ENS Rennes

Université de Rennes 1

Préparation à l'Agrégation Externe de Mathématiques

Pierre

Le Barbenchon

2018

2019

TABLE DES MATIÈRES

Introduction et conseils **6**

1 Couplages **8**
1.1 Couplages d'algèbre . . . 8
1.2 Couplages d'analyse . . . 11
1.3 Couplages d'informatique . . . 14

2 Plans de leçons **16**
2.1 Conseils . . . 16
2.2 Mes références préférées . . . 17
2.3 Métaplans d'algèbre . . . 18
101 : Groupe opérant sur un ensemble. Exemples et applications. . . . 18
104 : Groupes finis. Exemples et applications. . . . 20
105 : Groupe des permutations d'un ensemble fini. Applications. . . . 22
106 : Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications. . . . 25
108 : Exemples de parties génératrices d'un groupe. Applications. . . . 27
120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications. . . . 29
121 : Nombres premiers. Applications. . . . 31
123 : Corps finis. Applications. . . . 33
126 : Exemples d'équations en arithmétique . . . 35
141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications. . . . 38
151 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications. . . . 40
152 : Déterminant. Exemples et applications. . . . 42
153 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications. . . . 45
156 : Exponentielle de matrices. Applications. . . . 48
157 : Endomorphismes trigonalisables. Endomorphismes nilpotents. . . . 51
159 : Formes linéaires et dualité en dimension finie. Exemples et applications. . . . 53
162 : Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques. . . . 55
170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications. . . . 59
182 : Applications des nombres complexes à la géométrie. . . . 61
183 : Utilisation des groupes en géométrie. . . . 63

190 : Méthodes combinatoires, problèmes de dénombrement. 65
2.4 Métaplans d'analyse 67
203 : Utilisation de la notion de compacité. 67
208 : Espaces vectoriels normés, applications linéaires continues. Exemples. 69
214 : Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie. 72
219 : Extremums : existence, caractérisation, recherche. Exemples et applications. 74
220 : Equations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2. 76
221 : Equations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications. 78
223 : Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications. 80
224 : Exemples de développements asymptotiques de suites et de fonctions. . . . 83
226 : Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations . . . 85
228 : Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications. 88
229 : Fonctions monotones. Fonctions convexes. Exemples et applications. 90
230 : Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples. 92
233 : Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples. 94
236 : Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables. 97
239 : Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications. 99
243 : Convergence des séries entières, propriétés de la somme. Exemples et applications. 102
246 : Séries de Fourier. Exemples et applications. 105
250 : Transformation de Fourier. Applications. 107
260 : Espérance, variance et moments d'une variable aléatoire. 109
264 : Variables aléatoires discrètes. Exemples et applications. 111
265 : Exemples d'études et d'applications de fonctions usuelles et spéciales. . . . 113
2.5 Métaplans d'informatique 116
901 : Structures de données. Exemples et applications. 116
903 : Exemples d'algorithmes de tri. Correction et complexité. 118
907 : Algorithmique du texte. Exemples et applications. 120
909 : Langages rationnels et automates finis. Exemples et applications. 122
912 : Fonctions récursives primitives et non primitives. Exemples. 124
913 : Machines de Turing. Applications. 126
914 : Décidabilité et indécidabilité. Exemples. 128
915 : Classes de complexité. Exemples. 130
916 : Formules du calcul propositionnel : représentation, formes normales, satisfiabilité. Applications. 133
918 : Systèmes formels de preuve en logique du premier ordre. Exemples. 135
921 : Algorithmes de recherche et structures de données associées. 137
923 : Analyses lexicale et syntaxique. Applications. 139
924 : Théories et modèles en logique du premier ordre. Exemples. 141
925 : Graphes : représentations et algorithmes. 144
926 : Analyse des algorithmes : complexité. Exemples. 146
927 : Exemples de preuve d'algorithme : correction, terminaison. 148

928 : Problèmes NP-complets : exemples et réduction. . . . 150
929 : Lambda-calcul pur comme modèle de calcul. Exemples. . . . 153
930 : Sémantique des langages de programmation. Exemples. . . . 155
931 : Schémas algorithmiques. Exemples et applications. . . . 158
932 : Fondements des bases de données relationnelles. . . . 160
2.6 Les plans que j'ai rédigés . . . 163
106 : Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications. . . . 163
123 : Corps finis. Applications. . . . 163
126 : Exemples d'équations en arithmétique. . . . 163
141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications. . . . 163
152 : Déterminant. Exemples et applications. . . . 163
153 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications. . . . 163
156 : Exponentielle de matrices. Applications. . . . 164
159 : Formes linéaires et dualité en dimension finie. Exemples et applications. . . . 164
214 : Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie. . . . 164
223 : Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications. 164
226 : Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations. . . . 164
233 : Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples. . . . 164
243 : Power series : convergence and properties. Examples and applications. . . . 164
265 : Exemples d'études et d'applications de fonctions usuelles et spéciales. . . . 164
913 : Machines de Turing. Applications. . . . 165
914 : Décidabilité et indécidabilité. Exemples. . . . 165
916 : Formules du calcul propositionnel : représentation, formes normales, satisfiabilité. Applications. . . . 165
926 : Analyse des algorithmes : complexité. Exemples. . . . 165
927 : Exemples de preuve d'algorithme : correction, terminaison. . . . 165
929 : Lambda-calcul pur comme modèle de calcul. Exemples. . . . 165
930 : Sémantique des langages de programmation. Exemples. . . . 165
931 : Schémas algorithmiques. Exemples et applications. . . . 165
932 : Fondements des bases de données relationnelles. . . . 165

3 Développements 212
3.1 Conseils . . . 212
3.2 Ma liste des développements de mathématiques . . . 213
3.3 Ma liste des développements d'informatique . . . 214
3.4 Développements de mathématiques . . . 215
Primalité des nombres de Mersenne . . . 215
Isométries du cube et du tétraèdre . . . 219
Dénombrement des matrices diagonalisables de $\mathbb{F}_q$ . . . 223
Loi de réciprocité quadratique . . . 226
Décomposition de Dunford . . . 230
Image de l'exponentielle . . . 234
Convergence de polygones vers l'isobarycentre . . . 238
Banach–Steinhaus . . . 242
Méthode de Newton . . . 246
Réciproques partielles du théorème de Césaro . . . 249

Formule des compléments . . . 254
Cauchy–Lipschitz et lemme de Gronwall . . . 260
Translatés d'une fonction $\mathcal{C}^1$ . . . 264
Méthode de Gradient à pas optimal . . . 267
Nombres de Bell . . . 271
Formule d'inversion de la fonction caractéristique . . . 275
Théorème des extrema liés . . . 280
Nombres de zéros des solutions d'une équation différentielle . . . 284
Morphismes d'algèbre de $\mathcal{C}(K, \mathbb{R})$ sur $\mathbb{R}$ . . . 288
Théorème Central Limite . . . 290
Générateurs de $\mathrm{SL}_2(\mathbb{Z})$ . . . 294
Automorphismes de $\mathfrak{S}_n$ . . . 299
Etude du groupe $O(p, s)$ . . . 302
Théorème de Carathéodory . . . 305
Théorème de Fermat modulaire . . . 309
Méthode QR . . . 312
Irréductibilité des polynômes cyclotomiques . . . 315
Formule de Poisson et Shannon . . . 320
Formule de Poisson et équivalent de Θ . . . 325
Formule de Poisson et fonction Θ . . . 330
3.5 Développements d'informatiques . . . 334
Tri par tas . . . 334
Master Theorem . . . 338
Indécidabilité de la validité d'une formule en logique du premier ordre . . . 340
Machine de Turing $\Longrightarrow$ μ-recursif . . . 344
Transformation de Tseitin . . . 347
Théorème de Cook . . . 351
B-arbres . . . 355
Cocke–Younger–Kasami . . . 359
Tri topologique . . . 363
Automate des occurrences . . . 366
3–Coloration d'un graphe . . . 369
μ-recursive $\Longrightarrow$ λ-définissable . . . 372
Décidabilité de l'arithmétique de Presburger . . . 376
Décidabilité de l'arithmétique de Presburger (Version à ne pas faire) . . . 379
Équivalence entre sémantiques opérationnelles . . . 382
Complétude de la logique de Hoare . . . 387
Théorème de Scott–Curry . . . 392
Caractérisation de Premier pour l'analyse $LL(1)$ . . . 395
Indécidabilité de la satisfiabilité d'une requête . . . 399
3.6 Autres développements . . . 405
Prolongement de la fonction Zéta de Riemann . . . 405
Générateurs de $GL_n(\mathbb{Z})$ . . . 413
Théorème de Structure des groupes abéliens finis . . . 416
Invariants de similitude . . . 419
Knuth Morris Pratt (Complexité) . . . 423
Caractérisation de RE . . . 426
3.7 Liste de pleins de développements . . . 428
3.7.1 Livre coécrit . . . 428
3.7.2 Développements de mathématiques . . . 429
3.7.3 Développements d'informatique . . . 433

4 Mon mémoire sur la leçon 223 **435**

5 Compte-rendu oraux **448**
5.1 Oral d'informatique . . . 448
5.2 Oral de modélisation . . . 452
5.3 Oral de mathématiques . . . 455

6 Appendice **458**
6.1 Maths . . . 458
Conventions Transformation de Fourier . . . 458
Théorèmes classiques . . . 460
Exercices classiques . . . 461
Théorèmes de densité dans les L^p . . . 465
Compacité en dimension finie . . . 466
Théorèmes de dimension d'un espace vectoriel . . . 467
D'Alembert Gauss avec Théorème d'Inversion Locale . . . 469
Inversion de Pascal et nombre de surjections . . . 470
La fonction de répartition F_X caractérise la loi de X . . . 472
Lien entre irréductibles de $\mathbb{Q}[X]$ et de $\mathbb{Z}[X]$ . . . 476
Le polynôme minimal est irréductible . . . 477
Equivalence des normes non respectée . . . 478
6.2 Informatique . . . 480
Borne inférieure Complexité des tris par comparaisons . . . 480
Algorithmes classiques . . . 481
Schémas algorithmiques . . . 483
Propriétés de clôture des langages rationnels et algébriques . . . 484
Problèmes NP-complets . . . 485
2Sat est dans P . . . 488
Réductions classiques . . . 490
Problèmes indécidables et réduction . . . 491
Fonctions primitives récursives usuelles . . . 496
Sémantiques du langage de programmation IMP . . . 500
Règles de la sémantique opérationnelle à grands pas . . . 505
Règles de la sémantique opérationnelle à petits pas . . . 506
Règles de la logique de Hoare . . . 507
λ-calcul . . . 508
Bases de données . . . 512

Index **517**
Index mathématique . . . 517
Index informatique . . . 520

Bibliographie **523**

INTRODUCTION ET CONSEILS

J'ai regroupé dans ce document tout ce que j'ai construit durant mon année d'agrégation 2018/2019 en préparation à l'Université Rennes 1 et l'École Normale Supérieure de Rennes. Il y a donc mes **couplages**, mes **plans** plus ou moins détaillés de leçons et mes **développements**. J'y ai ajouté une **liste des différents développements** que j'ai croisés ou que certains de mes amis ont fait. Enfin, en bonus, je vous ai mis plusieurs documents en **appendice** que j'ai rédigé après les avoir mis en forme pendant l'agrégation.

Je voudrais remercier Emilie Tezenas, Maxence Brévard, Clarence Kineider, David Xu, Julie Parreaux, Théo Untrau, Vincent Béhani, Rémi Moreau, François Ernoult, Thomas Cavallazzi, Bastien Jean, Antoine Sabut, Antoine Leblond avec qui j'ai passé l'agrégation et grâce à qui j'ai pu écrire tout ce qui va suivre suite à de nombreuses discussions et de confrontations de nos développements.

Merci beaucoup aux professeurs qui nous ont encadrés pendant toute la préparation : Matthieu Romagny, Thibaut Deheuvels, François Schwarzentruber, Lilian Besson, Sophie Pinchinat, Nathalie Bertrand, Karine Beauchard, Jeremy Le Borgne, Agnès David et bien d'autres.

J'ai utilisé beaucoup d'idées qui étaient présentes dans les développements et plans de Antoine Mouzard, Aude Le Gluher, Théo Pierron, Fabrice Grela, Florian Lemonnier, Paul Alphonse, Adrien Fontaine et d'autres...

Merci à Emilie Tezenas pour son aide pour tous les développements de la section "Plein de développements".

Je voudrais remercier aussi Clémentine Laurens, Gaspard Tamagny, Mathias Déhais, Marie Trin et Gurvan Mével qui ont, en passant l'agrégation durant 2019/2020, corrigé de nombreuses coquilles qui se trouvaient dans le document.

Merci à Clémentine Laurens pour son aide dans la rédaction de nombreuses questions de plans et son avis précieux sur des questions de mises en page et autres facilités de lecture du document.

Un remerciement particulier à David Xu qui a fait la couverture de ce document et à François Ernoult qui a fait l'icône du livre pour ma page web.

Enfin merci à Lisa pour son aide, son appui et sa patience durant toute l'écriture folle de ce document.

Plan d'attaque de l'année que je propose (ce n'est pas forcément la meilleure idée et ce n'est pas le même pour tout le monde) :

- Commence à faire des leçons assez tôt, à regarder des développements, à revoir des notions du programme que tu as besoin de revoir, te plonger dans les livres petit à petit.
- Fais tes couplages de maths pendant les vacances de la Toussaint, même si tu ne rédiges pas les développements, il faut au moins avoir une idée de ce qui est faisable en regardant en diagonale les exemples de développements des années précédentes, les couplages vont forcément bouger, ce n'est pas définitif, mais c'est bien d'avoir une bonne base, ensuite en faisant chaque développement tu te rendras compte de ce que tu aimes et ce que tu aimes moins, de ce que tu es capable et de ce qui est trop compliqué.
- Fin novembre, il faut avoir vu au moins une fois chaque développement qui seront dans les leçons à préparer pour les oraux de janvier
- Prépare au mieux les oraux blancs de janvier durant décembre
- Commence à faire des plans de maths pour te remettre dans le bain après les oraux blancs
- Pendant les vacances de février, tu peux faire des débuts de sujets (2h) pour être efficace sur la rédaction de début de copie
- Un mois et demi avant les écrits, reprends le programme officiel et surligne toutes les notions que tu veux revoir, et travaille-les dans les livres en te mettant un ordre de priorité des notions
- Prends des vacances après les écrits, c'est important
- Fais tes couplages d'infos dans les deux semaines qui suivent les écrits
- Travaille tes développements et plan d'info
- Après les oraux d'info, reprends les maths, en révisant développements et plans.

Conseils :

- Connais tes développements sur le bout des doigts
- Entraîne-toi sur tes développements en écrivant et en parlant à voix haute en même temps
- Aies réfléchi à un plan pour chaque leçon (même si c'est inspiré d'autres plans existants, le tout c'est d'être content de la cohérence du plan que tu feras peut-être avec des patchworks de plein de plans différents)
- Fais-toi des plannings avec les notions qu'il faut revoir avec des plages horaires, les cours auxquels tu veux aller, les leçons, etc...
- Incorpore tes développements le mieux possible dans tes plans, c'est très important

Attention :

- Les développements et plans que je présente ici sont ceux avec lesquels je suis allé à l'agreg
- Tout cela est assez personnel, cela peut ne pas convenir à tout le monde, c'est une question de choix et de goût ! (notamment le fait de faire ces couplages à la Toussaint)
- Quand je mets trois développements dans une leçon, j'en propose seulement 2 le jour J ceux sur lesquels je suis le plus à l'aise (tout en mettant les autres développements dans le plan mais sans les référencer comme développements)
- Il peut y avoir des erreurs (n'hésitez pas à me le dire dans ce cas pour que je corrige le plus tôt possible)

Si tu trouves une erreur, une typo, une faute d'orthographe, n'hésite pas à m'envoyer un mail pour que je corrige et que ça serve pour les prochains :

pierre.le-barbenchon@ens-rennes.fr

Voilà, maintenant fonce, et fais-toi plaisir ! ! !

CHAPITRE 1

COUPLAGES

1.1 Couplages d'algèbre

101 Groupe opérant sur un ensemble. Exemples et applications.

— Isométries du cube et du tétraèdre

— Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

---

104 Groupes finis. Exemples et applications.

— Isométries du cube et du tétraèdre

— Automorphismes de $\mathfrak{S}_n$

— Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

---

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

— Isométries du cube et du tétraèdre

— Automorphismes de $\mathfrak{S}_n$

---

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

— Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

— Etude du groupe $O(p, s)$

---

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

— Automorphismes de $\mathfrak{S}_n$

— Générateurs de $SL_2(\mathbb{Z})$

— Isométries du cube et du tétraèdre

---

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

— Primalité des nombres de Mersenne

— Théorème de Fermat modulaire

---

121 Nombres premiers. Applications.

— Primalité des nombres de Mersenne
— Loi de réciprocité quadratique
— Théorème de Fermat modulaire

---

123 Corps finis. Applications.

— Primalité des nombres de Mersenne
— Loi de réciprocité quadratique

---

126 Exemples d'équations en arithmétique.

— Loi de réciprocité quadratique
— Théorème de Fermat modulaire
— Théorème de Carathéodory

---

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

— Primalité des nombres de Mersenne
— Irréductibilité des polynômes cyclotomiques

---

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

— Translatés d'une fonction $\mathcal{C}^1$
— Théorème de Carathéodory

---

152 Déterminant. Exemples et applications.

— Convergence de polygones vers l'isobarycentre
— Théorème des extrema liés

---

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

— Décomposition de Dunford
— Image de l'exponentielle

---

156 Exponentielle de matrices. Applications.

— Etude du groupe $O(p, s)$
— Image de l'exponentielle

---

157 Endomorphismes trigonalisables. Endomorphismes nilpotents.

— Décomposition de Dunford
— Méthode QR

---

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

— Théorème des extrema liés
— Morphismes d'algèbre de $\mathcal{C}(K, \mathbb{R})$ sur $\mathbb{R}$
— Translatés d'une fonction $\mathcal{C}^1$

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

— Méthode QR

— Méthode de gradient à pas optimal

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

— Loi de réciprocité quadratique

— Etude du groupe $O(p, s)$

182 Applications des nombres complexes à la géométrie.

— Convergence de polygones vers l'isobarycentre

— Générateurs de $SL_2(\mathbb{Z})$

183 Utilisation des groupes en géométrie.

— Isométries du cube et du tétraèdre

— Générateurs de $SL_2(\mathbb{Z})$

190 Méthodes combinatoires, problèmes de dénombrement.

— Loi de réciprocité quadratique

— Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

— Nombres de Bell

— Théorème de Fermat modulaire

1.2 Couplages d'analyse

203 Utilisation de la notion de compacité.

— Cauchy Lipschitz et lemme de Gronwall

— Morphismes d'algèbre de $\mathcal{C}(K, \mathbb{R})$ sur $\mathbb{R}$

---

208 Espaces vectoriels normés, applications linéaires continues. Exemples.

— Cauchy Lipschitz et lemme de Gronwall

— Banach–Steinhaus

---

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

— Image de l'exponentielle

— Théorème des extrema liés

---

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

— Méthode de Newton

— Méthode de gradient à pas optimal

— Théorème des extrema liés

---

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

— Cauchy Lipschitz et lemme de Gronwall

— Nombres de zéros des solutions d'une équation différentielle

---

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

— Translatés d'une fonction $\mathcal{C}^1$

— Nombres de zéros des solutions d'une équation différentielle

---

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

— Méthode de Newton

— Réciproques partielles de Césaro

---

224 Exemples de développements asymptotiques de suites et de fonctions.

— Formule de Poisson et équivalent Θ

— Nombres de zéros des solutions d'une équation différentielle

---

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

— Méthode de Newton

— Méthode de gradient à pas optimal

— Convergence de polygones vers l'isobarycentre

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

— Méthode de Newton

— Translatés d'une fonction $\mathcal{C}^1$

229 Fonctions monotones. Fonctions convexes. Exemples et applications.

— Méthode de Newton

— Méthode de gradient à pas optimal

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

— Nombres de Bell

— Réciproques partielles de Césaro

233 Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples.

— Méthode QR

— Méthode de gradient à pas optimal

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

— Formule des compléments

— Formule d'inversion de la fonction caractéristique

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

— Formule des compléments

— Formule de Poisson et Shannon

— Formule d'inversion de la fonction caractéristique

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

— Formule de Poisson et équivalent Θ

— Nombres de Bell

246 Séries de Fourier. Exemples et applications.

— Banach–Steinhaus

— Formule de Poisson et application au choix

250 Transformation de Fourier. Applications.

— Formule d'inversion de la fonction caractéristique

— Formule de Poisson et Shannon

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

— Formule d'inversion de la fonction caractéristique
— Théorème Central Limite

---

264 Variables aléatoires discrètes. Exemples et applications.

— Formule d'inversion de la fonction caractéristique
— Théorème Central Limite

---

265 Exemples d'études et d'applications de fonctions usuelles et spéciales.

— Formule des compléments
— Formule de Poisson et fonction Θ

1.3 Couplages d'informatique

901 Structures de données. Exemples et applications.

— Tri par tas

— B-arbres

---

903 Exemples d'algorithmes de tri. Correction et complexité.

— Tri par tas

— Tri topologique

---

907 Algorithmique du texte. Exemples et applications.

— Automate des occurrences

— Cocke-Younger-Kasami

---

909 Langages rationnels et automates finis. Exemples et applications.

— Automate des occurrences

— Décidabilité de Presburger

---

912 Fonctions récursives primitives et non primitives. Exemples.

— Machine de Turing $\implies$ μ-recursif

— μ-recursif $\implies$ λ-définissable

---

913 Machines de Turing. Applications.

— Machine de Turing $\implies$ μ-recursif

— Théorème de Cook

---

914 Décidabilité et indécidabilité. Exemples.

— Indécidabilité de la validité d'une formule du premier ordre

— Décidabilité de Presburger

— Indécidabilité de la satisfiabilité d'une requête

---

915 Classes de complexité. Exemples.

— Théorème de Cook

— 3-Coloration d'un graphe

— Cocke-Younger-Kasami

---

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

— Théorème de Cook

— Transformation de Tseitin

---

918 Systèmes formels de preuve en logique du premier ordre. Exemples.

IMPASSE

921 Algorithmes de recherche et structures de données associées.
— Automate des occurrences
— B-arbres

923 Analyses lexicale et syntaxique. Applications.
— Cocke-Younger-Kasami
— Caractérisation de PREMIER pour l'analyse $LL(1)$

924 Théories et modèles en logique du premier ordre. Exemples.
— Indécidabilité de la validité d'une formule du premier ordre
— Décidabilité de Presburger

925 Graphes : représentations et algorithmes.
— 3-Coloration d'un graphe
— Tri topologique

926 Analyse des algorithmes : complexité. Exemples.
— Tri par tas
— Master Theorem

927 Exemples de preuve d'algorithme : correction, terminaison.
— Complétude de la logique de Hoare
— Tri topologique

928 Problèmes NP-complets : exemples et réduction.
— Théorème de Cook
— 3-Coloration d'un graphe
— Transformation de Tseitin

929 Lambda-calcul pur comme modèle de calcul. Exemples.
— μ-recursif $\implies$ λ-définissable
— Théorème de Scott–Curry

930 Sémantique des langages de programmation. Exemples.
— Équivalence entre sémantiques opérationnelles
— Complétude de la logique de Hoare

931 Schémas algorithmiques. Exemples et applications.
— Master Theorem
— Cocke-Younger-Kasami

932 Fondements des bases de données relationnelles.
— B-arbres
— Indécidabilité de la satisfiabilité d'une requête

CHAPITRE 2

PLANS DE LEÇONS

2.1 Conseils

— C'est vous qui choisissez le niveau de votre leçon

— Ne mettre que des choses que l'on maitrise !

— Ce n'est pas obligatoire de remplir les 3 pages

— Il vaut mieux avoir moins de pages mais que des choses que l'on maitrise

— Je vous présente ici mes plans, ils sont loin d'être parfait

— Ils ne sont d'ailleurs là que pour vous aider et vous guider, il faut que vous vous appropriiez des leçons [1]

— Personnalisez vos plans, car c'est finalement très personnel et c'est que comme ça que vous ferez un travail en profondeur !

— Le jury n'est pas obligé d'être d'accord avec vos choix (dans une certaine mesure), mais votre but est de montrer que vous avez réfléchi à l'agencement de votre plan et que vous savez justifier vos choix.

ATTENTION : Ici, je mets le squelette de mes plans, ils sont volontairement très légers [2], c'est juste pour aider, donner les grandes parties et l'articulation des idées. En aucun cas, il ne faut les utiliser tel quel. Il ne reste plus qu'à les travailler ! [3]

1. tiens, ça fait deux "i" collés, c'est rigolo
2. certains plus que d'autres, en fonction du temps de travail dessus
3. Autrement dit tout faire

2.2 Mes références préférées

Il y a beaucoup de références dans les plans qui vont suivre, certaines références sont utiles que pour certains tout petits détails et donc sont dispensables en fonction des plans que l'on fait. Les références que j'utilise sont parfois personnelles et ne conviennent pas à tout le monde. Par exemple, *Algebraic Number Theory* de I.Stewart et D.Tall était un livre sur lequel j'avais travaillé en stage donc je l'aime bien mais il nécessite d'y passer du temps, un temps qui pourrait être consacré à d'autres choses utiles aussi, donc tout est une question de choix personnels. Cependant je vous mets tout de même mes références préférées qui peuvent vous guider dans ce que vous aimez et n'aimez pas en terme de livres.

Pour les livres de bases de maths, mes incontournables sont :

— Gourdon Algèbre [GOU08a]
— Gourdon Analyse [GOU08b]
— Perrin (Cours d'Algèbre) [PER96]
— Hauchecorne (Les contre-exemples) [HAU07]
— Grifone (Algèbre Linéaire) [GRI11]
— les Oraux X-ENS [FGN03] [FGN13b] [FGN14] [FGN12] [FGN18] [FGN09] [FGN13a]
— Rouvière (Petit Guide du Calcul Diff) [ROU09]
— Ulmer (Théorie des groupes) [ULM12]

Ensuite pour les domaines plus spécifiques, mes coups de coeur sont :

— Pour les équations différentielles, le Benzoni-Gavage [BG10]
— Pour les distributions, le Lesfari [LES12]
— Pour les séries de Fourier et la transformée de Fourier, le El Amrani [EA08]
— Pour les fonctions usuelles et spéciales, le Jolissaint [JOL16]
— Pour l'analyse numérique, le Quarteroni [QSS07]
— Pour la théorie algébrique des nombres, le Stewart and Tall [ST15]

Pour les livres de bases d'informatique, mes incontournables sont :

— Carton [CAR14]
— Cormen [CLRS10]
— Lassaigne-Rougemont [LDR93]

Ensuite pour les domaines plus spécifiques, mes coups de coeur sont :

— Pour la sémantique, le Nielson & Nielson [NN07]
— Pour la logique du premier ordre, le David Nour Raffalli [DNR04]
— Pour l'analyse lexicale et syntaxique, le Legendre, Schwarzentruber [LS15]
— Pour la NP-complétude, le Garey Johnson [GJ79]

2.3 Métaplans d'algèbre

Leçon 101
Groupe opérant sur un ensemble. Exemples et applications.

Rapport du jury :

Dans cette leçon, il faut bien dominer les deux approches de l'action de groupe : l'approche naturelle et l'approche *via* le morphisme du groupe agissant vers le groupe des permutations de l'ensemble sur lequel il agit. La formule des classes et ses applications immédiates sont incontournables. Des exemples de natures différentes doivent être présentés : actions sur un ensemble fini, sur un espace vectoriel (en particulier les représentations), sur un ensemble de matrices, sur des groupes ou des anneaux. Les exemples issus de la géométrie ne manquent pas (groupes d'isométries d'un solide ou d'un polygone régulier). Il est important de savoir calculer des stabilisateurs et des orbites notamment dans le cadre de l'action par conjugaison. Les théorèmes de Sylow peuvent avoir leur place dans cette leçon.

Parmi les applications des actions de groupes, on pourra citer des résultats de dénombrement, comme par exemple la formule de Lucas qui permet de calculer efficacement les cœfficients binomiaux.

