaison se prouve à l'aide d'un ordre bien fondé non trivial. C'est sûrement l'algorithme le plus intéressant à étudier pour la leçon [927]

Références :
- K.NOUR, R.DAVID, C.RAFFALLI *Introduction à la logique : Théorie de la démonstration - Cours et exercices corrigés*, Broché
- F.BAADER, T.NIPKOW *Term Rewriting and All That* , Broché (1999)

1.1.10 Automate des items [911][923]

Résultat On construit l'automate des items sur un exemple bien choisi. Attention, il s'agit d'analyse ascendante, alors que seul l'analyse descendante est explicitement au programme [1].

1. En 2011

Références :
- A.AHO,R.SETHI,J.ULLMAN *Compilateurs : principes, techniques et outils* aka "le Dragon"
- R.WILHELM, D.MAURER *Les compilateurs : théorie, construction et génération*

1.1.11 Automate des occurrences [907][908][921]

Résultat On expose l'automate des occurrences, associé à l'algorithme de Knuth-Morris-Pratt de reconnaissance d'un motif dans un texte. Il reconnaît le langage $\Sigma^* x$ et est minimal. Il faut penser à faire des dessins des mots, pour que les manipulations des notions de préfixes et suffixes ne soient pas trop obscures. On peut aller plus loin expliquant la non minimalité si on recherche plusieurs motifs. Il faut être prêt à expliciter le calcul de la fonction de transition via le calcul des bords (fait dans *Crochemore*).

Références :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*
- M. CROCHEMORE *L'algorithmique du texte*, Broché (2001)

1.1.12 B-Arbres [901][907][921][925]

Résultat On présente les B-Arbres, un cas particulier d'ABR et la façon de les rééquilibrer lors de l'insertion.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*
- C.FROIDEVAUX,M.-C. GAUDEL, M.SORIA *Types de données et algorithmes*, McGraw-Hill, Collection Informatique,1990, 575 pages.

1.1.13 Caractérisation des ensembles RE [912][922]

Résultat On montre une partie des caractérisations des ensembles *RE* présentes dans *Lalement*. Par exemple, on pourra montrer que pour $A \subset \mathbb{N}$, il y a équivalence entre

1. A et RE,
2. A est l'image d'une fonction primitive récursive $\mathbb{N} \to \mathbb{N}$ ou $A = \emptyset$,
3. A est l'image d'une fonction partielle récursive $\mathbb{N} \to \mathbb{N}$,
4. A est la projection d'un ensemble $B \subset \mathbb{N}^2$ μ-récursif.

Comme dans d'autres cas il faut se méfier de cette référence qui nécessite d'avoir déjà beaucoup de recul sur la logique, et il est donc plus prudent de bien préparer ce développement à l'aide des deux autres références.

Références :
- R.LALEMENT *Logique, réduction, résolution*, Relié
- R.CORI, D.LASCAR *Logique mathématique, tome 2 : Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles*, Broché
- P.WOLPER *Introduction à la calculabilité*, Broché

1.1.14 CNS de rationalité d'un langage [909]

Résultat On montre qu'un langage est rationnel si et seulement lui-même et son complémentaire vérifient le lemme de l'étoile par blocs.

Référence :
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert
- J. SAKAROVITCH *Eléments de théorie des automates* , Relié (2003)

1.1.15 Comparaison tri rapide/tri fusion [902][903][926]

Résultat On analyse deux approches diviser pour régner du tri par comparaison, pour en montrer les différences (stabilité, constantes).

Référence :
- D.BEAUQUIER, J.BRESTEL, Ph. CHRÉTIENNE *Eléments d'algorithmique*
- C.FROIDEVAUX,M.-C. GAUDEL, M.SORIA *Types de données et algorithmes*, McGraw-Hill, Collection Informatique,1990, 575 pages.
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.16 Complétude de la logique de Hoare [927]

Résultat On montre la complétude de la logique de Hoare.

Référence :
- K. R. APT, E.-R. OLDEROG *Verification of Sequential and Concurrent Programs*
- G.WINSKEL *The Formal Semantics of Programming Languages*

1.1.17 Complétude de la méthode de résolution [917][918][919][924]

Résultat On montre la complétude de la méthode de résolution via la complétude de la méthode de coupure et le théorème de compacité. Attention c'est long, et il ne faut pas maltraiter le passage technique sur le lemme de relèvement : on s'expose donc à de nombreuses questions sur lesquelles il faudra être au point.

Référence :
- R.CORI,D.LASCAR *Logique mathématique 1 - Calcul propositionnel ; algèbre de Boole ; calcul des prédicats*, Broché (2003)
- R.LASSAIGNE, M.ROUGEMONT *Logique et complexité*, Hermès (1996)

1.1.18 Composantes fortement connexes [901][925]

Résultat On calcule les composantes fortement connexes d'un graphe orienté en utilisant les propriétés du parcours en profondeur (théorème du chemin blanc) et le graphe transposé (on inverse l'orientation des arêtes).

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.19 Construction d'un analyseur lexical [923]

Résultat On construit un analyseur lexical sur un exemple bien choisi.

Références :
- A.AHO,R.SETHI,J.ULLMAN *Compilateurs : principes, techniques et outils* aka "le Dragon"
- R.WILHELM, D.MAURER *Les compilateurs : théorie, construction et génération*

1.1.20 Construction d'un analyseur syntaxique [923]

Résultat On construit un analyseur syntaxique sur un exemple bien choisi.

Références :
- A.AHO,R.SETHI,J.ULLMAN *Compilateurs : principes, techniques et outils* aka "le Dragon"
- R.WILHELM, D.MAURER *Les compilateurs : théorie, construction et génération*

1.1.21 Décidabilité de l'arithmétique de Presburger [908][909][914][922][924]

Résultat On montre qu'étant donné une formule, il existe un algorithme qui décide si elle est démontrable ou non dans le modèle $(\mathbb{N}, +)$. On montre même que l'ensemble de n-uplets qui satisfont cette formule est un langage rationnel, en construisant un automate qui le reconnaît.

Référence :
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert
- M.SIPSER *Introduction to the Theory of Computation*, Relié

1.1.22 Distance d'édition [906][907][921]

Résultat On expose un algorithme de programmation dynamique qui calcul la distance d'édition entre deux mots, et donne les transformations successives pour passer de l'un à l'autre.

Référence :
- M. CROCHEMORE *L'algorithmique du texte*, Broché (2001)
- PAPADIMITRIOU *Algorithms*

1.1.23 Ensemble de formules indépendant [916]

Résultat On montre que tout ensemble $\mathcal{A}$ fini de formules propositionnelles admet un sous-ensemble indépendant équivalent, ie tel que $\forall F \in \mathcal{A}, \mathcal{A} \setminus \{F\} \nvDash F$. Dans le cas d'un ensemble dénombrable, on a toujours un ensemble indépendant équivalent, mais ce n'est plus forcément un sous-ensemble de l'ensemble de départ (on pourra exhiber un contre-exemple).

Référence :
- R.CORI,D.LASCARLogique mathématique 1 - Calcul propositionnel; algèbre de Boole; calcul des prédicats, Broché (2003)

1.1.24 Enveloppe convexe [902]

Résultat On calcule à l'aide du diviser pour régner l'enveloppe convexe d'un ensemble fini de points de l'espace dont on considérera les abscisses. Pour régner sur deux parties convexes disjointes, il s'agit de trouver les deux segments qui permettent de reconstituer une nouvelle enveloppe convexe. La complexité temporelle de cet algorithme est de $O(n \log n)$.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.25 Equivalence entre RE et avoir un énumérateur, R et avoir un énumérateur dans l'ordre hiérarchique [922]

Résultat On montre d'une part l'équivalence entre être un langage RE et avoir un énumérateur, et d'autre part être un langage R et avoir un énumérateur dans l'ordre hiérarchique.

Référence :
- J.-M. AUTEBERT *Calculabilité et décidabilité*, Broché (1992)

1.1.26 Équivalence langage algébrique/reconnu par automate à pile [910][911]

Résultat On montre l'équivalence entre être un langage engendré par une grammaire algébrique et être reconnu par un automate à pile. (On admet que tout mot généré par une grammaire hors-contexte peut être généré par une dérivation à gauche).

Références :
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert
- P.WOLPER *Introduction à la calculabilité*, Broché

1.1.27 Exemple d'un programme Prolog [917][918][924]

Résultat On donne l'exemple canonique du *Stern* d'un programme Prolog. On peut bien sur en choisir un autre.

Référence :
- J.STERN *Fondements mathématiques de l'informatique*

1.1.28 Exemple de langages déterministes [910]

Résultat On exhibe quelques langages algébriques déterministes, en considérant le langage $\mathcal{P}_r(L) := \{u\#v | u \in L \text{ et } uv \in L\}$ avec $\# \notin L$. On démontre et utilise alors la propriété suivante :

L est algébrique déterministe implique $\mathcal{P}_r(L)$ aussi.

Référence :
- R.FLOYD, C.BEIGEL *Le langage des machines* Broché (1995) p.349

1.1.29 Fonction primitive récursive $\Leftrightarrow$ fonction calculable [912][913][915]

Résultat Faire les deux sens étant bien trop long en 15mn, on se contente de montrer le sens primitive récursive $\Rightarrow$ calculable en admettant l'existence des bijections primitives récursives β_1^3 et β_3^1 (résultat à mettre dans le plan !). On construit par morceaux successifs une fonction récursive qui simule l'exécution d'une machine de Turing.

Référence :
- R.CORI, D.LASCAR *Logique mathématique, tome 2 : Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles*, Broché
- P.WOLPER *Introduction à la calculabilité*, Broché
- J.STERN *Fondements mathématiques de l'informatique*

1.1.30 Hachage parfait [901][921]

Résultat On montre que dans le cas où les clefs sont statiques (gravure CD-ROM, mot-clef langage de programmation) on peut construire en temps raisonnable un hachage avec accès en temps au pire $O(1)$ et un espace linéaire. L'idée consiste à hacher deux fois pour éviter les collisions, et d'utiliser l'inégalité de Markov pour s'assurer qu'on obtient une complexité temporelle acceptable "rapidement".

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.31 Indécidabilité de la terminaison d'un système de réécriture [913][914][920][922]

Résultat On montre l'indécidabilité de la terminaison d'un système de réécriture par réduction du problème de l'arrêt universel d'une machine de Turing. Pour cela on considère un système de réécriture dont les termes sont des configurations d'une machine de Turing.

Référence :
- F.BAADER, T.NIPKOW *Term Rewriting and All That* , Broché (1999)

1.1.32 Insertion dans un arbre rouge-noir [901][921][925][927]

Résultat On présente les ARN, un cas particulier d'ABR et la façon de les rééquilibrer lors d'une insertion.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.33 Insertion dans un AVL et rééquilibrage par rotation [901][921][925][927]

Résultat On présente les AVL, un cas particulier d'ABR et la façon de les rééquilibrer.

Référence :
- D.BEAUQUIER, J.BRESTEL, Ph. CHRÉTIENNE *Eléments d'algorithmique*

1.1.34 L est engendré par une grammaire $\Leftrightarrow$ L est énuméré par une Machine de Turing ($L \in RE$) [913][922]

Résultat On montre qu'un langage est engendré par une grammaire si et seulement s'il est énuméré par une Machine de Turing.

Référence :
- P.WOLPER *Introduction à la calculabilité*, Broché

1.1.35 La fonction d'Ackermann n'est pas primitive récursive [912][913][922]

Résultat On montre que la fonction d'Ackermann définie par

$$\begin{cases} \forall m, & f(0,m) = 2^m \\ \forall n, & f(n,0) = 1 \\ \forall n,m, & f(n+1,m+1) = f(n, f(n+1,m)) \end{cases}$$

n'est pas primitive récursive. Il y a beaucoup de choses intéressantes à dire sur cette fonction, à vous de choisir ce que vous voulez en dire exactement dans le temps imparti.

Référence :
- P.WOLPER *Introduction à la calculabilité*, Broché
- P.DEHORNOY *Mathématiques de l'informatique*, Broché

1.1.36 La fonction du Castor Affairé n'est pas calculable par une machine de Turing [913]

Résultat On montre qu'il existe des fonctions non calculables par machine de Turing, en donnant l'exemple de la fonction du *castor affairé* définie par :

$$\Phi : M \mapsto \begin{cases} \text{nombre de 1 sur le ruban de la configuration terminale} & \text{si } M \text{ termine} \\ 0 & \text{sinon} \end{cases}$$

$$C_{aff} : n \mapsto sup_{M \in \mathcal{M}_n} \Phi(M).$$

où pour $n \in \mathbb{N}$, on appelle $\mathcal{M}_n$ l'ensemble des machines de Turing à n états, d'alphabet de ruban $\{\#, 1\}$ et qu'on suppose d'entrée vide.

On a en corollaire que le problème de l'arrêt d'une machine de Turing à partir de l'entrée vide est indécidable.

Référence :
- P.DEHORNOY *Mathématiques de l'informatique*, Broché

1.1.37 Le complémentaire d'un langage déterministe est déterministe [910][911]

Résultat On montre que le complémentaire d'un langage déterministe est déterministe en modifiant préalablement un automate à pile $\mathcal{A}$ le reconnaissant, pour contourner le blocage si $\mathcal{A}$ n'est pas complet ou la pile vidée, ainsi que les ε-transitions.

Référence :
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert

1.1.38 Le langage de pile est rationnel [908][909][911]

Résultat On montre que le langage de pile d'un automate à pile est rationnel, en considérant le langage miroir et les langages de Dyck vus comme monoïdes polycycliques.

Référence :
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert

1.1.39 Le langage des décideurs n'est ni dans RE, ni dans co-RE [913][914][915][922]

Résultat On montre que le langage des décideurs,

$$\mathcal{D}_{MT} = \{< M > | M \text{ est un décideur, ie M s'arrête sur toute entrée}\}$$

n'est ni dans co-RE par réduction du problème de l'arrêt, ni dans RE par un argument diagonal.

Référence :
- ? ?

1.1.40 Le problème du 3-Couplage est NP-complet [904]

Résultat On montre que le problème du 3-couplage (ou 3D-MATCHING), généralisation du problème du mariage, est NP-complet par réduction de 3-SAT.

Références :
- J.-F. REY *Calculabilité, complexité et approximation*
- PAPADIMITRIOU *Algorithms*

1.1.41 Lemme de déduction [917][918]

cf 2009/2010

1.1.42 Lemme de Newman [920]

Résultat On montre par induction le lemme de Newman qui dit qu'un système de réécriture terminant et localement confluent est confluent.

Référence :
- F.BAADER, T.NIPKOW *Term Rewriting and All That* , Broché (1999)

1.1.43 Lemme des paires critiques [919][920]

Résultat On montre par disjonction des cas le lemme des paires critiques qui dit qu'un système est localement confluent si et seulement toutes ses paires critiques sont joignables.

Référence :
- F.BAADER, T.NIPKOW *Term Rewriting and All That* , Broché (1999)

1.1.44 Lemme d'Odgen [910]

Résultat On montre le lemme d'Odgen, analogue du lemme de l'étoile pour les langages algébriques.