S'ils le désirent, les candidats peuvent aller plus loin en décrivant les actions naturelles de $PGL(2, \mathbb{F}_q)$ sur la droite projective, ou de $SL_2(\mathbb{Z})$ sur le demi-plan de Poincaré.

En notant que l'injection du groupe de permutations dans le groupe linéaire par les matrices de permutations donne lieu à des représentations, ils pourront facilement en déterminer le caractère.

Questions possibles :

- Démontrer la relation orbite/stabilisateur.

Plan détaillé :

I - Actions de groupes
  1) Définitions
     Les deux façons de voir des actions de groupes
  2) Orbites et stabilisateurs
     Définition
     Transitive
     Libre
     etc.
  3) Formules usuelles
     Relation Orbite/Stabilisateur
     Formule des classes
     Formule de Burnside

II - Actions naturelles
  1) Par translation
     Définition

Description du stabilisateur

2) Par conjugaison

Définition

Description du stabilisateur

Exemple : utilisation du centralisateur dans les Automorphismes de $\mathfrak{S}_n$

III - Actions de groupes et algèbre linéaire

1) Par équivalence

Définition

Invariance du rang

2) Par similitude

Définition

Invariance du rang, de la trace, du déterminant

Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

Invariants de similitudes

3) Par congruence

Formes quadratiques

IV - Action de groupes et géométrie

1) Isomorphismes exceptionnels

Dénombrement

Isomorphismes exceptionnels [CG18, p.49]

2) Espace affine

Angles orientés [TAU05]

3) Isométries

Isométries du cube et du tétraèdre

Développements :

- Isométries du cube et du tétraèdre
- Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

Références :

♥♥♥ - [ULM12] Félix ULMER, *Théorie des Groupes*

♥♥♥ - [CAL98] Josette CALAIS, *Éléments de Théorie des Groupes*

♥♥ - [CG18] Philippe CALDERO et Jerôme GERMONI, *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2*

♥ - [TAU05] Patrice TAUVEL, *Géométrie*

Leçon 104
Groupes finis. Exemples et applications.

Rapport du jury :

Dans cette leçon il faut savoir manipuler correctement les éléments de différentes structures usuelles ($\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{S}_n$, etc.) comme, par exemple, en proposer un générateur ou une famille de générateurs, savoir calculer un produit de deux permutations, savoir décomposer une permutation en produit de cycles à supports disjoints. Il est important que la notion d'ordre d'un élément soit mentionnée et comprise dans des cas simples. Le théorème de structure des groupes abéliens finis doit être connu. Il est bon de connaître les groupes d'ordre p et p^2 pour p premier ainsi que les groupes d'ordre inférieur à 8.

Les exemples doivent figurer en bonne place dans cette leçon. Les groupes d'automorphismes fournissent des exemples très naturels. On peut aussi étudier les groupes de symétries $\mathfrak{A}_4$,$\mathfrak{S}_4$, $\mathfrak{A}_5$ et relier sur ces exemples géométrie et algèbre, les représentations ayant ici toute leur place ; il est utile de connaître les groupes diédraux.

S'ils le désirent, les candidats peuvent ensuite mettre en avant les spécificités de groupes comme le groupe quaternionique, les sous-groupes finis de $SU(2)$ ou les groupes $GL_n(\mathbb{F}_q)$.

Questions possibles :

- Quels sont tous les groupes d'ordre 8 ?
  Réponse : voir [ULM12]
- Pourquoi $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?
  Réponse : regarder les éléments d'ordre 4
- Donner un exemple de sous-groupe non distingué.
  Réponse : $< (1,2) >$ n'est pas distingué dans $\mathfrak{S}_n$.
- Prouver que si $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}$, alors n et m sont premiers entre eux.
- Démontrer que si G est un groupe d'ordre 200, alors il existe un sous-groupe distingué d'ordre 25.
- Soit G un groupe. $Int(G)$ est-il un sous-groupe distingué de $Aut(G)$?
  Réponse : Oui.
- Exprimer $Int(G)$ sous la forme d'un quotient.
  Réponse : $Int(G) = G/Z(G)$.

Plan détaillé :

I - Théorie des groupes finis [ULM12]
  1) Définitions
     Ordre
  2) Lagrange
     $|G| = [G : H]|H|$
  3) Actions de groupe

II - Groupes abéliens [COM98]
  1) Groupe cyclique

$\mathbb{Z}/n\mathbb{Z}$

2) Théorème de structure

existence et unicité

III - Groupes non abéliens

1) Groupe symétrique [PER96]

Automorphismes de $\mathfrak{S}_n$

2) Géométrie

Groupes diédraux [ULM12]

Isométries affines [CG18]

Isométries du cube et du tétraèdre

3) Groupe Linéaire sur les corps finis

Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

Développements :

- Isométries du cube et du tétraèdre
- Dénombrement des matrices diagonalisables de $\mathbb{F}_q$
- Automorphismes de $\mathfrak{S}_n$

Références :

♥♥♥ - [ULM12] Félix ULMER, *Théorie des Groupes*

♥♥♥ - [COM98] François COMBES, *Algèbre et Géométrie*

♥♥ - [PER96] Daniel PERRIN, *Cours d'Algèbre*

♥♥ - [CG18] Philippe CALDERO et Jerôme GERMONI, *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2*

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

Rapport du jury :

Parmi les attendus, il faut savoir relier la leçon avec les notions d'orbites et d'actions de groupes. Il faut aussi savoir décomposer une permutation en cycles à supports disjoints, tant sur le plan théorique (preuve du théorème de décomposition), que pratique (sur un exemple). Il est important de savoir déterminer les classes de conjugaisons du groupe symétrique par la décomposition en cycles, d'être capable de donner des systèmes de générateurs.

L'existence du morphisme signature est un résultat non trivial mais ne peut pas constituer, à elle seule, l'objet d'un développement. Il est bon d'avoir en tête que tout groupe fini se plonge dans un groupe symétrique et de savoir calculer la signature des permutations ainsi obtenues dans des cas concrets.

Les applications sont nombreuses, il est très naturel de parler du déterminant, des polynômes symétriques ou des fonctions symétriques des racines d'un polynôme.

On peut également parler du lien avec les groupes d'isométries des solides.

S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant aux automorphismes du groupe symétrique, à des problèmes de dénombrement, aux représentations des groupes des permutations ou encore aux permutations aléatoires.

Questions possibles :

- Peut-on engendre $\mathfrak{S}_n$ avec moins de $n-1$ transpositions ?

  Réponse : non, il faut que le graphe des entiers de 1 à n avec comme arêtes les transpositions soit connexe !
- Calculer le nombre de dérangements de $\mathfrak{S}_n$. (Un dérangement est un $\sigma \in \mathfrak{S}_n$ tel que $\sigma(i) \neq i$ pour tout $i \in [\![1, n]\!]$)
- Soit la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$. Calculer σ^2019.
- Donner tous les morphismes de $(\mathfrak{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$.
- On sait que $\forall n \neq 6$, $Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$. Que se passe-t-il pour $n = 6$?
- Donner une idée de la preuve de la simplicité de $\mathfrak{A}_5$.
- S_4 est-il simple ?

  Réponse : non

Points essentiels :

- Système de générateurs avec des utilisations précises

Plan détaillé :

I - Généralités sur les permutations [CAL98] [PER96]

1) Définitions

bijection

$\mathfrak{S}_n$

Action

Support

Transposition

Cycle

Décomposition unique en cycle à support disjoints

Théorème de Cayley

2) Morphisme signature

Définition signature

Prop : seul morphisme non trivial

Déf : $\mathfrak{A}_n$

II - Structure de $\mathfrak{S}_n$ et $\mathfrak{A}_n$ [PER96]

1) Générateurs

(ij) pour $i \neq j$

$(1i)$ pour $i \in \{2, \dots, n\}$

$(i\ i+1)$ pour $i \in \{1, \dots, n-1\}$

(12) et $(123\dots n)$

2) Automorphismes

Definition

Intérieur

Automorphismes de $\mathfrak{S}_n$

3) $\mathfrak{A}_n$

D'indice 2

3-cycle engendrent $\mathfrak{A}_n$

A_n est simple pour $n \neq 4$

c'est le groupe dérivé de $\mathfrak{S}_n$

III - Applications

1) Déterminant [GOU08a]

Forme n-linéaire alternée

Définition du déterminant

Formule du déterminant

2) Action de groupes [CG18]

Groupe des isométries

Isométries du cube et du tétraèdre

Nombre de coloriages du cube

3) Polynomes symétriques [GOU08a]

Définition

Développements :

- Automorphismes de $\mathfrak{S}_n$
- Isométries du cube et du tétraèdre

Références :

♥♥♥ - [PER96] Daniel PERRIN, *Cours d'Algèbre*

♥♥♥ - [CAL98] Josette CALAIS, *Éléments de Théorie des Groupes*

♥♥♥ - [ULM12] Félix ULMER, *Théorie des Groupes*

♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*

♥♥ - [CG18] Philippe CALDERO et Jerôme GERMONI, *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2*

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

Rapport du jury :

Cette leçon ne doit pas se résumer à un catalogue de résultats épars sur $GL(E)$. Il est important de savoir faire correspondre les sous-groupes du groupe linéaire avec les stabilisateurs de certaines actions naturelles (sur des formes quadratiques, symplectiques, sur des drapeaux, sur une décomposition en somme directe, etc.). On doit présenter des systèmes de générateurs de $GL(E)$ et étudier la topologie de ce groupe en précisant pourquoi le choix du corps de base est important. Les liens avec le pivot de Gauss sont à détailler. Il faut aussi savoir réaliser $\mathfrak{S}_n$ dans $GL(n,\mathbb{K})$ et faire le lien entre signature et déterminant, et entre les classes de conjugaison et les classes de similitude.

S'ils le désirent, les candidats peuvent aller plus loin en remarquant que la théorie des représentations permet d'illustrer l'importance de $GL_n(\mathbb{C})$ et de son sous-groupe unitaire.

Questions possibles :

- Quelle forme a une matrice de $\mathcal{O}_2(\mathbb{R})$?
- Enumérer les sous-groupes finis de $SO_3(\mathbb{R})$.
  Réponse : $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{D}_n$, $\mathfrak{A}_4$, S_4, $\mathfrak{A}_5$.
- De quelle topologie peut-on munir un groupe fini ?
  Réponse : La topologie discrète, qui a la propriété de rendre le groupe compact pour cette topologie.
- Montrer que $O_n(\mathbb{R})$ peut être plongé dans $SO_{n+1}(\mathbb{R})$.
- Tout groupe fini peut-il être plongé dans un $SO_n(\mathbb{R})$?
  Réponse : Oui
- Montrer que $\mathfrak{S}_n$ se plonge dans $\mathfrak{A}_{n+2}$ mais pas dans $\mathfrak{A}_{n+1}$.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Groupe Linéaire en algèbre linéaire [PER96] [GRI11]
- Cadre $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, E de dimension finie n
- Définition
- Isomorphisme matriciel et application linéaire
- Action de groupe (équivalence, similitude)
- Matrices de permutations

II - Générateurs de $GL(E)$ et $SL(E)$ [PER96]
- Définition de $SL_n(\mathbb{K})$
- Définition dilatation / transvection
- Théorème : transvections et dilatations engendrent $GL(E)$
- Corollaire : transvections engendrent $SL(E)$
- Déf : Centre

Déf : $PGL(E)$ et $PSL(E)$

III - Sur les corps finis [CG18]

Dénombrement de $GL_n(\mathbb{F}_q)$

Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

Isomorphismes exceptionnels [CG18, p.49]

IV - Groupe orthogonal [PER96]

Définition $O(E)$

Décomposition polaire

$O_n(\mathbb{K})$ compact

$O_n(\mathbb{K})$ groupe maximal

Définition $SO(E)$

Etude du groupe $O(p,s)$

Réflexion, renversement

Classification en dimension 2 et 3 sur $\mathbb{R}$

V - Topologie de $GL(E)$

$GL_n(\mathbb{K})$ est ouvert dans $\mathcal{M}_n(\mathbb{K})$

$GL_n(\mathbb{K})$ est dense dans $\mathcal{M}_n(\mathbb{K})$

$GL_n(\mathbb{C})$ est connexe par arcs (contrairement à $GL_n(\mathbb{R})$)

$O_n(\mathbb{K})$ est compact

Développements :

- Etude du groupe $O(p,s)$
- Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

Références :

♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*

♥♥♥ - [PER96] Daniel PERRIN, *Cours d'Algèbre*

♥♥♥ - [GRI11] Joseph GRIFONE, *Algèbre Linéaire*

♥♥♥ - [CG18] Philippe CALDERO et Jerôme GERMONI, *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2*

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

Rapport du jury :

C'est une leçon qui doit être illustrée par des exemples très variés qui peuvent être en relation avec les groupes de permutations, les groupes linéaires ou leurs sous-groupes, comme $SL_n(\mathbb{K})$, $O_n(\mathbb{R})$ ou $SO_n(\mathbb{R})$. Les groupes $\mathbb{Z}/n\mathbb{Z}$, fournissent aussi des exemples intéressants. La connaissance de parties génératrices s'avère très utile dans l'analyse des morphismes de groupes ou pour montrer la connexité par arcs de certains sous-groupes de $GL_n(\mathbb{R})$ par exemple.

Tout comme dans la leçon 106, la présentation du pivot de Gauss et de ses applications est envisageable. Il est important de présenter les différents systèmes de générateurs du groupe symétrique et de savoir mettre en évidence l'intérêt du choix de ces systèmes dans divers exemples.

Le candidat pourra également parler des générateurs du groupe diédral et, si il le souhaite, il pourra donner une présentation par générateurs et relations d'un groupe (groupe diédral, groupe symétrique, ou groupe des tresses).

Il est également possible de parler du logarithme discret et de ces applications à la cryptographie (algorithme de Diffie-Hellman, cryptosystème de El Gamal).

Questions possibles :

- Existe-t-il des familles génératrices de $\mathbb{Z}$ de cardinal strictement supérieur à 1 et minimales (dans le sens où, si l'on retire l'un quelconque des éléments de cette famille, elle n'est plus génératrice) ?

  Réponse : Oui : par exemple, $(2, 3)$ est une telle famille génératrice de $\mathbb{Z}$.
- Démontrer qu'on peut en réalité construire des familles génératrices de $\mathbb{Z}$ minimales de n'importe quel cardinal.
- Enumérer les groupes abéliens d'ordre 600.
- Expliciter la construction de S_3 par générateurs/relations.
- Donner tous les sous groupes d'ordre 6.

  Réponse : $\mathfrak{S}_3$ et $\mathbb{Z}/6\mathbb{Z}$
- Montrer à l'aide des transvections que $SL_n(K)$ est connexe par arcs.

  Réponse : Indice : Il faut montrer que $SL_n(K)$ est étoilé par rapport à I_n.
- La matrice $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ est-elle une matrice de transvection ?

Motivations :

Les parties génératrices de groupe sont très importantes car elles ont plusieurs avantages : de représenter un groupe de manière simple, avec un système de générateurs et des relations (exemple : groupe diédral), de faciliter les preuves de certaines propriétés (il suffit parfois de prouver des résultats sur un système de générateur, comme la surjectivité d'un morphisme par exemple [4]). J'ai choisi de séparer mon plan en 3 grandes parties, une première sur les groupes abéliens fini (qui sont simples à étudier grâce au théorème de structure des groupes abéliens finis), les groupes finis mais qui ne sont pas abéliens (comme $\mathfrak{S}_n$ ou $\mathbb{D}_n$) et enfin les groupes infinis (comme $GL_n(\mathbb{R})$ ou $SL_n(\mathbb{R})$).

4. voir la surjectivité de l'action de groupe dans le développement Isométries du cube et du tétraèdre

Plan détaillé :

I - Groupes abéliens finis [PER96] [COM98]

$\mathbb{Z}/n\mathbb{Z}$

Groupes cycliques

Groupes monogènes

$\mathbb{F}_q^\times$ est cyclique

Générateurs de $\mathbb{Z}/n\mathbb{Z}$

$\mathrm{Aut}(\mathfrak{S}_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Théorème de structure des groupes abéliens finis

II - Groupes non abéliens finis

1) Groupe symétrique [ULM12]

Systèmes de générateurs

Isométries du cube et du tétraèdre

Automorphismes de $\mathfrak{S}_n$

$\mathfrak{A}_n$ engendré par les 3-cycles

2) Groupe diédral [ULM12] [CAL98]

Système de générateurs

Présentation du groupe diédral avec r et s et les formules qui les lient

III - Groupes infinis

Groupe linéaire $GL(E)$ engendré par les transvections et dilatations [PER96]

$SL(E)$ engendré par les transvections

$O(E)$, $SO(E)$

Générateurs de $SL_2(\mathbb{Z})$

Remarques :

Je mets les deux développements isométries et automorphismes car ils rentrent dans cette leçon, mais ce serait maladroit de mettre que des développements autour du groupe symétrique, d'où la nécessité[5] de mettre un autre développement sur un autre sujet (ici, générateurs de $SL_2(\mathbb{Z})$)

Développements :

- Générateurs de $SL_2(\mathbb{Z})$
- Automorphismes de $\mathfrak{S}_n$
- Isométries du cube et du tétraèdre

Références :

♥♥♥ - [PER96] Daniel PERRIN, *Cours d'Algèbre*

♥♥♥ - [ULM12] Félix ULMER, *Théorie des Groupes*

♥♥♥ - [COM98] François COMBES, *Algèbre et Géométrie*

♥♥♥ - [CAL98] Josette CALAIS, *Éléments de Théorie des Groupes*

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

Rapport du jury :

Dans cette leçon, l'entier n n'est pas forcément un nombre premier. Il est utile de connaître et d'étudier le groupe des inversibles de l'anneau et les idéaux de $\mathbb{Z}/n\mathbb{Z}$.

Il est nécessaire de bien maîtriser le théorème chinois et sa réciproque. S'ils le désirent, les candidats peuvent poursuivre en donnant une généralisation du théorème chinois lorsque deux éléments ne sont pas premiers entre eux, ceci en faisant apparaître le PGCD et le PPCM de ces éléments.

Il faut bien sûr savoir appliquer le théorème chinois à l'étude du groupe des inversibles et, ainsi, retrouver la multiplicativité de l'indicatrice d'Euler. Toujours dans le cadre du théorème chinois, il est bon de distinguer clairement les propriétés de groupes additifs et d'anneaux.

Enfin, il est indispensable de présenter quelques applications arithmétiques des propriétés des anneaux $\mathbb{Z}/n\mathbb{Z}$, telles que l'étude de quelques équations diophantiennes bien choisies. De même, les applications cryptographiques telles que l'algorithme RSA sont naturelles dans cette leçon.

S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant au calcul effectif des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$, au logarithme discret, ou à la transformée de Fourier rapide. Il est également possible de parler des nombres p-adiques.

Questions possibles :

- Quels sont les nilpotents de $\mathbb{Z}/n\mathbb{Z}$?
- Quels sont les idempotents de $\mathbb{Z}/n\mathbb{Z}$?

Plan détaillé :

I - Structure de $\mathbb{Z}/n\mathbb{Z}$

1) Structure de groupe [RB06]

Groupe cyclique

Sous-groupe de $\mathbb{Z}/n/Z$

Isomorphe à $\mathbb{U}_n$

Générateurs de $\mathbb{Z}/n\mathbb{Z}$

Théorème de Structure

2) Structure d'anneau [PER96]

Inversibles de $\mathbb{Z}/n\mathbb{Z}$

Indicatrice d'Euler φ

$\mathbb{Z}/n\mathbb{Z}$ est un corps SSI n premier

$\mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$

$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(n)\mathbb{Z}$

3) Théorème chinois [RB06] [LAM12b]

Morphisme d'anneau

$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}$ si $n \wedge m = 1$

Généralisation

Calcul de $\varphi(n)$ [PER96]

II - Arithmétique [LAM12b]

1) Résidus quadratiques [LAM12b]

symbole de legendre

-1 est un carré dans $\mathbb{F}_q$ SSI $q \equiv 1$ [4]

Corollaire : théorème des 2 carrés

Loi de Réciprocité Quadratique

2) Nombres premiers et système RSA [LAM12b]

Petit théorème de Fermat

Nombre de Carmichael

Thrm de Wilson

Système RSA et chiffrement

Primalité des nombres de Mersenne

Algorithme de Lehmer Lucas [SPR02]

3) Résolution d'équations [LAM12b]

Système de congruence

Résolution d'équation

Réduction modulaire

Théorème de Fermat modulaire

Développements :

- Primalité des nombres de Mersenne
- Théorème de Fermat modulaire

Références :

♥♥♥♥♥ - [LAM12b] Jean-Pierre LAMOITIER, *Arithmétique Modulaire*

♥♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*

♥♥♥ - [RB06] Jean-Jacques RISLER et Pascal BOYER, *Algèbre pour la licence 3 : Groupes, Anneaux, Corps*

♥♥ - [PER96] Daniel PERRIN, *Cours d'Algèbre*

♥♥♥ - [SPR02] Philippe SAUX-PICART et Éric RANNOU, *Cours de calcul formel, Corps finis, Systèmes polynomiaux, applications*

Leçon 121
Nombres premiers. Applications.

Rapport du jury :

Le sujet de cette leçon est très vaste. Aussi les choix devront être clairement motivés. La réduction modulo p n'est pas hors-sujet et constitue un outil puissant pour résoudre des problèmes arithmétiques simples. La répartition des nombres premiers est un résultat historique important qu'il faudrait citer. Sa démonstration n'est bien sûr pas exigible au niveau de l'agrégation.

Quelques résultats sur les corps finis et leur géométrie sont les bienvenus, ainsi que des applications en cryptographie.

Questions possibles :

- Exécuter le crible d'Eratosthène pour $n \leqslant 100$
- Trouver le PGCD de 1071 et 1029

  Réponse : 21, en utilisant l'algorithme d'Euclide
- Trouver des coefficients de Bézout de 120 et 23.

  Réponse : $-9 \times 120 + 47 \times 23 = 1$
- Montrer que la somme des inverses des nombres premiers diverge.

Plan détaillé :

I - Arithmétique dans $\mathbb{Z}$

1) Nombres premiers [GOU08a]

Définition d'un nombre premier

Définition de nombres premiers entre eux

Théorème de Bézout

Algorithme d'Euclide

Théorème de Gauss

2) Factorialité de $\mathbb{Z}$

Unicité de la décomposition en facteurs premiers

PGCD

PPCM

3) Répartition des nombres premiers

Prop : il y a une infinité de nombres premiers

Prop : il y a une infinité de nombres premiers jumeaux

Crible d'Eratosthène

Théorème de Dirichlet (faible et fort)

$\sum \frac{1}{p}$ diverge [FGN03]

lien avec la fonction ζ

$\pi(x) \sim \frac{x}{\log x}$ [DUV07]

II - Corps finis [PER96] [DUV07]
  1) Anneau $\mathbb{Z}/n\mathbb{Z}$ et corps finis
    Indicatrice d'Euler
    Prop : $\mathbb{Z}/n\mathbb{Z}$ corps SSI n premier
    Théorème de Wilson
    Caractéristique d'un corps
    Morphisme de Frobenius
    Construction des corps finis
  2) Les carrés de $\mathbb{F}_q$
    le nombre de carrés de $\mathbb{F}_q$ et de $\mathbb{F}_q^\times$
    (-1) est un carré SSI $q \equiv 1$ [4]
    Symbole de Legendre
    Théorème des deux carrés (cas premier)
    Loi de réciprocité quadratique
  3) Irréductibilité de polynômes
    Critère d'Eisenstein
    Critère modulaire
    Réciproque fausse $X^4 + 1$

III - Quelques familles de nombres premiers
  1) Nombres de Carmichael [SPR02]
    Petit théorème de Fermat
    Def Nombres de Carmichael
  2) Nombres de Fermat [COM98] [SPR02]
    Def
    Critère de primalité
  3) Nombres de Mersenne [SPR02]
    Primalité des nombres de Mersenne
    Algo de Lehmer Lucas

Développements :

- Théorème de Fermat modulaire
- Loi de réciprocité quadratique
- Primalité des nombres de Mersenne

Références :

♥♥♥ - [LAM12a] Jean-Pierre LAMOITIER, *Arithmétique Classique*

♥♥ - [PER96] Daniel PERRIN, *Cours d'Algèbre*

♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*

♥♥♥♥ - [DUV07] Daniel DUVERNEY, *Théorie des Nombres*

♥♥ - [COM98] François COMBES, *Algèbre et Géométrie*

♥♥ - [FGN03] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS, *Oraux X-ENS, Analyse 1*

♥♥♥ - [SPR02] Philippe SAUX-PICART et Éric RANNOU, *Cours de calcul formel, Corps finis, Systèmes polynomiaux, applications*

Leçon 123
Corps finis. Applications.

Rapport du jury :

Une construction des corps finis doit être connue et une bonne maîtrise des calculs dans les corps finis est indispensable. Les injections des divers $\mathbb{F}_q$ doivent être connues. Les applications des corps finis (y compris pour $\mathbb{F}_q$ avec q non premier !) ne doivent pas être oubliées, par exemple l'étude de polynômes à coefficients entiers et de leur irréductibilité peut figurer dans cette leçon. Le calcul des degrés des extensions et le théorème de la base télescopique sont incontournables. La structure du groupe multiplicatif doit aussi être connue. L'étude des carrés dans un corps fini et la résolution d'équations de degré 2 sont envisageables.

S'ils le désirent, les candidats peuvent aller plus loin en détaillant des codes correcteurs ou en étudiant l'irréductibilité des polynômes à coefficients dans un corps fini.

Questions possibles :

- Comment on montre que $\mathbb{F}_q^\times$ est cyclique ?
- Montrer que A/I est un corps si et seulement I est maximal.
- Que vaut $\left[\mathbb{F}_3[X]/\langle X^2+1\rangle : \mathbb{F}_3\right]$?
- Démontrer que si $q^d - 1 \mid q^n - 1$, alors $d \mid n$.
- Résoudre l'équation diophantienne $y^2 = 41x + 3, (x, y) \in \mathbb{Z}^2$.
- Expliciter un isomorphisme entre $\mathbb{F}_2[X]/(X^2+X+1)$ et $\mathbb{F}_2[X]/(X^3+X^2+1)$

Points essentiels :

- unicité des corps de rupture à isomorphisme (non unique) près
- les carrés dans les corps finis

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Construction des corps finis [PER96]
- Caractéristique
- Morphisme de Frobenius
- Corps de rupture
- Inclusions des corps finis

II - Etude sur les corps finis

1) Dénombrement et géométrie [CG18]
- Dénombrement de $GL_n(\mathbb{F}_q)$, $SL_n(\mathbb{F}_q)$, $PGL_n(\mathbb{F}_q)$, $PSL_n(\mathbb{F}_q)$
- Isomorphismes exceptionnels

2) Etude des carrés de $\mathbb{F}_q$ [PER96]
- Nombre de carrés dans $\mathbb{F}_q^\times$

$\mathbb{F}_q^\times$ cyclique

$(\mathbb{F}_q^\times)^2$ cyclique

Symbole de Legendre

(-1) est un carré SSI $q \equiv 1$ [4]

Théorème des deux carrés (cas premier)

Loi de réciprocité quadratique

III - Polynômes irréductibles sur $\mathbb{F}_q$ [PER96]

1) Critères irréductibles

Critère d'Eisenstein

Critère modulaire

Réciproque fausse $X^4 + 1$

Autres théorèmes d'irréductibilité de polynômes

2) Polynômes cyclotomiques

Définition

Irréductibilité des polynômes cyclotomiques

IV - Application au système RSA [SPR02]

But : Trouver des nombres premiers très très grands

Primalité des nombres de Mersenne

Algorithme de Lehmer Lucas

Explication système RSA [LAM12b]

Développements :

- Primalité des nombres de Mersenne
- Loi de réciprocité quadratique

Références :

♥♥♥♥ - [PER96] Daniel PERRIN, *Cours d'Algèbre*

♥♥ - [CG18] Philippe CALDERO et Jerôme GERMONI, *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2*

♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*

♥♥♥ - [LAM12b] Jean-Pierre LAMOITIER, *Arithmétique Modulaire*

♥♥♥ - [SPR02] Philippe SAUX-PICART et Éric RANNOU, *Cours de calcul formel, Corps finis, Systèmes polynomiaux, applications*

Leçon 126
Exemples d'équations en arithmétique

Rapport du jury :

Pour la session 2019, le titre de cette leçon devient **Exemples d'équations en arithmétique.** Ce nouvel intitulé traduit le souhait d'élargir le contexte de la leçon, au delà des seules équations sur $\mathbb{Z}$ pour étudier aussi des équations dans $\mathbb{Z}/n\mathbb{Z}$ et dans les corps finis.

Malgré le changement d'intitulé, les équations diophantiennes occupent une place importante et doivent absolument être abordées dans cette leçon. On doit présenter les notions de bases servant à aborder les équations de type $ax + by = d$ (identité de Bezout, lemme de Gauss) mais aussi bien entendu la méthode de descente de Fermat et l'utilisation de la réduction modulo un nombre premier p. La leçon peut aussi dériver vers la notion de factorialité, illustrée par des équations de type Mordell, Pell-Fermat, et même Fermat (pour $n = 2$, ou pour les nombres premiers de Sophie Germain). La résolution des systèmes linéaires sur $\mathbb{Z}$ peut être abordée.

Il est naturel de s'intéresser à la résolution des systèmes de congruences, à la recherche de racines carrées dans les corps finis. Les candidats peuvent plus généralement aborder la recherche des racines des polynômes dans les corps finis.

S'il le désirent, les candidats peuvent étudier les coniques sur les corps finis et la recherche de points sur ces coniques.

Questions possibles :

- Expliquer la descente de Fermat !
  Réponse : voir le Hindry [HIN08]
- Pourquoi $\mathbb{F}_q^*$ est-il cyclique ?
- Résoudre dans $\mathbb{Z}^2$ l'équation $y^2 = x^3 + 7$.

Motivations :

On veut résoudre des équations sur les entiers. J'attaque cette leçon en voulant résoudre 4 grandes équations ($ax + by = c$, $x^n + y^n = z^n$, $x^2 + py = a$ et $x^2 - dy^2 = \pm 1$), je vais expliquer la motivation d'introduction de ces équations. La première est une équation diophantienne linéaire, c'est équivalent à la résolution d'un système linéaire avec une matrice à coefficients entiers, on peut l'attaquer sur $\mathbb{Z}$ ou sur $\mathbb{Z}/n\mathbb{Z}$, en utilisant l'algorithme d'Euclide ou le théorème chinois. La deuxième est l'équation de Fermat, qui est insoluble[6] pour $n \geqslant 3$ (Adrew Wiles 1994), on va introduire les triplets pythagoriciens qui sont utiles pour étudier le cas $n = 2$ et montrent aussi que $x^4 + y^4 = z^4$ n'admet pas de solutions non triviales (utilisation de la descente de Fermat). La troisième vient de l'étude des carrés dans les corps finis, en effet, dans $\mathbb{F}_p$, l'équation se réécrit $x^2 = a$, on veut donc savoir si a est un résidu quadratique dans $\mathbb{F}_p$. On introduira le symbole de Legendre et la loi de réciprocité quadratique qui nous aident à résoudre cette équation. La quatrième est l'équation de Pells Fermat, j'admets sa résolution (il faut prouver qu'il existe une solution fondamentale et que toute puissance de cette solution est solution de l'équation [HIN08]), je présente le contexte dans lequel elle apparait en théorie algébrique des nombres, lorsqu'on étudie des corps de nombres quadratiques[7]. Si on regarde l'anneau des entiers, on peut tomber sur $\mathbb{Z}[\sqrt{d}]$ et la norme de cette anneau est $N(a+\sqrt{d}b) = a^2 - db^2$. Or les inversibles de cet anneau sont les éléments de norme égale à ± 1. Ainsi résoudre Pells-Fermat est équivalent à trouver les inversibles de l'anneau $\mathbb{Z}[\sqrt{d}]$.

6. il n'y a pas de solutions non triviales (i.e. pas de solutions avec x, y, z non tous nuls)
7. extension finie de degré 2 sur $\mathbb{Q}$

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Equations diophantiennes

1) Equations linéaires sur $\mathbb{Z}$ [LAM12a]

$ax + by = c$

Bézout

Algorithme d'Euclide

Congruence

Equations diophantiennes linéaires

2) Equations linéaires modulaire [LAM12b]

Théorème chinois

II - Méthodes de résolution

1) Réduction modulaire

$x^2 = 3y + 5$ pas de solution entière modulo 3 donc pas de solution entière

2) Utilisation de l'analyse

$n^2 - 5n + 2 = 0$ a pour solution sur $\mathbb{R}$ $\frac{5 \pm \sqrt{17}}{1}$ non entières

III - Théorème de Fermat [HIN08]

$x^n + y^n = z^n$

Triplets pythagoriciens

$x^4 + y^4 = z^2$ n'a pas de solutions (par descente de Fermat)

Corollaire Fermat pour $n = 4$ n'a pas de solutions

Théorème de Fermat (admis)

Théorème de Fermat modulaire

IV - Les carrés de $\mathbb{F}_q$ [CG18] [PER96]

$x^2 + py = q$

Solution SSI $\left(\frac{q}{p}\right) = 1$

Utilisation du symbole de Legendre

Loi de réciprocité quadratique

V - Théorie algébrique des nombres

$a^2 + db^2 = \pm 1$ (Pells Fermat)

Corps quadratique $\mathbb{Q}(\sqrt{d})$

Entier de Gauss

Inverses de $\mathbb{Z}[\sqrt{d}]$

Résolution des équations de Pells Fermat

Développements :

- Théorème de Fermat modulaire
- Loi de réciprocité quadratique

Références :

♥♥♥♥ - [LAM12a] Jean-Pierre LAMOITIER, *Arithmétique Classique*

♥♥♥♥ - [LAM12b] Jean-Pierre LAMOITIER, *Arithmétique Modulaire*

♥♥♥♥ - [HIN08] Marc HINDRY, *Arithmétique*

♥♥♥♥ - [PER96] Daniel PERRIN, *Cours d'Algèbre*

♥♥♥♥ - [ST15] Ian STEWART et David TALL, *Algebraic Number Theory*

♥♥♥ - [CG18] Philippe CALDERO et Jerôme GERMONI, *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2*

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

Rapport du jury :

La présentation du bagage théorique permettant de définir corps de rupture, corps de décomposition, ainsi que des illustrations dans différents types de corps (réel, rationnel, corps finis) sont inévitables. Les corps finis peuvent être illustrés par des exemples de polynômes irréductibles de degré 2, 3, 4 sur $\mathbb{F}_2$ ou $\mathbb{F}_3$. Il est nécessaire de présenter des critères d'irréductibilité de polynômes et des polynômes minimaux de quelques nombres algébriques.

Il faut savoir qu'il existe des corps algébriquement clos de caractéristique nulle autres que $\mathbb{C}$; il est bon de savoir montrer que l'ensemble des nombres algébriques sur le corps $\mathbb{Q}$ des rationnels est un corps algébriquement clos. Le théorème de la base télescopique, ainsi que les utilisations arithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes, est incontournable.

Questions possibles :

- Soit $P \in \mathbb{Z}[X]$ unitaire tel que $P(\alpha) = 0$ avec $\alpha \in \mathbb{Q}$. Montrer que $P = 0$.
- Montrer le lemme de Gauss.
- Montrer que $\Phi_8 = X^4 + 1$ est réductible dans tous les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.
- Quel est le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$.
- Donner $[\mathbb{Q}(j, \sqrt[3]{5}) : \mathbb{Q}]$.
- Démontrer qu'un idéal I d'un anneau A est premier si et seulement si A/I est intègre.
- Démontrer qu'un idéal I d'un anneau A est maximal si et seulement si A/I est un corps.
- Soient K un corps et $P \in K[X]$. Démontrer que P est irréductible si et seulement si $K[X]/(P)$ est un corps.
- Donner un exemple de corps qui ne soit pas parfait.
- Montrer qu'une extension de corps est primitive si et seulement si elle admet un nombre fini d'extensions intermédiaires.
- Quels sont les polynômes irréductibles sur $\mathbb{F}_2$? Sur $\mathbb{F}_3$?
- Que dire d'une matrice dont le polynôme caractéristique est scindé ? Et d'une matrice dont le polynôme minimal est scindé ?
- Expliquer le lien entre le polynôme minimal d'un élément d'un corps et le polynôme minimal d'une matrice.

Motivations :

Les polynômes irréductibles à une indéterminée sont extrêmement interessants à étudier, car comme $\mathbb{K}[X]$ est un anneau euclidien dès lors que $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ est donc principal et factoriel. On veut donc factoriser les polynômes en produits de polynômes irréductibles, mais pour cela il faut connaitre les polynômes irréductibles. On va donc donner des critères d'irréductibilité de polynômes. Ensuite on s'intéresse aux racines de polynômes et on va avoir deux approches différentes (dans le II et le III), la première est, à partir d'un polynôme, on veut trouver une extension de corps qui contienne les racines de ce polynôme (corps de rupture, corps de décomposition), la seconde, est d'avoir des éléments, et on veut trouver des polynômes ayant ces éléments pour racines (corps algébriquement clos et théorie algébrique des nombres).

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Polynômes irréductibles
  1) Définitions [GOU08a]
    Définition de polynômes
    Division euclidienne
  2) Critères d'irréductibilité [PER96]
    Critère d'Eisenstein
    Critère modulaire
    Réciproque fausse X^4+1

II - Extensions de corps
  1) Définitions
  2) Corps de rupture
    Définition
    Unicité
    Primalité des nombres de Mersenne
  3) Corps de décomposition
    Définition
    Unicité

III - Théorie algébrique des nombres
  1) Algébriquement clos
    Définition
    Théorème de D'alembert Gauss (voir appendice)
    Cloture algébrique d'un corps
  2) Corps quadratiques
    Définition
    Théorème de l'élément primitif
    $\mathbb{Q}(\sqrt{d})$
  3) Corps cyclotomiques
    Définition des corps cyclotomiques
    Définition des polynomes cyclotomiques
    Irréductibilité des polynômes cyclotomiques

Développements :

- Primalité des nombres de Mersenne
- Irréductibilité des polynômes cyclotomiques

Références :

♥♥ - [PER96] Daniel PERRIN, *Cours d'Algèbre*
♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*
♥♥♥ - [ST15] Ian STEWART et David TALL, *Algebraic Number Theory*
♥♥♥ - [CAL06] Josette CALAIS, *Extensions de Corps, Théorie de Galois*

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

Rapport du jury :

Dans cette leçon, il est indispensable de présenter les résultats fondateurs de la théorie des espaces vectoriels de dimension finie en ayant une idée de leurs preuves. Ces théorèmes semblent simples car ils ont été très souvent pratiqués, mais leur preuve demande un soin particulier. Il est important de savoir justifier pourquoi un sous-espace vectoriel d'un espace vectoriel de dimension finie est aussi de dimension finie. Le pivot de Gauss ainsi que les diverses notions et caractérisations du rang trouvent leur place dans cette leçon. Les applications sont nombreuses, on peut par exemple évoquer l'existence de polynômes annulateurs ou alors décomposer les isométries en produits de réflexions.

On pourra utiliser les caractérisations du rang pour démontrer l'invariance du rang par extension de corps, ou pour établir des propriétés topologiques (sur $\mathbb{R}$ ou $\mathbb{C}$).

S'ils le désirent, les candidats peuvent déterminer des degrés d'extensions dans la théorie des corps ou s'intéresser aux nombres algébriques.

On pourra également explorer des applications en analyse comme les extrémas liés ou l'étude de l'espace vectoriel engendré par les translatés d'une application de $\mathbb{R}$ dans $\mathbb{R}$.

Dans un autre registre, il est pertinent d'évoquer la méthode des moindres carrés dans cette leçon, par exemple en faisant ressortir la condition de rang maximal pour garantir l'unicité de la solution et s'orienter vers les techniques de décomposition en valeurs singulières pour le cas général. On peut alors naturellement explorer l'approximation d'une matrice par une suite de matrices de faible rang.

Questions possibles :

- Pourquoi un sous-espace vectoriel F d'un espace vectoriel E de dimension finie est de dimension finie ?

  Réponse : il faut considérer une base de E

Points essentiels :

- L'ordre des différents résultats (voir l'appendice sur l'ordre des résultats sur la dimension d'un espace vectoriel)

Plan détaillé :

I - Théorie de la dimension [GRI11]

Définition de famille génératrice

Définition de famille libre

Propriétés liées à ces notions

Définition base

Cardinal d'une base est unique

Théorème de la base incomplète

Prop : un sous-espace vectoriel d'un espace vectoriel de dimension finie est de dimension finie

Dimension de $\mathcal{L}(E,F)$ et E^* (espace dual)

II - Notion du rang

Théorème du rang

Application linéaire

Définition du rang d'une matrice

Théorème de Carathéodory

Prop : $\operatorname{rg} {}^tA = \operatorname{rg} A$

Système de Cramer

Matrices équivalentes ont même rang

Forme linéaire

Hyperplans

III - Application

1) Algèbre linéaire

Théorème de codiagonalisabilité (récurrence sur la dimension de E)

2) Espace de solutions d'une EDO linéaire

Translatés d'une fonction $\mathcal{C}^1$

3) Extension de corps [CAL06]

Degré de $\mathbb{L}/\mathbb{K}$

$[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L})$

base télescopique

Développements :

- Théorème de Carathéodory
- Translatés d'une fonction $\mathcal{C}^1$

Références :

♥♥♥♥♥ - [GRI11] Joseph GRIFONE, *Algèbre Linéaire*

♥♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*

♥ - [CAL06] Josette CALAIS, *Extensions de Corps, Théorie de Galois*

Leçon 152
Déterminant. Exemples et applications.

Rapport du jury :

Dans cette leçon, il faut commencer par définir correctement le déterminant. Il est possible d'entamer la leçon en disant que le sous-espace des formes n-linéaires alternées sur un espace de dimension n est de dimension 1 et, dans ce cas, il est essentiel de savoir le montrer. Le plan doit être cohérent ; si le déterminant n'est défini que sur $\mathbb{R}$ ou $\mathbb{C}$, il est délicat de définir $\det(XI_n - A)$ avec A une matrice carrée. L'interprétation du déterminant comme volume est essentielle. On peut rappeler son rôle dans les formules de changement de variables, par exemple pour des transformations de variables aléatoires.

Le calcul explicite est important, mais le jury ne peut se contenter d'un déterminant de VANDERMONDE ou d'un déterminant circulant. Les opérations élémentaires permettant de calculer des déterminants, avec des illustrations sur des exemples, doivent être présentées. Il est bienvenu d'illustrer la continuité du déterminant par une application, ainsi que son caractère polynomial. Pour les utilisations des propriétés topologiques, on n'omettra pas de préciser le corps de base sur lequel on se place.

S'ils le désirent, les candidats peuvent s'intéresser aux calculs de déterminants sur $\mathbb{Z}$ avec des méthodes multimodulaires. Le résultant et les applications simples à l'intersection ensembliste de deux courbes algébriques planes peuvent aussi trouver leur place dans cette leçon pour des candidats ayant une pratique de ces notions.

Remarques :

Pour définir $\det(XI_n - A)$, soit on se place sur le corps des fractions $\mathbb{K}(X)$ pour pouvoir avec un déterminant sur $\mathbb{K}[X]$, soit on peut dire que tout marche sur des anneaux unitaires et on utilise

$$A \in GL_n(\mathbb{K}[X]) \iff \det(A) \in \mathbb{K}[X]^\times$$

en remarquant que $\mathbb{K}[X]^\times = \mathbb{K}^*$

Questions possibles :

- Calculer le déterminant d'une matrice de Gram.
- Donner une interprétation géométrique du déterminant de Gram.

  Réponse : Soit $x_1, \cdots, x_n$ une base d'un espace vectoriel E. Alors $G(x_1, \cdots, x_n) =$ (volume du parallélépipède$x_1 \cdots x_n)^2$.
- Calculer un déterminant de Van Der Monde.
- Calculer le déterminant d'une matrice circulante.
- Soit $A \in \mathcal{M}_n(\mathbb{R})$ telle que $A = Comm(A)$. Que dire de A ?
- Quelles sont les propriétés topologiques de $\mathrm{GL}_n(\mathbb{R})$?
- Prouver que $det(AB) = det(A)det(B)$.
- Donner une interprétation géométrique de la formule de changement de variable, en terme de volume des parallélépipèdes infinitésimaux.

Motivations :

Le déterminant est un outil très puissant pour avoir le caractère lié ou libre d'une famille de vecteurs. Il a ensuite de nombreuses applications en analyse et en algèbre. On voit notamment des propriétés de régularité en analyse (caractère $\mathcal{C}^\infty$), d'utilisation pour le changement de variables et de calcul de volume. On voit aussi son utilisation dans le polynôme caractéristique. Il faut ensuite savoir calculer le déterminant, utilisation des cofacteurs, des comatrices, calculer des déterminants classiques (Van Der Monde, circulant, Cauchy, Gram) et le polynôme caractéristique d'une matrice compagnon par exemple.

Points essentiels :

- L'espace des formes n-linéaires alternées est de dimension 1

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - L'application déterminant

1) Formes n-linéaires alternées

Définition

Théorème : L'espace des formes n-linéaires alternées est de dimension 1

Formule du déterminant

Déterminant d'un endomorphisme

Déterminant d'une matrice

$\det A = \det {}^t A$

$\det AB = \det A \det B$

Prop : semblable implique même déterminant

2) Régularité de la fonction det

Le déterminant est $\mathcal{C}^1$, différentiable, $\mathcal{C}^\infty$

Application : 2 matrices semblables sur $\mathbb{C}$ le sont sur $\mathbb{R}$

II - Calcul du déterminant

Déterminant 2×2 et 3×3

Déterminant d'une matrice diagonale

Déterminant d'une matrice triangulaire

Déterminant d'une matrice par blocs

Cofacteurs

Comatrice

Calcul de l'inverse

Pivot de Gauss

Déterminant de Van Der Monde

Déterminant circulant

Application : Convergence de polygones vers l'isobarycentre

III - Le déterminant en algèbre linéaire

1) Système de Cramer
   Système compatible
   Résolution
   Formule
2) Polynômes caractéristiques
   Définition
   Théorème de Cayley

IV - Le déterminant d'autres domaines
1) Changement de variables [GOU08b]
   Théorème
   Exemple
2) Inégalité d'Hadamard
   Théorème des extrema liés
3) Volume [GRI11]
4) Formes quadratiques [DSP11]
   Discriminant

Développements :

- Convergence de polygones vers l'isobarycentre
- Théorème des extrema liés

Références :

♥♥♥♥ - [GRI11] Joseph GRIFONE, *Algèbre Linéaire*
♥♥♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*
♥♥ - [GOU08b] Xavier GOURDON, *Analyse*
♥♥ - [DSP11] Clément DE SEGUINS PAZZIS, *Invitations aux formes quadratiques*

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

Rapport du jury :

Cette leçon ne doit pas être un catalogue de résultats autour de la réduction qui est ici un moyen pour démontrer des théorèmes ; les polynômes d'endomorphismes doivent y occuper une place importante. Il faut consacrer une courte partie de la leçon à l'algèbre $\mathbb{K}[u]$ et connaître sa dimension sans hésitation. Il est ensuite possible de s'intéresser aux propriétés globales de cette algèbre.

Les liens entre réduction d'un endomorphisme u et la structure de l'algèbre $\mathbb{K}[u]$ sont importants, tout comme ceux entre les idempotents et la décomposition en somme de sous-espaces caractéristiques. Il faut bien préciser que, dans la réduction de Dunford, les composantes sont des polynômes en l'endomorphisme, et en connaître les conséquences théoriques et pratiques.

L'aspect *applications* est trop souvent négligé. Il est possible, par exemple, de mener l'analyse spectrale de matrices stochastiques. On attend d'un candidat qu'il soit en mesure, pour une matrice simple de justifier la diagonalisabilité et de déterminer un polynôme annulateur (voire minimal). Il est bien sûr important de ne pas faire de confusion entre diverses notions de multiplicité pour une valeur propre λ donnée (algébrique ou géométrique). Enfin, calculer A^k ne nécessite pas, en général, de réduire A (la donnée d'un polynôme annulateur de A suffit souvent). Il est possible d'envisager des applications aux calculs d'exponentielles de matrices.

S'il le souhaite, le candidat pourra étudier des équations matricielles et de calcul fonctionnel, avec par exemple l'étude de l'extraction de racines ou du logarithme.

Questions possibles :

- La matrice $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ est-elle diagonalisable ?
- Soient u un endomorphisme d'un espace vectoriel E, π_u son polynôme minimal et pour tout $x \in E$, $\pi_{u,x}$ sont polynôme minimal en x. Démontrer qu'il existe $x \in E$ tel que $\pi_u = \pi_{u,x}$.
- Existe-t-il des matrices sans valeur propre ?

  Réponse : Oui. Un exemple intéressant de telle matrice est donné sur $\mathbb{R}^2$ par $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ avec $\theta \not\equiv 0[\pi]$: matrice de rotation sur $\mathbb{R}^2$, qui envoie tout vecteur non nul sur un vecteur non colinéaire. Cette matrice n'admet donc aucune valeur propre sur $\mathbb{R}$ (mais elle en admet sur $\mathbb{C}$).
- Démontrer que $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$ est diagonalisable si et seulement si $a \neq c$ ou $b = 0$.
- Montrer que si un endomorphisme admet un polynôme annulateur scindé à racines simples sur un corps K, alors il est diagonalisable sur K.

  Réponse : Indice : Utiliser le lemme des noyaux.
- Donner des exemples d'endomorphismes normaux.

  Réponse : Les endomorphismes autoadjoints, symétriques, hermitiens, orthogonaux.
- Démontrer que lorsque deux endomorphismes commutent, les sous-espaces propres de l'un sont stables par l'autre.
- Donner une symétrie vectorielle non diagonalisable en caractéristique 2.

Réponse : $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

- Donner la structure de la démonstration de la densité des matrices diagonalisables dans $\mathcal{M}_n(\mathbb{C})$. Pourquoi cette preuve ne fonctionne-t-elle pas sur $\mathbb{R}$?
- Donner un exemple de matrice de $\mathcal{M}_n(\mathbb{R})$ ne pouvant pas être approchée par des matrices diagonalisables.

  Réponse : $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ convient. En effet, son polynôme caractéristique est $X^2 + 1$, dont le discriminant est négatif. Or, l'application Δ qui associe à une matrice de $\mathcal{M}_2(\mathbb{R})$ le discriminant de son polynôme caractéristique est continue sur $\mathcal{M}_2(\mathbb{R})$ (car polynomiale en les composantes). Donc A n'est pas approchable par des matrices diagonalisables (car une matrice diagonalisable de $\mathcal{M}_2(\mathbb{R})$ a un polynôme caractéristique de discriminant positif).

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Polynômes d'endomorphisme
  1) Définition
     Définition
     Algèbre
     Prop : $\mathbb{K}[u]$ est fermé
     Image de l'exponentielle
  2) Polynôme minimal
     Définition : engendre l'idéal de $\mathbb{K}[X]$
     Prop : en dim finie, il y a toujours un polynome annulateur
     Contre-exemple : la dérivation de $\mathbb{R}[X]$ dans $\mathbb{R}[X]$
     Application : calcul de l'inverse
  3) Polynôme caractéristique
     Définition
     Cayley Hamilton

II - Diagonalisabilité et trigonalisabilité
  1) Trigonalisabilité
     Définition
     CNS
  2) Diagonalisabilité
     Définition
     CNS

III - Réductions d'endomorphisme
  1) Dunford
     Lemme des noyaux
     Décomposition de Dunford
     Calcul de l'exponentielle
  2) Jordan
     Cas nilpotent
     Cas général
  3) Frobenius
     Invariants de Similitude

Développements :

- Décomposition de Dunford
- Image de l'exponentielle

Références :

♥♥♥♥ - [GRI11] Joseph GRIFONE, *Algèbre Linéaire*

♥♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*

♥♥♥♥ - [MM16] Roger MANSUY et Rached MNEIMNÉ, *Algèbre Linéaire, Réduction des Endomorphismes*

♥♥♥ - [COG00] Michel COGNET, *Algèbre Linéaire*

Leçon 156
Exponentielle de matrices. Applications.

Rapport du jury :

Bien que ce ne soit pas une leçon d'analyse, il faut toutefois pouvoir justifier clairement la convergence de la série exponentielle. La distinction entre le cas réel et complexe doit être clairement évoqué.

Les questions de surjectivité ou d'injectivité doivent être abordées. Par exemple la matrice $A = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ est-elle l'exponentielle d'une matrice à coefficients réels ? La matrice définie par blocs $B = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$ est-elle l'exponentielle d'une matrice à coefficients réels ?

La décomposition de Dunford multiplicative (décomposition de Jordan) de $\exp A$ trouve toute son utilité dans cette leçon. Notons que l'exponentielle fait bon ménage avec la décomposition polaire dans bon nombre de problèmes sur les sous-groupes du groupe linéaire. L'étude du logarithme (quand il est défini) trouve toute sa place dans cette leçon. Si l'on traite du cas des matrices nilpotentes, on pourra évoquer le calcul sur les développements limités.

Il est bon de connaître l'image par exponentielle de certains sous-ensembles de matrices (ensemble des matrices symétriques, hermitiennes, ou antisymétriques).

Les applications aux équations différentielles méritent d'être présentées sans toutefois constituer l'essentiel de la leçon. On pourra par exemple faire le lien entre réduction et comportement asymptotique, mais le jury déconseille aux candidats de proposer ce thème dans un développement de cette leçon, sauf à avoir bien compris comment les apports algébriques permettent ici de simplifier les conclusions analytiques.

S'ils le désirent, les candidats peuvent s'aventurer vers les sous-groupes à un paramètre du groupe linéaire (on peut alors voir si ces sous-groupes constituent des sous-variétés fermées de $GL_n(\mathbb{R})$) ou vers les algèbres de Lie.

Questions possibles :

- Pourquoi l'exponentielle matricielle est bien définie ?
- Pour $A \in \mathcal{A}_n(\mathbb{R})$, que peut-on dire de $\exp(A)$?
- Que vaut $\det(\exp A)$? Le montrer !
  Réponse : $\det(\exp A) = \exp(\mathrm{Tr}(A))$
- Soit $A = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$. Est-ce que A est dans l'image de l'exponentielle ?
  Réponse : $A \in \exp(\mathcal{M}_n(\mathbb{C}))$ mais $A \notin \exp(\mathcal{M}_n(\mathbb{R}))$
- Montrer que $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$.
- Pourquoi l'exponentielle d'un polynôme en $M \in \mathcal{M}_n(\mathbb{C})$ est-elle un polynôme en M ?
- Pourquoi l'exponentielle matricielle est-elle de classe $\mathcal{C}^1$?
- Donner la différentielle de $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C})$.

Motivations :

On va étudier ici l'exponentielle de matrices. Plus généralement, pour une algèbre de Banach, on peut définir l'exponentielle. Pour les matrices, on a besoin de l'exponentielle de matrices pour résoudre des équations différentielles linéaires à coefficients constants. (Une autre motivation que je ne présenterai pas à l'oral car je ne la maitrise pas est de parler de groupes de Lie et/ou groupe à un paramètre).