Référence :
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert

1.1.45 Les langages reconnaissables à croissance bornée sont les langages minces [] ! ? !

Résultat

Référence :
- J. SAKAROVITCH *Eléments de théorie des automates* , (2003)

1.1.46 LK (LJ) ⇒ NK (NJ) [918]

Résultat On montre que pour la logique intuitionniste si $\Gamma \vdash_{LJ} A$, alors $\Gamma \vdash_{NJ} A$, et de même pour la logique classique.

Référence :
- K.NOUR, R.DAVID, C.RAFFALLI *Introduction à la logique : Théorie de la démonstration - Cours et exercices corrigés*, Dunod

1.1.47 Méthode Ziv-Lempel 77 de compression [901][907]

Résultat On donne un algorithme de compression, et on discute de son taux de compression selon les différents paramètres.

Référence :
- INARTI *Compression d'image*
- J.-G.DUMAS, S.VARRETTE, É.TANNIER, J.-L.ROCH *Théorie des codes : Compression, cryptage, correction*

1.1.48 Minorant pour le problème du commérage [925][926]

Résultat Le problème du commérage modélise la diffusion d'informations au sein d'un graphe. Par la méthode du potentiel, on montre que le problème se résout en au moins $\log_p N$ étapes, où N est le nombre de sommets du graphe, et $p = \frac{1\sqrt{5}}{2}$.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*
- KRUMME CYBENKO VENKATORAMAN *Gossiping in Minimal Time*

1.1.49 NL = co-NL [915][925]

Résultat On montre que $NL = co - NL$ en considérant le problème NL canonique ST-Connectivity qui consiste en savoir si un sommet d'un graphe est accessible à partir d'un autre donné.

Référence :
- M.SIPSER *Introduction to the Theory of Computation*, Relié

1.1.50 Plus longue sous-séquence commune [906][907][921]

Résultat On expose un algorithme de programmation dynamique qui calcule la plus longue sous-séquence commune de deux mots donnés, et donne le passage de l'un à l'autre.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.51 Preuve de la division euclidienne via la logique de HOARE [927]

Résultat On met en oeuvre la logique de Hoare sur l'exemple de l'algorithme de la division euclidienne. Attention à la terminaison par le variant de boucle qui n'est pas bien référencée.

Référence :
- K. R. APT, E.-R. OLDEROG *Verification of Sequential and Concurrent Programs*
- L. ALBERT, P.GASTIN, B.PETAZZONI *Cours et exercices d'informatique : classes préparatoires, 1er et 2nd cycles universitaires*
- G.WINSKEL *The Formal Semantics of Programming Languages*

1.1.52 Preuve de la factorielle via la logique de HOARE [927]

Résultat On met en oeuvre la logique de Hoare sur l'exemple de l'algorithme de la factorielle.

Référence :
- K.R.APT, E.-R.OLDEROG *Verification of Sequential and Concurrent Programs*
- J.-M. AUTEBERT *Calculabilité et décidabilité*, Broché (1992)

1.1.53 Problème de séparation par automate (PSA) [904][908][909][915]

Résultat On montre que le problème de savoir si pour deux langages K et L fixés, il existe un automate à k états acceptant les mots de K et rejetant ceux de L est NPC. Pour cela on procède par réduction de 3-SAT, en forçant pour ϕ une FNC par la construction de K et L l'automate à donner un valuation qui satisfait ϕ.

Référence :
- R.FLOYD, C.BEIGEL *Le langage des machines* Broché (1995)

1.1.54 Problème du voyageur de commerce euclidien approché [904][915][925]

Résultat On donne dans le cas euclidien un algorithme polynomial qui donne une approximation 2 du Problème du voyageur de commerce (PVC ou TSP), en utilisant un arbre couvrant minimal. On peut montrer également que dans le cas général il n'existe pas d'approximation, en considérant la réduction du problème du chemin hamiltonien au PVC. Attention de bien mentionner que le cas euclidien reste NPC.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*
- PAPADIMITRIOU *Algorithms*

1.1.55 Problèmes indécidables de la théorie des langages algébriques [910][914][922]

Résultat On utilise l'indécidabilité du problème de correspondance de POST pour montrer que pour des grammaires algébriques, le problème de l'équivalence des langages, de l'intersection vide, du langage universel et de l'ambiguïté sont indécidables.

Référence :
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert

1.1.56 Rationalité des facteurs itérants d'un langage régulier [909]

Résultat On montre que l'ensemble des facteurs itérants d'un langage régulier , ie $\{v|\exists u, w, uv^*w \subset L\}$, est lui-même un langage rationnel. Pour cela, on montre d'abord que tout automate déterministe complet est équivalent à un automate déterministe complet régulier à gauche.

Référence :
- J. SAKAROVITCH *Eléments de théorie des automates* , (2003)

1.1.57 Recherche avec k différences [906][907][921]

Résultat On expose un algorithme de programmation dynamique qui recherche un motif dans un texte en autorisant k différences, et donnant les opérations pour passer du motif cherché au motif trouvé.

Référence :
- M. CROCHEMORE *L'algorithmique du texte*, Broché (2001)

1.1.58 Recherche des deux points les plus proches [902]

Résultat On expose un algorithme utilisant le paradigme diviser pour régner qui retourne les deux points les plus proches d'un ensemble fini de point de l'espace en temps $0(n \log n)$ au lieu du $O(n^2)$ de l'algorithme naïf.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.59 Savoir si le complémentaire d'un langage algébrique est algébrique est indécidable [910][914]

Résultat On montre que le problème de savoir si le complémentaire d'un langage algébrique est algébrique est indécidable, par réduction au problème de l'arrêt d'une machine de Turing.

Référence :
- J.-F. REY *Calculabilité, complexité et approximation*

1.1.60 Théorème de Cook-Levin [904][913][915][916]

Résultat On démontre le théorème de Cook qui dit que 3-SAT est NP-Complet. On procède à une réduction de tout problème NP, en utilisation la caractérisation que leur langage est reconnu par une machine de Turing non déterministe polynomiale. Pour cela on considère un tableau des configurations d'une telle machine de Turing non déterministe polynomiale reconnaissant un problème NP, et on construit une FNC en conséquence.

Référence :
- P.WOLPER *Introduction à la calculabilité*, Dunod
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert

1.1.61 Théorème de Highman et Sous-mot $(L) \in$ Rat(Σ) [909]

Résultat On démontre le théorème de Highman qui affirme que sur un alphabet fini, les antichaînes -ie les suites de mots dont aucun n'est sous-mot d'un autre- sont finies (par leur nombre). On obtient en corollaire que pour L un langage sur Σ quelconque, alors SOUS-MOT$(L) \in Rat(\Sigma)$.

Référence :
- B.PETAZZONI *Seize problèmes d'informatique : Avec corrigés détaillés et programmes en Caml*, Broché

1.1.62 Théorème de Kleene [908][909]

Résultat On démontre le théorème de Kleene selon lequel les langages rationnels sont exactement les langages reconnus par automate fini. On utilisera dans le premier sens l'automate des termes dérivés d'Antimirov, et dans l'autre l'algorithme de Brzozowski-McCluskey (BMC) passant par les automates généralisés.

Référence :
- J. SAKAROVITCH *Eléments de théorie des automates* , (2003)

1.1.63 Théorème de lecture unique [911][917]

Résultat On montre que la définition inductive des formules du premier ordre est non-ambiguë. Cela a pour conséquence l'écriture arborescente d'un terme.

Référence :
- R.CORI,D.LASCARLogique mathématique 1 - Calcul propositionnel ; algèbre de Boole ; calcul des prédicats, Broché (2003)

1.1.64 Théorème de Löwenheim-Skolem [917][924]

Résultat On montre le théorème de Löwenheim-Skolem (descendant) qui affirme que pour un langage L du premier ordre dénombrable, une théorie consistante T admet un modèle au plus dénombrable. On construit un tel modèle à partir d'un modèle de T. On peut même montrer que toute théorie consistante dans un langage du premier ordre non fini donné admet un modèle de même cardinal que ce langage.

Référence :
- K.NOUR, R.DAVID, C.RAFFALLI *Introduction à la logique : Théorie de la démonstration - Cours et exercices corrigés*, Broché p.95, p.300 exo 2.33
- R.CORI, D.LASCAR *Logique mathématique, tome 2 : Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles*, Broché p.196

1.1.65 Théorème de Rice [913][914][922]

Résultat On montre le théorème de Rice, affirmant que toute propriété non triviale d'un langage (c'est-à-dire qui n'est pas toujours vraie ou toujours fausse) est indécidable, par réduction du problème *LU* du langage universel qu'on montre indécidable par un argument diagonal.

Référence :
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert

1.1.66 Théorème de Savitch [913][915]

Résultat On montre que toute fonction calculable par machine de Turing non déterministe en espace $s(n) \geq \log(n)$ est calculable par une machine de Turing déterministe en espace $s^2(n)$. Un corollaire important est que $PSPACE = NPSPACE$.

Référence :
- O.CARTON *Langages formels, calculabilité et complexité* , Vuibert

1.1.67 Théorie des ordres denses [914][922][924]

Résultat On expose la théorie des ordres denses, et on démontre que ses modèles sont infinis, qu'elle est cohérente, décidable et même complète.

Référence :
- K.NOUR, R.DAVID, C.RAFFALLI *Introduction à la logique : Théorie de la démonstration - Cours et exercices corrigés*, Broché

1.1.68 Transformée de Fourier discrète [112][902]

Résultat On montre que l'on peut multiplier deux polynômes en $O(n \log n)$ grâce à un algorithme de type "Diviser Pour Régner".

Références :
- P. SAUX-PICART, E. RANNOU *Cours de calcul formel pour les filles*, Ellipses ()
- PAPADIMITRIOU *Algorithms*
- J.-G.DUMAS, S.VARRETTE, É.TANNIER, J.-L.ROCH *Théorie des codes : Compression, cryptage, correction*

1.1.69 Tri des réseaux, tri bitonique [903]

Résultat Le tri des réseaux est un tri par comparaison triant des éléments en un temps sous-linéaire. Pour passer sous le minorant des tris par comparaison, on effectue plusieurs comparaisons en parallèle. C'est un développement d'électronique.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.70 Tri par bacs [903]

Résultat On expose le tri par bac (aussi appelé par paquets), qui comme son nom l'indique trie les objets à trier dans des bacs (par exemple un bac peut correspondre au chiffre des unités, on obtient le tri par base). On obtient une complexité moyenne en temps de $O(n)$, mais on a supposé les éléments uniformément répartis.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.71 Tri par tas [901][903][927]

Résultat On expose l'algorithme du tri par tas, qui comme son nom l'indique tri en utilisant la structure de TAS_{max}. Ce tri sur place s'exécute en temps $O(n \log n)$.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

1.1.72 Tri des suffixes [902][903][907]

Résultat On donne un algorithme de tri des suffixes d'un texte de taille n en temps $n \log n$, au lieu de n^2 dans le cas général, utilisant un lemme de dédoublement pour faire du diviser pour régner. Attention à bien connaître le tri par bac que l'on utilise pour sa stabilité.

Référence :
- M. CROCHEMORE *L'algorithmique du texte*, Broché (2001)

1.1.73 Tri topologique [903][925]

Résultat On trie les sommets d'un graphe orienté tel que pour chaque sommet les arêtes sortantes vont vers des sommets supérieurs à lui. Pour cela on utilise les propriétés du parcours en profondeur d'un graphe. Ce tri est utile à l'ordonnancement des tâches.

Référence :
- T. H. CORMEN, C. E. LEISERSON, R. L. RIVEST, C. STEIN *Introduction à l'algorithmique, 2ème édition*

Leçon	dév'
901 Structures de données : exemples et applications.	Hachage Parfait, Dijkstra
902 Diviser pour régner : exemples et applications.	Additionneur n-bit, Comparaison tri rapide/fusion
903 Exemples d'algorithmes de tri. Complexité.	Comparaison rapide/fusion, Tri suffixe,
904 Problèmes NP-complets : exemples.	Théorème de Cook, PSA, PVC euclidien approché
906 Programmation dynamique : exemples et applications.	Recherche avec k-différences, CYK, Floyd-Warschall
907 Algorithmique du texte : exemples et applications.	Recherche avec k différences, Automate des occurrences, Tri suffixe
908 Automates finis. Exemples et applications.	Kleene, Automate des occurrences, Décidabilité de Presburger
909 Langages rationnels. Exemples et applications.	Kleene, PSA
910 Langages algébriques. Exemples et applications.	Exemple de langage déterministes, CYK
911 Automates à pile. Exemples et applications.	Complémentaire d'un dét est dét équivalence pile/alg
912 Fonctions récursives primitives et non primitives. Exemples.	fonction rec => fonction calc Caractérisation des ensembles RE
913 Machines de Turing. Applications.	Théorème de Cook, Indécidabilité de la terminaison d'un système de rééc,
914 Décidabilité et indécidabilité. Exemples.	Décidabilité de Presburger, Indécidabilité de la terminaison d'un système de rééc, Théorème de Rice
915 Classes de complexité : exemples.	Savitch, Cook, PVC eucl approx
916 Formules du calcul propositionnel : représentation, formes normales, satisfiabilité. Applications.	Cook Additionneur n-bit
917 Logique du premier ordre : syntaxe et sémantique.	Lowenheim-Skolem Complétude de la méthode de résolution
918 Systèmes formels de preuve en logique du premier ordre : exemples.	Complétude de la méthode de résolution LK => LJ
919 Unification : algorithmes et applications.	Démo de l'algo d'unification, Complétude de la méthode de résolution
920 Réécriture et formes normales. Exemples.	Lemme des paires critiques, Indécidabilité de la terminaison
921 Algorithmes de recherche et structures de données associées.	Automate des occurences, Hachage parfait
922 Ensembles récursifs, récursivement énumérables. Exemples.	Théorème de Rice Caractérisation des ensembles RE
923 Analyses lexicale et syntaxique : applications.	construction sur un ex d'un analyseur lexical ou syntaxique
924 Théories et modèles en logique du premier ordre. Exemples.	Décidabilité de Presburger, Lowenheim-Skolem
925 Graphes : représentations et algorithmes.	Dijkstra, PVC eucl approx, Floyd-Warshall
926 Analyse des algorithmes : complexité. Exemples.	Dijkstra, Compraraison rapide/fusion
927 Exemples de preuve d'algorithme : correction, terminaison.	Dijkstra, Unification, Division euclidienne via Hoare

Chapitre 2

Mathématiques

2.1 Référence des développements d'algèbre

2.1.1 Action de A_n sur $k[X_1, \ldots, X_n]$ [104][105]

Résultat On démontre, en utilisant l'action du groupe A_n sur $k[X_1, \ldots, X_n]$ donnée par : pour $\sigma \in A_n$, $(\sigma.P)(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$, que l'assertion : $\forall \sigma \in A_n, \sigma.P = P$ est équivalente à :

$$\exists!(Q, R) \text{ symétriques } P(X_1, \ldots, X_n) = Q(X_1, \ldots, X_n) + \Delta(X_1, \ldots, X_n)R(X_1, \ldots, X_n)$$

où $\Delta(X_1, \ldots, X_n)$ est le déterminant de Vandermonde de $(X_1, \ldots, X_n)$.