J'ai rédigé le plan de cette leçon (voir ici)

I - Exponentielle de matrices

1) Définition de l'exponentielle [GOU08a]

Définition avec série entière de rayon infini

$\exp(PAP^{-1}) = P \exp AP^{-1}$

$\exp({}^tA) = {}^t \exp A$

Prop : Si A, B commutent, alors $\exp(A+B) = \exp A \exp B$

$\exp(A)^{-1} = \exp(-A)$

$\det \exp A = \exp(Tr(A))$

$\exp(A) \in \mathbb{K}[A]$

Corollaire : $\exp(A)$ commute avec A

2) Calcul de l'exponentielle

A diagonale

N nilpotente

A diagonalisable

Les valeurs propres de $\exp A$ sont les exponentielles des valeurs propres de A

Utilisation d'une relation de récurrence pour calculer l'exponentielle

Utilisation du binôme de Newton (attention à la commutativité)

Décomposition de Dunford

Dunford multiplicatif

Jordan

II - Propriétés de la fonction exponentielle

1) Régularité [ROU09]

exp continue, même différentiable et $\mathcal{C}^\infty$

Utilisation du Théorème d'Inversion Locale pour avoir un $\mathcal{C}^1$ difféo local

Définition du log des matrices nilpotentes dans les unipotentes

Définition avec une série entière

2) Injectivité et surjectivité

Image de l'exponentielle [BMP05]

exp non injective pour $n \geqslant 2$ sur $\mathbb{R}$ et pour $n \geqslant 1$ sur $\mathbb{C}$

$\exp : \mathcal{D}_n(\mathbb{R}) \to \mathcal{M}_n(\mathbb{R})$ est injective [FGN09]

Homéomorphisme $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ (avec aussi version complexe avec matrices hermitiennes)

Utilisation de la décomposition polaire pour avoir

$$GL_n(\mathbb{R}) \simeq O_n(\mathbb{R}) \times \mathbb{R}^{\frac{n(n+1)}{2}}$$

Etude du groupe $O(p,s)$

$\exp : \mathcal{A}_n(\mathbb{R}) \to SO_n(\mathbb{R})$ surjective non injective [FGN13a]

III - Applications aux équations différentielles [DEM16] [BER17]

1) Linéaire homogène autonome

Solution $Y' = AY + B$

Equation de Sylvester $Y' = AY + YB$

stabilité asymptotique ou non en fonction des valeurs propres (Dunford)

2) Non linéaire

Théorème de Lyapunov pour le cas non linéaire

Développements :

- Etude du groupe $O(p,s)$
- Image de l'exponentielle

Références :

♥♥♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*

♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥♥ - [ROU09] François ROUVIÈRE, *Petit Guide de Calcul Différentiel*

♥♥♥ - [BER17] Florent BERTHELIN, *Equations Différentielles*

♥♥♥ - [DEM16] Jean-Pierre DEMAILLY, *Analyse numérique et équations différentielles*

♥♥♥ - [BMP05] Vincent BECK, Jérôme MALICK et Gabriel PEYRÉ, *Objectif Agrégation*

♥♥ - [FGN09] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS, *Oraux X-ENS, Algèbre 2*

♥♥ - [FGN13a] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS, *Oraux X-ENS, Algèbre 3*

Leçon 157
Endomorphismes trigonalisables. Endomorphismes nilpotents.

Rapport du jury :

Il est bon de savoir expliquer pourquoi l'application induite par un endomorphisme trigonalisable (respectivement nilpotent) sur un sous-espace stable est encore trigonalisable (respectivement nilpotent). L'utilisation des noyaux itérés est fondamentale dans cette leçon, par exemple pour déterminer si deux matrices nilpotentes sont semblables. Il est intéressant de présenter des conditions suffisantes de trigonalisation simultanée ; l'étude des endomorphismes cycliques a toute sa place dans cette leçon. L'étude des nilpotents en dimension 2 débouche naturellement sur des problèmes de quadriques et l'étude sur un corps fini donne lieu à de jolis problèmes de dénombrement. S'ils le désirent, les candidats peuvent aussi présenter la décomposition de Frobenius, ou des caractérisations topologiques des endomorphismes nilpotents, ou encore des propriétés topologiques de l'ensemble des endomorphismes nilpotents.

Questions possibles :

- Comment on prouve la codiagonalisabilité de deux matrices ?
- Donner un conter exemple de 2 matrices cotrigonalisables qui ne commutent pas.
- Comment distinguer 2 matrices nilpotentes de même indice ?

  Réponse : en calculant la dimension des noyaux des itérés
- Comment caractériser les matrices nilpotentes ?

  Réponse : avec Jordan
- Montrer que A est nilpotente si et seulement si $\chi_A = X^n$.

Plan détaillé :

I - Endomorphismes trigonalisables

1) Définition

Définition

2) Trigonalisation simultanée

Si u et v commutent les sous espaces propres de u sont stables par v

Si u et v commutent et sont trigonalisables, alors ils sont co-trigonalisables

Réciproque est fausse

3) Application à la décomposition d'endomorphismes

Décomposition LU

Décomposition QR (homéomorphisme)

Méthode QR

II - Endomorphismes nilpotents

1) Définition et Propriétés

Définition

Spectre réduit à $\{0\}$

$\forall k\ \mathrm{Tr}(A^k) = 0 \iff A\text{nilp}$

2) Structure

Pas de structure de sous espace vectoriel, par un idéal (contre exemple)

c'est un cône

3) Application à la réduction

Lemme des noyaux

Décomposition de Dunford

Jordan

Développements :

- Décomposition de Dunford
- Méthode QR

Références :

♥♥♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*

♥♥♥ - [GRI11] Joseph GRIFONE, *Algèbre Linéaire*

♥♥♥ - [MM16] Roger MANSUY et Rached MNEIMNÉ, *Algèbre Linéaire, Réduction des Endomorphismes*

♥♥ - [FGN09] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS, *Oraux X-ENS, Algèbre 2*

♥♥ - [CIA06] Philippe CIARLET, *Introduction à l'analyse numérique matricielle et à l'optimisation*

♥♥ - [AK02] Grégoire ALLAIRE et Sidi Mahmoud KABER, *Algèbre Linéaire Numérique*

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

Rapport du jury :

Il est important de bien placer la thématique de la dualité dans cette leçon ; celle-ci permet de mettre en évidence des correspondances entre un morphisme et son morphisme transposé, entre un sous-espace et son orthogonal (canonique), entre les noyaux et les images ou entre les sommes et les intersections. Bon nombre de résultats d'algèbre linéaire se voient dédoublés par cette correspondance. Les liens entre base duale et fonctions de coordonnées doivent être parfaitement connus. Le passage d'une base à sa base duale ou antédualte, ainsi que les formules de changement de base, doivent être maîtrisés. On pourra s'intéresser aux cas spécifiques où l'isomorphisme entre l'espace et son dual est canonique (cas euclidien, cas des matrices).

Savoir calculer la dimension d'une intersection d'hyperplans via la dualité est important dans cette leçon. L'utilisation des opérations élémentaires sur les lignes et les colonnes permet facilement d'obtenir les équations d'un sous-espace vectoriel ou d'exhiber une base d'une intersection d'hyperplans.

Cette leçon peut être traitée sous différents aspects : géométrique, algébrique, topologique ou analytique. Il faut que les développements proposés soient en lien direct avec la leçon. Enfin rappeler que la différentielle d'une fonction à valeurs réelles est une forme linéaire semble incontournable.

Il est possible d'illustrer la leçon avec un point de vue probabiliste, en rappelant que la loi d'un vecteur aléatoire X est déterminée par les lois unidimensionnelles de $X.u$ pour tout vecteur u.

Questions possibles :

- Pourquoi une forme linéaire injective est continue ?
- Démontrer que pour tout $n \geq 2$, tout hyperplan de $\mathcal{M}_n(K)$ rencontre $GL_n(K)$.
- Pourquoi le rang d'un projecteur est-il égal à sa trace, en caractéristique nulle ? Donner un contre-exemple en caractéristique non nulle.

  Réponse : Contre-exemple en caractéristique non nulle :$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{F}_2)$. On a bien $rg(P) = 2$ mais $tr(P) = 0$.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Forme linéaire et hyperplan

1) Définitions

Déf Forme linéaire

2) Lien avec les hyperplans [GRI11]

Noyaux d'une forme linéaire

Somme directe

II - Dualité

1) Base duale

Isomorphisme entre E et E^*

Bidual E^{**}

Isomorphisme canonique de E dans E^{**}

2) Orthogonalité

Def $A^\perp$ B°

Propriété d'inclusion et d'égalité de cardinaux

Translatés d'une fonction $\mathcal{C}^1$

Prop : L'ensemble $H^\perp$ des formes linéaires sur E qui s'annulent sur H est une droite de E^*.

Corollaire : Morphismes d'algèbre de $\mathcal{C}(K, \mathbb{R})$ sur $\mathbb{R}$

3) Transposées

Définition

III - Application en analyse et en algèbre

1) En analyse : Différentielle

Définition

Théorème des extrema liés

2) En algèbre

Intersection d'hyperplan (utilisation du Pivot de Gauss)

Développements :

- Morphismes d'algèbre de $\mathcal{C}(K, \mathbb{R})$ sur $\mathbb{R}$
- Translatés d'une fonction $\mathcal{C}^1$
- Théorème des extrema liés

Remarques :

Attention car pour les morphismes d'algèbres, on a des formes linéaires sur un espace qui n'est pas de dimension finie, donc soit on préfère faire les deux autres, soit on le fait car on utilise un lemme qui est une généralisation d'un résultat de dimension finie

Références :

♥♥♥♥ - [GRI11] Joseph GRIFONE, *Algèbre Linéaire*

♥♥♥ - [GOU08a] Xavier GOURDON, *Algèbre*

♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

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

Rapport du jury :

Dans cette leçon, les techniques liées au simple pivot de Gauss constituent l'essentiel des attendus. Il est impératif de faire le lien avec la notion de système échelonné, (dont on donnera une définition précise et correcte), et de situer l'ensemble dans le contexte de l'algèbre linéaire (sans oublier la dualité). Un point de vue opératoire doit accompagner l'étude théorique et l'intérêt algorithmique des méthodes présentées doit être expliqué. On pourra illustrer cela par des exemples simples (où l'on attend parfois une résolution explicite).

Parmi les conséquence théoriques, les candidats pourront notamment donner des systèmes de générateurs de $GL_n(\mathbb{K})$ et $SL_n(\mathbb{K})$. Ils peuvent aussi présenter les relations de dépendance linéaire sur les colonnes d'une matrice échelonnée qui permettent de décrire simplement les orbites de l'action à gauche de $GL_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$ donnée par $(A, P) \mapsto PA$.

S'ils le désirent, les candidats peuvent exploiter les propriétés des systèmes d'équations linéaires pour définir la dimension des espaces vectoriels et obtenir une description de l'intersection de deux sous-espaces vectoriels donnés par des systèmes générateurs, ou d'une somme de deux sous-espaces vectoriels donnés par des équations.

De même, des discussions sur la résolution de systèmes sur $\mathbb{Z}$ et la forme normale de Hermite peuvent trouver leur place dans cette leçon. Enfin, il est possible de présenter les décompostions LU et de Choleski, en évaluant le coût de ces méthodes ou encore d'étudier la résolution de l'équation normale associée aux problèmes des moindres carrés et la détermination de la solution de norme minimale par la méthode de décomposition en valeurs singulières.

Questions possibles :

- Comment utiliser le pivot de Gauss pour déterminer l'image d'une matrice ? Son noyau ?
- Quelle méthode itérative pour résoudre $Ax = b$ utilise-t-on en pratique ?

  Réponse : le gradient conjugué souvent
- Quelle est la complexité de Gauss Seidel ?
- A quoi cela sert la décomposition LU (puisque sa complexité est en n^3 comme le pivot de Gauss) ?

  Réponse : Si on veut changer le membre de b, on aura des opérations en n^2 pour résoudre le système une fois qu'on aura fait le calcul de $A = LU$ en n^3
- Donner des applications du pivot de Gauss.

  Réponse : calculer le rang d'une matrice, le rang invariant par changement de corps, calculer l'inverse d'une matrice, résoudre $Ax = b$, générateurs de $GL_n(\mathbb{K})$,...
- Combien ça coûte de calculer A^{-1} ?

  Réponse : $O(n^3)$
- Combien ça coûte de calculer $A^{-1}b$ une fois que A^{-1} est calculé ?

  Réponse : $O(n^2)$
- Donc quel est l'avantage de la décomposition LU ?

  Réponse : avantage d'une constante dans le grand O qui est meilleure dans LU que dans l'inverse de A

- Pour une matrice tridiagonale[8], quelle est la complexité de la décomposition LU ?

  Réponse : linéaire
- Qu'est ce que vous pouvez dire sur les systèmes de Cramer ?
- Montrer que pour b fixé, $Ax = b$ admet une unique solution SSI A est inversible
- Comment on calcule l'inverse d'une matrice A avec le pivot de Gauss ?
- On considère $2k+1$ cailloux chacun de masse $(m_i)_1^{2k+1}$, on suppose que dès qu'on enlève un cailloux, parmi les $2k$ restants, il existe un ensemble de k cailloux dont le poids total est le même que les k autres. Montrer que toutes les masses sont égales.

  Réponse : il faut poser un système linéaire de taille $(2k+1) \times (2k+1)$,

$$\begin{cases} \varepsilon_{1,1}m1 & + & \varepsilon_{1,2}m_2 & + & \dots & + & \varepsilon_{1,2k+1}m_{2k+1} & = & 0 \\ \varepsilon_{2,1}m1 & + & \varepsilon_{2,2}m_2 & + & \dots & + & \varepsilon_{2,2k+1}m_{2k+1} & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ \varepsilon_{2k+1,1}m1 & + & \varepsilon_{2k+1,2}m_2 & + & \dots & + & \varepsilon_{2k+1,2k+1}m_{2k+1} & = & 0 \end{cases}$$

  avec $\varepsilon_{i,j}$ valant 0 si $i = j$, et ± 1 en fonction de si j appartient aux k premiers cailloux ou aux k autres. On a $(1, \dots, 1)$ qui est solution car il y a k cailloux avec des 1 et k cailloux avec des -1. Il faut montrer que la dimension de $\ker A$ est 1

Je suis tombé sur cette leçon le jour de l'agrégation (voir section 5.3)

Plan détaillé :

I - Systèmes d'équations linéaires

Def : avec p équations et q inconnues

Lien avec les matrices, écriture sous la forme $AX = b$

Prop : si matrice carrée et inversible, une unique solution

Prop : solution grâce aux déterminants du système de Cramer

Prop : si matrice carrée, non inversible, deux cas possibles : $b \in \mathrm{Im}(A)$ et infinité de solution, $b \notin \mathrm{Im}(A)$ et pas de solutions

Def : systèmes sur-déterminés et sous-déterminés

II - Pivot de Gauss et application

1) Opérations élémentaires

Permutation

Dilatation

Transvection

Prop : on peut donc ajouter, à une ligne, une combinaison linéaire des autres lignes

Prop : ces opérations préservent les solutions du système

2) Systèmes échelonnés

Déf de système échelonné

Exemple de deux systèmes échelonné et non échelonné

3) Pivot de Gauss

Définition

Complexité en $O(n^3)$

8. juste une diagonale avec une sur-diagonale et une sous-diagonale

Application du pivot de Gauss

— résoudre AX=b

— trouver le rang d'une famille de vecteurs

— calculer le déterminant

— calculer l'inverse d'une matrice

— engendrer $GL_n(\mathbb{K})$ par les dilatations et transvections

— engendrer $SL_n(\mathbb{K})$ par les transvections

— savoir si une famille est libre

— savoir si une famille est génératrice

— trouver l'intersection de l'intersection de deux sous-espaces vectoriels

III - Décompositions pour faciliter la résolution

1) Décomposition LU

Théorème de décomposition LU

Complexité $O(n^3)$ pour trouver la décomposition avec pivot de Gauss, mais ensuite résolution en $O(n^2)$ (utile pour résoudre $AX = b$ avec des b différents)

2) Décomposition QR

Théorème de décomposition QR sur $\mathbb{R}$

Théorème de décomposition QR sur $\mathbb{C}$

Complexité $O(n^3)$

Méthode QR

IV - Méthodes itératives

1) Méthodes itératives $MX = NX + b$ $(A = M - N)$

Jacobi

Gauss Seidel

Relaxation

2) Méthode du gradient à pas optimal

Théorème d'équivalence entre $\bar{X}$ est solution de $AX = b$ SSI $\bar{X}$ minimise la fonctionnelle convexe

$$f : \begin{cases} \mathbb{R}^n & \to & \mathbb{R} \\ X & \mapsto & \frac{1}{2}\langle AX, X\rangle - \langle b, X\rangle \end{cases}$$

Algorithme du gradient à pas optimal

Remarque sur comment trouver le α_{k+1}

inégalité de Kantorovich

Méthode de gradient à pas optimal

<u>En annexe :</u>

- un exemple du pivot de Gauss avec les opérations de base et la mise sous forme échelonnée
- une décomposition LU
- une décomposition QR
- un graphe d'une fonction $f : \mathbb{R}^2 \to \mathbb{R}$ avec l'idée du gradient à pas optimal

Développements :

- Méthode QR
- Méthode de gradient à pas optimal

Références :

♥♥♥♥ - [GRI11] Joseph GRIFONE, *Algèbre Linéaire*

♥♥♥ - [CIA06] Philippe CIARLET, *Introduction à l'analyse numérique matricielle et à l'optimisation*

♥♥♥♥ - [AK02] Grégoire ALLAIRE et Sidi Mahmoud KABER, *Algèbre Linéaire Numérique*

♥♥♥ - [QSS07] Alfio QUARTERONI, Riccardo SACCO et Fausto SALERI, *Méthodes Numériques*

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

Rapport du jury :

Il faut tout d'abord noter que l'intitulé implique implicitement que le candidat ne doit pas se contenter de travailler sur $\mathbb{R}$. Le candidat pourra parler de la classification des formes quadratiques sur le corps des complexes et sur les corps finis. L'algorithme de Gauss doit être énoncé et pouvoir être mis en œuvre sur une forme quadratique simple.

Les notions d'isotropie et de cône isotrope sont un aspect important de cette leçon. On pourra rattacher cette notion à la géométrie différentielle.

Motivations :

On peut voir une forme quadratique comme un polynôme homogène de degré 2. On se sert de formes quadratiques dans différents domaines des mathématiques comme la différentiabilité où la différentielle seconde apparait comme une forme quadratique (Hessienne) mais aussi dans l'étude des coniques par exemple. J'ai construit mon plan autour de l'action

$$\begin{cases} GL_n(\mathbb{R}) \times \mathcal{M}_n(\mathbb{R}) & \to & \mathcal{M}_n(\mathbb{R}) \\ (P, A) & \mapsto & {}^tPAP \end{cases}$$

Je commence par parler des formes quadratiques en général (partie I), puis de la réduction en étudiant l'action par congruence (partie II), ensuite l'orthogonalité autrement dit le stabilisateur d'une forme quadratique représentée par une matrice A pour l'action par congruence (partie III), et enfin la classification des formes quadratiques sur différents corps (partie IV).

Points essentiels :

- la réduction de Gauss

Plan détaillé :

I - Forme quadratique et isotropie
- Définition
- Forme polaire
- Représentation matricielle
- Dimension
- Noyaux
- Rang
- Cône isotrope

II - Réductions
- Action par congruence
- Réduction de Gauss matricielle

Réduction de Gauss analytique

Diagonalisation

III - Orthogonalité

$O(q) = \{M \in GL_n(\mathbb{K}), {}^tMAM = A\}$ où A représente la forme quadratique q dans une base $\mathcal{B}$

Etude du groupe $O(p,s)$ pour une forme quadratique q de signature (p,s)

IV - Classification

Sur $\mathbb{C}$

Sur $\mathbb{R}$

Sur $\mathbb{F}_q$

Application : Loi de réciprocité quadratique

Développements :

- Etude du groupe $O(p,s)$
- Loi de réciprocité quadratique

Références :

♥♥♥♥♥ - [DSP11] Clément DE SEGUINS PAZZIS, *Invitations aux formes quadratiques*

♥♥ - [CG18] Philippe CALDERO et Jerôme GERMONI, *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2*

Leçon 182
Applications des nombres complexes à la géométrie.

Rapport du jury :

Cette leçon ne doit pas rester au niveau de la classe de Terminale. L'étude des inversions est tout à fait appropriée, en particulier la possibilité de ramener un cercle à une droite et inversement ; la formule de PTOLÉMÉE illustre bien l'utilisation de cet outil. On peut parler des suites définies par récurrence par une homographie et leur lien avec la réduction dans $SL_2(\mathbb{C})$.

S'ils le désirent, les candidats peuvent aussi étudier l'exponentielle complexe et les homographies de la sphère de RIEMANN. La réalisation du groupe SU_2 dans le corps des quaternions et ses applications peuvent trouver leur place dans la leçon. Il est possible de présenter les similitudes, les homographies et le birapport.

Questions possibles :

- Donner l'équation d'un cercle passant par 3 points z_a, z_b et z_c

  Réponse : Le déterminant $\begin{vmatrix} 1 & 1 & 1 & 1 \\ z & z_a & z_b & z_c \\ \overline{z} & \overline{z_a} & \overline{z_b} & \overline{z_c} \\ z\overline{z} & z_a\overline{z_a} & z_b\overline{z_b} & z_c\overline{z_c} \end{vmatrix}$

- Préciser la nuance entre orthogonalité et perpendicularité.
- On sait que les médiatrices des côtés d'un triangle (dans $\mathbb{R}^2$) sont concourantes. Réciproquement, si on a trois droites concourantes, sont-elles toujours les médiatrices des côtés d'un triangle ?

Plan détaillé :

I - Géométrie euclidienne

1) Lien entre $\mathbb{R}^2$ et $\mathbb{C}$

Définition affixe

2) Angles [TAU05]

Angles orientés

Action

3) Transformation du plan

Rotation

Translation

4) Barycentre

Définition

Repères barycentriques

Associativité des barycentres

Convergence de polygones vers l'isobarycentre

II - Géométrie projective

1) Espace projectif

projection stéréographique

$\mathbb{P}^1(\mathbb{C}) \simeq \mathbb{S}^2$

2) Homographie et birapport

Définition homographie

Générateurs de $SL_2(\mathbb{Z})$

Définition birapport

Conservation du birapport

Groupe circulaire

Développements :

- Convergence de polygones vers l'isobarycentre
- Générateurs de $SL_2(\mathbb{Z})$

Références :

♥♥♥♥ - [EID09] Jean-Denis EIDEN, *Géométrie analytique classique*

♥♥♥♥ - [AUD06] Michèle AUDIN, *Géométrie*

♥♥♥ - [TAU05] Patrice TAUVEL, *Géométrie*

♥♥♥ - [BOY15] Pascal BOYER, *Algèbre et Géométries*

Leçon 183
Utilisation des groupes en géométrie.

Rapport du jury :

C'est une leçon dans laquelle on s'attend à trouver des utilisations variées. On s'attend à ce que soient définis différents groupes de transformations (isométries, déplacements, similitudes, translations) et à voir résolus des problèmes géométriques par des méthodes consistant à composer des transformations. De plus, les actions de groupes sur la géométrie permettent aussi de dégager des invariants essentiels (angle, birapport, excentricité d'une conique). Les groupes d'isométries d'une figure sont incontournables.

Questions possibles :

- Définir une isométrie affine et une isométrie affine positive.
- $Isom^+$ est-il toujours d'indice 2 dans $Isom$?

Plan détaillé :

I - Géométrie affine [CG18]
  1) Groupe affine
     Définition affine
     Lien avec le groupe linéaire
  2) Action sur $GA(E)$
     Dilatation
     Translation
     Ellipse de Steiner
  3) Applications
     Pappus
     Desargues
     Menelaüs

II - Géométrie euclidienne
  1) Angles orientés [TAU05] [BOY15]
     Définition
     Action
  2) Isométries affines [CG18]
     Définition
     Isométries du cube et du tétraèdre
     Groupe icosaèdre

III - Géométrie projective [BOY15]
  1) Espaces projectifs.
     Desargues
     Pappus
  2) Homographie et birraport
     Définition homographie et l'action associée
     Générateurs de $SL_2(\mathbb{Z})$
     Définition birapport
     Préservation du birapport

Développements :

- Isométries du cube et du tétraèdre
- Générateurs de $SL_2(\mathbb{Z})$

Références :

♥♥♥♥ - [AUD06] Michèle AUDIN, *Géométrie*

♥♥♥ - [TAU05] Patrice TAUVEL, *Géométrie*

♥♥♥♥ - [BOY15] Pascal BOYER, *Algèbre et Géométries*

♥♥♥ - [CG18] Philippe CALDERO et Jerôme GERMONI, *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2*

Leçon 190
Méthodes combinatoires, problèmes de dénombrement.

Rapport du jury :

Il est nécessaire de dégager clairement différentes méthodes de dénombrement et de les illustrer d'exemples significatifs. De nombreux domaines de mathématiques sont concernés par des problèmes de dénombrement, cet aspect varié du thème de la leçon doit être mis en avant. L'utilisation de séries génératrices est un outil puissant pour le calcul de certains cardinaux. De plus, il est naturel de calculer des cardinaux classiques et certaines probabilités. Il est important de connaître l'interprétation ensembliste de la somme des coefficients binomiaux et ne pas se contenter d'une justification par le binôme de Newton. L'introduction des corps finis (même en se limitant aux cardinaux premiers) permet de créer un lien avec l'algèbre linéaire. Les actions de groupes peuvent également conduire à des résultats remarquables.

S'ils le désirent, les candidats peuvent aussi présenter des applications de la formule d'inversion de Möebius ou de la formule de Burnside. Des candidats ayant un bagage probabiliste pourront explorer le champ des permutations aléatoires, en présentant des algorithmes pour générer la loi uniforme sur le groupe symétrique $\mathfrak{S}_n$ et analyser certaines propriétés de cette loi uniforme (points fixes, cycles, limite $n \to +\infty$...).

Questions possibles :

- Donner le nombre de nombres à 3 chiffres ayant au moins un chiffre pair dans leur écriture décimale.

  Réponse : Considérer les nombres à 3 chiffres ayant que des chiffres impairs

- Combien existe-t-i de collier de perles avec 4 perles bleues, 3 perles blanches et 2 perles rouges ? (sachant qu'on peut faire coulisser les perles sur tout le collier qui est circulaire)

  Réponse : utiliser la formule de Burnside avec le groupe diédral

- Montrer la formule d'inversion de Pascal et en déduire le nombre de surjections de $[\![1;n]\!]$ dans $[\![1;p]\!]$ avec $p > n$.

  Réponse : voir Appendice

- Donner la relation de récurrence qui caractérise les nombres de Catalan. Donner une (ou plusieurs) interprétation(s) de ces nombres.
- Dénombrer les mots de taille n à partir des mots primitifs de taille $k \leq n$ sur un alphabet de 7 lettres.

Plan détaillé :

I - Outils basiques [FFF12] [DB04]

1) Ensembles finis

   $|A| = |B|$ SSI bijection entre A et B

   $|A \sqcup B| = |A| + |B|$

   Formule du crible

   Lemme des bergers

   Lemme des tiroirs

2) Combinatoire

Définition coefficient binomiaux
Triangle de Pascal
Arrangements

II - Formules d'inversion et séries génératrices
1) Formules d'inversion
Formule Pascal
Application : nombre de sujections
Formule de Möebius [PER96]
Indicatrice d'Euler
2) Séries formelles [FGN18]
Nombres de Catalan
Nombres de Bell

III - Action de groupes
1) Coloriages
Théorème de Fermat modulaire [LR03]
2) Action de groupes [ULM12]
Equations des classes
Application : Loi de réciprocité quadratique
Formule de Burnside
Nombres de coloriages du cube

IV - Dénombrement sur les corps finis
Définition $\mathbb{F}_q$
Nombre de bases de $\mathbb{F}_q^n$
Groupe linéaire
Dénombrement des matrices diagonalisables de $\mathbb{F}_q$
$SL_n(\mathbb{F}_q)$
Isomorphismes exceptionnels [CG18]

Développements :

- Théorème de Fermat modulaire
- Nombres de Bell
- Dénombrement des matrices diagonalisables de $\mathbb{F}_q$
- Loi de réciprocité quadratique

Références :

♥♥♥♥ - [DB04] Jean DE BIASI, *Mathématiques pour le CAPES et l'Agrégation interne*
♥♥♥ - [ULM12] Félix ULMER, *Théorie des Groupes*
♥♥♥ - [PER96] Daniel PERRIN, *Cours d'Algèbre*
♥♥♥♥ - [FFF12] Dominique FOATA, Jacques FRANCHI et Aimé FUCHS, *Calcul des probabilités*
♥♥♥ - [CG18] Philippe CALDERO et Jerôme GERMONI, *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2*
♥♥♥ - [FGN18] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS, *Oraux X-ENS, Algèbre 1*
♥♥ - [LR03] Bruce LANDMAN et Aaron ROBERTSON, *Ramsey Theory on the Integers*

2.4 Métaplans d'analyse

Leçon 203
Utilisation de la notion de compacité.

Rapport du jury :

Il est important de ne pas concentrer la leçon sur la compacité en général et d'éviter la confusion entre *utilisation de la notion compacité* et *notion de compacité*. Le jury recommande vivement de rester en priorité dans le cadre métrique. Néanmoins, on attend des candidats d'avoir une vision synthétique de la compacité. Des exemples d'applications comme le théorème de Heine et le théorème de Rolle doivent y figurer et leur démonstration être connue. Par ailleurs, le candidat doit savoir quand la boule unité d'un espace vectoriel normé est compacte. Des exemples significatifs d'utilisation comme le théorème de Stone-Weierstrass (version qui utilise la compacité), des théorèmes de point fixe, voire l'étude qualitative d'équations différentielles, sont tout à fait envisageables. Le rôle de la compacité pour des problèmes d'existence d'extrema mériterait d'être davantage étudié. On peut penser ensuite à des exemples en dimension $n \geqslant 2$.

Pour aller plus loin, les familles normales de fonctions holomorphes fournissent des exemples fondamentaux d'utilisation de la compacité. Les opérateurs auto-adjoints compacts sur un espace de Hilbert relèvent également de cette leçon, et on pourra développer l'analyse de leurs propriétés spectrales.

Questions possibles :

- Pour f est continue et bornée, montrer qu'elle atteint ses bornes ?
- Si f est coercive, est-elle minorée ?
- Comment on montre que les compacts de $\mathbb{R}$ sont les fermés bornés ?
- Montrer que f est continue en a SSI $\forall x_n \to a$, on a $f(x_n) \xrightarrow[n\to\infty]{} f(a)$.
- Montrer que si $f : [0,1] \to \mathbb{R}$ est continue et telle que
$$\int_0^1 f(x)x^k dx = 0 \quad \forall k \in \mathbb{N}$$
Alors f est identiquement nulle.
Réponse : Utiliser la convergence uniforme de polynômes vers f sur $[0,1]$
- Quelle est la limite uniforme d'une suite de polynômes sur $\mathbb{R}$?
Réponse : C'est un polynome

Motivations :

La notion de compacité est une notion utile pour étudier des ensembles infinis avec des outils finis. En effet, de n'importe quel sous recouvrement quelconque de notre ensemble, on peut extraire un sous recouvrement **fini** de notre ensemble. Cela aura un rôle important dans l'étude des fonctions. Ainsi une fois avoir étudié les propriétés générales avec la définition de Borel–Lebesgue et de Bolzano–Weierstrass qui sont équivalentes dans le cadre métrique, on va étudier ce que la compacité apporte aux fonctions continues (*Heine* : uniforme continuité d'une fonction continue sur un compact, etc.), puis ce que l'on peut dire des espaces de fonctions continues sur un compact (Par exemple, on sait que les fonctions continues bornées vers un Banach forment un espace complet pour la norme uniforme, comme les fonctions continues sur un compact sont bornées, on a donc la complétude des fonctions continues sur un compact).

Je me place dans un cadre métrique

Plan détaillé :

I - Généralité et cadre
  1) Borel–Lebesgue
    Définition
    Morphismes d'algèbre de $\mathcal{C}(K,\mathbb{R})$ sur $\mathbb{R}$
  2) Bolzano–Weierstraß
    Définition
    Compacts de $\mathbb{R}$ pour $|.|$
    Compacts de $\mathbb{R}^n$ pour $\|.\|_\infty$
  3) Propriétés
    Théorème de Tychonoff fini et dénombrable
    Théorème de Riesz

II - Fonction continue sur un compact
  1) Uniforme continuité
    Théorème de Heine
    Théorème de Dini
  2) Extrema
    Théorème de Rolle
  3) Point fixe
    Théorème variante du point fixe de Picard avec $|f(x)-f(y)|<|x-y|$

III - Espace de fonctions continues sur un compact
  1) Complétude
    Théorème de complétude de $(\mathcal{C}(K,F),\|.\|_\infty)$ pour F complet
    Rappel : Point fixe de Picard
    Cauchy Lipschitz et lemme de Gronwall
  2) Relative Compacité
    Définition
    Théorème d'Ascoli
    Cauchy Peano
    Injection des Sobolev
  3) Convergence uniforme
    Approximation uniforme par des Polynomes
    Théorème de Stone Weierstraß

Développements :

- Morphismes d'algèbre de $\mathcal{C}(K,\mathbb{R})$ sur $\mathbb{R}$
- Cauchy Lipschitz et lemme de Gronwall

Références :

♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*
♥♥♥ - [QUE16] Hervé QUEFFELEC, *Topologie*
♥♥♥♥ - [RDO98] Edmond RAMIS, Claude DESCHAMPS et Jacques ODOUX, *Cours de Mathématiques 3 : Topologie et éléments d'analyse*

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

Rapport du jury :

Le jury rappelle qu'une telle leçon doit contenir beaucoup d'illustrations et d'exemples, notamment avec quelques calculs élémentaires de normes subordonnées (notion qui met en difficulté un trop grand nombre de candidats). Le lien avec la convergence des suites du type $X_{n+1} = AX_n$ doit être connu (et éventuellement illustré, sans que cela puisse être mis au cœur de la leçon, de considérations d'analyse numérique matricielle). Lors du choix de ces exemples, le candidat veillera à ne pas mentionner des exemples pour lesquels il n'a aucune idée de leur pertinence et à ne pas se lancer dans des développements trop sophistiqués.

La justification de la compacité de la boule unité en dimension finie doit être maîtrisée. Il faut savoir énoncer le théorème de Riesz sur la compacité de la boule unité fermée d'un espace vectoriel normé. Le théorème d'équivalence des normes en dimension finie, ou le caractère fermé de tout sous-espace de dimension finie d'un espace normé, sont des résultats fondamentaux à propos desquels les candidats doivent se garder des cercles vicieux. Des exemples d'espaces vectoriels normés de dimension infinie ont leur place dans cette leçon et il faut connaître quelques exemples de normes usuelles non équivalentes, notamment sur des espaces de suites ou des espaces de fonctions et également d'applications linéaires qui ne sont pas continues. On peut aussi illustrer le théorème de Riesz sur des exemples simples dans le cas des espaces classiques de dimension infinie.

Les espaces de Hilbert ont également leur place dans cette leçon, mais le jury met en garde contre l'écueil de trop s'éloigner du cœur du sujet.

Questions possibles :

- Comment on prouve l'équivalence des normes en dimension finie ?
- Qu'en est-il de l'exemple de l'appendice ?
- Comment on prouve le théorème de Riesz ?
- Donner des normes non équivalentes et montrer qu'elles ne le sont pas

  Réponse : Les normes $\|.\|_\infty$, $\|.\|_1$, $\|.\|_2$ sur $\mathcal{C}(\mathbb{R}, \mathbb{R})$
- Donner un schéma de preuve pour le théorème de Banach-Steinhaus.

Motivations :

L'étude des espaces normés est très riche et permet d'obtenir beaucoup de résultats. Tout d'abord, elle se justifie par le fait que nous vivons dans un espace vectoriel normé. Une norme est plus adaptée dans ce cadre que la distance. Elle permet notamment d'avoir des théorèmes tels que le théorème de Riesz qui donne une caractérisation des espaces vectoriels normés de dimension finie.On peut aussi parler de complétude et introduire les espaces de Banach. De plus, la structure d'espace vectoriel permet de parler d'applications linéaires qui permettent d'étudier des objets localement (à l'ordre 1) comme par exemple approcher des équations différentielles par son linéarisé ou juste de parler de différentielles qui sont des applications linéaires continues. La linéarité permet de prouver la continuité d'une application en étudiant la continuité en un seul point (par exemple 0).

Plan détaillé :

I - Espace Vectoriel Normé

1) Normes

Normes

Continuité

Équivalence des normes en dimension finie

Il existe des normes non équivalentes en dimension infinie

2) Application linéaire

Définition des applications linéaires

EVN avec la norme d'opérateur

Norme sous multiplicative

3) Dimension finie

Prop : les application linéaires sont continues

Prop : les compacts sont exactement les fermés bornés

Théorème de Riesz

II - Espace de Banach

1) Définitions et propriétés

Théorème de Riesz–Fisher pour la complétude des L^p

$(\mathcal{C}_b(E,F), \|.\|_\infty)$ complet si F est complet

Théorème de Point Fixe de Picard

Cauchy Lipschitz et lemme de Gronwall

2) Théorème de Baire et applications

Théorème de Baire

Banach–Steinhaus

Théorème de l'application ouverte

Théorème d'isomorphisme de Banach

III - Espace de Hilbert [HL99]

1) Définition

Cauchy–Schwarz

Prop : le produit scalaire fournit une norme

Définition Hilbert

2) Projection sur un convexe fermé

Théorème de projection

Corollaire : supplémentaire orthogonal

Corollaire : théorème de densité

Corollaire : théorème de représentation de Riesz

Développements :

- Cauchy Lipschitz et lemme de Gronwall
- Banach–Steinhaus

Références :

♥♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥ - [HAU07] Bertrand HAUCHECORNE, *Les contre-exemples en Mathématiques*

♥♥♥♥ - [ROU09] François ROUVIÈRE, *Petit Guide de Calcul Différentiel*

♥♥♥ - [HL99] Francis HIRSCH et Gilles LACOMBE, *Éléments d'analyse fonctionnelle*

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

Rapport du jury :

Il s'agit d'une leçon qui exige une bonne maîtrise du calcul différentiel. Même si le candidat ne propose pas ces thèmes en développement, on est en droit d'attendre de lui des idées de démonstration des deux théorèmes fondamentaux qui donnent son intitulé à la leçon. Il est indispensable de savoir mettre en pratique le théorème des fonctions implicites au moins dans le cas de deux variables réelles. On attend des applications en géométrie différentielle notamment dans la formalisation de la méthode des multiplicateurs de Lagrange. En ce qui concerne la preuve du théorème des extrema liés, la présentation de la preuve par raisonnement "sous-matriciel" est souvent obscure ; on privilégiera si possible une présentation géométrique s'appuyant sur l'espace tangent. Plusieurs inégalités classiques de l'analyse peuvent se démontrer avec ce point de vue : arithmético-géométrique, Hölder, Carleman, Hadamard,...

Pour aller plus loin, l'introduction des sous-variétés est naturelle dans cette leçon. Il s'agit aussi d'agrémenter cette leçon d'exemples et d'applications en géométrie, sur les courbes et les surfaces.

Questions possibles :

- Expliciter le lien entre le théorème des fonctions implicites et le théorème de Cauchy-Lipschitz.
- Calculer la différentielle en tout point de l'application déterminant $det : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$.

  Réponse : Indications : On commence par calculer la différentielle de cette application en I_n. On la calcule ensuite en tout point $M \in GL_n(\mathbb{R})$. Enfin, on étend la formule à $\mathcal{M}_n(\mathbb{R})$ tout entier, par densité de $GL_n(\mathbb{R})$ dans $\mathcal{M}_n(\mathbb{R})$ et continuité de l'application det (qui est polynomiale en les composantes).

Motivations :

On voudrait étendre l'inversion de fonctions pour des fonctions à plusieurs varaibles. Quand $f : \mathbb{R} \to \mathbb{R} \in \mathcal{C}^1$, on peut inverser localement dès que la dérivée est non nulle. On va donc avoir un résultat similaire en ayant la jacobienne qui est inversible, c'est ce qu'on appelle le théorème d'inversion locale. Un théorème qui en découle est le théorème des fonctions implicites, qui permet de représenter localement une courbe par le graphe d'une fonction (sous certaines hypothèses). Une autre application de l'inversion locale est l'équivalence entre les définitions des sous variétés. C'est pour cela qu'on parlera de sous variétés et du théorème des extrema liés dans cette leçon. D'autant plus qu'on peut prouver le théorème des extrema liés seulement avec le théorème d'inversion locale, cependant le rapport du jury nous rappelle qu'il préfère la preuve géométrique avec les sous-variétés.

J'ai rédigé le plan de cette leçon (voir ici)

Je me place dans le cadre de $\mathbb{R}^p$

I - Théorème d'Inversion Locale

1) Théorème d'Inversion Locale

Version locale

Version globale

Version holomorphe

2) Application en analyse

Changement de coordonnées

fonctions classiques : exp, det, l'inverse, ...

perturbation de l'identité

3) Application en géométrie et en algèbre

Théorème de D'Alembert Gauss

Formes quadratiques

Lemme de Morse

Image de l'exponentielle

II - Théorème des Fonctions Implicites

1) Théorème des Fonctions Implicites

Théorème

Lien avec Cauchy–Lipschitz, Théorème de Point Fixe de Picard et TIL [ROU09]

2) Application

Solution approchée de racines de polynomes

Développement asymptotique d'une intégrale (exercice du [ROU09])

III - Sous-variétés

1) Définitions

Sous-variétés

Plan tangent

2) Extrema liés

Théorème des extrema liés

Inégalité arithmético-géométrique

Inégalité de Hölder

Développements :

- Image de l'exponentielle
- Théorème des extrema liés

Références :

♥♥♥♥♥ - [ROU09] François ROUVIÈRE, *Petit Guide de Calcul Différentiel*

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

Rapport du jury :

Comme souvent en analyse, il est tout à fait opportun d'illustrer dans cette leçon un exemple ou un raisonnement à l'aide d'un dessin. Il faut savoir faire la distinction entre propriétés locales (caractérisation d'un extremum local) et globales (existence par compacité, par exemple). Dans le cas important des fonctions convexes, un minimum local est également global. Les applications de la minimisation des fonctions convexes sont nombreuses et elles peuvent illustrer cette leçon.

L'étude des algorithmes de recherche d'extremums y a toute sa place : méthode du gradient et analyse de sa convergence, méthode à pas optimal,... Le cas particulier des fonctionnelles sur $\mathbb{R}^n$ de la forme $\frac{1}{2}\langle Ax, x\rangle - \langle b, x\rangle$, où A est une matrice symétrique définie positive, ne devrait pas poser de difficultés (la coercivité de la fonctionnelle pose problème à de nombreux candidats). Les problèmes de minimisation sous contrainte amènent à faire le lien avec les extrema liés et la notion de multiplicateur de Lagrange. Sur ce point, certains candidats ne font malheureusement pas la différence entre recherche d'extremums sur un ouvert ou sur un fermé. Une preuve géométrique des extrema liés sera fortement valorisée par rapport à une preuve algébrique, formelle et souvent mal maîtrisée. On peut ensuite mettre en œuvre ce théorème en justifiant une inégalité classique : arithmético-géométrique, Hölder, Carleman, etc... Enfin, la question de la résolution de l'équation d'Euler-Lagrange peut donner l'opportunité de mentionner la méthode de Newton.

Les candidats pourraient aussi être amenés à évoquer les problèmes de type moindres carrés, ou, dans un autre registre, le principe du maximum et des applications.

Plan détaillé :

I - Existence et Unicité

Définition

1) Utilisation de la compacité

Existence

2) Utilisation de la convexité

Convexe + local $\Longrightarrow$ global

3) Hilbert [HL99]

Projection sur un convexe

Théorème de Lax-Milgram

4) Fonctions holomorphes

Principe du maximum

II - Localisation et calcul différentiel

1) 1er ordre

Lien entre f' et extrema

2) 2nd ordre

Lien entre f'' et extrema

3) Extrema sous contraintes

Théorème des extrema liés

III - Optimisation

1) Newton

Méthode de Newton

2) Gradient à pas optimal

Méthode de gradient à pas optimal

Développements :

- Théorème des extrema liés
- Méthode de gradient à pas optimal
- Méthode de Newton

Références :

♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥ - [AK02] Grégoire ALLAIRE et Sidi Mahmoud KABER, *Algèbre Linéaire Numérique*

♥♥♥♥ - [ROU09] François ROUVIÈRE, *Petit Guide de Calcul Différentiel*

♥♥ - [HL99] Francis HIRSCH et Gilles LACOMBE, *Éléments d'analyse fonctionnelle*

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

Rapport du jury :

Une nouvelle fois, le jury s'alarme des nombreux défauts de maîtrise du théorème de Cauchy- Lipschitz et, plus généralement, de l'extrême faiblesse des connaissances sur les équations différentielles. Il est regrettable de voir des candidats ne connaître qu'un énoncé pour les fonctions globalement lipschitziennes ou, plus grave, mélanger les conditions sur la variable de temps et d'état. Les notions de solution maximale et de solution globale sont souvent confuses. Le théorème de sortie de tout compact est attendu. Bien évidemment, le jury attend des exemples d'équations différentielles non linéaires. Le lemme de Grönwall semble trouver toute sa place dans cette leçon mais est trop rarement énoncé. L'utilisation du théorème de Cauchy-Lipschitz doit pouvoir être mise en œuvre sur des exemples concrets. Les études qualitatives doivent être préparées et soignées.

Pour les équations autonomes, la notion de point d'équilibre permet des illustrations pertinentes comme par exemple les petites oscillations du pendule. Trop peu de candidats pensent à tracer et discuter des portraits de phase alors que l'intitulé de la leçon y invite clairement.

Il est possible d'évoquer les problématiques de l'approximation numérique dans cette leçon en présentant le point de vue du schéma d'Euler. On peut aller jusqu'à aborder la notion de problèmes raides et la conception de schémas implicites pour autant que le candidat ait une maîtrise convenable de ces questions.

Questions possibles :

- Comment on démontre le Lemme de Gronwall ?
- Que dit le théorème de Cauchy Peano ?
- Tracer le portrait de phase de l'équation différentielle suivante

$$X' = AX \text{ avec } A = \begin{pmatrix} -1 & 2 \\ -3 & 4 \end{pmatrix}$$

Motivations :

On sait résoudre des équations d'inconnue x, on s'intéresse ici à des équations où les inconnus sont des fonctions $y(x)$, ce sont des équations différentielles. On va étudier l'existence et l'unicité des solutions grâce à des théorèmes puissants comme le théorème de Cauchy Lipschitz. Ensuite, on s'intéressera aussi à la stabilité des solutions. Soit une solution y de condition initiale $y(t_0) = y_0$, si on fait varier un petit peu la condition initiale autour de y_0, est-ce que la solution reste proche de y ? (stabilité) Est-ce que la solution tend vers y ? (asymptotique stabilité).

Plan détaillé :

I - Existence et Unicité de solutions

Définition solution maximale et globale

Lemme de Gronwall

Cauchy Lipschitz localement lipschitzien

Cauchy Peano

Cauchy Lipschitz et lemme de Gronwall

Lemme des bouts

II - Exemples d'études

1) EDO linéaires

Résolution

Variation de la constante

2) Équations différentielles particulières

Bernoulli

Ricatti

3) $y'' + qy = 0$

Nombres de zéros des solutions d'une équation différentielle

III - Stabilité des systèmes différentielles autonomes

1) Définitions

stable

asymptotique stable

2) Linéaire

Théorème

Portraits de phase en dimension 1 et 2

3) Non linéaire

Théorème de Lyapunov [ROU09]

Développements :

- Cauchy Lipschitz et lemme de Gronwall
- Nombres de zéros des solutions d'une équation différentielle

Références :

♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥♥♥ - [DEM16] Jean-Pierre DEMAILLY, *Analyse numérique et équations différentielles*

♥♥♥ - [ROU09] François ROUVIÈRE, *Petit Guide de Calcul Différentiel*

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

Rapport du jury :

Le jury attend d'un candidat qu'il sache déterminer rigoureusement la dimension de l'espace vectoriel des solutions. Le cas des systèmes à coefficients constants fait appel à la réduction des matrices qui doit être connue et pratiquée. Le jury attend qu'un candidat puisse mettre en œuvre la méthode de variation des constantes pour résoudre une équation différentielle linéaire d'ordre 2 simple (à coefficients constants par exemple) avec second membre ; un trop grand nombre de candidats se trouve déstabilisés par ces questions.

L'utilisation des exponentielles de matrices a toute sa place ici et doit être maitrisée. Les problématiques de stabilité des solutions et le lien avec l'analyse spectrale devraient être exploitées.

Le théorème de Cauchy-Lipschitz linéaire constitue un exemple de développement pertinent pour cette leçon. Les résultats autour du comportement des solutions, ou de leurs zéros, de certaines équations linéaires d'ordre 2 (Sturm, Hill-Mathieu,...) sont aussi d'autres possibilités.

Pour aller plus loin, la résolution au sens des distributions d'équations du type $T' = 0$, ou des situations plus ambitieuses, trouvera sa place dans cette leçon.

Questions possibles :

- Soit A une matrice. Démontrer que $\frac{\mathrm{d}}{\mathrm{d}t}\exp(tA) = A\exp(tA)$.
- Résoudre $y'' - y = \tan^2(t)$.
- Soient $A \in \mathcal{M}_n(\mathbb{R})$ et $B \in \mathcal{M}_{n,m}(\mathbb{R})$. Soit $T \in \mathbb{R}$. On considère l'application Φ définie de $\mathcal{C}^0([0,T],\mathbb{R}^m)$ dans $\mathbb{R}^m$ par : $\Phi : u \mapsto \int_0 Te^{(T-t)A}Bu(t)\mathrm{d}t$. Montrer que $Ker(\Phi)$ est fermé.

Plan détaillé :

I - Existence et Unicité de solutions [GOU08b]
- Définition solution maximale / globale
- Théorème de Cauchy Lipschitz
- Écriture matricielle de système différentiel

II - Résolution explicite [LES15]
- Ensemble des solutions
- Translatés d'une fonction $\mathcal{C}^1$
- Wronskien
- Variation de la constante
- Cas coefficients constants avec $\exp A$

III - Étude asymptotique

1) Points d'équilibre
- Stabilité
- Théorème de Lyapunov

2) Etude de $y'' + qy = 0$ [QZ07]

Nombres de zéros des solutions d'une équation différentielle

IV - Équation différentielles sur les distributions [LES12]

$T' = 0$

$xT = 0$

$xT = 1$

Développements :

- Translatés d'une fonction $\mathcal{C}^1$
- Nombres de zéros des solutions d'une équation différentielle

Références :

♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥♥♥ - [DEM16] Jean-Pierre DEMAILLY, *Analyse numérique et équations différentielles*

♥♥ - [LES12] Ahmed LESFARI, *Distributions, analyse de Fourier et transformation de Laplace*

♥♥♥ - [LES15] Ahmed LESFARI, *Équations différentielles ordinaires et équations aux dérivées partielles*

♥♥♥ - [QZ07] Hervé QUEFFELEC et Claude ZUILY, *Analyse pour l'agrégation*

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

Rapport du jury :

Cette leçon permet souvent aux candidats de s'exprimer. Il ne faut pas négliger les suites de nombres complexes mais les suites vectorielles (dans R^n) ne sont pas dans le sujet. Le jury attire l'attention sur le fait que cette leçon n'est pas uniquement à consacrer à des suites convergentes, mais tout comportement asymptotique peut être présenté. Le théorème de Bolzano-Weierstrass doit être cité et le candidat doit être capable d'en donner une démonstration. On attend des candidats qu'ils parlent des limites inférieure et supérieure d'une suite réelle bornée, et qu'ils en maîtrisent le concept. Les procédés de sommation peuvent être éventuellement évoqués mais le théorème de Césaro doit être mentionné et sa preuve maîtrisée par tout candidat à l'agrégation. Les résultats autour des sous-groupes additifs de $\mathbb{R}$ permettent d'exhiber des suites denses remarquables et l'ensemble constitue un joli thème. Des thèmes des leçons 225 et 226 peuvent également se retrouver dans cette leçon.

Pour aller plus loin, un développement autour de l'équirépartition est tout à fait envisageable. La méthode de Newton peut aussi illustrer la notion de vitesse de convergence.

Questions possibles :

- Montrer qu'une suite de Cauchy dont une sous-suite converge est convergente.
- Comment caractérise-t-on la convergence quadratique d'une suite $(u_n)_{n\in\mathbb{N}}$ qui converge vers une limite l ?

  Réponse : Il y a convergence quadratique d'une suite (u_n) vers l lorsqu'il existe une constante $C > 0$ telle que pour tout $n \in \mathbb{N}$, on ait $|u_{n+1} - l| \leqslant C|u_n - l|^2$ et (u_n) converge vers l.
- Comment on prouve que $\mathrm{Adh}(u_n) = \bigcap_{n\in\mathbb{N}} \overline{\{u_k, k \geqslant n\}}$.

  Réponse : Soit $l \in \bigcap_{n\in\mathbb{N}} \overline{\{u_k, k \geqslant n\}}$. Par équivalence, pour tout $n \in \mathbb{N}$, $l \in \overline{\{u_k, k \geqslant n\}}$. Ainsi $\forall n \in \mathbb{N}$, $\forall \varepsilon > 0$, $\exists k \geqslant n$ tel que $u_k \in \mathrm{B}(l, \varepsilon)$. En permutant les deux quantificateurs $\forall$ du début, on trouve $\forall \varepsilon > 0$, $\forall n \in \mathbb{N}$, $\exists k \geqslant n$ tel que $u_k \in \mathrm{B}(l, \varepsilon)$ qui est la définition d'une valeur d'adhérence car on peut alors construire une sous suite qui converge vers l. On a procédé par équivalence, donc l'égalité est vraie.
- Soit une suite (z_n) dans $\mathbb{C}$ qui est bornée et qui n'admet qu'une seule valeur d'adhérence α. Montrer que (z_n) converge vers cette valeur α.

  Réponse : On pose la suite $u_n = |z_n - \alpha|$ qui est une suite réelle. On a $\liminf u_n = \limsup u_n = 0$ car α est la seule valeur d'adhérence de z_n qui est supposée bornée. Donc (u_n) converge vers 0. Ainsi $|z_n - \alpha| \xrightarrow[n\to+\infty]{} 0$. Ce qui nous donne $z_n \xrightarrow[n_\infty]{} \alpha$ dans $\mathbb{C}$.
- Donner une suite ayant $\mathbb{N}$ comme ensemble de valeurs d'adhérence.

  Réponse : On peut prendre la suite u_n définie par $u_0 = 0$, $u_1 = 1$, $u_2 = 0$, $u_3 = 1$, $u_4 = 2$, $u_5 = 0$, $u_6 = 1$, $u_7 = 2$, $u_8 = 3$, $u_9 = 0\ldots$ Ainsi, pour chaque $n \in \mathbb{N}$, (u_n) passe une infinité de fois par n.
- Donner une suite ayant $\mathcal{D}$ un ensemble dénombrable fermé d'éléments comme ensemble de valeurs d'adhérence.

  Réponse : On s'appuie sur la question précédente. Si $\mathcal{D} = \{x_n, n \in \mathbb{N}\}$, on pose la suite $v_n = x_{u_n}$ avec u_n la suite définie dans la question précédente.

  On veut prouver que $\mathcal{D} = \bigcap_{n\in\mathbb{N}} \overline{\{v_k, k \geqslant n\}}$ grâce à la Question 2.

On a $\mathcal{D} \supset \bigcap_{n\in\mathbb{N}} \overline{\{v_k, k \geqslant n\}}$ car $\{v_n, n \in \mathbb{N}\} \subset \{x_n, n \in \mathbb{N}\}$ et que $\mathcal{D}$ est fermé.

Réciproquement, puisque (u_n) passait une infinité de fois par n pour tout $n \in \mathbb{N}$, (v_n) va passer une infinité de fois par chaque x_n. Donc $\mathcal{D} \subset \bigcap_{n\in\mathbb{N}} \overline{\{u_k, k \geqslant n\}}$, ainsi $\mathrm{Adh}(u_n) = \mathcal{D}$.

- Donner une suite ayant F un fermé de $\mathbb{R}$ comme ensemble de valeurs d'adhérence.

  Réponse : Puisque $\mathbb{R}$ est séparable et que F est un sous-ensemble de $\mathbb{R}$, alors F est séparable, donc il existe une famille $\mathcal{D}$ dénombrable et dense dans F. On applique la question précédente, on a donc une suite (w_n) dont les valeurs d'adhérence sont incluses dans F, car F est fermé. De plus, pour tout $x \in F$, pour tout $\varepsilon > 0$, il existe une sous suite de (w_n) qui converge vers une valeur de F qui est proche de ε de la valeur x (car $\mathcal{D}$ est dense dans F). Donc x est valeur d'adhérence de (w_n), donc $F = \mathrm{Adh}(w_n)$.

- Soit $(u_n)_{n\in\mathbb{N}}$ une suite récurrente bornée définie par un $f \in \mathcal{C}^1$ et telle que (u_n) converge vers une limite l. De plus, $|f'(l)| > 1$, que peut-on dire du comportement de (u_n) lorsque n tend vers l'infini ?

  Réponse : Le point fixe l est un point répulsif, donc pour converger vers l, il faut que la suite stationne au bout d'un moment sur l.