Référence :
- R. GOBLOT, *Algèbre commutative*, Dunod (2001)

2.1.2 Action de $PSL_2(\mathbb{Z})$ sur le demi-plan de Poincaré [108][139][141]

Résultat On démontre que $PSL_2(\mathbb{Z})$ est engendré par la translation et la symétrie en étudiant son action sur le demi-plan complexe supérieur $\mathbb{P}$ appelé demi-plan de Poincaré. On peut également, à condition de le définir correctement, trouver un domaine fondamental pour cette action et classifier les réseaux de $\mathbb{C}$ à isomorphisme près.

Références :
- M. ALESSANDRI, *Thèmes de géométrie, groupes en situation géométrique*, Dunod (1999)
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2001)

2.1.3 Algorithme des facteurs invariants [119][140]

Résultat On démontre, de manière algorithmique, que toute matrice à coefficients dans un anneau principal est équivalente à une matrice diagonale dont les coefficients diagonaux sont appelés facteurs invariants. La suite des facteurs invariants est unique lorsqu'on exige la condition de divisibilité. On peut ne traiter que l'existence et se placer uniquement dans le cas d'un anneau euclidien.

Références :
- V. BECK, J. MALICK, G.PEYRÉ, *Objectif agrégation* (2ème édition), H&K (2005)
- R. GOBLOT, *Algèbre commutative*, Dunod (2001)

2.1.4 Alternative de Steiner [139][141]

Résultat On démontre que si on considère deux cercles $\mathcal{C}$ et $\mathcal{C}'$ dont l'un est intérieur à l'autre et une suite de cercles $(\mathcal{C}_k)$ tels que $\mathcal{C}_{k+1}$ soit tangent aux cercles $\mathcal{C}$ et $\mathcal{C}'$ et tangent extérieurement à $\mathcal{C}_k$ alors on a une seule des deux possibilités :
- il existe un entier n tel que $\mathcal{C}_n = \mathcal{C}_1$, et ce quel que soit le cercle initial $\mathcal{C}_1$ (toute suite de cercles se referme),
- aucun cercle $\mathcal{C}_k$, $k > 1$ ne coïncide avec le cercle $\mathcal{C}_1$ et ce quel que soit le cercle initial $\mathcal{C}_1$ (aucune suite de cerles ne se referme).

On utilise pour cela une homographie envoyant deux cerles quelconques sur deux cercles concentriques.

Référence :
- J.-D. EIDEN *Géométrie analytique et classique*, Calvage et Mounet (2009)

2.1.5 Automorphismes du disque unité [139]

Résultat On montre que les bijections biholomorphes du disque unité ouvert dans lui-même sont toutes de la forme, pour a un point du disque et λ un complexe de module 1 :

$$z \mapsto \lambda \frac{z-a}{1-\bar{a}z}$$

en utilisant notamment le lemme de Schwarz.

Référence :
- W. RUDIN *Analyse réelle et complexe*, Sciences Sup (1998)

2.1.6 Calcul de plusieurs déterminants classiques [123]

Résultat On calcule le plus de déterminants classiques possible en 15mn. On pourra traiter par exemple le Vandermonde, le circulant, Hürwitz ou Smith.

Références :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 2*, Cassini
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)

2.1.7 Coloriages des polyèdres réguliers [106][133][145]

Résultat On dénombre les différents modèles de dodécaèdres à six faces blanches et six faces noires que l'on peut former. On peut également considérer plus de couleurs ou même p couleurs.

Référence :
- M. ARTIN *Algebra*, Prentice Hall (1991)

2.1.8 Commutant d'un endomorphisme [120][124][133]

Résultat On peut démontrer que la dimension du commutant pour un endomorphisme diagonalisable est la somme des carrés des ordres de multiplicité des valeurs propres et que la dimension du commutant d'un endomorphisme quelconque est supérieure ou égale à la dimension de l'espace. On peut également démontrer que lorsque $\chi_u = \pi_u$,

$$\Gamma(u) = \{P(u), P \in k[X]\}.$$

Références :
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 2*, Cassini (2005)

2.1.9 Comptage de racines et formes quadratiques [131]

Résultat On ramène le comptage du nombre de racines réelles ou complexes distinctes d'un polynôme à l'étude de la signature d'une forme quadratique.

Référence :
- F. GANTMACHER *Théorie des matrices*, Dunod ()

2.1.10 Convergence d'une suite de polygones [123][137][139][226]

Résultat On montre que pour $(x_1, \ldots, x_n)$ un n-uplet de complexes, en définissant une suite polygones $\mathcal{P}_n$ (non nécessairement convexe, on prend les points dans l'ordre) où $\mathcal{P}_{n+1}$ est le polygone formé par les milieux des côtés de $\mathcal{P}_n$, cette suite converge vers le n-uplet $(g, \ldots, g)$ où g est l'isobarycentre de $(x_1, \ldots, x_n)$.

Référence :
Pas de livre ! Voir la page suivante : http://favetto.free.fr/agreg.pdf
Le calcul du déterminant circulant est présent dans Gourdon ou Oraux X-ENS.

2.1.11 Critère de parité de Gale [123][132]

Résultat On montre que pour le polytope cyclique $C_d(n)$ (dont les sommets sont n points de la courbe des moments en dimension d), un ensemble S de d sommets forme une face si et seulement s'il vérifie le critère de parité de Gale, obtenu grâce à un déterminant de Vandermonde :

$$\forall i, j \notin S, 2|\#\{k/k \in S, i < k < j\}$$

On peut étendre la méthode et montrer que tout ensemble de sommets de cardinal $|S| \leq \frac{d}{2}$ est une face de $C_d(n)$. Attention à bien connaître les notions de base sur les polytopes.

Référence :
- G.M. ZIEGLER *Lectures on Polytopes*, Grad. Texts in Math. , vol. 152, Springer (1995).

2.1.12 Décomposition de Bruhat [105][106][119][128][140]

Résultat On montre que toute matrice inversible est équivalente à une matrice de permutation et on applique ce résultat à l'action sur les drapeaux et les couples de drapeaux.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2001)

2.1.13 Décomposition de Dunford [124][128]

Résultat On démontre que tout endomorphisme u est la somme d'un endomorphsime diagonalisable d et d'un endomorphisme nilpotent n commutant entre eux et que cette décomposition est unique. On peut également démontrer que d et n sont des polynômes en u ou que l'on peut remplacer diagonalisable par semi-simple.

Références :
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)
- V. BECK, J. MALICK, G.PEYRÉ, *Objectif agrégation (2ème édition)*, H&K (2005)

2.1.14 Décomposition de Dunford effective via Newton [116][124][128]

Résultat On démontre de façon effective la décomposition de Dunford en appliquant la méthode de Newton dans l'anneau $k[X]/(\pi)$ où π est le produit des facteurs irréductibles de χ_u (le polynôme caractéristique de u) pour un endomorphisme u donné.

Référence :
- J.-J. RISLER *Groupes pour la licence 3*, Dunod (2006)

2.1.15 Décomposition polaire [106][124][133]

Résultat On démontre que toute matrice inversible peut s'écrire comme le produit d'une matrice unitaire et d'une matrice hermitienne définie positive. On peut également démontrer l'homéomorphisme réalisé par cette décomposition entre $\mathcal{GL}_n(\mathbb{C})$ et $\mathcal{H}_n^{++} \times \mathcal{U}_n$, le corollaire de maximalité de $\mathcal{U}_n$ dans $\mathcal{GL}_n(\mathbb{C})$ ou que tout sous-groupe G de $\mathcal{GL}_n(\mathbb{C})$ stable par adjoint est homéomorphe à $(G \cap \mathcal{H}_n^{++}) \times (G \cap \mathcal{U}_n)$.

Références :
- R. MNEINMNÉ, F. TESTARD *Introduction aux groupes de Lie classiques*, Hermann (1994)
- D. SERRE *Les matrices*, Dunod ()

2.1.16 Dénombrement des polynômes irréductibles sur un corps fini [112][116][145]

Résultat On démontre à l'aide de la formule d'inversion et la fonction de Möbius μ que le nombre $I_{n,q}$ de polynômes irréductibles unitaires de degré n sur un corps fini à q éléments vérifie :

$$I_{n,q} = \sum_{d|n} \mu(\frac{n}{d})q^d$$

Référence :
- M. MIGNOTTE *Algèbre concrète*, Ellipses (2002)

2.1.17 Ellipse de Steiner [139]

Résultat On démontre, à l'aide des théorèmes de Poncelet, que tout triangle de sommet d'affixes z_1, z_2, z_3 possède une ellipse tangente en les milieux de ses cotés et que ses foyers ont pour affixes les racines du polynôme dérivé de $P(X) = (X - z_1)(X - z_2)(X - z_3)$. Ce développement est peu référencé et la seule référence est un peu plus générale.

Référence :
- M. MARDEN *Geometry of polynomials*, American Mathematical Society (1970)

2.1.18 Ellipsoïde de John-Löwner [123][137][203][219][229]

Résultat On démontre que tout compact K de $\mathbb{R}^n$ peut être entouré par un unique ellipsoïde de volume minimal centré en zéro.

Références :
- M. ALESSANDRI, *Thèmes de géométrie, groupes en situation géométrique*, Dunod (1999)
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 3*, Cassini (2008)

2.1.19 Endomorphismes cycliques, invariants de similitude et réduction de Frobenius [124][132]

Résultat On démontre la décomposition de Frobenius : toute matrice est semblable à une matrice par blocs de matrices-compagnons, mais en utilisant une méthode plus algébrique que matricielle, en détaillant le cas des endomorphismes cycliques (qui donnent les matrices-compagnons) et en utilisant de la dualité.

Référence :
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)

2.1.20 Endomorphismes de $\mathcal{M}_n(\mathbb{C})$ préservant $\mathcal{GL}_n(\mathbb{C})$ [119][120][128]

Résultat On trouve la forme des endomorphismes de $\mathcal{M}_n(\mathbb{C})$ préservant $\mathcal{GL}_n(\mathbb{C})$.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2001)

2.1.21 Endomorphismes normaux [124][133]

Résultat On démontre que les matrices normales (qui commutent avec leur symétrique hermitienne) sont semblables, via une matrice de passage unitaire, à des matrices par blocs réels de taille 1 et 2 où les blocs de taille 2 sont la somme d'une homothétie et d'une matrice anti-symétrique.

Référence :
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)

2.1.22 Endomorphismes semi-simples [116][124]

Résultat On démontre qu'un endomorphisme u est semi-simple (i.e. tel que tout sous-espace stable par u possède un supplémentaire stable par u) si et seulement si son polynôme minimal π_u est un produit de facteurs irréductibles. On peut se limiter ou non à faire la démonstration dans $\mathbb{C}$.

Références :
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)
- V.BECK,J.MALICK,G.PEYRÉ,*Objectif agrégation (2ème édition)*, H&K(2005)

2.1.23 Enveloppe convexe du groupe orthogonal [106][132][133][137]

Résultat On démontre que l'enveloppe convexe de $\mathcal{O}_n(\mathbb{R})$ dans $\mathcal{M}_n(\mathbb{R})$ est la boule unité pour le produit scalaire et la norme associée canoniques en utilisant la décomposition polaire et la caractérisation des projections par le signe du produit scalaire. On peut également montrer que $\mathcal{O}_n(\mathbb{R})$ est l'ensemble des points extrémaux de la boule unité.

Références :
- TAUVEL, *Géométrie*
- M. ALESSANDRI, *Thèmes de géométrie, groupes en situation géométrique*, Dunod (1999)
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2001)

2.1.24 Équation de Fermat pour $n = 2$ et 4 [109][110]

Résultat On résout sur $\mathbb{N}^3$, l'équation $x^2 + y^2 = z^2$ et on montre qu'il n'existe pas de solution non nulle pour l'équation $x^4 + y^4 = z^4$ qui sont deux cas particuliers du grand théorème de Fermat.

Références :
- J. COMBES *Algèbre et géométrie*, Bréal (1998)
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)

2.1.25 Équations diophantiennes et séries génératrices [145][224][243]

Résultat On montre que, pour $(\alpha_1, \dots \alpha_p)$, p entiers premiers entre eux dans leur ensemble, le nombre S_n de solutions $(n_1, \dots, n_p)$ de l'équation diophantienne $\alpha_1 n_1 + \dots + \alpha_p n_p = n$ vérifie :

$$S_n \sim \frac{1}{\alpha_1 \dots \alpha_p} \frac{n^{p-1}}{(p-1)!}$$

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 2*, Cassini (2005)

2.1.26 Générateurs de $\mathcal{GL}_n(\mathbb{C})$ et $\mathcal{SL}_n(\mathbb{C})$ [106][108][133]

Résultat On montre que $\mathcal{SL}_n(\mathbb{C})$ est engendré par les transvections puis que $\mathcal{GL}_n(\mathbb{C})$ est engendré par les transvections et les dilatations (on peut aussi être plus précis et distinguer le cas réel) en faisant des opérations élémentaires. On fait ensuite une application pour étudier la connexité par arcs de ces groupes dans le cas réel puis le cas complexe.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 2*, Cassini (2005)

2.1.27 Générateurs du groupe affine [108][141]

Résultat On montre que le groupe affine $GA(\mathcal{E})$ d'un espace affine est généré par les dilatations affines.

Référence :
- Y. LADEGAILLERIE *Géométrie affine, projective, euclidienne et analagmatique*, Dunod ()

2.1.28 Groupe simple d'ordre 60 [104][105]

Résultat : On montre qu'à isomorphisme près $\mathcal{A}_5$ est le seul groupe simple de cardinal 60 (on utilise les théorèmes de Sylow).

Références :
- D. PERRIN, *Cours d'algèbre*, Ellipses (1998)
- J. COMBES *Algèbre et géométrie*, Bréal (1998)

2.1.29 Groupes de pavage [108][141]

Résultat On montre qu'à conjugaison par une application affine près, il n'existe que 5 groupes de pavage du plan (attention à bien définir un groupe de pavage).

Référence :
- GOBLOT, *Géométrie*

2.1.30 Groupes d'ordre 8 [104][145]

Résultat : On montre, en utilisant le produit semi-direct, qu'à isomorphisme près, les groupes d'ordre 8 sont : $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, D_4 (le groupe diédral des isométries du plan laissant invariant un carré) ou $\mathbb{H}_8$ le groupe des quaternions (qui peut être vu comme un groupe de matrices 2×2).

Références :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2001)

2.1.31 Groupes d'ordre 12 [104][145]

Résultat On montre, en utilisant les théorèmes de Sylow et le produit semi-direct, que les groupes d'ordre 12 sont isomorphes à : $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (abéliens), $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, $V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$ (non abéliens) où V_4 est le groupe de Klein (plus petit groupe non cyclique).

Références :
- S. FRANCINOU, H. GIANELLA, *Exercices de mathématiques pour l'agrégation*, Masson (1994)

2.1.32 Groupes d'ordre pq [104][109][110]

Résultat On démontre qu'un groupe d'ordre pq avec p et q premiers entre eux est isomorphe à :
- $\mathbb{Z}/pq\mathbb{Z}$ si $q \neq 1[p]$,
- $\mathbb{Z}/pq\mathbb{Z}$ si $q = 1[p]$ et G est abélien,
- $\mathbb{Z}/q\mathbb{Z} \rtimes_\theta \mathbb{Z}/p\mathbb{Z}$ si $q \neq 1[p]$ et G n'est pas abélien (avec $\theta(\bar{1})$ d'ordre p).

Référence :
- J. COMBES *Algèbre et géométrie*, Bréal (1998)

2.1.33 Irréductibilité des polynômes cyclotomiques [109][116]

Résultat On démontre que les polynômes cyclotomiques sont irréductibles sur $\mathbb{C}$, mais on peut également le faire pour des racines de l'unité plus générales.

Références :
- I. GOZARD *Théorie de Galois*, Ellipses (1997)
- D. PERRIN, *Cours d'algèbre*, Ellipses (1998)

2.1.34 Irréductibilité du déterminant [116][123]

Résultat On démontre que si k est un corps, le polynôme :

$$D = \sum_{\sigma \in \mathcal{S}_n} \prod_{i=1}^{n} X_{i,\sigma(i)}$$

est irréductible dans $k[X_{1,1}, \ldots, X_{i,j}, \ldots, X_{n,n}]$.

Référence :
- J. BRIANÇON, P. MAISONOBE *Éléments d'algèbre commutative*, Ellipses (2004)

2.1.35 Isométries du tétraèdre et du cube [104][105][133][141]

Résultat On démontre que le groupe des isométries du tétraèdre est isomorphe à $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ et le groupe des isométries du cube est isomorphe à $\mathcal{A}_4$. Il faut savoir identifier les transfomations associées aux éléments de ces groupes.

Références :
- Y. LADEGAILLERIE *Géométrie affine, projective, euclidienne et analagmatique*, Dunod ()
- M. ALESSANDRI, *Thèmes de géométrie, groupes en situation géométrique*, Dunod (1999)

2.1.36 Le groupe circulaire [139][141]

Résultat On démontre que le groupe engendré par les homographies complexes et la symétrie $z \mapsto \bar{z}$, appelé groupe circulaire, est également l'ensemble des applications bijectives de la sphère de Riemann $\hat{\mathbb{C}}$ dans elle-même qui préservent l'ensemble des cercles et des droites.

Références :
- M. AUDIN, *Géométrie*, EDP Sciences (2006)
- R. VIDONNE *Groupe ciculaire, rotations et quaternions*, Ellipses (2002)

2.1.37 Lemme de Morse [131][214][215][218][219]

Résultat On montre que si f une fonction réelle de classe $\mathcal{C}^3$ définie sur un ouvert U (contenant 0) de $\mathbb{R}^n$ dont la hessienne est inversible en 0 et est de signature (en tant que forme quadratique) $(p, n-p)$ alors il existe un changement de coordonnées $x \mapsto u(x)$ local de classe $\mathcal{C}^1$ tel que :

$$f(x) - f(0) = u_1^2(x) + \ldots + u_p^2(x) - u_{p+1}^2(x) - \ldots - u_n^2(x)$$

localement autour de 0 en utilisant notamment la formule de Taylor avec reste intégral. Il faut connaître l'application à la position par rapport à l'hyperplan tangent d'une hypersurface (ou au moins d'une surface).

Référence :
- F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)

2.1.38 Loi de réciprocité quadratique [109][110][112]

Résultat On montre que si p et q sont deux nombres premiers impairs, en utilisant le symbole de Legendre :

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

et que de plus -1 est un résidu quadratique modulo p si et seulement si le reste de la division de p par 4 est égal à 1 et 2 est un résidu quadratique modulo p si et seulement si le reste de la division de p par 8 est égal à 1 ou 7.

Référence :
- P. SAMUEL, *Théorie algébrique des nombres*, Hermann (1997)

2.1.39 Méthode de relaxation [140][224][226][232]

Résultat On montre que si la méthode de relaxation appliquée à A converge, alors $w \in]0;2[$, et qu'on a équivalence dans le cas où A est hermitienne définie positive.

Références :
- J.-P. DEMAILLY *Analyse numérique*, Broché (2006)
- M. SCHATZMAN *Analyse numérique : Une approche mathématique*, Broché (2004)

2.1.40 Méthode du gradient à pas optimal [140][219][226][229][232]

Résultat On montre que la méthode du gradient à pas optimal qui sert à minimiser une fonctionnelle sur $\mathbb{R}^n$ (qui consiste à se placer sur la plus grande pente) est convergente et on donne une majoration de l'erreur à l'aide de l'inégalité de Kantorovitch (qui est démontrée de façon plus simple dans *Oraux X-ENS Analyse 1*).

Références :
- J.-B. HIRIART-URRUTY *Optimisation et analyse convexe*, PUF (1998)
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 1*, Cassini (?)

2.1.41 Méthode du gradient conjugué [140][219][226][232]

Résultat On décrit la méthode du gradient conjugué, qui dans le cas d'une fonction

$$J : \mathbb{R}^n \to \mathbb{R}, x \mapsto \frac{1}{2} < Ax, x > - < b, x >$$

avec $A \in \mathcal{S}_n^{++}(\mathbb{R})$ et $b \in \mathbb{R}^n$, calcule l'unique minimum de J en n étape au plus.

Référence :
- P.G.CIARLET *Introduction à l'analyse numérique matricielle et à l'optimisation : Cours et exercices corrigés*, Broché 2006
- P.G.CIARLET *Introduction à l'analyse numérique matricielle et à l'optimisation : Cours et exercices corrigés*, Broché 2006

2.1.42 Partitions de $[\![1, n]\!]$ [145][230][243]

Résultat On étudie la série génératrice de terme général $\frac{D_n}{n!}$ où D_n est le nombre de partitions de $[\![1, n]\!]$ et on montre qu'elle vaut $e^{e^x - 1}$.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2001)

2.1.43 Primalité des nombres de Mersenne [109][110][112][116]

Résultat On étudie la primalité des nombres de Mersenne (i.e. de la forme $2^n - 1$) via le test de Lucas-Lehmer.

Référence :
- P. SAUX-PICART, E. RANNOU *Cours de calcul formel pour les filles*, Ellipses ()

2.1.44 Probabilité que deux nombres soient premiers entre eux [110][145][230]

Résultat On montre que la probabilité pour que deux nombres entiers choisis au hasard soient premiers entre eux est égale à $\frac{6}{\pi^2}$ (ce qui implique leur densité) en utilisant notamment la formule du crible, et la fonction de Möbius.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2008)

2.1.45 Réduction des endomorphismes autoadjoints [124][133]

Résultat On montre que tout endomorphisme autoadjoint admet une base orthonormale de vecteurs propres.

Référence :
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)

2.1.46 Résultant et élimination d'inconnues [123]

Résultat On montre comment éliminer une variable dans la recherche de zéros communs entre deux polynômes en n variables, c'est à dire de résoudre un système d'équations polynomiales, par la méthode du résultant.

Références :
- P. SAUX-PICART, E. RANNOU *Cours de calcul formel pour les filles*, Ellipses ()
- P. SAMUEL, *Théorie algébrique des nombres*, Hermann (1997)

2.1.47 Section planaire d'un cône [131]

Résultat On explique pourquoi on appelle coniques certaines figures du plan en montrant que ce sont les sections d'un cône par un plan.

Référence :
- Y. LADEGAILLERIE *Géométrie affine, projective, euclidienne et analagmatique*, Dunod ()

2.1.48 Série des inverses des nombres premiers [110][230]

Résultat On étudie la convergence de la série des inverses des nombres premiers.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2008)

2.1.49 Simplicité de $\mathcal{A}_n$ pour $n \geqslant 5$ [104][105][108]

Résultat On montre la simplicité du groupe alterné $\mathcal{A}_n$ pour $n \geqslant 5$ en montrant d'abord la simplicité de $\mathcal{A}_5$ via notamment la conjugaison des 3-cycles.

Référence :
- D. PERRIN, *Cours d'algèbre*, Ellipses (1998)

2.1.50 Simplicité de $PSL(E)$ pour $dim(E) \geqslant 3$ [104][132]

Résultat On montre la simplicité du groupe projectif linéaire lorsque la dimension de l'espace est supérieure ou égale à 3.

Référence :
- R. GOBLOT, *Algèbre commutative*, Dunod (2001)

2.1.51 Simplicité de $\mathcal{SO}(3)$ [106][133]

Résultat On montre que $\mathcal{SO}(3)$ est simple en justifiant l'appartenance de tous les retournements à un sous-groupe non trivial de $\mathcal{SO}(3)$ par des arguments de connexité (en fait on utilise des structures d'algèbre de Lie).

Références :
- S. GONNORD, N. TOSEL *Calcul différentiel* Ellipses (1998)
- D. PERRIN, *Cours d'algèbre*, Ellipses (1998)

2.1.52 Sous-espaces de $\mathcal{C}(\mathbb{R},\mathbb{C})$ de dimension finie stables par translation [120][124][221]

Résultat On montre que les sous-espaces vectoriels de $\mathcal{C}(\mathbb{R},\mathbb{C})$ de dimension finie n stables par translation quelconque sont exactement les espaces de solution des équations différentielles linéaires homogène d'ordre n à coefficients constants. Le résultat sur le déterminant d'une famille libre de fonctions est démontré dans Oraux X-ENS Analyse.

Références :
- E. LEICHTNAM, *Exercices d'oraux X-ENS : tome Analyse*, Ellipses (1999) p.92
- V.BECK,J.MALICK,G.PEYRÉ,*Objectif agrégation (2ème édition)*, H&K(2005)

2.1.53 Sous-groupes compacts de $\mathcal{GL}_n(\mathbb{R})$ [106][119][131][133][203][206][229]

Résultat On montre que tout sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ est conjugué à un sous-groupe du groupe orthogonal $\mathcal{O}_n(\mathbb{R})$, en utilisant un théorème de point fixe. On pourra remarquer que ce théorème est un corollaire de l'existence de l'ellipsoïde de John-Loewner (c.f. Francinou, Gianella, *Oraux X-ENS Algèbre 3*).

Référence :
- M. ALESSANDRI, *Thèmes de géométrie, groupes en situation géométrique*, Dunod (1999)

2.1.54 Sous-groupes finis de $\mathcal{SO}(3)$ [104][106][119][133][141][145]

Résultat On démontre que les sous-groupes finis de $\mathcal{SO}(3)$ sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$, un groupe diédral D_n, $\mathcal{S}_4$, $\mathcal{A}_4$ ou $\mathcal{A}_5$. Si l'on veut traiter ceci dans un temps raisonnable, on peut se limiter à la partie d'analyse combinatoire puis faire les groupes cycliques et diédraux en laissant de côté le dodécaèdre par exemple (attention à la définition de polyèdre régulier et connaître les liens entre les éléments de ces groupes et les transformations géométriques).

Références :
- Y. LADEGAILLERIE *Géométrie affine, projective, euclidienne et analagmatique*, Dunod ()
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2008)

2.1.55 Structure de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ [104][108][109]

Résultat On montre que pour $\alpha \geq 2$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$ pour un entier premier $p \geq 3$ et $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Référence :
- D. PERRIN, *Cours d'algèbre*, Ellipses (1998)

2.1.56 Surjectivité de l'exponentielle matricielle [124][214][215]

Résultat On montre grâce au théorème d'inversion locale que toute matrice inversible admet un antécédent polynomial par l'exponentielle.

Référence :
- I.NURDIN *Agrégation de mathématiques Epreuve orale : 68 thèmes pour se préparer efficacement*, Broché (2006)
- M.COSTE `http://agreg-maths.univ-rennes1.fr/documentation/docs/Exponentielle.pdf`

2.1.57 Théorème de Birkhoff [105][137][229]

Résultat On montre que l'enveloppe convexe des matrices de permutation est l'ensemble des matrices bistochastiques (attention le serpent ne fonctionne pas tout de suite, il faut réindexer d'abord).

Référence :
- D. SERRE *Les matrices*, Dunod ()

2.1.58 Théorème de Brauer [105][119][133]

Résultat On montre que deux matrices de permutations sont semblables si et seulement si leurs permutations associées sont conjuguées.

Référence :
- V.BECK, J.MALICK, G.PEYRÉ,*Objectif agrégation (2ème édition)*, H&K(2005)

2.1.59 Théorème de Burnside [104][106][124][128][132]

Résultat On montre qu'un sous-groupe de $\mathcal{GL}_n(\mathbb{C})$ est fini si et seulement s'il est d'exposant fini.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 2*, Cassini (2008)
- M. ALESSANDRI, *Thèmes de géométrie, groupes en situation géométrique*, Dunod (1999)

2.1.60 Théorème de Cartan-Dieudonné [108][120][131][132]

Résultat On démontre qu'une isométrie est la composée d'un nombre fini de réflexion inférieur ou égal à la dimension de l'espace. Le résultat est à connaître mais un peu long à présenter.

Référence :
- M. COGNET *Algèbre bilinéaire*, () p.96

2.1.61 Théorème de Chevalley-Warning [112]

Résultat On montre que si k est un corps fini de caractéristique p et que $P_1, \ldots, P_r$ sont des éléments de $k[X_1, \ldots, X_n]$ vérifiant $\deg P_1 + \ldots + \deg P_r < n$, alors le nombre de zéros communs dans k^n entre ces polynômes est un multiple de p.

Références :
- J.-P. SERRE, *Cours d'arithmétique*, PUF (1994)
- P. SAMUEL, *Théorie algébrique des nombres*, Hermann (1997)

2.1.62 Théorème de Desargues par le calcul barycentrique [137]

Résultat On montre que si on suppose que A, B, C et A' , B' , C' sont six points distincts du plan formant deux triangles ABC et $A'B'C$ avec (BC) et $(B'C')$ se coupant en L, (CA) et $(C'A')$ en M et (AB) et $(A'B')$ en N, alors L, M et N sont alignés si et seulement si les droites (AA'), (BB') et (CC') sont concourantes ou parallèles (on distingue les cas où les trois points L, M et N ne sont pas tous distincts) en procédant de manière exclusivement analytique via le calcul barycentrique. La géométrie projective serait adaptée à la formulation de ce théorème mais elle n'est plus au programme.