  Quitte à prendre $-f$, on suppose que $f'(l) > 1$, ainsi comme f' est continue et $f'(l) > 1$, il existe $\alpha > 0$ tel que sur l'intervalle $J :=]l - \alpha; l + \alpha[$, on ait $f' > 1$. Puisque (u_n) converge vers l, il existe un rang n_0 tel que pour tout $n \geqslant n_0$, $|u_n - l| < \alpha$.

  Pour $n \geqslant n_0$, on utilise l'égalité des accroissements finis pour f sur $]l, u_n[$, ce qui nous donne $e \in]l, u_n[$ et $|f(u_n) - f(l)| = |f'(e)||u_n - l|$. De plus, on sait que $f'(e) > 1$ car $]l, u_n[\subset J$. Ainsi pour $n \geqslant n_0$, $|u_{n+1} - l| = |f(u_n) - f(l)| = |f'(e)||u_n - l| > |u_n - l|$. On a alors $|u_{n+1} - l| > |u_n - l|$, ce qui est absurde car on sait que (u_n) converge vers l. Donc l'intervalle $]l, u_n[$ est vide. Ainsi pour tout $n \geqslant n_0$, $u_n = l$ car l est un point fixe de f, donc dès que la suite atteint la valeur l, elle stationne.

- Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_n = \sin\left(\frac{\pi}{2}(2+\sqrt{3})^n\right)$ pour tout $n \in \mathbb{N}$. Montrer que (u_n) converge.

  Réponse : On calcule $(2+\sqrt{3})^n$:

  $$\forall n \in \mathbb{N}, \quad (2+\sqrt{3})^n = \sum_{k=0}^{n} \binom{n}{k} \sqrt{3}^k 2^{n-k} = a_n + \sqrt{3} b_n$$

  avec a_n et b_n entiers. En calculant $(2-\sqrt{3})^n$, on trouve $a_n - \sqrt{3}b_n$ (avec les mêmes a_n et b_n). Ainsi, $(2+\sqrt{3})^n = a_n + \sqrt{3}b_n = 2a_n - (a_n - \sqrt{3}b_n) = 2a_n - (2-\sqrt{3})^n$ avec $a_n \in \mathbb{Z}$. Donc $\sin\left(\frac{\pi}{2}(2+\sqrt{3})^n\right) = \sin\left(\frac{\pi}{2}(2a_n - (2-\sqrt{3})^n)\right) = \sin\left(\pi a_n - \frac{\pi}{2}(2-\sqrt{3})^n\right) = (-1)^{a_n+1} \sin\left(\frac{\pi}{2}(2-\sqrt{3})^n\right)$ qui converge vers 0 car $(2-\sqrt{3})^n$ converge vers 0 quand n tend vers $+\infty$. Donc (u_n) converge vers 0.

Motivations :

Dès l'antiquité, les Grecs essayaient d'approcher π au moyen de suites, en faisant tendre des polygones internes et externes à un cercle. On veut donc étudier des suites pour deux raisons, la première est de vouloir approcher un objet et donc on crée une suite (point de vue où l'on a une limite et on crée une suite), la deuxième est d'avoir une suite et de vouloir étudier sa limite ou du moins son comportement (point de vue où l'on a une suite et on veut avoir sa limite). Grâce aux suites, on peut approcher des réels (π, e, γ, ϕ,...), des zéros de fonctions (Newton, sécante,...), des intégrales de Riemann (rectangles, trapèzes, point milieu,...), des équations différentielles (schéma d'Euler, Runge Kutta,...). Dans la dernière partie, on voudra affaiblir la notion de convergence usuelle, en parlant de convergence au sens de Césaro. Cela permet de faire converger la suite $((-1)^n)_{n\in\mathbb{N}}$ par exemple, alors qu'elle ne converge pas de manière classique. On aurait pu parler aussi de convergence au sens d'Abel qui est encore plus faible que celle de Césaro.

J'ai rédigé le plan de cette leçon (voir ici) et j'ai écrit Mon mémoire sur la leçon 223.

Plan détaillé :

I - Convergence
- Déf : limite dans $\mathbb{R}$ et dans $\mathbb{C}$
- Prop : fonction continue et caractérisation séquentielle de la limite
- Prop : opérations sur les limites
- Déf : suites de Cauchy
- Prop : monotonie + borné implique convergence
- Thrm des gendarmes
- Déf : Suites adjacentes
- Application : Critère spécial des séries alternées
- Exemples de suites : arithmétiques / géométriques, etc
- Équivalence de suites

II - Valeur d'adhérence
- Déf : borne sup / borne inf
- Déf : limsup / liminf
- Déf : sous-suite
- Déf : valeurs d'adhérence
- Prop : $\mathrm{Adh}(u_n) = \bigcap_{n\in\mathbb{N}} \overline{\{u_k, k \geqslant n\}}$
- Prop : Adh fermé
- Thrm : Bolzano-Weierstrass
- Application : principe des compacts décroissants

III - Utilisation des suites
1) Trouver des zéros de fonctions
   - Dichotomie
   - Méthode de Newton
2) Intégrales
   - Intégrales de Riemann
3) Équations différentielles
   - Schéma d'Euler explicite
   - Schéma d'Euler implicite

IV - Convergence au sens de Césaro
- Théorème de Césaro
- Réciproques partielles de Césaro
- Définition : convergence au sens de Césaro
- Application : Fejer, Dirichlet

Développements :
- Réciproques partielles de Césaro
- Méthode de Newton

Références :
- ♥♥♥♥ [GOU08b] Xavier GOURDON, *Analyse*
- ♥♥♥ [COM95] Jean COMBES, *Suites et séries*
- ♥♥ [ROU09] François ROUVIÈRE, *Petit Guide de Calcul Différentiel*

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

Rapport du jury :

Cette leçon doit permettre aux candidats d'exprimer leur savoir-faire sur les techniques d'analyse élémentaire que ce soit sur les suites, les séries ou les intégrales. On peut par exemple établir un développement asymptotique à quelques termes des sommes partielles de la série harmonique, ou bien la formule de Stirling que ce soit dans sa version factorielle ou pour la fonction Γ. On peut également s'intéresser aux comportements autour des singularités de fonctions spéciales célèbres. Du côté de l'intégration, on peut évaluer la vitesse de divergence de l'intégrale de la valeur absolue du sinus cardinal, avec des applications pour les séries de Fourier, voire présenter la méthode de Laplace.

Par ailleurs, le thème de la leçon permet l'étude de suites récurrentes (autres que le poncif $u_{n+1} = \sin u_n$), plus généralement de suites ou de fonctions définies implicitement, ou encore des études asymptotiques de solutions d'équations différentielles (sans résolution explicite).

On peut aller plus loin en abordant des techniques de phase stationnaire et en en discutant des applications.

Plan détaillé :

I - Définition et premiers exemples
- 1) Comparaison [GOU08b] [ROM04]
  - Echelles de comparaison
- 2) DL
  - Définition
  - Taylor Young
- 3) Développement asymptotique
  - Sommation
  - Composition
  - Intégration des relations de comparaison

II - Etude asymptotique de suites et de fonctions explicites
- 1) Suites récurrentes
  - Points fixes
  - Méthode de Newton
- 2) Utilisation de Série Intégrale
  - Sommation partielle/Equivalence des restes
  - Série harmonique
  - Euler MacLaurin [GOU08b]
  - Stirling
  - Comparaison Série-Intégrale
  - Série de Bertrand
- 3) Utilisation de fonctions

Formule de Poisson et équivalent Θ

III - Etude asymptotique de suites et de fonctions implicites

1) Nombre de zéros d'une équation différentielle [QZ07]

Nombres de zéros des solutions d'une équation différentielle

2) Etude intégrale

Théorème des fonctions implicites

Exo 79 du Rouvière [ROU09]

Développements :

- Nombres de zéros des solutions d'une équation différentielle
- Formule de Poisson et équivalent Θ

Références :

♥♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥ - [QZ07] Hervé QUEFFELEC et Claude ZUILY, *Analyse pour l'agrégation*

♥♥ - [ROM04] Jean-Etienne ROMBALDI, *Éléments d'analyse réelle*

♥♥ - [ROU09] François ROUVIÈRE, *Petit Guide de Calcul Différentiel*

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

Rapport du jury :

Citer au moins un théorème de point fixe est évidemment pertinent et savoir le mettre en oeuvre sur un exemple simple est indispensable. Le jury est toutefois surpris que des candidats évoquent un théorème de point fixe dans les espaces de Banach... sans être capables de définir ce qu'est un espace de Banach ou d'en donner un exemple ! On peut déjà commencer par énoncer un théorème de point fixe sur $\mathbb{R}$. Le jury attend d'autres exemples que la sempiternelle suite récurrente $u_{n+1} = \sin u_n$ (dont il est souhaitable de savoir expliquer les techniques sous-jacentes et le jury ne se privera pas de vérifier ce point sur un exercice). La notion de points attractifs ou répulsifs peut illustrer cette leçon.

L'étude des suites linéaires récurrentes d'ordre p est souvent mal connue, notamment le lien avec l'aspect vectoriel, d'ailleurs ce dernier point est trop souvent négligé. Le comportement des suites vectorielles définies par une relation linéaire $X_{n+1} = AX_n$ fournit pourtant un matériel d'étude conséquent.

La formulation de cette leçon invite résolument à évoquer les problématiques de convergence d'algorithmes (notamment savoir estimer la vitesse) d'approximation de solutions de problèmes linéaires et non linéaires : dichotomie, méthode de Newton (avec sa généralisation au moins dans $\mathbb{R}^2$), algorithme du gradient, méthode de la puissance, méthodes itératives de résolution de systèmes linéaires, schéma d'Euler,...

Questions possibles :

- Donner un équivalent de la suite $u_{n+1} = \sin u_n$.

  Réponse : $u_n \sim \sqrt{\frac{3}{n}}$ (voir Gourdon Analyse [GOU08b, p.218])

Motivations :

Les suites récurrentes sont des suites particulières beaucoup étudiées car elles ont des propriétés génériques et que c'est un outil facile pour créer une suite. La suite récurrente est très liée à la fonction servant à la définir. En effet, si f est continue, la suite récurrente liée à f convergera forcément vers un point fixe de f si elle converge (d'où l'étude des points fixes dans la première partie). On s'intéressera ensuite à 3 problèmes que l'on résoudra grâce aux suites récurrentes : l'approximation d'un zéro d'un fonction, l'approximation d'une solution de $AX = B$, l'approximation d'une solution d'équation différentielle par les schémas d'Euler.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Suites récurrentes

1) Définitions et théorie

Définition d'une suite récurrente

Prop : si f est continue en la limite l, on a $f(l) = l$.

Convergence de polygones vers l'isobarycentre

Prop : croissance et décroissance de la suite

2) Suites particulières

Arithmétique

Géométrique

Récurrente à coefficients constants

3) Théorie de point fixe

Propriétés élémentaires de fonctions continues sur un compact

Théorème de point fixe de Picard

Application : Cauchy Lipschitz

II - Recherche de zéros d'une fonction

1) Dichotomie

Principe et algorithmie

2) Newton

Méthode de Newton

III - Recherche de solutions approchées de $AX = B$

1) Jacobi Gauss Seidel

Thrm : Convergence SSI $\rho(M^{-1}N) < 1$

Jacobi

Gauss Seidel

Relaxation

2) Gradient à pas optimal

Thrm : $AX = B$ SSI X minimise $f : x \mapsto 1/2\langle Ax, x\rangle - \langle B, x\rangle$

Algorithme

Méthode de gradient à pas optimal

IV - Recherche de solution approchée d'équation différentielle

1) Schéma d'Euler explicite

Discrétisation du temps

Algorithme

2) Schéma d'Euler implicite

Algorithme

Avantages et inconvénients par rapport à explicite

En annexe :

- Convergence des polygones vers l'isobarycentre
- Méthode de la Dichotomie
- Méthode de Newton
- Schéma d'Euler explicite

Développements :

- Méthode de gradient à pas optimal
- Méthode de Newton
- Convergence de polygones vers l'isobarycentre

Références :

♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥ - [AK02] Grégoire ALLAIRE et Sidi Mahmoud KABER, *Algèbre Linéaire Numérique*

♥♥ - [QSS07] Alfio QUARTERONI, Riccardo SACCO et Fausto SALERI, *Méthodes Numériques*

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

Rapport du jury :

Cette leçon permet des exposés de niveaux très variés. Les théorèmes de base doivent être maîtrisés et illustrés par des exemples intéressants, par exemple le théorème des valeurs intermédiaires pour la dérivée. Le jury s'attend évidemment à ce que le candidat connaisse et puisse calculer la dérivée des fonctions usuelles. Les candidats doivent disposer d'un exemple de fonction dérivable de la variable réelle qui ne soit pas continûment dérivable. La stabilité par passage à la limite des notions de continuité et de dérivabilité doit être comprise par les candidats. De façon plus fine, on peut s'intéresser à des exemples de fonctions continues nulle part dérivables.

Les propriétés de régularité des fonctions convexes peuvent être mentionnées. Pour aller plus loin, la dérivabilité presque partout des fonctions lipschitziennes ou des fonctions monotones relève de cette leçon. L'étude des liens entre dérivée classique et dérivée au sens des distributions de fonctions telles que la fonction de Heaviside, de la valeur absolue ou de la fonction $x \mapsto \int_a^x f(y)dy$, f étant intégrable, peuvent trouver leur place dans cette leçon. On peut aussi relier la dérivée faible et la limite du taux d'accroissement au sens des distributions et établir le lien entre fonction croissante et dérivée faible positive.

Plan détaillé :

I - Continuité et dérivabilité

1) Continuité

Définition

Déf : uniformément continu

2) Dérivabilité

Déf : lien avec la continuité

Déf : taux d'accroissement

Déf : dérivabilité

Déf : $\mathcal{C}^1$

Déf : $\mathcal{C}^\infty$

II - Théorème principaux

1) Théorèmes de base

Thrm des valeurs intermédiaires

Thrm de Rolle

Thrm des accroissements finis

Taylor

2) Suites et séries

limite uniforme des fonctions continues

Thrm de Dini

Thrm de dérivation sous le signe somme

Formule de Poisson et fonction Θ

3) Intégrales à paramètre

Thrm de continuité sous l'intégrale

Thrm de dérivation sous l'intégrale

Application : fonction Gamma

III - Fonctions particulières

1) Fonctions lipschitzienne

Prop : Lipschitzienne implique uniformément continue

2) Fonctions monotones

Prop : Nombre dénombrable de point de discontinuité

3) Fonctions convexes

Prop : continuité sur l'ouvert de définition

Méthode de Newton

4) Solutions d'équations différentielles linéaires

Translatés d'une fonction $\mathcal{C}^1$

IV - Distributions

1) Définitions

2) Dérivations

Développements :

- Translatés d'une fonction $\mathcal{C}^1$
- Méthode de Newton
- Formule de Poisson et fonction Θ

Références :

♥♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥ - [ROM04] Jean-Etienne ROMBALDI, *Éléments d'analyse réelle*

♥♥♥ - [HAU07] Bertrand HAUCHECORNE, *Les contre-exemples en Mathématiques*

♥♥♥ - [EA11] Mohammed EL AMRANI, *Suites et séries numériques, suites et séries de fonctions*

♥♥ - [LES12] Ahmed LESFARI, *Distributions, analyse de Fourier et transformation de Laplace*

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

Rapport du jury :

L'énoncé et la connaissance de la preuve de l'existence de limites à gauche et à droite pour les fonctions monotones sont attendues. Ainsi on doit parler des propriétés de continuité et de dérivabilité à gauche et à droite des fonctions convexes de la variable réelle. Il est souhaitable d'illustrer la présentation de la convexité par des dessins clairs. On notera que la monotonie concerne les fonctions réelles d'une seule variable réelle, mais que la convexité concerne également les fonctions définies sur une partie convexe de $\mathbb{R}^n$, qui fournissent de beaux exemples d'utilisation. L'étude de la fonctionnelle quadratique ou la minimisation de $\|Ax-b\|^2$ pourront illustrer agréablement cette leçon.

Pour aller plus loin, la dérivabilité presque partout des fonctions monotones est un résultat remarquable (dont la preuve peut être éventuellement admise). L'espace vectoriel engendré par les fonctions monotones (les fonctions à variation bornée) relève de cette leçon. Enfin, la dérivation au sens des distributions fournit les caractérisations les plus générales de la monotonie et de la convexité ; les candidats maîtrisant ces notions peuvent s'aventurer utilement dans cette direction.

Motivations :

On va étudier les fonctions monotones et les fonctions convexes car ce sont des fonctions particulières qui présentent certains avantages. Par exemple, les fonctions convexes nous donnent la continuité sur l'ouvert de définition. Les fonctions monotones sont stables par composition et permettent de donner des critères de convergence pour les suites récurrentes. Les fonctions convexes peuvent servir en optimisation (en utilisant la différentiabilité).

I - Fonctions monotones [GOU08b]

1) Définition

Définition

Lien avec les suites récurrentes $u_{n+1} = f(u_n)$

2) Régularité

Dénombrabilité du nombre de points de discontinuité

limite à droite et à gauche

escalier de Cantor

Prop : croissant si $f' \geqslant 0$

Prop : Si f est positive, $\int^x f$ est croissante

F_X fonction de répartition croissante, discontinuité si atome

3) Utilisation

Théorème de Dini

Comparaison Série-Intégrale

II - Fonctions convexes [ROM04]

1) Définition

Définition de la convexité

Inégalité de convexité et concavité

Inégalité de Hölder

Inégalité de Hoeffding

2) Caractérisation

f convexe ssi $f'' \geqslant 0$

en dimension 1, $f(\frac{x+y}{2}) \leqslant \frac{f(x)+f(y)}{2}$

3) Régularité

Continuité sur l'ouvert de définition

Dérivabilité

III - Optimisation

1) Existence et unicité d'extrema

Méthode de Newton

Méthode de la sécante

2) Méthode de descente

Méthode de gradient à pas optimal

Développements :

- Méthode de Newton
- Méthode de gradient à pas optimal

Références :

♥♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥ - [ROM04] Jean-Etienne ROMBALDI, *Éléments d'analyse réelle*

♥♥ - [BMP05] Vincent BECK, Jérôme MALICK et Gabriel PEYRÉ, *Objectif Agrégation*

♥♥ - [RDO98] Edmond RAMIS, Calude DESCHAMPS et Jacques ODOUX, *Cours de Mathématiques 3 : Topologie et éléments d'analyse*

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

Rapport du jury :

De nombreux candidats commencent leur plan par une longue exposition des conditions classiques assurant la convergence ou la divergence des séries numériques. Sans être hors sujet, cette exposition ne doit pas former l'essentiel de la matière de la leçon. Un thème important de la leçon est en effet le comportement asymptotique des restes et sommes partielles (équivalents, développements asymptotiques — par exemple pour certaines suites récurrentes — cas des séries de Riemann, comparaison séries et intégrales,...). Le manque d'exemples est à déplorer.

On peut aussi s'intéresser à certaines sommes particulières, que ce soit pour exhiber des nombres irrationnels (voire transcendants), ou mettre en valeur des techniques de calculs non triviales (par exemple en faisant appel aux séries de Fourier ou aux séries entières).

Enfin, si le jury apprécie que le théorème des séries alternées (avec sa version sur le contrôle du reste) soit maîtrisé, il rappelle aussi que ses généralisations possibles utilisant la transformation d'Abel trouvent toute leur place dans cette leçon.

Plan détaillé :

I - Séries numériques

Définition

$\sum u_n$ converge implique $u_n \to 0$

Définition de la convergence absolue

Prop : Equivalence entre :

(i) E est de Banach

(ii) $\sum u_n$ converge absolument $\implies$ $\sum u_n$ converge dans E

Déf : série semi-convergente

Ex : $\sum \frac{(-1)^n}{n}$

Prop : Règle de produit de Cauchy des séries

II - Critère de convergence

1) Séries à termes positifs

$u_n \leqslant v_n$ implique $\sum u_n \leqslant \sum v_n$

Série de Riemann

Série de Bertrand

Critère de D'Alembert

Critère de Cauchy

2) Autres critères

Critère des séries alternées

Transformation d'Abel

III - Comportement des restes et sommes partielles

1) Majoration classique des restes

$\left|\sum u_n\right| \leqslant \sum |u_n|$

$u_n, v_n \geqslant 0$, si $u_n \leqslant v_n$ et $\sum u_n, \sum v_n$ convergent, alors $\sum_{n+1}^{\infty} u_k \leqslant \sum_{n+1}^{\infty} v_k$

Majoration des restes des séries alternées

2) Relations de comparaison

thrm classiques

3) Comparaison série-intégrale

Principe

Application : Réciproques partielles de Césaro

IV - Utilisation des séries entières

Théorème d'Abel

Exemples [GOU08b]

Nombres de Bell

Développements :

- Réciproques partielles de Césaro
- Nombres de Bell

Références :

♥♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥♥ - [COM95] Jean COMBES, *Suites et séries*

♥♥♥ - [HAU07] Bertrand HAUCHECORNE, *Les contre-exemples en Mathématiques*

♥♥♥ - [EA11] Mohammed EL AMRANI, *Suites et séries numériques, suites et séries de fonctions*

Leçon 233
Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples.

Rapport du jury :

Pour la session 2019, l'intitulé de cette leçon sera reformulé en **Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples.**

Le jury reprend une formulation antérieure de l'intitulé car la leçon se focalisait trop exclusivement sur la résolution de systèmes linéaires par des méthodes itératives. Le jury souhaite un sujet plus ouvert et des propositions qui ne négligent plus la recherche de vecteurs propres et, de manière générale, l'exploitation de techniques d'analyse pour aborder la résolution approchée de systèmes linéaires et de leurs propriétés spectrales et approfondir la compréhension des algorithmes.

Dans cette leçon de synthèse, les notions de norme matricielle et de rayon spectral sont centrales, en lien avec le conditionnement et avec la convergence des méthodes itératives ; elles doivent être développées et maîtrisées. Le conditionnement d'une matrice symétrique définie positive doit être connu et un lien avec $\sup_{\|x\|=1} {}^t xAx$ doit être fait. Le résultat général de convergence, relié au théorème du point fixe de Banach, doit être enrichi de considérations sur la vitesse de convergence.

Le jury invite les candidats à étudier diverses méthodes issues de contextes variés : résolution de systèmes linéaires, optimisation de fonctionnelles quadratiques (du type $\frac{1}{2}\langle Ax, x\rangle - \langle b, x\rangle$), recherche de valeurs propres,... Parmi les points intéressants à développer, on peut citer les méthodes de type Jacobi pour la résolution de systèmes linéaires, les méthodes de gradient dans le cadre quadratique, les méthodes de puissance et QR pour la recherche de valeurs propres. Les candidats pourront illustrer leur propos sur des matrices issues de schémas numériques pour les équations différentielles ou aux dérivées partielles linéaires.

Questions possibles :

- À quoi sert la décomposition QR ?

  Réponse : Elle peut servir à résoudre des systèmes linéaires de la forme $AX = B$, ou encore à rechercher les valeurs propres d'une matrice.

Motivations :

La résolution du système $AX = B$ est une question importante en mathématiques, car c'est un problème qui revient souvent : en arithmétique, pour résoudre des systèmes linéaires, en algèbre linéaire pour calculer des projections, en analyse numérique pour approcher des solutions d'équations différentielles, etc. On a différentes méthodes pour résoudre ce système, des méthodes directes comme le pivot de Gauss, des méthodes approchées comme les méthodes de Jacobi, Gauss Seidel et relaxation. On peut aussi utiliser des méthodes de gradient pour minimiser une fonctionnelle qui aura pour solution la solution du système linéaire. Parfois on sait que le système n'a pas de solution ($B \notin \mathrm{Im}(A)$) mais on veut approcher le mieux possible une "solution" proche ($\inf_X \|AX - B\|$), c'est ce qu'on appelle le problème des moindres carrés.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Outil matriciel [AK02]

Définition d'une norme matricielle

Définition d'une norme subordonnée

Prop : une norme subordonnée est une norme matricielle

Définition du rayon spectral

Prop : $\rho(A) = \lim \left(\|A^k\|\right)^{1/k}$

Définition du conditionnnement

Propriétés du conditionnement

II - Résolution exacte et approchée de $AX = B$

1) Résolution exacte

Pivot de Gauss

Méthode LU

Méthode QR

2) Pb des moindres carrés [AK02]

Problème de minimisation

3) Approximation [CIA06]

Jacobi

Gauss Seidel

Relaxation

Méthode de gradient à pas optimal

III - Recherche de valeurs propres et vecteurs propres

1) Méthode de la puissance

Théorème

2) Méthode QR

Méthode QR

Explication de la recherche de valeurs propres et vecteurs propres

IV - Approximation d'une solution d'équation différentielle

1) Euler explicite

Théorème

Avantage et inconvénient

2) Euler implicite

Théorème

Avantage et inconvénient

Développements :

- Méthode QR
- Méthode de gradient à pas optimal

Références :

♥♥♥ - [GRI11] Joseph GRIFONE, *Algèbre Linéaire*

♥♥♥ - [CIA06] Philippe CIARLET, *Introduction à l'analyse numérique matricielle et à l'optimisation*

♥♥♥♥ - [AK02] Grégoire ALLAIRE et Sidi Mahmoud KABER, *Algèbre Linéaire Numérique*

♥♥♥ - [QSS07] Alfio QUARTERONI, Riccardo SACCO et Fausto SALERI, *Méthodes Numériques*

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

Rapport du jury :

Cette leçon doit être très riche en exemples, que ce soit l'intégrale $\int_0^\infty \frac{\sin t}{t} dt$ ou bien d'autres encore. Il est tout à fait pertinent de commencer par les différentes techniques élémentaires (intégration par parties, changement de variables, décomposition en éléments simples, intégrale à paramètres,...). On peut également présenter des utilisations du théorème des résidus, ainsi que des exemples faisant intervenir les intégrales multiples comme le calcul de l'intégrale d'une gaussienne. Le calcul du volume de la boule unité de $\mathbb{R}^n$ ne doit pas poser de problèmes insurmontables. Le calcul de la transformation de Fourier d'une gaussienne a sa place dans cette leçon.

On peut aussi penser à l'utilisation du théorème d'inversion de Fourier ou du théorème de Plancherel. Certains éléments de la leçon précédente, comme par exemple l'utilisation des théorèmes de convergence monotone, de convergence dominée et/ou de Fubini, sont aussi des outils permettant le calcul de certaines intégrales.

Enfin, il est tout à fait pertinent d'évoquer les méthodes de calcul approché d'intégrales (méthodes des rectangles, méthode de Monte-Carlo, etc.).

Questions possibles :

- Comment calculer $\int_0^\infty \frac{\sin t}{t} dt$? (intégrale de Dirichlet)

Motivations :

L'intégrale possède diverses applications que ce soit pour calculer des aires et des volumes, pour généraliser la notion de somme discrète ou pour calculer des moyennes continues. On a besoin notamment en physique de calculer de nombreuses intégrales venant d'équations différentielles par exemple. On s'intéresse donc ici aux calculs d'intégrales allant des méthodes les plus classiques (changement de variables, intégration par parties) à d'autres méthodes plus compliquées (Transformée de Fourier, convolution, Théorème des Résidus). On a parfois besoin de méthodes itératives pour calculer des intégrales (comme les méthodes des rectangles, des trapèzes, du point milieu, de Simpson, de Monte-Carlo).