Référence :
- R.GOBLOT *Géométrie*

2.1.63 Théorème de Dirichlet faible [109][110][116]

Résultat On démontre qu'il existe une infinité de nombres premiers de la forme $an + 1$ pour a entier naturel donné en utilisant notamment les propriétés de polynômes cyclotomiques. Attention aux erreurs de notation dans la référence.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2008)

2.1.64 Théorème de Frobenius-Zolotarev [106][108][112][123]

Résultat On démontre que si p est un nombre premier impair, alors pour $u \in \mathcal{GL}_n(\mathbb{F}_p)$, si on note $\left(\frac{a}{p}\right)$ le symbole de Legendre (qui vaut 1 si a est un carré modulo p et -1 sinon) et $\varepsilon(u)$ la signature de u en tant que permutation sur l'ensemble fini de vecteurs de $\mathbb{F}_p^n$, on a :

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

Références :
- V.BECK, J.MALICK, G.PEYRÉ,*Objectif agrégation (2ème édition)*, H&K (2005)
- D. PERRIN, *Cours d'algèbre*, Ellipses (1998)

2.1.65 Théorème de Gauss pour les polygones réguliers constructibles [109][110][112][116][120][139][141]

Résultat On admet le théorème de Wantzel (qui peut faire l'objet d'un développement) et on montre le théorème de Gauss qui affirme que "le" polygone régulier à n cotés est constructible si et seulement si n est de la forme $n = 2^s p_1 \dots p_r$ où les p_i sont des nombres premiers de Fermat distincts. On utilise sans le dire le théorème de correspondance de Galois.

Référence :
- A.CHAMBERT-LOIR, *Algèbre corporelle* Éditions de l'École Polytechnique (2005)
- J.CARREGA *Théorie des corps*

2.1.66 Théorème de Gershgörin [124]

Résultat On montre un domaine d'inclusion pour les valeurs propres d'une matrice complexe et on précise le résultat : le nombre de valeurs propres dans une composante connexe du domaine est égal au nombre de disques la recontrant par notamment des arguments liés au théorème des résidus.

Référence :
- D. SERRE *Les matrices*, Dunod ()

2.1.67 Théorème de Hahn-Banach [132][137][208]

Résultat On démontre que l'on peut séparer un convexe fermé et un convexe compact disjoint par un hyperplan ou de manière équivalente que toute forme linéaire continue sur un sous-espace vectoriel se prolonge en une forme linéaire continue sur l'espace vectoriel tout entier. Ce résultat utilise le lemme de Zorn en dimension infinie et la démonstration en dimension finie -plus simple- est conseillée si l'on souhaite inclure ce développement dans la leçon sur les barycentres ou les formes linéaires notamment.

Références :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 3*, Cassini (2010)
- F. GANTMACHER *Théorie des matrices*, Dunod ()

2.1.68 Théorème de Jordan [139][203]

Résultat On démontre que si Γ est une courbe fermée simple de classe $\mathcal{C}^1$ (en particulier cette courbe est de Jordan), alors $\mathbb{C} \setminus \Gamma$ a deux composantes connexes l'une bornée, l'autre non.

Référence :
- S. GONNORD, N. TOSEL *Calcul différentiel* Ellipses (1998)

2.1.69 Théorème de Kronecker [116]

Résultat On montre qu'un polynôme unitaire irréductible de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module inférieur ou égal à 1 est un polynôme cyclotomique en utilisant un argument de descente infinie via les sommes de Newton.

Référence - S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2008)

2.1.70 Théorème de l'élément primitif [116][120]

Résultat On montre que si K est un corps et $K \hookrightarrow L$ est une extension de degré fini de K, alors le nombre de K-morphismes de L dans une clôture algébrique de K est plus grand que 1 et inférieur à $[L : K]$ avec égalité si et seulement si l'extension L est séparable. À réserver aux spécialistes ...

Référence :
- J.-P. ESCOFFIER *Théorie de Galois* Dunod (2000)

2.1.71 Théorème de Lie-Kolchin [106][119][124][128]

Résultat On montre qu'un sous-groupe G de $\mathcal{GL}_n(\mathbb{C})$ connexe et résoluble (i.e. il existe une suite finie $G_0, G_1, \ldots, G_n$ de $n+1$ sous-groupes de G telle que : $\{I\} = G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n = G$ où $\forall i \in [0, n-1]$, G_i est un sous-groupe distingué de G_{i+1} et le groupe quotient G_{i+1}/G_i est abélien) est conjugué à un sous-groupe des matrices triangulaires supérieures. Autrement dit un sous-groupe G de $\mathcal{GL}_n(\mathbb{C})$ connexe et résoluble est simultanément trigonalisable (toutes ses matrices sont triangulaires supérieures dans une même base). Ce développement est très intéressant puisqu'il est lié aux représentations linéaires des groupes finis mais difficile puisqu'il faut être au point sur la résolubilité.

Référence :
- A. CHAMBERT-LOIR *Algèbre Corporelle* Éditions de l'École Polytechnique (2005)

2.1.72 Théorème de Molien [105][106][120][123][124][145]

Résultat On étudie, pour un sous groupe fini G de $\mathcal{GL}_n(\mathbb{C})$, l'action de ce sous-groupe fini sur les polynômes homogènes de degré k. On démontre ensuite une égalité avec la série génératrice des dimensions $a_k(G)$ des stabilisateurs pour cette action :

$$\sum_{k=0}^{\infty} a_k(G) X^k = \frac{1}{\#G} \sum_{g \in G} \frac{1}{\det(id_{\mathbb{C}^n} - Xg)}$$

Référence :
- G.PEYRÉ *L'algèbre discrète de la transformée de Fourier : Niveau M1* Broché

2.1.73 Théorème de Pascal [123][137]

Résultat On démontre que lorsqu'un hexagone (pas forcément régulier) est inscrit dans une conique, alors les points d'intersection des côtés opposés sont alignés. Attention à bien préciser la définition de point d'intersection pour que la preuve fonctionne. La vision projective serait adaptée à ce théorème mais la géométrie projective n'est plus au programme.

Référence :
- Y. LADEGAILLERIE *Géométrie affine, projective, euclidienne et analagmatique*, Dunod ()

2.1.74 Théorème de Perron-Frobenius [123]

Résultat On démontre que si une matrice réelle A a tous ses coefficients strictements positifs, alors son rayon spectral est une valeur propre dont l'espace propre associé est de dimension 1 et qu'elle admet un vecteur propre pour cette valeur propre dont tous les coefficients sont strictements positifs. On peut remarquer que ce théorème implique dans certains cas l'existence d'une probabilité invariante pour une chaîne de Markov.

Référence :
- D. SERRE *Les matrices*, Dunod ()

2.1.75 Théorème de Riesz [120][203][208]

Résultat On montre un théorème du à Riesz affirmant que la boule unité fermée d'un espace vectoriel normé E est compacte si et seulement si E est de dimension finie. En particulier on montrera l'équivalence des normes en dimension finie.

Référence :
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 3*, Cassini (2011)

2.1.76 Théorème de Sophie Germain [109][110]

Résultat On démontre que si p est un nombre premier tel que $2p+1$ est aussi un nombre premier, alors il n'existe pas de triplet d'entiers (x, y, z) non nuls et non multiples de p tels que $x^p + y^p = z^p$ (ce qui est un cas particulier du grand théorème de Fermat).

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2008)

2.1.77 Théorème de Wantzel [116][141]

Résultat On démontre qu'un nombre x est constructible si et seulement s'il existe une "tour" d'extensions : $\mathbb{Q} = L_0 \subset L_1 \subset \ldots \subset L_n$ telles que $x \in L_n$ et $[L_{i+1} : L_i] = 2$ (conditions sur les degrés des extensions : L_{i+1} doit être une extension quadratique de L_i).

Référence :
- J.-C. CARREGA *Théorie des corps : la règle et le compas*, Hermann (1981)

2.1.78 Théorème des deux carrés [109][110]

Résultat On montre qu'un entier naturel est somme de deux carrés d'entiers naturels si et seulement si chacun de ses facteurs premiers de la forme $4k + 3$ intervient à une puissance paire dans la décomposition en produit de nombres premiers, en étudiant l'anneau des entiers de Gauss $\mathbb{Z}[i]$.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2008)

2.1.79 Théorème des extrema liés et application [120][214][219]

Résultat On démontre que l'existence d'un minimum en a pour une fonction f de classe $\mathcal{C}^1$ sur $\mathbb{R}^n$ sur un ensemble X de la forme $X = \{x \in \mathbb{R}^n | g_1(x) = \ldots = g_p(x) = 0\}$ où $g_1, \ldots, g_p$ sont de classe $\mathcal{C}^1$ (X est en particulier une sous-variété de $\mathbb{R}^n$) implique l'existence de multiplicateurs de Lagrange $\lambda_1, \ldots, \lambda_p$ tels que :

$$df(a) = \lambda_1 dg_1(a) + \ldots + \lambda_p dg_p(a).$$

On peut appliquer ce résultat à l'existence d'une valeur propre pour un endomorphisme symétrique ou à la minimalité de $\mathcal{SO}_n(\mathbb{R})$ dans $\mathcal{SL}_n(\mathbb{R})$ pour la norme 2.

Référence :
- M. ALESSANDRI, *Thèmes de géométrie, groupes en situation géométrique*, Dunod (1999)
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)

2.1.80 Théorème min-max de Courant-Fisher [132][133]

Résultat On donne dans le cas d'un endomorphisme autoadjoint u une formule pour obtenir sa $k^{\text{è}}$ valeur propre (ordre croissant compté avec multiplicité) :

$$\lambda_k = \min_{dim(F)=k} \max_{1=\|x\| \in F} < u(x), x >$$

On remarquera les formules simples pour la plus grande et la plus petite valeur propre, et que ces formules induisent que la $k^{\text{è}}$ valeur propre est une fonction 1-lipschitzienne de u.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 3*, Cassini

2.1.81 Théorèmes de Sylow [104]

Résultat On démontre que si G est un groupe fini dont la décomposition en facteurs premiers de son cardinal s'écrit : $\#G = p^\alpha m$ avec $\alpha > 0$, alors le nombre n_p de ses p-sous-groupes de Sylow (i.e. de cardinal p^α) vérifie n_p divise m et $n_p = 1[p]$ et que les p-sous-groupes de Sylow sont conjugués entre eux.

Référence :
- D. PERRIN, *Cours d'algèbre*, Ellipses (1998)

2.1.82 Transformée de Fourier discrète [112][902]

Résultat On montre que l'on peut multiplier deux polynômes en $O(n \log n)$ grâce à un algorithme de type "Diviser Pour Régner".

Références :
- P. SAUX-PICART, E. RANNOU *Cours de calcul formel pour les filles*, Ellipses ()
- PAPADIMITRIOU *Algorithms*
- J.-G.DUMAS, S.VARRETTE, É.TANNIER, J.-L.ROCH *Théorie des codes : Compression, cryptage, correction*

2.1.83 Un homéomorphisme réalisé par l'exponentielle matricielle [133]

Résultat On démontre que l'exponentielle matricelle complexe réalise un homéomorphisme entre l'ensemble des matrices hermitiennes $\mathcal{H}_n$ et l'ensemble des matrices hermitiennes définies positives $\mathcal{H}_n^{++}$ (et également entre l'ensembles des matrices symétriques réelles et l'ensemble des matrices symétriques réelles définies positives) en utilisant des considérations topologiques.

Références :
- R. MNEINMNÉ, F. TESTARD *Introduction aux groupes de Lie classiques*, Hermann (1994)
- J.-E. ROMBALDI *Thèmes pour l'agrégation de mathématiques*, EDP Sciences (1999)

Leçon algèbre	dév'
104 Groupes finis. Exemples et applications.	Simplicité de $\mathcal{A}_n$ Critère de finitude de Burnside $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$
105 Groupe des permutations d'un ensemble fini. Applications.	Simplicité de $\mathcal{A}_n$ Bruhat
106 Groupe linéaire d'un espace vectoriel de dimension finie E , sous-groupes de GL(E). Applications.	Ss-gp compacts de GLn Burnside $Conv(\mathcal{O}_n)$
108 Exemples de parties génératrices d'un groupe. Applications.	Simplicité de $\mathcal{A}_n$ $PSL_2(\mathbb{Z})$
109 Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.	Dirichlet faible $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$
110 Nombres premiers. Applications.	Dirichlet faible $P(p \wedge q = 1)$
112 Corps finis. Applications.	Chevalley-Warning Dén polyn irréductibles
116 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.	Dirichlet faible Dénombrement sur un corps fini
119 Exemples d'actions de groupes sur les espaces de matrices.	Bruhat Sous-groupes compacts de GL_n
120 Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.	Molien Ss-esp stables par translation
123 Déterminant. Exemples et applications.	Suite de polygone John-Löwner Critère de Gale
124 Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.	Ss-esp stables par translation Burnside
128 Endomorphismes trigonalisables. Endomorphismes nilpotents.	Burnside Bruhat
131 Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.	Sous-groupes compacts de GL_n Lemme de Morse
132 Formes linéaires et hyperplans en dimension finie. Exemples et applications.	Critère de Gale Burnside $Conv(\mathcal{O}_n)$
133 Endomorphismes remarquables d'un espace vectoriel euclidien (dimension finie).	$Conv(\mathcal{O}_n)$ Sous-groupes compacts de GL_n
137 Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.	Suite de polygones John-Löwner
139 Applications des nombres complexes à la géométrie.	$PSL(\mathbb{Z}_2)$ Suite de polygones
140 Systèmes d'équations linéaires. Systèmes échelonnés. Résolution. Exemples et applications.	Bruhat Gradient conjugué
141 Utilisation des groupes en géométrie.	? $PSL(\mathbb{Z}_2)$
145 Méthodes combinatoires, problèmes de dénombrement.	Partitions de n Polynômes irréductibles $P(p \wedge q = 1)$

2.2 Référence des développements d'analyse

2.2.1 Calcul de l'intégrale de Dirichlet [236][239]

Résultat On calcule la valeur de l'intégrale de Dirichlet. Il y a différentes façons de le faire, données dans la référence. La plus longue semble la plus adaptée.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 3*, Cassini (2010)

2.2.2 Complétude de $\mathbb{L}^p$ [108]

Résultat On montre que les espaces $\mathbb{L}^p$ sont complets en montrant que les suites de Cauchy convergent .

Références :
- W. RUDIN *Analyse réelle et complexe*, Dunod (2009)
- H. BREZIS *Analyse fonctionnelle*, Dunod

2.2.3 Continuité des fonctions convexes [203][229]

Résultat On montre qu'une fonction convexe sur un ouvert convexe Ω est lipschitzienne sur tout compact de Ω.

Référence :
- H. BREZIS *Analyse fonctionnelle*, Dunod

2.2.4 Convergence d'une suite de polygones [123][137][139][226]

Résultat On montre que pour $(x_1, \ldots, x_n)$ un n-uplet de complexes, en définissant une suite polygones $\mathcal{P}_n$ (non nécessairement convexe, on prend les points dans l'ordre) où $\mathcal{P}_{n+1}$ est le polygone formé par les milieux des côtés de $\mathcal{P}_n$, cette suite converge vers le n-uplet $(g, \ldots, g)$ où g est l'isobarycentre de $(x_1, \ldots, x_n)$.

Référence :
Pas de livre ! Voir la page suivante : http://favetto.free.fr/agreg.pdf
Le calcul du déterminant circulant est présent dans Gourdon ou Oraux X-ENS.

2.2.5 Convergence d'une suite définie par récurrence [206][224][226]

Résultat On étudie la suite définie par la récurrence $u_{n+1} = 1 - \lambda u_n$ avec $u_0, \lambda \in]0, 1[$.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 1*, Cassini

2.2.6 Critère de Kitaï [208][226]

Résultat On montre que, si E est un espace vectoriel sur $\mathbb{C}$ métrique complet séparable, pour qu'un opérateur A soit hypercyclique (c'est-à-dire qu'il existe $x \in E$, $(A^n(x))_{n\in\mathbb{N}}$ est dense dans E), il suffit qu'il existe X et Y denses dans E et $B : Y \to Y$ tels que pour tout $x \in X$ et $y \in Y$ on ait $A_n(x) \to 0$, $B_n(y) \to 0$ et $AB(y) = y$.

Référence :
- S. GONNORD,N. TOSEL *Topologie et analyse fonctionnelle* Ellipses

2.2.7 Critère de Raab-Duhamel [230]

Résultat On donne le critère de Raab-Duhamel pour la convergence de série à termes strictement positifs tels que $\frac{u_{n+1}}{u_n} = 1 - \frac{a}{n} + O(\frac{1}{n^\beta})$, avec $\beta > 1$.

Référence :
- X. GOURDON, *Les maths en tête (Analyse)*, Ellipses (2008)

2.2.8 Densité des polynômes orthogonaux [208][239][240]

Résultat On montre la densité de familles de polynômes orthogonaux pour le produit scalaire associé à un poids quelconque en utilisant le procédé d'orthonormalisation de Gram-Schmidt puis des techniques hilbertiennes.

Référence :
- V.BECK, J.MALICK, G.PEYRÉ,*Objectif agrégation (2ème édition)*, H&K(2005)

2.2.9 Ellipsoïde de John-Löwner [123][137][203][219][229]

Résultat On démontre que tout compact K de $\mathbb{R}^n$ peut être entouré par un unique ellipsoïde de volume minimal centré en zéro.

Références :
- M. ALESSANDRI, *Thèmes de géométrie, groupes en situation géométrique*, Dunod (1999)
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 3*, Cassini (2008)

2.2.10 Équation du pendule [220]

Résultat On étudie l'équation du pendule simple $\ddot{\theta} = -\sin\theta$ en montrant notamment que les solutions maximales sont globales et périodiques par des techniques d'étude implicite d'équations différentielles.

Référence :
- DEMAILLY *Analyse numérique*

2.2.11 Équations diophantiennes et séries génératrices [145][224][243]

Résultat On montre que, pour $(\alpha_1, \dots \alpha_p)$, p entiers premiers entre eux dans leur ensemble, le nombre S_n de solutions $(n_1, \dots, n_p)$ de l'équation diophantienne $\alpha_1 n_1 + \ldots + \alpha_p n_p = n$ vérifie :

$$S_n \sim \frac{1}{\alpha_1 \ldots \alpha_p} \frac{n^{p-1}}{(p-1)!}$$

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 2*, Cassini (2005)

2.2.12 Équirépartition modulo 1 [224]

Résultat On montre l'équivalence, pour une suite $(x_n)_{n\in\mathbb{N}}$, entre les trois assertions suivantes (la première étant la définition de l'équirépartition modulo 1 et la dernière est appelé critère de Weyl) :
- $\forall a, b \in]0, 1[, \lim_{N\to\infty} \frac{1}{N} card\{x_m \in [a, b] | m \leq N\} = b - a$
- $\forall f \in \mathcal{C}([0, 1], \mathbb{C}), f(0) = f(1), \frac{1}{N} \sum_{n=0}^{N} f(x_n) \to_{N\to\infty} \int_0^1 f(t)dt$
- $\forall k \in \mathbb{Z}^*, \frac{1}{N} \sum_{n=0}^{N} e^{2i\pi k x_n} \to_{N\to\infty} 0$.

Références :
- A. CHAMBERT-LOIR *Exercices d'analyse (tome 1)*, Masson
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 1*, Cassini

2.2.13 Espace de Bergman [239]

Résultat On montre, pour un ouvert $\Omega \subsetneq \mathbb{C}$, que l'espace de Bergman $A^2(\Omega)$ (qui est l'ensemble des fonctions holomorphes et de carré intégrable sur Ω) est un espace de Hilbert et on donne une base de cet espace via des techniques de majorations utilisant la formule de Cauchy. On peut même étudier un noyau donnant une égalité entre une fonction de $A^2(\Omega)$ et une moyenne sur l'ouvert via ce noyau.

Référence :
- A. CHAMBERT-LOIR *Exercices d'analyse (tome 3)*, Masson

2.2.14 Étude du système proie-prédateur de Lotka-Volterra [220]

Résultat On étudie le système de Lotka-Volterra en montrant notamment la cyclicité du phénomène (courbes fermées) par des techniques d'études d'équations différentielles implicites. Attention à développer un peu l'argument de monotonie de la référence à la fin de la démonstration. Il existe des généralisations de ce type d'étude lorsque les trajectoires sont compactes (cf. Gonnord-Tosel Calcul différentiel).

Référence :
- A. CHAMBERT-LOIR *Exercices d'analyse (tome 3)*, Masson

2.2.15 Étude d'un système dynamique discret et de son équivalent continu [220][224][226]

Résultat Soit $f \in \mathcal{C}^1([0,1])$ telle que $f(0) = f(1) = 0$, $f'(0) \in]-1, 0[$ et $-x < f(x) < 0$ $\forall x \in]0,1[$. On étudie le système dynamique donné par une suite $(x_n)_n \in \mathbb{N}$ définie par $x_0 \in]0,1[$ et $x_{n+1} = x_n + f(x_n)$, et on compare les cas discret et continu.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 1(?)*, Cassini

2.2.16 Exemple de Stoyanov [239][240][246]

Résultat On donne un exemple de variables aléatoires f et g telles que f est à densité et g discrète alors que leurs fonctions caractéristiques coïncident sur $[-1, 1]$. Cet exemple est à mettre en relation avec le théorème de Shannon.

Référence :
- J.-Y. OUVRARD *Probabilités (tome 2)* Cassini

2.2.17 Fenêtre de Viviani [214]

Résultat On étudie la fenêtre de Viviani qui est la courbe gauche de l'intersection entre une sphère et un plan : on calcule notamment l'aire délimitée par cette courbe (attention à ne pas se tromper avec son complémentaire).

Références :
- F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)
- Guy LAVILLE *Courbes et surfaces*, Ellipses

2.2.18 Fonction de Lebesgue [229]

Résultat On montre, en la construisant, l'existence d'une fonction croissante nulle en 0 et égale à 1 en 1 de dérivée nulle presque partout sur $[0, 1]$ en utilisant notamment l'ensemble de Cantor.

Référence :
- M. BRIANE, J. PAGÈS *Théorie de l'intégration*, Vuibert

2.2.19 Fonctions à variation bornée [229]

Résultat On étudie une classe de fonctions qui n'oscillent pas trop et on montre finalement que ce sont des différences de deux fonctions croissantes. On peut également donner un contre-exemple à cette classe de fonctions.

Références :
- X. GOURDON, *Les maths en tête (Analyse)*, Ellipses (2008)
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 2*, Cassini (2005)

2.2.20 Formule des compléments [236][239]

Résultat On montre par des méthodes de calcul d'intégrales et notamment le théorème des résidus une formule pour la fonction Γ (qui est valable dans une partie du plan complexe) :

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}$$

La démonstration de la référence peut éviter la discussion sur la détermination du logarithme mais augmente les calculs en changeant le contour d'intégration en prenant un rectangle.

Référence :
- AMAR - MATHERON *Analyse complexe*, Cassini

2.2.21 Formule d'Euler-Mac Laurin [218][224]

Résultat On démontre une formule analogue à la formule de Taylor avec reste intégral sauf que l'on intègre par partie avec un point milieu ce qui change le terme polynomial et fait apparaître les polynômes de Bernouilli. On peut ensuite faire de multiples applications : développement asymptotique de la série harmonique ou prolongement de la fonction ζ ou de la fonction ξ (l'ordre 1 pour Euler-Mac Laurin peut suffire).

Référence :
- A. CHAMBERT-LOIR *Exercices d'analyse (tome 1)*, Masson

2.2.22 Formule d'inversion de Fourier [239][240]

Résultat On montre la formule d'inversion de Fourier : si f est une fonction admettant des limites à gauche et à droite en un point a et dérivable à gauche et à droite en ce point :

$$\frac{1}{2}(f(a^+) - f(a^-)) = \lim_{A \to \infty} \int_{-A}^{A} e^{iax} \hat{f}(x) dx$$

en utilisant le lemme de Riemann-Lebesgue et en découpant l'intégrale. Cette formule est l'analogue du théorème de Dirichlet pour la séries de Fourier. Attention à bien définir la transformée de Fourier pour éviter l'apparition ou la disparition des facteurs 2π.

Référence :
- J.-M. BONY *Méthodes mathématiques pour les sciences physiques*, Éditions de l'École Polytechnique

2.2.23 Formule sommatoire de Poisson [230][239][240][246]

Résultat On montre que pour une fonction F continue sur $\mathbb{R}$ telle qu'il existe $\alpha > 1$, $x \mapsto x^\alpha F(x)$ admet une limite finie en $+\infty$ et $\sum_{\mathbb{Z}} |\hat{F}(n)| < \infty$ alors on a :

$$\sum_{\mathbb{Z}} \hat{F}(n) = \sum_{\mathbb{Z}} F(n)$$

et on peut l'appliquer à la fonction Θ de Jacobi :

$$\Theta(x) = \sum_{\mathbb{Z}} e^{-n^2 \pi x} = \frac{1}{\sqrt{x}} \sum_{\mathbb{Z}} e^{-n^2 \pi \frac{1}{x}} = \frac{1}{\sqrt{x}} \Theta(\frac{1}{x})$$

Références :
- C. ZUILY, H. QUÉFFÉLEC, *Analyse pour l'agrégation (3ème édition)*, Dunod (2007)
- X. GOURDON, *Les maths en tête (Analyse)*, Ellipses (2008)

2.2.24 Formules de Green [215]

Résultat

Référence :

2.2.25 Inégalité de Carleman [230]

Résultat On montre, pour une suite $(a_n)_{n\in\mathbb{N}}$ à termes positifs, l'inégalité de Carleman :

$$\sum_{i=1}^{\infty}(\prod_{k=1}^{i} a_k)^{1/i} \leq e\sum_{1}^{\infty} a_i$$

et que la constante e est optimale sans jamais être atteinte.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 1*, Cassini

2.2.26 Intégrale de Fresnel [236][239][240]

Résultat On calcule $\int_0^{+\infty} e^{ix^2}dx$ en utilisant $\int_0^{+\infty} x^{\alpha-1}e^{ix}dx$ pour $\alpha \in]0,1[$ en utilisant des théorèmes d'intégrales à paramètres.

Références :
- X. GOURDON, *Les maths en tête (Analyse)*, Ellipses (2008)
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 3*, Cassini (2010)

2.2.27 Le billard elliptique [214][215][219]

Résultat On montre que dans un billard elliptique il existe une trajectoire fermée à trois rebonds (on construit une trajectoire en utilisant les tangentes à l'ellipse pour les rebonds). Cette trajectoire est un triangle de périmètre maximal inscrit dans l'ellipse. On peut même démontrer qu'il existe une trajectoire fermée à n rebonds pour tout $n \geq 2$.

Référence :
- F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)

2.2.28 Le folium de Descartes [214]

Résultat On fait une étude complète de la courbe plane définie par $x+y=3xy$. On peut donner également l'aire délimitée par la boucle qui vaut $\frac{3}{2}$.

Référence :
- F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)

2.2.29 Le processus de Galton-Watson [224][226][229]

Résultat On étudie un processus de branchement régissant des dynamiques de populations et le comportement de celles-ci (extinction ou survie). Attention néanmoins aux questions probabilistes liées à ce développement.

Référence :
- M.BENAIM, N. EL KAROUI *Promenade aléatoire*, Éditions de l'École Polytechnique (2004)

2.2.30 Lemme de Morse [131][214][215][218][219]

Résultat On montre que si f une fonction réelle de classe $\mathcal{C}^3$ définie sur un ouvert U (contenant 0) de $\mathbb{R}^n$ dont la hessienne est inversible en 0 et est de signature (en tant que forme quadratique) $(p, n-p)$ alors il existe un changement de coordonnées $x \mapsto u(x)$ local de classe $\mathcal{C}^1$ tel que :

$$f(x) - f(0) = u_1^2(x) + \ldots + u_p^2(x) - u_{p+1}^2(x) - \ldots - u_n^2(x)$$

localement autour de 0 en utilisant notamment la formule de Taylor avec reste intégrale. Il faut connaître l'application à la position par rapport à l'hyperplan tangent d'une hypersurface (ou au moins d'une surface).

Référence :
- F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)

2.2.31 Lois Γ, lois β [236]

Résultat On effectue des calculs avec les densités des lois Γ et β et on exprime notamment la constante de normalisation des lois β avec la fonction Γ.

Référence :
- COTTRELL - DUHAMEL *Exercices de probabilités*, Cassini (2004)

2.2.32 Méthode de la phase stationnaire [236][239]

Résultat On étudie la comportement asymptotique pour un intervalle $[a, b]$ donné, f une fonction continue sur $[a, b]$ et g une fonction de classe $\mathcal{C}^2$ sur $[a, b]$ possédant un unique point stationnaire x_s sur $[a, b]$ d'une intégrale via une déformation du chemin d'intégration par un difféomorphisme local, ce qui donne :

$$\int_a^b f(x)e^{i\lambda g(x)}dx \sim_{\lambda\to\infty} \sqrt{\frac{2\pi}{\lambda|g''(x_s)|}} f(x_s)e^{i\lambda g(x_s)}e^{isgn(g''(x_s))\frac{\pi}{4}}$$

où $g''(x_s)$ est non nul. On peut également traiter le cas où $g''(x_s)$ est nul. Ceci est un raffinement de la méthode de Laplace et un cas particulier de la méthode du col. Les hypothèses sur les fonctions sont liées au comportement spécial de fonction du type Bessel par exemple.

Références :
- E. LEICHTNAM, *Exercices d'oraux X-ENS : tome Analyse*, Ellipses (1999)
- Jean DIEUDONNE *Calcul infinitésimal* Hermann

2.2.33 Méthode de Laplace [218][236][239]

Résultat On étudie le comportement asymptotique pour un intervalle I donné, f une fonction continue sur I et g une fonction de classe $\mathcal{C}^2$ sur I possédant un unique point stationnaire x_s sur I d'une intégrale via une déformation du chemin d'intégration par un difféomorphisme local, ce qui donne :

$$\int_I e^{\lambda g(x)}dx \sim_{\lambda\to\infty} \sqrt{\frac{\pi}{\lambda|g''(x_s)|}} f(x_s)e^{\lambda g(x_s)}$$

où $g''(x_s)$ est non nul. On peut appliquer ensuite ceci pour obtenir l'équivalent de Stirling pour la fonction Γ. On peut également traiter le cas où $g''(x_s)$ est nul. Ceci est un cas particulier de la méthode du col. Les hypothèses sur les fonctions sont liées au comportement spécial de fonction du type Bessel par exemple.