I - Calcul direct

1) Intégrales de fonctions à une seule variable [GOU08b]

Primitive directe

IPP

Changement de variable simple

Décomposition en éléments simples

2) Intégrales de fonctions à plusieurs variables [BP12]

Changement de variable sur $\mathbb{R}^d$

Fubini

II - Méthodes utilisant l'étude d'une fonction ou d'une suite de fonctions

1) Suites et séries de fonctions [BP12]
   - Convergence dominée
   - Interversion intégrale somme
2) Intégrales à paramètres
   - Continuité sous le signe intégral
   - Dérivabilité sous le signe intégral
   - Transformation de Fourier
   - Formule d'inversion de la fonction caractéristique
3) Analyse complexe et Théorème des résidus [JOL16]
   - Formule de Cauchy
   - Théorème des résidus
   - Formule des compléments

III - Calcul approché

1) Méthodes itératives [QSS07]
   - Rectangles
   - Trapèzes
   - Point milieu
   - Simpson
2) Monté-Carlo [TOU99]
   - Méthode de Monté Carlo

Développements :

- Formule d'inversion de la fonction caractéristique
- Formule des compléments

Références :

♥♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥♥ - [BP12] Marc BRIANE et Gilles PAGÈS, *Théorie de l'intégration*

♥♥ - [JOL16] Paul JOLISSAINT, *Fonctions d'une variable complexe, théorie de Cauchy élémentaire et applications*

♥♥ - [QSS07] Alfio QUARTERONI, Riccardo SACCO et Fausto SALERI, *Méthodes Numériques*

♥ - [TOU99] Paul TOULOUSE, *Thèmes de probabilités et statistique*

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

Rapport du jury :

Les candidats incluent les théorèmes de régularité (version segment — a minima — mais aussi version "convergence dominée") ce qui est pertinent mais la leçon ne doit pas se réduire seulement à cela. Cette leçon doit être riche en exemples, ce qui parfois n'est pas suffisamment le cas, et peut être encore enrichie par des études et méthodes de comportements asymptotiques. Les propriétés de la fonction Γ d'Euler fournissent un développement standard, mais non sans risque (on pourra y inclure le comportement asymptotique, voire son prolongement analytique) ; certains candidats sont trop ambitieux pour le temps dont ils disposent. Le jury invite donc à bien préciser ce que le candidat souhaite montrer pendant son développement. Les différentes transformations classiques (Fourier, Laplace,...) relèvent aussi naturellement de cette leçon. On peut en donner des applications pour obtenir la valeur d'intégrales classiques (celle de l'intégrale de Dirichlet par exemple). Le théorème d'holomorphie sous le signe intégrale est trop peu souvent cité.

Pour aller encore plus loin, on peut par exemple développer les propriétés des transformations mention- nées (notamment la transformée de Fourier, par exemple en s'attardant sur le lien entre régularité de la fonction et décroissance de sa transformée de Fourier), ainsi que de la convolution.

Questions possibles :

- Comment on prouve Riemann–Lebesgue ?
  Réponse : en faisant une IPP puis en utilisant la densité des fonctions $\mathcal{C}_1$ dans L^1
- Qu'est ce que vous connaissez comme transformée de Fourier ?
  Réponse : la gaussienne, l'indicatrice d'un segment, $(1+x^2)^{-1}$
- Comment on construit une suite régularisante ?
  Réponse : on peut utiliser des fonctions plateaux
- Pour ρ_n une approximation de l'unité et $f \in L^p$, pourquoi $\|\rho_n \star f - f\|_p \xrightarrow[n\to\infty]{} 0$?
- A quoi cela peut servir d'avoir la densité de $\mathcal{C}_0^\infty$ dans L^p ?
- A quoi ça sert d'avoir $\widehat{f \star g} = \widehat{f}\widehat{g}$?
  Réponse : Transformée de Fourier discrète pour le produit de polynômes ?
- Calculer la transformée de Fourier de $\arctan\left(\frac{1}{x}\right)$.
- Que vaut $L^p \star L^q$?
  Réponse : $L^p \star L^q$ donne L^r où $\frac{1}{p} + \frac{1}{q} = 1 + \frac{1}{r}$
- Montrer que pour tout $a \in \mathbb{R}$, $\int_0^{+\infty} e^{a|x|} e^{-\frac{x^2}{2}} \mathrm{d}x < +\infty$.
- Dans le théorème de convergence, pourquoi peut-on s'affranchir de l'hypothèse de domination de la dérivée, dans le cas holomorphe ?
  Réponse : Utiliser le développement en série entière.
- Calculer $\int_0^{+\infty} \frac{e^{-ax} - e^{-bx}}{x} \mathrm{d}x$.

Points essentiels :

- La convolution régularise les fonctions
- La transformée de Fourier inverse régularité et décroissance à l'infini

Plan détaillé :

I - Régularité des intégrales à paramètre

1) Continuité et dérivabilité [BP12]

Théorème de continuité

Théorème de dérivabilité

Exemple de la fonction Gamma

2) Holomorphie [JOL16]

Théorème d'holomorphie sous l'intégrale

Théorème des résidus

Formule des compléments

II - Convolution [BP12] [HL99]

1) Convolution

Définition

Propriétés

Théorème avec les espaces L^p.

2) Approximation de l'unité

Lien avec la convolution

Propriétés

Lien avec la densité des fonctions $\mathcal{C}_0^\infty(\mathbb{R})$ dans les $L^p(\mathbb{R})$.

III - Transformation de Fourier [QZ07]

1) Transformée de Fourier

Définition

Propriétés

Transformée de Fourier inverse

Formule de Poisson et Shannon

2) Fonction caractéristique

Définition

Propriétés

Lien avec les moments

Formule d'inversion de la fonction caractéristique

Lien avec la convergence en loi

Astuces de l'agrégatif :

Pour la convolution il faut retenir que $L^p \star L^q = L^r$ avec $\frac{1}{p} + \frac{1}{q} = 1 + \frac{1}{r}$

Remarques :
Attention, je ne parle pas de transformée de Laplace et de méthode de Laplace mais cela a toute sa place dans cette leçon, c'est seulement un choix personnel.

Développements :

- Formule d'inversion de la fonction caractéristique
- Formule des compléments
- Formule de Poisson et Shannon

Références :

♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥♥♥ - [BP12] Marc BRIANE et Gilles PAGÈS, *Théorie de l'intégration*

♥♥ - [JOL16] Paul JOLISSAINT, *Fonctions d'une variable complexe, théorie de Cauchy élémentaire et applications*

♥♥♥ - [HL99] Francis HIRSH et Gilles LACOMBE, *Éléments d'analyse fonctionnelle*

♥♥♥ - [QZ07] Hervé QUEFFELEC et Claude ZUILY, *Analyse pour l'agrégation*

♥♥♥ - [HAU07] Bertrand HAUCHECORNE, *Les contre-exemples en Mathématiques*

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

Rapport du jury :

Les candidats évoquent souvent des critères (Cauchy, D'Alembert) permettant d'estimer le rayon de convergence mais oublient souvent la formule de Cauchy-Hadamard ou toute technique utilisant une majoration ou un équivalent. Le jury attend bien sûr que le candidat puisse donner des arguments justifiant qu'une série entière en 0 dont le rayon de convergence est R est développable en série entière en un point z_0 intérieur au disque de convergence et de minorer le rayon de convergence de cette série. Sans tomber dans un catalogue excessif, on peut indiquer les formules de développement de fonctions usuelles importantes (exp, log, $1/(1-z)$, sin, ...). S'agissant d'exemples fondamentaux et classiques, le jury attend que le candidat puisse les donner sans consulter ses notes. En ce qui concerne la fonction exponentielle, le candidat doit avoir réfléchi au point de vue adopté sur sa définition et donc sur l'articulation entre l'obtention du développement en série entière et les propriétés de la fonction. À ce propos, les résultats sur l'existence du développement en série entière pour les fonctions dont on contrôle toutes les dérivées successives sur un voisinage de 0 sont souvent méconnus. Le comportement de la série entière dans le disque de convergence vis à vis des différents modes de convergence (convergence absolue, convergence uniforme, convergence normale) doit être maîtrisé.

Le théorème d'Abel (radial ou sectoriel) trouve toute sa place mais doit être agrémenté d'exercices pertinents. Réciproquement, les théorèmes taubériens offrent aussi de jolis développements. On pourra aller plus loin en abordant quelques propriétés importantes liées à l'analyticité de la somme d'une série entière ou encore la résolution de certaines équations différentielles ordinaires par la méthode du développement en série entière.

Questions possibles :

- Donner une fonction développable en série de Taylor mais qui n'est pas analytique

  Réponse : $x \mapsto e^{-\frac{1}{x^2}}$

Motivations :

Les séries entières sont des cas particuliers de séries de fonctions. Elles ont beaucoup d'applications, que ce soit en équations différentielles ou en dénombrement (série génératrices). On peut voir les séries entières de deux façons, la première est comme un objet algébrique (c'est la vision de la partie I) et on peut aussi étudier la fonction qui à z associe la série entière (c'est le point de vue analytique de la partie II). Attention aux séries de Taylor qui convergent mais qui ne coïncident pas avec la série entière de la fonction que l'on considère (ex : $\exp(-\frac{1}{x^2})$). Historiquement, les Grecs avaient du mal avec les sommes infinis, ils connaissaient déjà la série géométrique. Ensuite au XVIIième siècle, on voulait trouver des développements d'autres fonctions. On ne parle pas encore de rayon de convergence. Euler voit les "séries entières" comme une généralisation des polynomes. Ensuite Taylor étudie cela et pense que toute fonction $\mathcal{C}^\infty$ était analytique, mais Cauchy prouve que ce n'est pas le cas. C'est lui qui cadre toute la théorie, le rayon de convergence et le lien avec l'analycité.

Points essentiels :

- le lien entre fonction analytique et développement de Taylor.
- rayon de convergence et les moyens de le calculer

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Un objet algébrique et analytique [GOU08b]

1) Définition et rayon de convergence

Définition

Théorème du rayon de convergence

Critère de D'Alembert

Critère de Cauchy

2) Opérations algébriques

Somme

Multiplication par un scalaire

Structure d'espace vectoriel

Produit de Cauchy

Composition

Inverse

3) Comportement sur le disque de convergence

Théorème taubérien

Théorème d'Abel

Formule de Poisson et équivalent Θ

II - Régularité de la fonction série entière

1) Continuité et dérivabilité

Continuité

Dérivabilité

Primitive d'une série entière

2) Prolongement analytique [QZ07]

Développement de Taylor

Définition d'une fonction analytique

3) Lien avec l'holomorphie [GOU08b]

Théorème d'holomorphie de la série entière sur le disque de convergence

Théorème des zéros isolés

Formule de Cauchy

III - Applications des séries entières

1) Équations différentielles [GOU08b]

Résolution d'une équation différentielle par une série entière

Fonction de Bessel

2) Dénombrement

Nombres de Catalan [FGN18, p.9]

Nombres de Bell

En annexe :

- développements en série entière de exp, sin, cos, sh, ch, $(1+x)^\alpha$, log, arctan, argth, arcsin, argsh.

Développements :

- Nombres de Bell
- Formule de Poisson et équivalent Θ

Références :

♥♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥ - [QZ07] Hervé QUEFFELEC et Claude ZUILY, *Analyse pour l'agrégation*

♥♥ - [FGN18] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS, *Oraux X-ENS, Algèbre 1*

Leçon 246
Séries de Fourier. Exemples et applications.

Rapport du jury :

Les différents résultats autour de la convergence (L^2, Fejér, Dirichlet, ...) doivent être connus. On prendra garde au sens de la notation $\sum_{n\in\mathbb{Z}}$ (qu'il est plus prudent d'éviter car elle est souvent inadaptée). Il faut avoir les idées claires sur la notion de fonctions de classe $\mathcal{C}^1$ par morceaux (elles ne sont pas forcément continues). Le théorème d'isométrie bijective entre espaces L^2 et ℓ^2 doit apparaitre. Dans le cas d'une fonction continue et $\mathcal{C}^1$ par morceaux on peut conclure sur la convergence normale de la série Fourier sans utiliser le théorème de Dirichlet. Il est classique d'obtenir des sommes de séries remarquables comme conséquence de ces théorèmes.

On peut aussi s'intéresser à la formule de Poisson et à ses conséquences. L'existence d'exemples de séries de Fourier divergentes, associées à des fonctions continues (qu'ils soient explicites ou obtenus par des techniques d'analyse fonctionnelle) peuvent aussi compléter le contenu.

Il est souhaitable que cette leçon ne se réduise pas à un cours abstrait sur les coefficients de Fourier. La résolution d'équations aux dérivées partielles (par exemple l'équation de la chaleur ou l'équation des ondes avec une estimation de la vitesse de convergence) peut illustrer de manière pertinente cette leçon, mais on peut penser à bien d'autres applications (inégalité isopérimétrique, comportements remarquables des fonctions à spectre lacunaire,...).

Questions possibles :

- Calculer $\sum_{-\infty}^{+\infty}\frac{1}{n^2}, \sum_{-\infty}^{+\infty}\frac{1}{n^4}$ en utilisant les coefficients de Fourier.

  Réponse : voir Gourdon Analyse

- Comment on prouve Riemann-Lebesgue ?

  Réponse : pour les fonctions $\mathcal{C}^1$ puis par densité dans L^1

- Calculer les coefficients de Fourier de $\begin{cases} [-\pi,\pi] & \to & \mathbb{R} \\ x & \mapsto & |x| \end{cases}$

  Réponse : $c_n(f) = \begin{cases} \frac{\pi}{2} & \text{si } n=0 \\ 0 & \text{si } n \text{ est pair (non nul)} \\ -\frac{2}{\pi n^2} & \text{si } n \text{ est impair} \end{cases}$

- Existe-t-il $f \in \mathcal{C}(0,2\pi)$ périodique telle que $c_n(f)$ décroit en $\frac{1}{\ln n}$?

  Réponse : non

Motivations :

Les coefficients de Fourier sont très utiles notamment en physique pour exprimer un signal qu'avec une suite indexée sur $\mathbb{Z}$. On calcule facilement à partir d'une fonction f ses coefficients de Fourier $c_n(f)$, inversement, on veut savoir sous quelles hypothèses, on peut retrouver la fonction f à partir de ses coefficients de Fourier. On va donc avec des théorèmes de convergence (Fejer, Dirichlet) utilisant les noyaux associés [9]. Puis je parle de coefficients de Fourier dans L^2, on pourra

9. je ne parle pas du noyau de Poisson dans cette leçon, mais on pourrait

ainsi montrer que les polygones orthogonaux forment une base hilbertienne de L^2. Je prends comme convention

$$\boxed{\forall n \in \mathbb{Z},\ \forall f \in L^1([0,2\pi]),\quad c_n(f) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-inx}dx}$$

Plan détaillé :

I - Coefficients et séries de Fourier dans L^1

1) Définitions

Définitions des $c_n(f)$

Lemme de Riemann Lebesgue

2) Séries de Fourier

Définition

II - Noyaux trigonométriques

1) Noyaux

Dirichlet

Fejer

2) Théorèmes de convergence

Banach–Steinhaus

Théorème de Fejer

Théorème de Dirichlet

Formule de Poisson et fonction Θ ou Formule de Poisson et Shannon

III - Étude dans L^2

Définition dans L^2 Hilbert

Base hilbertienne des polynomes triognométriques par Fejer

Isométrie et égalité de Parseval

Exemple de calcul de sommes : $\sum_{-\infty}^{+\infty} \frac{1}{n^2}, \sum_{-\infty}^{+\infty} \frac{1}{n^4}$

Développements :

- Banach–Steinhaus
- Formule de Poisson et fonction Θ
- Formule de Poisson et Shannon

Références :

♥♥♥ - [GOU08b] Xavier GOURDON, *Analyse*

♥♥♥♥♥ - [EA08] Mohammed EL AMRANI, *Analyse de Fourier dans les espaces fonctionnels*

♥♥ - [QZ07] Hervé QUEFFELEC et Claude ZUILY, *Analyse pour l'agrégation*

♥♥ - [HAU07] Bertrand HAUCHECORNE, *Les contre-exemples en Mathématiques*

Leçon 250
Transformation de Fourier. Applications.

Rapport du jury :

Cette leçon offre de multiples facettes. Les candidats peuvent adopter différents points de vue : L^1, L^2 et/ou distributions. L'aspect "séries de FOURIER" n'est toutefois pas dans l'esprit de cette leçon ; il ne s'agit pas de faire de l'analyse de FOURIER sur n'importe quel groupe localement compact mais sur $\mathbb{R}$ ou $\mathbb{R}^d$.

La leçon nécessite une bonne maîtrise de questions de base telle que la définition du produit de convolution de deux fonctions de L^1. En ce qui concerne la transformation de FOURIER, elle ne doit pas se limiter à une analyse algébrique de la transformation de FOURIER. C'est bien une leçon d'analyse, qui nécessite une étude soigneuse des hypothèses, des définitions et de la nature des objets manipulés. Le lien entre la régularité de la fonction et la décroissance de sa transformée de FOURIER doit être fait, même sous des hypothèses qui ne sont pas minimales. Les candidats doivent savoir montrer le lemme de RIEMANN-LEBESGUE pour une fonction intégrable.

La formule d'inversion de FOURIER pour une fonction L^1 dont la transformée de FOURIER est aussi L^1 est attendue ainsi que l'extension de la transformée de FOURIER à l'espace L^2 par FOURIER-PLANCHEREL. Des exemples explicites de calcul de transformations de FOURIER, classiques comme la gaussienne ou $(1+x^2)^{-1}$, paraissent nécessaires.

Pour aller plus loin, la transformation de FOURIER des distributions tempérées ainsi que la convolution dans le cadre des distributions tempérées peuvent être abordées. Rappelons une fois de plus que les attentes du jury sur ces questions restent modestes, au niveau de ce qu'un cours de première année de master sur le sujet peut contenir. Le fait que la transformée de FOURIER envoie $\mathscr{S}(\mathbb{R}^d)$ dans lui même avec de bonnes estimations des semi-normes doit alors être compris et la formule d'inversion de FOURIER maîtrisée dans ce cadre. Des exemples de calcul de transformée de FOURIER peuvent être donnés dans des contextes liés à la théorie des distributions comme par exemple la transformée de FOURIER de la valeur principale. Dans un autre registre, il est aussi possible d'orienter la leçon vers l'étude de propriétés de fonctions caractéristiques de variables aléatoires.

La résolution de certaines équations aux dérivées partielles telles que, par exemple, l'équation de la chaleur sur $\mathbb{R}$, peut être abordée, avec une discussion sur les propriétés qualitatives des solutions.

Questions possibles :

- Calculer la transformée de Fourier de $\mathbb{1}_{[a,b]}$.
- Calculer la transformée de Fourier de la gaussienne.
- Calculer la transformée de Fourier de $(1+x^2)^{-1}$.

Motivations :

On va étudier la transformée de Fourier qui est un outil très puissant pour résoudre des équations différentielles. La transformée de Fourier inverse régularité et décroissance à l'infini. On définit proprement la transformée de Fourier sur L^1, puis par un argument de densité de $L^1 \cap L^2$ dans L^2, on peut prolonger la transformée à L^2 (Fourier-Plancherel), l'avantage d'avoir la transformée de Fourier sur L^2 est que c'est un espace de Hilbert. On parlera ensuite de l'espace de Schwartz qui est stable par transformée de Fourier donc cela sera simple de définir la transformée

de Fourier inverse. Puis on parlera de la fonction caractéristique qui est en fait qu'une variante de la transformée de Fourier pour les probabilités [10]. J'utilise comme convention

$$\boxed{\hat{f}(\xi) = \int_{-\infty}^{+\infty} f(x)e^{-i\xi x}dx}$$

Il existe d'autres conventions (voir appendice)

Plan détaillé :

I - Transformation de Fourier dans $L^1(\mathbb{R})$
- 1) Définition
  - Définition
  - Exemple
  - Propriétés
  - Riemann Lebesgue
- 2) Convolution et dérivation
  - Lien entre la convolution et la transformée de Fourier
  - Lien entre la dérivation et la transformée de Fourier
  - Transformée de Fourier inverse

II - Transformation de Fourier dans $L^2(\mathbb{R})$ et $\mathcal{S}(\mathbb{R})$
- 1) Dans $L^2(\mathbb{R})$
  - Fourier Plancherel
  - Théorème de densité
  - Formule d'inversion
- 2) Dans $\mathcal{S}(\mathbb{R})$
  - Définition des fonctions à décroissances rapides
  - Définition de $\mathcal{S}(\mathbb{R})$
  - Stabilité de $\mathcal{S}(\mathbb{R})$ par transformée de Fourier
  - Formule de Poisson et Shannon

III - Fonction caractéristique
- Définition $\varphi_X(t)$
- Formule d'inversion de la fonction caractéristique
- Lien avec les moments
- Lien avec l'indépendance
- Lien avec la convergence en loi
- Application : Théorème Central Limite

Développements :

- Formule d'inversion de la fonction caractéristique
- Formule de Poisson et Shannon

Références :

♥♥♥♥♥ - [EA08] Mohammed EL AMRANI, *Analyse de Fourier dans les espaces fonctionnels*

♥♥ - [LES12] Ahmed LESFARI, *Distributions, analyse de Fourier et transformation de Laplace*

♥♥♥ - [BL07] Philippe BARBE et Michel LEDOUX, *Probabilité*

♥♥ - [OUV00] Jean-Yves OUVRARD, *Probabilités 2*

10. il n'y a plus de signe "moins" dans la définition

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

Rapport du jury :

Le jury attend des candidats qu'ils donnent la définition des moments centrés, qu'ils rappellent les implications d'existence de moments (décroissance des L^p). Les variables aléatoires à densité sont trop souvent négligées. Le candidat peut citer — mais doit surtout savoir retrouver rapidement — les espérances et variances de lois usuelles, notamment Bernoulli, binomiale, géométrique, Poisson, exponentielle, normale. La variance de la somme de variables aléatoires indépendantes suscite souvent des hésitations. Les inégalités classiques (de Markov, de Bienaymé-Chebyshev, de Jensen et de Cauchy-Schwarz) pourront être données, ainsi que les théorèmes de convergence (lois des grands nombres et théorème central limite). La notion de fonction génératrice des moments pourra être présentée ainsi que les liens entre moments et fonction caractéristique.

Pour aller plus loin, le comportement des moyennes empiriques pour une suite de variables aléatoires indépendantes et identiquement distribuées n'admettant pas d'espérance pourra être étudié. Pour les candidats suffisamment à l'aise avec ce sujet, l'espérance conditionnelle pourra aussi être abordée.

Questions possibles :

- Les moments d'une variable aléatoire caractérisent-ils sa loi ?

  Réponse : Oui si la variable aléatoire est bornée, mais non dans le cas général ! La recherche de contre-exemples dans le cas non borné peut d'ailleurs faire l'objet d'un développement, dans cette leçon.

- Soit X une variable aléatoire réelle. Montrer que $\lim_{t\to+\infty} P(X \geq t) = 0$.

Plan détaillé :

I - Notion d'espérance
  1) Définition
     Variables centrées
     Lemme de transfert
  2) Calcul
     Variable discrète
     Variable continue
     Exemple de la loi de Cauchy sans espérance
  3) Propriétés
     Propriété de linéarité
     Inégalité de Jensen
     Inégalité de Markov
     Propriétés liées à l'indépendance

II - Moments d'une variable aléatoire
  1) Moments L^p

Hölder

Inclusion des L^p

Minkowski

2) Variance Covariance et indépendance

Définition Variance

Propriétés de la variance

Inégalité de Bienaymé Tchebychev

Définition de la covariance

Utilisation de l'indépendance

3) Fonction caractéristique et moments

Définition

Lien entre la fonction caractéristique et les moments

Formule d'inversion de la fonction caractéristique

III - Théorème Limite

1) Loi des grands nombres

Théorème

Monte Carlo

2) Théorème Central Limite

Théorème Central Limite

Développements :

- Formule d'inversion de la fonction caractéristique
- Théorème Central Limite

Références :

♥♥♥♥ - [BL07] Philippe BARBE et Michel LEDOUX, *Probabilité*

♥♥♥ - [OUV00] Jean-Yves OUVRARD, *Probabilités 2*

Leçon 264
Variables aléatoires discrètes. Exemples et applications.

Rapport du jury :

Le jury attend des candidats qu'ils rappellent la définition d'une variable aléatoire discrète et que des lois usuelles soient présentées, en lien avec des exemples classiques de modélisation. Le lien entre variables aléatoires de BERNOULLI, binomiale et de POISSON doit être discuté. Il peut être d'ailleurs intéressant de mettre en avant le rôle central joué par les variables aléatoires de BERNOULLI.

Les techniques spécifiques aux variables discrètes, notamment à valeurs entières, devront être mises en évidence, comme par exemple la caractérisation de la convergence en loi, la notion de fonction génératrice. Pour aller plus loin, le processus de GALTON-WATSON peut se traiter intégralement à l'aide des fonctions génératrices et cette voie a été choisie par plusieurs candidats : cela donne un développement de très bon niveau pour ceux qui savent justifier les étapes délicates.

Pour aller beaucoup plus loin, les candidats pourront étudier les marches aléatoires, les chaînes de MARKOV à espaces d'états finis ou dénombrables, les sommes ou séries de variables aléatoires indépendantes.

Questions possibles :

- Pourquoi on ne peut pas truquer 2 dés à six faces pour que leur somme vérifie une loi uniforme ?

  Réponse : utiliser la fonction génératrice

- Montrer qu'une suite de variables aléatoires suivants des lois binomiales $\mathcal{B}(n, p_n)$ avec $\lim_{n\to\infty} np_n = \lambda$ converge en loi vers une variable aléatoire suivant une loi de Poisson de paramètre λ.

Plan détaillé :

I - Variables aléatoires discrètes [FFF12]
  1) Définition
     Définition
  2) Lois usuelles
     Bernoulli
     Binomiale
     Géométrique
     Poisson
     Hypergéométrique
  3) Conditionnement
     Définition
     Formule de Bayes

II - Moments et indépendance
  1) Espérance et variance

Définitions

Théorème de transfert

2) Indépendance

Définition

Lien avec l'espérance

III - Transformations usuelles

1) Fonctions génératrices [FFF12]

Avec les variables aléatoires usuelles

Lien avec l'indépendance

2) Fonctions caractéristiques [FFF12] [OUV00]

Définition

Convergence en loi

Formule d'inversion de la fonction caractéristique

IV - Théorèmes Limites

Approximation d'une loi de Poisson par une suite de binomiales

Loi des Grands Nombres

Monté Carlo

Théorème Central Limite

Corollaire : Théorème de Moivre-Laplace

Développements :

- Formule d'inversion de la fonction caractéristique
- Théorème Central Limite

Références :

♥♥♥♥ - [BL07] Philippe BARBE et Michel LEDOUX, *Probabilité*

♥♥♥ - [OUV00] Jean-Yves OUVRARD, *Probabilités 2*

♥♥♥♥ - [FFF12] Dominique FOATA, Jacques FRANCHI et Aimé FUCHS, *Calcul des probabilités*

Leçon 265
Exemples d'études et d'applications de fonctions usuelles et spéciales.

Rapport du jury :

Cette leçon est très riche ; c'est une leçon de synthèse qui doit permettre d'explorer de nombreux pans du programme. Évidemment, la leçon ne doit pas se cantonner au seul champ des fonctions usuelles (logarithme, exponentielle, trigonométriques, hyperboliques et réciproques). Le jury attend surtout d'un agrégé qu'il soit en mesure de présenter rapidement les définitions et les propriétés fondamentales de ces fonctions, qu'il sache les tracer sans difficultés, qu'il puisse mener l'étude aux bornes de leur domaine, ainsi que discuter leurs prolongements éventuels, leurs développements de Taylor ou en série entière, leurs applications au calcul intégral, les équations fonctionnelles associées ou formules particulières, etc. Le jury n'attend pas un catalogue mais plutôt un choix pertinent et réfléchi, avec des applications en probabilité, convexité, études de courbes, ou autour des développements asymptotiques. Les déterminations du logarithme complexe peuvent tout à fait mériter une discussion approfondie dans cette leçon et donner lieu à des développements de bon niveau, pouvant aller jusqu'à leur interprétation géométrique.

Le domaine des fonctions spéciales est très vaste. Il faut absolument éviter l'écueil d'une taxonomie fastidieuse et dépourvue de motivation ; il vaut bien mieux se concentrer sur des exemples restreints, mais fouillés, par exemple une étude approfondie (d'une) des fonctions Γ, ζ ou θ, leurs propriétés fonctionnelles, leurs prolongements, leur étude asymptotique aux bornes et les domaines d'applications de ces fonctions.