Références - F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)
- C. ZUILY, H. QUÉFFÉLEC, *Analyse pour l'agrégation (3ème édition)*, Dunod (2007)

2.2.34 Méthode de Newton pour les polynômes [218][224][226][232]

Résultat On montre d'une part la convergence dans le cas où f'' est bornée et que le point d'annulation de f recherché n'est pas critique de la méthode de Newton et on donne même un équivalent de la convergence de la méthode dans différents cas polynomiaux (on recherche les racines des polynômes) en utilisant notamment la formule de Taylor.

Références :
- F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)
- A. CHAMBERT-LOIR *Exercices d'analyse (tome 2)*, Masson

2.2.35 Méthode de relaxation [140][224][226][232]

Résultat On montre que si la méthode de relaxation appliquée à A converge, alors $w \in]0; 2[$, et qu'on a équivalence dans le cas où A est hermitienne définie positive.

Références :
- J.-P. DEMAILLY *Analyse numérique*, Broché (2006)
- M. SCHATZMAN *Analyse numérique : Une approche mathématique*, Broché (2004)

2.2.36 Méthode de Romberg [218]

Résultat On étudie la méthode d'intégration de Romberg qui est une méthode récursive de calcul numérique d'intégrale, basée sur l'application du procédé d'extrapolation de Richardson à la méthode des trapèzes, c'est à dire que l'on accélère la vitesse de convergence de la méthode des trapèzes notamment.

Référence :
- DEMAILLY *Analyse numérique*

2.2.37 Méthode de trichotomie [229][232]

Résultat On expose la méthode de trichotomie qui permet de calculer le minimum d'une fonction convexe définie sur $[a, b] \subset \mathbb{R}$, avec une convergence géométrique, en $\frac{\sqrt{5}-1}{2}$.

Référence :
- A.CHAMBERT-LOIR,S.FERMIGIER, *Exercices d'analyse (tome 2)*

2.2.38 Méthode du gradient à pas optimal[140][226][229][232]

Résultat On montre que la méthode du gradient à pas optimal qui sert à minimiser une fonctionnelle sur $\mathbb{R}^n$ (qui consiste à se placer sur la plus grande pente) est convergente et on donne une majoration de l'erreur à l'aide de l'inégalité de Kantorovitch (qui est démontrée de façon plus simple dans *Oraux X-ENS Analyse 1 Francinou Gianella*).

Références :
- J.-B. HIRIART-URRUTY *Optimisation et analyse convexe*, PUF (1998)
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 1*, Cassini

2.2.39 Méthode du gradient conjugué [140][219][226][232]

Résultat On décrit la méthode du gradient conjugué, qui dans le cas d'une fonction

$$J : \mathbb{R}^n \to \mathbb{R}, x \mapsto \frac{1}{2} < Ax, x > - < b, x >$$

avec $A \in \mathcal{S}_n^{++}(\mathbb{R})$ et $b \in \mathbb{R}^n$, calcule l'unique minimum de J en n étape au plus.

Référence :
- P.G.CIARLET *Introduction à l'analyse numérique matricielle et à l'optimisation : Cours et exercices corrigés*, Broché 2006

2.2.40 Partitions de $[\![1, n]\!]$ [145][230][243]

Résultat On étudie la série génératrice de terme général $\frac{D_n}{n!}$ où D_n est le nombre de partitions de $[\![1, n]\!]$ et on montre qu'elle vaut e^{e^x-1}.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2001)

2.2.41 Probabilité que deux nombres soient premiers entre eux [110][145][230]

Résultat On montre que la probabilité pour que deux nombres entiers choisis au hasard soient premiers entre eux est égale à $\frac{6}{\pi^2}$ (ce qui implique leur densité) en utilisant notamment la formule du crible, et la fonction de Möbius.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2008)

2.2.42 Prolongement de la fonction ζ de Riemann [230][239][240]

Résultat Montrer le prolongement à $\mathbb{C}\setminus 1$ est pratiquement impossible dans le temps imparti sauf si l'on considère que beaucoup de résultats sont connus notamment sur la méromorphie de Γ (en les mettant dans le plan par exemple) et que l'on connaît toutes les formules par coeur qui feront peut-être l'objet de questions ce qui fait de ce développement une réalisation délicate. On peut éventuellement se limiter à d'autres parties du plan complexe et utiliser la formule d'Euler-Mac Laurin par exemple.

Références :
- A. CHAMBERT-LOIR *Exercices d'analyse (tome 1 & 2)*, Masson (?)
- C. ZUILY, H. QUÉFFÉLEC, *Analyse pour l'agrégation (3ème édition)*, Dunod (2007)

2.2.43 Redressement d'un champ de vecteurs [214][215]

Résultat On montre à l'aide du théorème d'inversion locale que tout champ de vecteurs peut être redressé au voisinage d'un point non singulier, i.e. transformé en champ constant par changement de coordonnées. Cela signifie qu'à difféomorphisme près, il n'existe qu'un seul type de champ de vecteurs sans point singulier.

Référence :
- F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)

2.2.44 Série des inverses des nombres premiers [110][230]

Résultat On étudie la convergence de la série des inverses des nombres premiers.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2008)

2.2.45 Série génératrice des nombres de Bernoulli [243]

Résultat On étudie la série génératrice des nombres de Bernoulli $B_n(0)$ où $B_n(x)$ est le n-ième polynôme de Bernouilli et on montre notamment que :

$$\sum_{0}^{\infty} \frac{B_n(0)}{n!} t^n = \frac{t}{e^t - 1}$$

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS Oraux X-ENS Analyse 2, Cassini (2005) p.297

2.2.46 Sous-espaces de $\mathcal{C}(\mathbb{R}, \mathbb{C})$ de dimension finie stables par translation [120][124][221]

Résultat On montre que les sous-espaces vectoriels de $\mathcal{C}(\mathbb{R}, \mathbb{C})$ de dimension finie n stables par translation quelconque sont exactement les espaces de solution des équations différentielles linéaires homogène d'ordre n à coefficients constants. Le résultat sur les déterminant d'une famille libre de fonctions est démontré dans Oraux X-ENS Analyse.

Références :
- E. LEICHTNAM, *Exercices d'oraux X-ENS : tome Analyse*, Ellipses (1999) p.92
- V.BECK,J.MALICK,G.PEYRÉ,*Objectif agrégation (2ème édition)*, H&K(2005)

2.2.47 Sous-groupes compacts de $\mathcal{GL}_n(\mathbb{R})$ [119][131][133][203][206][229]

Résultat On montre que tout sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ est conjugué à un sous-groupe du groupe orthogonal $\mathcal{O}_n(\mathbb{R})$, en utilisant un théorème de point fixe. On pourra remarquer que ce théorème est un corollaire de l'existence de l'ellipsoïde de John-Loewner (c.f. Francinou, Gianella, *Oraux X-ENS Algèbre 3*).

Référence :
- M. ALESSANDRI, *Thèmes de géométrie, groupes en situation géométrique*, Dunod (1999)

2.2.48 Suites homographiques [224][226]

Résultat On étudie le comportement de la suite complexe $u_{n+1} = h(u_n)$ où h est une homographie.

Référence : - C. TISSERON *Géométrie affine et projective*, Hermann

2.2.49 Surjectivité de l'exponentielle matricielle [124][214][215]

Résultat On montre grâce au théorème d'inversion locale que toute matrice inversible admet un antécédent polynomial par l'exponentielle.

Référence :
- I.NURDIN *Agrégation de mathématiques Epreuve orale : 68 thèmes pour se préparer efficacement*, Broché (2006)
- M.COSTE `http://agreg-maths.univ-rennes1.fr/documentation/docs/Exponentielle.pdf`

2.2.50 Test du χ^2 [252]

Résultat On explique le test d'indépendance du χ^2 pour deux variables via la statistique de test de Pearson. Attention à être au point sur la notion de test en statistiques.

Référence :
- Alain MONFORT *Cours de statistique*, Economica

2.2.51 Théorème de d'Alembert-Gauss [203][214]

Résultat On montre que tout polynôme non constant à coefficients dans $\mathbb{C}$ admet une racine dans $\mathbb{C}$ par des considérations topologiques (notamment de la connexité) et le théorème d'inversion locale.

Référence :
- S. GONNORD, N. TOSEL *Calcul différentiel* Ellipses (1998)

2.2.52 Théorème de Banach-Steinhaus et une application [208][246]

Résultat On montre le théorème de Banach-Steinhaus, et on en déduit qu'il existe des fonctions différentes de leur série de Fourier.

Références :
- H. BREZIS *Analyse fonctionnelle*, Dunod
- X. GOURDON, *Les maths en tête (Analyse)*, Ellipses (2008)

2.2.53 Théorème de Bernstein [218][243]

Résultat On montre qu'une fonction infiniment dérivable dont toutes les dérivées d'ordre pair sont positives est analytique.

Référence :
- X. GOURDON, *Les maths en tête (Analyse)*, Ellipses (2008)

2.2.54 Théorème de Birkhoff [105][137][229]

Résultat On montre que l'enveloppe convexe des matrices de permutation est l'ensemble des matrices bistochastiques (attention le serpent ne fonctionne pas tout de suite, il faut réindexer d'abord).

Référence :
- D. SERRE *Les matrices*, Dunod ()

2.2.55 Théorème de Brouwer [203][206][214][215]

Résultat On montre que toute application continue de la boule unité fermée dans elle-même admet un point fixe. Il existe plusieurs façons de démontrer ce résultat notamment dans des cas particulier : on choisit une démonstration adaptée à la leçon dans laquelle on souhaite l'inclure : dans le cas $\mathcal{C}^1$ on utilise notamment le lemme de Milnor puis une approximation des fonctions continues par les fonctions de classe $\mathcal{C}^1$ pour le cas général, dans le cas de la dimension 2 on peut utiliser des arguments de connexité et le théorème de relèvement pour étudier un groupe topologique (contrairement à ce qui est fait dans Rouvière mais cette démonstration n'est pas référencée). Il faut être prêt aux questions sur les autres cas.

Références :
- F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)
- S. GONNORD, N. TOSEL *Calcul différentiel* Ellipses (1998)

2.2.56 Théorème de Cauchy-Lipschitz [206][220][221][226]

Résultat On montre, dans le cas linéaire ou non, le théorème d'existence et d'unicité d'une solution maximale pour une équation différentielle par un théorème de point fixe.

Références :
- DEMAILLY *Analyse numérique*
- C. ZUILY, H. QUÉFFÉLEC, *Analyse pour l'agrégation (3ème édition)*, Dunod (2007)

2.2.57 Théorème de Chudnowski [203]

Résultat On démontre que si $f : I \to \mathbb{R}$ est une fonction continue définie sur un segment $I = [a, b]$ ne contenant pas d'entier, alors il existe une suite $(P_n)_{n\in\mathbb{N}}$ de polynômes à coefficients entiers convergeant uniformément vers f sur I en construisant une suite de polynômes qui converge vers la constante $\frac{1}{2}$ puis en utilisant une approximation dyadique des réels.

Références :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 2*, Cassini (2005)
- A. CHAMBERT-LOIR *Exercices d'analyse (tome 1)*, Masson
- E. LEICHTNAM, *Exercices d'oraux X-ENS : tome Analyse*, Ellipses (1999) 5.2)

2.2.58 Théorème de D.J. Newmann [239]

Résultat On démontre que si une fonction $f : \mathbb{R}_+ \to \mathbb{C}$ est intégrable sur tout intervalle de la forme $[0, \alpha[$ pour α réel positif, et que la fonction :

$$g(z) = \int_0^\infty f(t)e^{-zt}dt$$

admet un prolongement holomorphe sur $\{z \in \mathbb{C}|\Re(z) \leq 0\}$, alors l'intégrale généralisée de f sur $[0, \infty[$ existe et :

$$g(0) = \int_0^\infty f(t)dt$$

La dernière partie est simplifiable pour gagner du temps en remplaçant l'intégration par parties par un argument de convergence dominée. Ce résultat est notamment utile pour démontrer le théorème des nombres premiers.

Référence :
- C. ZUILY, H. QUÉFFÉLEC, *Analyse pour l'agrégation (3ème édition)*, Dunod (2007)

2.2.59 Théorème de Féjèr [240][246]

Résultat On montre que pour une fonction f continue et 2π-périodique, la moyenne de Césaro de sa série de Fourier converge uniformément vers f en considérant, de manière analogue au théorème de Dirichelt pour les séries de Fourier, la moyenne de la série de Fourier comme un produit de convolution puis en découpant l'intégrale. On peut remplacer continue par $\mathbb{L}^p$ pour $1 \leq p < \infty$ pour avoir la convergence en norme p mais c'est plus difficile à démontrer. À noter que le théorème de Weierstrass sur la densité dans les fonctions continues est un corollaire du théorème de Féjèr.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 2*, Cassini (2005)

2.2.60 Théorème de Hadamard-Lévy [214][215]

Résultat On montre qu'une fonction de classe $\mathcal{C}^1$ est un difféomorphisme de $\mathbb{R}$ sur $\mathbb{R}$ si et seulement si sa différentielle est inversible et f est propre (l'image de tout compact est un compact). Il existe des cas particuliers simplifiant la démonstration qui peuvent suffire à un développement : f est de classe $\mathcal{C}^2$ ou f est une isométrie par exemple.

Références :
- C. ZUILY, H. QUÉFFÉLEC, *Analyse pour l'agrégation (3ème édition)*, Dunod (2007)
- S. GONNORD, N. TOSEL *Calcul différentiel* Ellipses (1998)

2.2.61 Théorème de Hahn-Banach [132][137][208]

Résultat On démontre que l'on peut séparer un convexe fermé et un convexe compact disjoint par un hyperplan ou de manière équivalente que toute forme linéaire continue sur un sous-espace vectoriel se prolonge en une forme linéaire continue sur l'espace vectoriel tout entier. Ce résultat utilise le lemme de Zorn en dimension infinie et la démonstration en dimension finie -plus simple- est conseillée si l'on souhaite inclure ce développement dans la leçon sur les barycentres ou les formes linéaires notamment.

Références :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 3*, Cassini (2010)
- F. GANTMACHER *Théorie des matrices*, Dunod ()

2.2.62 Théorème de Jordan [139][203]

Résultat On démontre que si Γ est une courbe fermée simple de classe $\mathcal{C}^1$ (en particulier cette courbe est de Jordan), alors $\mathbb{C} \setminus \Gamma$ a deux composantes connexes l'une bornée, l'autre non.

Référence :
- S. GONNORD, N. TOSEL *Calcul différentiel* Ellipses (1998)

2.2.63 Théorème de Korovkine et théorème de Stone-Weierstrass [203]

Résultat On montre qu'une suite d'opérateurs positifs u_n sur l'espace des fonctions réelles continues sur un compact K vérifiant $||u_n(g) - g||_\infty \to_{n\to\infty} 0$ pour tous les éléments g d'une partie d'un sous-espace des fonctions réelles continues sur K dense va vérifier cette convergence pour toute fonction continue. On applique ensuite ce résultat à l'opérateur des polynômes de Bernstein pour montrer le théorème de Stone-Weierstrass.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 2*, Cassini (2005)

2.2.64 Théorème de Montel [203]

Résultat On montre que pour un ouvert U du plan complexe donné et si on note $\mathcal{H}(U)$ l'ensemble des fonctions holomorphes sur U , de toute suite de fonctions de $\mathcal{H}(U)$ bornée sur tout compact de U (i.e. uniformément sur tout compact) on peut extraire une sous-suite convergeant uniformément sur tout compact de U vers une fonction de $\mathcal{H}(U)$. On peut mettre ce théorème en regard du théorème d'Ascoli que l'on utilise pour la démonstration .

Référence :
- W. RUDIN *Analyse réelle et complexe*, Sciences Sup (1998)

2.2.65 Théorème de Plancherel [240]

Résultat On montre que la transformée de Fourier-Plancherel

$$\mathcal{P} : L^1(\mathbb{R}) \cap L^2(\mathbb{R}) \to L^2(\mathbb{R})$$
$$f \mapsto \frac{1}{\sqrt{2\pi}}\hat{f}$$

se prolonge en un isomorphisme isométrique de $L^2(\mathbb{R})$ sur $L^2(\mathbb{R})$.

Référence :
-J. FARAUT *Calcul intégral*, EDP Sciences (2006)

2.2.66 Théorème de Prohorov [203][229]

Résultat On montre via le lemme de Helly que de toute suite de mesures de probabilités réelle et tendue on peut extraire une sous-suite convergeant étroitement . Il faut être au point sur la convergence de mesure et le théorème de Banach-Alaoglu, il s'agit en fait d'un résultat de compacité séquentielle pour la topologie faible-$\star$. Le véritable théorème de Prohorov se place de manière plus général en supposant seulement une suite dans un espace polonais.

Référence :
- COTTRELL - DUHAMEL *Exercices de probabilités*, Cassini (2004)

2.2.67 Théorème de représentation conforme [203][219]

Résultat On démontre que tout ouvert simplement connexe de $\mathbb{C}$ différent de $\mathbb{C}$ est isomorphe au disque unité ouvert (il existe une application biholomorphe) en utilisant notamment le théorème de Montel : ce développement est long et difficile et peut engendrer beaucoup de questions.

Référence :
- H. CARTAN *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, Hermann (1985)

2.2.68 Théorème de Riesz [120][203][208]

Résultat On montre un théorème énoncé par Riesz affirmant que la boule unité fermée d'un espace vectoriel normé E est compacte si et seulement si E est de dimension finie. En particulier on montre l'équivalence des normes en dimension finie.

Référence :
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)

2.2.69 Théorème de Sarkovski [224][226]

Résultat On montre que si I est un intervalle de $\mathbb{R}$ et $f : I \to I$ a un point périodique de période 3, alors elle admet dans I des points périodiques pour toute période $k > 0$ (i.e. "la période 3 implique le chaos").

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Algèbre 1*, Cassini (2001) (exercice 2.21)

2.2.70 Théorème de Shannon [240]

On étudie l'espace $BL^2 = \{u \in \mathbb{L}^2(\mathbb{R}) | supp(\hat{u}) \subset [-\frac{1}{2}, \frac{1}{2}]\}$ et montre que c'est un espace de Hilbert, que les éléments de BL^2 possèdent un représentant continu (et même analytique) et on donne une base hilbertienne $(e_n)_{n\in\mathbb{N}}$:

$$\forall n \in \mathbb{N}, e_n : x \mapsto \frac{\sin \pi(x-n)}{\pi(x-n)}$$

et la convergence de sa décomposition sur la base hilbertienne est uniforme en utilisant notamment la transformée de Fourier. Ce théorème est fondamental en théorie du signal puisqu'il permet d'échantillonner correctement avant transmission.

Référence :
- Michel WILLEM *Analyse harmonique réelle*, Hermann

2.2.71 Théorème de Stabilité de Lyapounov [215][220][221]

Résultat On établit, en dimension finie, que si un point est stable pour le linéarisé d'un système différentiel, alors il est stable pour le système différentiel lui-même et est exponentiellement attractif en utilisant de l'algèbre linéaire puis la formule de Taylor-Young et l'équivalence des normes en dimension finie.

Référence :
- F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)

2.2.72 Théorème de Stampacchia [203][206][219]

Résultat On démontre qu'étant donnés : un espace de Hilbert $\mathcal{H}$ muni de $(.|.)$, K une partie convexe fermée non vide de $\mathcal{H}$, a une forme bilinéaire continue et coercive et L une forme linéaire continue, il existe un unique $u \in K$ tel que : $\forall v \in K$, $a(u, v-u) \geq L(v-u)$. On peut également montrer que si a est symétrique, alors u est l'unique élément qui minimise : $I(v) = \frac{1}{2}a(v,v) - L(v)$ et qu'ainsi u est unique. Ce théorème est un raffinement du théorème de Lax-Milgram qu'il faut connaître si l'on fait ce développement.

Référence :
- H. BREZIS *Analyse fonctionnelle*, Dunod

2.2.73 Théorème des 3 droites d'Hadamard [229]

Résultat On montre le théorème des 3 droites d'Hadamard qui est un résultat de log-convexité. Pour f holomorphe dans la bande $\Omega = \{z \in \mathbb{C} | 0 < Re(z) < 1\}$ et continue bornée sur $\bar{\Omega}$, on pose $M(\theta) = \sup_{t \in \mathbb{R}} |f(\theta + it)|$. On a alors

$$M(\theta) \leq M(1)^{\theta} M(0)^{1-\theta}$$

Ce résultat permet de montrer le théorème de Riesz-Thorin.

Référence :
- C. ZUILY, H. QUÉFFÉLEC, *Analyse pour l'agrégation (3ème édition)*, Dunod (2007)

2.2.74 Théorème des extrema liés et application [120][219][214]

Résultat On démontre que l'existence d'un minimum en a pour une fonction f de classe $\mathcal{C}^1$ sur $\mathbb{R}^n$ sur un ensemble X de la forme $X = \{x \in \mathbb{R}^n | g_1(x) = \ldots = g_p(x) = 0\}$ où $g_1, \ldots, g_p$ sont de classe $\mathcal{C}^1$ (X est en particulier une sous-variété de $\mathbb{R}^n$) implique l'existence de multiplicateurs de Lagrange $\lambda_1, \ldots, \lambda_p$ tels que :

$$df(a) = \lambda_1 dg_1(a) + \ldots + \lambda_p dg_p(a).$$

On peut appliquer ce résultat à l'existence d'une valeur propre pour un endomorphisme symétrique ou à la minimalité de $\mathcal{SO}_n(\mathbb{R})$ dans $\mathcal{SL}_n(\mathbb{R})$ pour la norme 2.

Références :
- M. ALESSANDRI, *Thèmes de géométrie, groupes en situation géométrique*, Dunod (1999)
- X. GOURDON, *Les maths en tête (Algèbre)*, Ellipses (2008)

2.2.75 Théorème d'inversion locale [206][214][215][226]

Résultat On donne la preuve classique du théorème d'inversion locale par une méthode de point fixe.

Références :
- F. ROUVIÈRE, *Petit guide du calcul différentiel*, Cassini (2009)

2.2.76 Théorème taubérien fort [224][230][243]

Résultat On démontre le théorème taubérien de Hardy-Littlewood : si une série entière dont le terme général $(a_n)_{n\in\mathbb{N}}$ est réel, est un $O(\frac{1}{n})$ et que la série entière est de rayon de convergence plus grand que 1 dont la somme admet une limite finie l en 1 à gauche, alors :

$$\sum_{0}^{\infty} a_n = l$$

Références :
- X. GOURDON, *Les maths en tête (Analyse)*, Ellipses (2008)
- C. ZUILY, H. QUÉFFÉLEC, *Analyse pour l'agrégation (3ème édition)*, Dunod (2007)

2.2.77 Théorèmes de Dini et Helly [203][229]

Résultat On montre les théorèmes de Helly et Dini. Le théorème de Helly assure l'existence d'une sous-suite convergeant simplement pour une suite de fonctions de $\mathbb{R} \to [-1, 1]$ toutes croissantes. Le théorème de Dini annonce que pour une suite de fonctions continues croissante sur $[a, b] \to \mathbb{R}$ convergeant simplement vers $f \in \mathcal{C}^0([a, b], \mathbb{R})$ la convergence est en fait uniforme.

Référence :
- S. FRANCINOU, H. GIANELLA, S.NICOLAS *Oraux X-ENS Analyse 2*, Cassini

2.2.78 Tipi de Cantor [203]

Résultat On définit le tipi de Cantor $\mathcal{T} \subset \mathbb{R}$, dont on montre ensuite les propriétés pathologiques.

Référence :
- S.WILLARD, *General Topology.* Addison-Wesley (1970)

2.2.79 Une équation de distributions [218]

Résultat On montre que les solutions $u \in \mathcal{D}'(\mathbb{R})$ de $(x - x_0)^\alpha u = 0$ sont exactement les combinaisons linéaires de dérivés du dirac en x_0 jusqu'à la $\alpha^{ième}$ exclue. On utilise les propriétés des supports d'une distribution, les partitions de l'unité, et un développement de Taylor.

Références :
- H.ZUILY *Distributions et EDPs*
- LACOMBE, MASSAT *Exercices corrigés*

2.2.80 Vecteurs propres de la transformation de Fourier sur $\mathbb{L}^2$ [239][240]

Résultat On montre que les fonctions de Hermite (qui sont à un coefficient près, les polynômes apparaissant lors de la dérivation à l'ordre n de e^{-x^2}) forment une base hilbertienne de $\mathbb{L}^2$ muni de la mesure associée à la densité $x \mapsto e^{-x^2}$ propre pour la transformation de Fourier.

Référence :
- A. KOLMOGOROV *Éléments de la théorie des fonctions et de l'analyse fonctionnelle*, Mir Ellipses (1994)

2.2.81 Zéros des solutions d'une équation différentielle linéaire [220][221]

Résultat On étudie implicitement le comportement des zéros des solutions d'une équation du type $y'' + q(t)y = 0$ avec q une fonction continue.

Références :
- A. CHAMBERT-LOIR *Exercices d'analyse (tome 3)*, Masson
- X. GOURDON, *Les maths en tête (Analyse)*, Ellipses (2008)
- S. GONNORD, N. TOSEL *Calcul différentiel* Ellipses (1998)

Leçon analyse	dév'
203 Utilisation de la notion de compacité.	Brouwer Ss-groupes compacts de GL_n
206 Théorèmes de point fixe. Exemples et applications.	Cauchy-Lipschitz Brouwer Ss-groupes compacts de GL_n
208 Espaces vectoriels normés, applications linéaires continues. Exemples.	Hahn-Banach ?
214 Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.	Lemme de Morse Brouwer
215 Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.	Liapunov Lemme de Morse
218 Applications des formules de TAYLOR.	Lemme de Morse Méthode de Laplace
219 Problèmes d'extremums.	Lemme de Morse John-Löwner
220 Équations différentielles $X' = f(t, X)$. Exemples d'études qualitatives des solutions.	Cauchy-Lipschitz Lotka-Volterra Liapunov
221 Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.	Cauchy-Lipschitz Liapunov Ss-esp stable par translation
224 Comportement asymptotique de suites numériques. Rapidité de convergence. Exemples.	Théorème taubérien fort Méthode de Newton
226 Comportement d'une suite réelle ou vectorielle définie par une itération $u_{n+1} = f(u_n)$. Exemples.	Suite de polygones Méthode de Newton
229 Fonctions monotones. Fonctions convexes. Exemples et applications.	3 droites d'Hadamard John-Löwner
230 Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.	Partition de n Carleman Formule de Poisson
232 Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.	Méthode du gradient Trichotomie Méthode de Newton
236 Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables réelles.	Méthode de Laplace Fresnel
239 Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.	Méthode de Laplace Formule de Poisson
240 Transformation de FOURIER, produit de convolution. Applications.	Formule de Poisson Fresnel
243 Convergence des séries entières, propriétés de la somme. Exemples et applications.	Partition de n Taubérien fort
246 Séries de FOURIER. Exemples et applications.	Formule de Poisson Féjèr
252 Loi binomiale. Loi de POISSON. Applications.	Impasse !

Bibliographie

[104] Groupes finis. Exemples et applications.

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

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

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

[109] Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

[110] Nombres premiers. Applications.

[112] Corps finis. Applications.

[116] Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

[119] Exemples d'actions de groupes sur les espaces de matrices.

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

[123] Déterminant. Exemples et applications.

[124] Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

[128] Endomorphismes trigonalisables. Endomorphismes nilpotents.

[131] Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

[132] Formes linéaires et hyperplans en dimension finie. Exemples et applications.

[133] Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

[137] Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.

[139] Applications des nombres complexes à la géométrie.

[140] Systèmes d'équations linéaires. Systèmes échelonnés. Résolution. Exemples et applications.

[141] Utilisation des groupes en géométrie.

[145] Méthodes combinatoires, problèmes de dénombrement.

[——] ————————————————————————————————————

[203] Utilisation de la notion de compacité.

[206] Théorèmes de point fixe. Exemples et applications.

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

[214] Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.

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

[218] Applications des formules de TAYLOR.

[219] Problèmes d'extremums.

[220] Équations différentielles $X' = f(t, X)$. Exemples d'études qualitatives des solutions.

[221] Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

[224] Comportement asymptotique de suites numériques. Rapidité de convergence. Exemples.

[226] Comportement d'une suite réelle ou vectorielle définie par une itération $u_{n+1} = f(u_n)$. Exemples.

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

[230] Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.

[232] Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.

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

[239] Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

[240] Transformation de FOURIER, produit de convolution. Applications.

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

[246] Séries de FOURIER. Exemples et applications.

[252] Loi binomiale. Loi de POISSON. Applications.

[——] ——————————————————————————————

[901] Structures de données : exemples et applications.

[902] Diviser pour régner : exemples et applications.

[903] Exemples d'algorithmes de tri. Complexité.

[904] Problèmes NP-complets : exemples.

[906] Programmation dynamique : exemples et applications.

[907] Algorithmique du texte : exemples et applications.

[908] Automates finis. Exemples et applications.

[909] Langages rationnels. Exemples et applications.

[910] Langages algébriques. Exemples et applications.

[911] Automates à pile. Exemples et applications.

[912] Fonctions récursives primitives et non primitives. Exemples.

[913] Machines de Turing. Applications.

[914] Décidabilité et indécidabilité. Exemples.

[915] Classes de complexité : exemples.

[916] Formules du calcul propositionnel : représentation, formes normales, satisfiabilité. Applications.

[917] Logique du premier ordre : syntaxe et sémantique.

[918] Systèmes formels de preuve en logique du premier ordre : exemples

[919] Unification : algorithmes et applications.

[920] Réécriture et formes normales. Exemples.

[921] Algorithmes de recherche et structures de données associées.

[922] Ensembles récursifs, récursivement énumérables. Exemples.

[923] Analyses lexicale et syntaxique : applications.

[924] Théories et modèles en logique du premier ordre. Exemples.

[925] Graphes : représentations et algorithmes.

[926] Analyse des algorithmes : complexité. Exemples.

[927] Exemples de preuve d'algorithme : correction, terminaison.