Il y a donc bien des manières, très différentes, de construire valablement cette leçon. Par exemple, on peut bâtir un exposé organisé selon des problématiques et des techniques mathématiques : suites et séries de fonctions, fonctions holomorphes et méromorphes, problèmes de prolongement, développements asymptotiques, calculs d'intégrales et intégrales à paramètres, transformées de Fourier ou de Laplace, *etc.* Mais on pourrait tout aussi bien suivre un fil conducteur motivé par un domaine d'application :

- en arithmétique pour évoquer, par exemple, la fonction ζ et la distribution des nombres premiers,
- en analyse des équations aux dérivées partielles où les fonctions spéciales interviennent notamment pour étudier le problème de Dirichler pour le Laplacien ou l'équation des ondes,
- en probabilités où la loi normale et la fonction erreur sont évidemment incontournables mais on peut aussi évoquer les lois Gamma et Bêta, les fonctions de Bessel et leurs liens avec la densité du χ^2 non centrée et celle de la distribution de Von Mises-Fisher ou plus simplement comme loi du produit de variables aléatoires normales indépendantes, la loi ζ et ses liens avec la théorie des nombres,...
- il est aussi possible d'évoquer les polynômes orthogonaux, leurs propriétés et leurs diverses applications, en physique (oscillateur harmonique et polynômes de Hermite), en probabilités (polynômes de Hermite pour les lois normales, de Laguerre pour les lois Gamma, de Jacobi pour les lois Bêta...), pour l'étude d'équations aux dérivées partielles ou pour l'analyse de méthodes numériques,
- en théorie des représentations de groupes avec les fonctions de Bessel,
- en algèbre en abordant les fonctions p-elliptiques.

Là encore, le jury renouvelle sa mise en garde d'éviter de faire un catalogue qui s'avérerait stérile, il s'agit bien plutôt de se tenir à détailler l'un ou l'autre de ces points de vue. Au final, cette leçon peut être l'occasion de montrer un véritable investissement personnel, adossé aux goûts du candidat.

Questions possibles :

- Montrer que $\frac{2}{e} < 1$.

  Réponse : Indication : Démontrer et utiliser l'inégalité de convexité $\forall x \in \mathbb{R}, e^x \geq x+1$.

- Démontrer la formule de Stirling.

  Réponse : Indication : Utiliser les intégrales de Wallis.

- Calculer $\lim_{n\to+\infty} \left(1+\frac{x}{n}\right)^n$.

- Montrer que la fonction logarithme définie par une intégrale (ce qui est la définition historique du logarithme) correspond bien à l'application réciproque de l'exponentielle.

- Sur quel domaine se prolonge Γ ?

  Réponse : sur $\mathbb{C}\backslash\mathbb{Z}^-$ sans zéros et avec des pôles d'ordre 1 en les entiers négatifs

- Sur quel domaine se prolonge ζ ?

  Réponse : sur $\mathbb{C}\backslash\{1\}$ avec un pôle d'ordre 1 en 1

Motivations :

J'attaque cette leçon sous un angle de prolongement. On commence par prolonger l'exponentielle, le cosinus et le sinus sur le plan complexe, ce qui donne les fonctions usuelles. On s'intéresse aussi au logarithme sur le plan complexe, qui se comporte très différemment du logarithme népérien. En effet, il faut faire attention à son ensemble de définition. Ensuite je m'intéresse aux fonctions spéciales suivantes : la fonction Γ d'Euler, la fonction ζ de Riemann et la fonction Θ de Jacobi. On va voir le lien qu'elles ont entre elles et comment on peut les prolonger sur $\mathbb{C}$ en des fonctions méromorphes. La fonction Γ a été introduite par Euler lorsqu'il cherchait un prolongement de la factorielle des entiers à $\mathbb{R}$. La fonction ζ a été introduite par Riemann pour étendre les séries de Riemann, c'est lui qui conjecturera que les zéros non triviaux de ζ sont sur la droite verticale de partie réelle égale à $1/2$. De plus, la fonction ζ possède un lien avec les nombres premiers et aide à prouver le théorème des nombres premiers (équivalent en $+\infty$ du cardinal des nombres premiers). Quant à la fonction Θ, c'est normalement une fonction holomorphe bipériodique à deux variables utile dans la pratique en physique, mais on ne s'intéressera ici qu'à une restriction, ce qui nous donne une fonction holomorphe à une variable.

J'ai rédigé le plan de cette leçon (voir ici)

I - Fonctions usuelles et variables complexes [JOL16]

1) Fonction usuelle

Exponentielle

Cosinus

Sinus

2) Logarithme

Inverse de l'exponentielle

Argument continu

Détermination principale du logarithme

Propriété : primitive de $\frac{1}{z}$.

3) Théorie de l'indice

Définition

Théorème de résidus

II - Fonction Gamma Γ [JOL16]

Définition

Régularité

Relation de récurrence

Stirling [ROU09]

Prolongement

Formule des compléments

Définition du produit infini

Formule de Weierstrass

Application à la loi Gamma en probabilité

III - Fonction Zeta ζ et fonction Theta Θ [JOL16] [GS09]

Définition

Théorème $\zeta(z) = \prod_{p\in\mathcal{P}} (1-p^{-z})^{-1}$

Définition de Theta $\Theta(u) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 u}$

Formule de Poisson et fonction Θ

Propriétés de Theta

Théorème qui lie Θ, ζ et Γ

Les zéros triviaux de ζ

Conjecture de Riemann

Théorème des nombres premiers

Développements :

- Formule des compléments
- Formule de Poisson et fonction Θ

Références :

♥♥♥♥♥ - [JOL16] Paul JOLISSAINT, *Fonctions d'une variable complexe, théorie de Cauchy élémentaire et applications*

♥♥♥ - [AM04] Eric AMAR et Etienne MATHERON, *Analyse complexe*

♥♥♥♥ - [GS09] Roland GROUX et Philippe SOULAT, *Les fonctions spéciales vues par les problèmes*

♥♥ - [ROU09] François ROUVIÈRE, *Petit guide de calcul différentiel*

2.5 Métaplans d'informatique

Leçon 901
Structures de données. Exemples et applications.

Rapport du jury :

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

Questions possibles :

- Donner les types abstraits, concrets et implantation possible pour une certaine structure.
  Réponse : Par exemple, type abstrait : file de priorité ; type concret : tas_min ; implantation : tableau
- Connaissez vous d'autres arbres que les ABRO et AVL ?
  Réponse : Arbres Rouge Noir, Arbre Splay
- Donner des utilisations de Union Find.
  Réponse : Algorithme de Kruskal

Plan détaillé :

I - Type abstrait de base
  1) opérations souhaitées
     find, create, insert, suppr, union, find_min, find_earlest
  2) tableau
     définition
     coût des opérations
  3) liste
     définition
     coût des opérations

II - Structure de données d'ordonnancement
  1) pile
     définition
     parcours en profondeur
  2) file
     définition
     parcours en largeur

3) file de priorité
   définition
   Tri par tas
   PRIM
   codage de HUFFMAN
4) graphe
   matrice d'adjacence
   liste d'adjacence

III - Structure de recherche : dictionnaire
1) arbres
   ABR
   AVL
   ABR optimaux
   B-arbres
2) table de hachage
   hachage parfait

IV - Partitionner un ensemble
   algorithmes liés à UNIONFIND
   KRUSKAL

Développements :

- Tri par tas
- B-arbres

Références :

♥♥♥♥ - [CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST et Clifford STEIN, *Algorithmique*

♥♥♥♥ - [FGS90] Christine FROIDEVAUX, Marie-Claude GAUDEL et Michèle SORIA , *Type de données et algorithmes*

Leçon 903
Exemples d'algorithmes de tri. Correction et complexité.

Rapport du jury :

Sur un thème aussi classique, le jury attend des candidats la plus grande précision et la plus grande rigueur.

Ainsi, sur l'exemple du tri rapide, il est attendu du candidat qu'il sache décrire avec soin l'algorithme de partition et en prouver la correction en exhibant un invariant adapté. L'évaluation des complexités dans le cas le pire et en moyenne devra être menée avec rigueur : si on utilise le langage des probabilités, il importe que le candidat sache sur quel espace probabilisé il travaille.

On attend également du candidat qu'il évoque la question du tri en place, des tris stables, des tris externes ainsi que la représentation en machine des collections triées.

Questions possibles :

- Appliquer les tris naïfs sur la liste `[2; 5; 1; 8; 3; 10]`.
- Montrer que la complexité minimale d'un tri par comparaison est $O(n \log n)$.
  Réponse : voir appendice
- Montrer la complexité du tri rapide.

Plan détaillé :

I - Le problème du tri
- définition du problème de tri
- définition de "stable"
- définition de "en place"
- critère de comparaison

II - Tri par comparaison
- propriété
- complexité minimale (voir appendice)

1) naïf
   - tri par sélection
   - tri par insertion
   - tri bulle
2) diviser pour régner
   - tri fusion
   - tri rapide
3) structure de données
   - Tri par tas

III - Tri linéaire
1) par dénombrement
2) par paquet
3) par base

IV - Autres tris
1) Tri topologique
2) tri externe

Développements :

- Tri topologique
- Tri par tas

Références :

♥♥♥♥ - [CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST et Clifford STEIN, *Algorithmique*

♥♥♥ - [FGS90] Christine FROIDEVAUX, Marie-Claude GAUDEL et Michèle SORIA , *Type de données et algorithmes*

Leçon 907
Algorithmique du texte. Exemples et applications.

Rapport du jury :

Cette leçon devrait permettre au candidat de présenter une grande variété d'algorithmes et de paradigmes de programmation, et ne devrait pas se limiter au seul problème de la recherche d'un motif dans un texte, surtout si le candidat ne sait présenter que la méthode naïve.

De même, des structures de données plus riches que les tableaux de caractères peuvent montrer leur utilité dans certains algorithmes, qu'il s'agisse d'automates ou d'arbres par exemple.

Cependant, cette leçon ne doit pas être confondue avec la 909, "*Langages rationnels et Automates finis. Exemples et applications.*". La compression de texte peut faire partie de cette leçon si les algorithmes présentés contiennent effectivement des opérations comme les comparaisons de chaînes : la compression LZW, par exemple, est plus pertinente dans cette leçon que la compression de Huffman.

Questions possibles :

- Donner le principe de l'algorithme de la plus longue sous séquence commune.
- Quelle est la différence entre Morris Pratt et Knuth Morris Pratt ?

  Réponse : la complexité spatiale

Motivations :

L'algorithmique du texte est présente partout dans notre quotidien. J'ai séparé mon plan en 4 parties. Une première sur la recherche de motif, essentielle pour les `Ctrl+F` afin de chercher un mot sur une page web, sur un document, dans un fichier de 500 pages qui recense plein de résultats utiles pour passer l'agrégation, etc. ; une deuxième sur l'analyse lexicale et syntaxique qui est nécessaire lors de la compilation de programmes informatiques ; une troisième sur la comparaison de texte, notamment dans l'étude des séquences de l'ADN où l'on cherche les ressemblances ; une quatrième sur la compression de texte, afin d'améliorer le stockage de données.

Plan détaillé :

I - Recherche d'un motif

algorithme naïf

Automate des occurrences pour l'algorithme de Morris Pratt

Algorithme de Knuth Morris Pratt

II - Analyse lexicale et syntaxique

1) analyse lexicale

utilisation de l'automate du motif

2) analyse syntaxique

Cocke-Younger-Kasami

III - Comparaison de texte

distance d'édition

plus longue sous séquence commune

IV - Compression

1) codage de Huffman

2) compression LZW

Développements :

- Automate des occurrences
- Cocke-Younger-Kasami

Références :

♥♥♥ - [CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST et Clifford STEIN, *Algorithmique*

♥♥♥ - [CHL01] Maxime CROCHEMORE, Christophe HANCART et Thierry LECROQ , *Algorithmique du texte*

Leçon 909
Langages rationnels et automates finis. Exemples et applications.

Rapport du jury :

Pour cette leçon très classique, il importe de ne pas oublier de donner exemples et applications, ainsi que le demande l'intitulé.

Une approche algorithmique doit être privilégiée dans la présentation des résultats classiques (déterminisation, théorème de Kleene, etc.) qui pourra utilement être illustrée par des exemples. Le jury pourra naturellement poser des questions telles que : connaissez-vous un algorithme pour décider de l'égalité des langages reconnus par deux automates ? quelle est sa complexité ?

Des applications dans le domaine de l'analyse lexicale et de la compilation entrent naturellement dans le cadre de cette leçon.

Questions possibles :

- Donner des idées de preuve pour le théorème de Kleene.
- Déterminiser un automate.
- Donner un exemple d'automate à n états dont l'automate déterminisé possède 2^n états.

Plan détaillé :

I - Langages rationnels, langages reconnaissables

1) langage rationnel

expression rationnelle

2) langage reconnaissable

automate

déterminisme

complet

3) équivalence entre les deux langages

théorème de Kleene

II - Propriétés des langages rationnels

1) stabilité et décidabilité

Décidabilité de Presburger

2) résiduels

Automate des occurrences

Algorithme de Hopcroft

recherche de motif

3) Lemme de l'étoile

En annexe :

- automate du complémentaire
- automate de l'union
- automate de l'intersection

Développements :

- Automate des occurrences
- Décidabilité de Presburger

Références :

♥♥♥♥♥ - [CAR14] Olivier CARTON, *Langages Formels : Calculabilité et complexité*

Leçon 912
Fonctions récursives primitives et non primitives. Exemples.

Rapport du jury :

Il s'agit de présenter un modèle de calcul : les fonctions récursives. S'il est bien sûr important de faire le lien avec d'autres modèles de calcul, par exemple les machines de TURING, la leçon doit traiter des spécificités de l'approche. Le candidat doit motiver l'intérêt de ces classes de fonctions sur les entiers et pourra aborder la hiérarchie des fonctions récursives primitives. Enfin, la variété des exemples proposés sera appréciée.

Questions possibles :

- Comment écrire la fonction mod en fonction μ-récursive ?

  Réponse : voir appendice

Plan détaillé :

I - Fonctions primitives récursives

1) syntaxe

   les fonctions de bases

2) sémantique

   la boucle for

   prédicat

   minimisation bornée

   bijection primitive récursive dont la réciproque est primitive récursive (voir appendice)

3) limite

   fonction Ackermann non primitive récursive

II - Fonctions μ-récursives

   minimisation non bornée

   prédicat sûr

   fonction totale/partielle

   boucle while

   la fonction Ackermann est μ-récursive

III - Modèle de calcul

1) thèse de Church

2) machine de Turing

   Machine de Turing $\implies$ μ-recursif

   Caractérisation de RE

3) λ-calcul

   μ-recursif $\implies$ λ-définissable

Développements :

- μ-recursif $\Longrightarrow$ λ-définissable
- Machine de Turing $\Longrightarrow$ μ-recursif

Références :

♥♥♥ - [LDR93] Richard LASSAIGNE et Michel DE ROUGEMONT, *Logique et fondements de l'informatique logique du 1er ordre, calculabilité et lambda-calcul*

♥♥♥♥ - [WOL06] Pierre WOLPER, *Introduction à la calculabilité*

Leçon 913
Machines de Turing. Applications.

Rapport du jury :

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

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Machine de Turing
- 1) Définitions
  - Def Machine de Turing
  - Def Configuration
  - Def Exécution
- 2) Variante
  - Plusieurs rubans
  - Double ruban infini
  - Machine non déterministe

II - Décidabilité et indécidabilité
- Définition Classe R
- Définition Classe RE
- Problème de l'arrêt
- Définition de la réduction
- Problème du mot

III - Calculabilité et thèse de Church
- 1) Thèse de Church
  - Énoncé
- 2) Fonctions μ-récursives
  - Caractérisation de RE
  - Machine de Turing $\Longrightarrow$ μ-recursif
- 3) λ-calcul
  - Théorème d'équivalence

IV - Complexité
- Classe P
- Classe NP
- Réduction polynomiale
- P $\neq$ NP
- Classe NP-complet
- Théorème de Cook

Développements :

- Théorème de Cook
- Machine de Turing $\Longrightarrow$ μ-recursif

Références :

♥♥♥♥♥ - [CAR14] Olivier CARTON, *Langages Formels : Calculabilité et complexité*

♥♥ - [LDR93] Richard LASSAIGNE et Michel DE ROUGEMONT, *Logique et fondements de l'informatique logique du 1er ordre, calculabilité et lambda-calcul*

♥♥♥ - [WOL06] Pierre WOLPER, *Introduction à la calculabilité*

Leçon 914
Décidabilité et indécidabilité. Exemples.

Rapport du jury :

Le programme de l'option offre de très nombreuses possibilités d'exemples. Si les exemples classiques de problèmes sur les machines de TURING figurent naturellement dans la leçon, le jury apprécie des exemples issus d'autres parties du programme : théorie des langages, logique,...

Le jury portera une attention particulière à une formalisation propre des réductions, qui sont parfois très approximatives.

Questions possibles :

- Montrer l'indécidabilité du problème de l'arrêt.

Motivations :

La frontière entre décidabilité et indécidabilité sépare certains problèmes en terme de possibilité de résolution grâce à une machine de Turing. En effet, on va avoir une correspondance entre problème et langage et la notion de décidabilité se transposera entre langages décidés par une machine de Turing et les problèmes décidables. La classe R est l'ensemble des problèmes décidables, cependant la classe RE représente les problèmes acceptés par une machine de Turing, il existe des problèmes qui sont indécidables et qui ne sont pas dans RE comme l'arithmétique de PEANO par exemple.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Généralisation et cadre
  1) Classe R et RE
    Définitions
    Caractérisation de RE
  2) Fonctions calculables et réductions
    Définitions

II - Technique pour prouver l'indécidabilité
  1) Problème de l'arrêt
    Définition
    Idée de preuve
  2) Utilisation de la réduction
    Propriétés

III - Décidabilité et indécidabilités de quelques problèmes (voir appendice)
  1) Machines de Turing
    Acceptation du mot (indécidable)
    Problème de POST (indécidable)

2) Automates finis

Acceptation du mot (décidable)

Universalité (décidable)

3) Grammaires algébriques

Acceptation du mot (décidable)

Vide (décidable)

Intersection (indécidable)

Universalité (indécidable)

4) Logique

Décidabilité de Presburger (décidable)

SAT (décidable)

Indécidabilité de la validité d'une formule du premier ordre (indécidable)

PEANO (indécidable)

En annexe :

- un arbre des réductions des problèmes indécidables (voir appendice).
- les inclusions des classes R, RE et indécidables (voir Carton [CAR14]).

Développements :

- Indécidabilité de la validité d'une formule du premier ordre
- Décidabilité de Presburger

Références :

♥♥♥♥ - [CAR14] Olivier CARTON, *Langages Formels : Calculabilité et complexité*

♥♥♥ - [WOL06] Pierre WOLPER, *Introduction à la calculabilité*

Leçon 915
Classes de complexité. Exemples.

Rapport du jury :

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

Se focaliser sur la décidabilité dans cette leçon serait hors sujet.

Questions possibles :

- Donner une autre définition de NP.
- Connaissez-vous un autre modèle de calcul pour calculer la complexité ?
- Donner un exemple de problème dans NP dont on ne sait pas s'il est dans P ou NP-dur.
- Expliquer QBF_SAT. Pourquoi il est PSpace-complet ?
- Qu'est ce qu'on appelle un problème de décision ?
- Donner une définition de la NP-difficulté d'un problème d'optimisation
- Pourquoi PSpace $\subset$ ExpTime ?
- Si on change de codage de l'entrée, est ce que la complexité change ?

  Réponse : oui, par exemple, si le codage est en unaire, le problème SubsetSum est dans P, on parle de problème pseudo-polynomiaux

Motivations :

On a classifié pendant la leçon **914**, les problèmes décidables et indécidables, on veut maintenant trouver une hiérarchie plus fine des problèmes décidables. On se place donc parmi les problèmes décidables. Il va falloir parler de modèle de calcul, car la complexité dépend a priori du modèle de calcul (cela donnera la séparation entre P et NP par exemple). On s'intéressera aux complexités temporelle et spatiale et le lien qu'il y a entre les deux.

Je suis tombé sur cette leçon le jour de l'agrégation (voir section 5.1)

Plan détaillé :

I - Outil : Machine de Turing

Définition Machine de Turing

Définition Complexité spatiale et temporelle

Lemme de lien entre les deux complexités

II - Complexité temporelle

1) Changement de modèle de calcul

Théorème d'accélération

Équivalence avec machine de Turing à ruban biinfini (et même complexité temporelle)

Équivalence avec machine de Turing à k rubans (et facteur carré sur la complexité)

Équivalence avec machine de Turing non déterministe (et facteur exponentiel sur la complexité)

2) Classes temporelles

Définition de TIME et NTIME

Définition de P, NP, EXPTIME et NEXPTIME

Exemple du problème du mot des langages algébriques qui est dans P [Cocke-Younger-Kasami]

Exemple de SAT qui est NP.

3) NP-complétude

Définition réduction polynomiale

Propriété, si A se réduit à B et B est dans P alors A est dans P

Définition NP-dureté

Propriété, si A se réduit à B et A est NP-dur, alors B est NP-dur

Définition NP-complétude

[Théorème de Cook]

Exemple CNF_SAT et 3_SAT sont NP-complets

Exemple [3-Coloration d'un graphe], Vertex_Cover, Circuit Hamiltonien et Voyageur de Commerce sont NP-complets

III - Complexité spatiale

1) Classes spatiales

Théorème de Savitch

Définition de SPACE et NSPACE

Définition de PSPACE, NPSPACE, EXPSPACE et NEXPSPACE

Exemple QBF_SAT est PSPACE

Définition de PSPACE-dureté

Définition de PSPACE-complétude

Exemple QBF_SAT est PSPACE-complet

2) Classe logarithmique

Définition des machines à 3 bandes qui servent à la réduction logarithmique

Définition de L et NL

Exemple PATH est dans NL

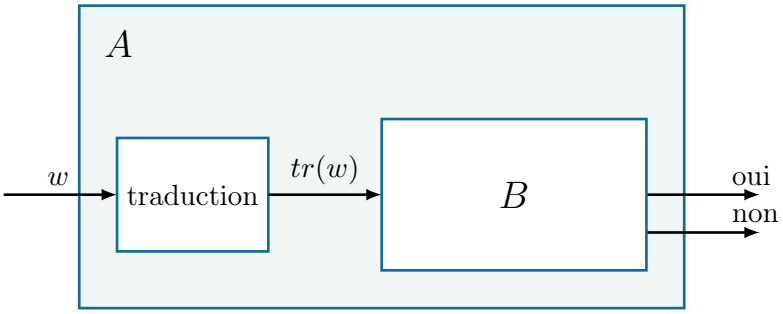
IV - Hiérarchie des complexités

Théorème des hiérarchies

inclusion de toutes les classes avec certaines inclusions strictes

En annexe :

- un schéma de réduction



- un arbre des réductions des problèmes NP-complet (voir appendice)
- les inclusions des classes (voir Carton [CAR14])

Développements :

- Cocke-Younger-Kasami
- Théorème de Cook
- 3-Coloration d'un graphe

Références :

♥♥♥♥♥ - [CAR14] Olivier CARTON, *Langages Formels : Calculabilité et complexité*

♥♥♥ - [WOL06] Pierre WOLPER, *Introduction à la calculabilité*

♥♥ - [GJ79] Michael GAREY et David JOHNSON, *Computers and Intractability : A Guide to the Theory of Np-Completeness*

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

Rapport du jury :

Le jury attend des candidats qu'ils abordent les questions de la complexité de la satisfiabilité.

Pour autant, les applications ne sauraient se réduire à la réduction de problèmes NP-complets à SAT.

Une partie significative du plan doit être consacrée à la représentation des formules et à leurs formes normales.

Questions possibles :

- Montrer rigoureusement la réduction de CnfSat à 3Sat.
- Montrer qu'une formule sous CNF équivalente à

$$(x_1 \wedge y_1) \vee (x_2 \wedge y_2) \vee \cdots \vee (x_n \wedge y_n)$$

  est de taille exponentielle en la taille de la formule de départ.
- Montrer que le système $\{\leftrightarrow, \neg\}$ n'est pas complet.
- Donner un système complet de connecteurs logiques qui ne contient qu'un seul connecteur logique.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Syntaxe
  1) Langage
     Vocabulaire
     Définition par induction
  2) Représentation
     Formule
     Arbre
  3) Résolution par réfutation
     Règle de coupure
     Règle de factorisation

II - Sémantique
  1) Valuation
     Définition
     Table de vérité
  2) Validité et satisfiabilité
     Définition validité

Définition satisfiabilité

3) Équivalence sémantique

Définition de tautologie

Lois de De Morgan

4) Lien entre syntaxe et sémantique

Théorème de correction et complétude

III - Satisfiabilité et formes normales

Théorème de Cook

1) Mise sous forme normale conjonctive

Définition

Propriété d'équivalence avec des formules de tailles exponentielles

Transformation de Tseitin

2) D'autres formes normales

Définition de forme normale disjonctive

Problème DnfSat dans P

Développements :

- Théorème de Cook
- Transformation de Tseitin

Références :

♥♥♥♥ - [LDR93] Richard LASSAIGNE et Michel DE ROUGEMONT, *Logique et fondements de l'informatique logique du 1er ordre, calculabilité et lambda-calcul*

♥♥ - [BA12] Mordechai BEN ARI, *Mathematical Logic for Computer Science*

♥♥♥ - [CL03] René CORI et Daniel LASCAR, *Logique Mathématique*

♥♥ - [DUP15] Jacques DUPARC, *Logique pas à pas*

Leçon 918
Systèmes formels de preuve en logique du premier ordre. Exemples.

IMPASSE

Ce n'est pas par difficulté de la leçon mais car mes couplages m'obligeaient à apprendre deux nouveaux développements à un mois des oraux. Donc cela justifie le fait qu'il faut faire ces couplages tôt dans l'année et bien travailler ces développements.

Après l'agreg, je vous écris ce que je pense que j'aurais fait comme plan :

Rapport du jury :

Le jury attend du candidat qu'il présente au moins la déduction naturelle ou un calcul de séquents et qu'il soit capable de développer des preuves dans ce système sur des exemples classiques simples. La présentation des liens entre syntaxe et sémantique, en développant en particulier les questions de correction et complétude, et de l'apport des systèmes de preuves pour l'automatisation des preuves est également attendue.

Le jury appréciera naturellement si des candidats présentent des notions plus élaborées comme la stratégie d'élimination des coupures mais est bien conscient que la maîtrise de leurs subtilités va au-delà du programme.

Plan détaillé :

I - Logique du premier ordre
- Syntaxe
- Sémantique

II - Système de preuves avec règles syntaxiques

1) Déduction naturelle
- Règles en annexe
- Théorème de correction et complétude

2) Calcul des séquents
- Règles en annexe
- Théorème de correction et complétude

III - Preuve par résolution
- Forme prénexe
- Skolémisation
- Unificateur
- Unificateur principal
- Règle de résolution et factorisation
- Exemples
- Modèles de Herbrand
- Théorème de Correction et complétude

Développements : Bah j'en ai pas ! On pourrait mettre :

- Théorème de complétude de la déduction naturelle
- Algorithme d'unification

Références :

♥♥♥♥ - [DNR04] René DAVID, Karim NOUR et Christophe RAFFALLI, *Introduction à la logique : Théorie de la démonstration*

♥♥♥♥♥ - [LAL00] René LALEMENT, *Logique, Réduction, Résolution*

Leçon 921
Algorithmes de recherche et structures de données associées.

Rapport du jury :

Le sujet de la leçon concerne essentiellement les algorithmes de recherche pour trouver un élément dans un ensemble : l'intérêt des structures de données proposées et de leur utilisation doit être argumenté dans ce contexte.

La recherche d'une clé dans un dictionnaire sera ainsi par exemple l'occasion de définir la structure de données abstraite "dictionnaire", et d'en proposer plusieurs implantations concrètes. De la même façon, on peut évoquer la recherche d'un mot dans un lexique : les arbres préfixes (ou *digital tries*) peuvent alors être présentés. Mais on peut aussi s'intéresser à des domaines plus variés, comme la recherche d'un point dans un nuage (et les *quad-trees*), et bien d'autres encore.

Plan détaillé :

I - Recherche dans un dictionnaire
- 1) Structures simples
  - liste non triée
  - tableau trié
- 2) Arbres
  - ABR
  - AVL
  - ABRO
  - B-arbres
- 3) Table de Hachage
  - Principe
  - Hachage parfait

II - Recherche dans un texte
- 1) Recherche naïve
  - Algo
  - Complexité
- 2) Automate des occurrences
  - Algorithme de Morris-Pratt
- 3) Algorithme de Knuth-Morris-Pratt
  - Principe
  - Complexité

Développements :

- B-arbres
- Automate des occurrences

Références :

♥♥♥♥ - [CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST et Clifford STEIN, *Algorithmique*

♥♥♥♥ - [FGS90] Christine FROIDEVAUX, Marie-Claude GAUDEL et Michèle SORIA , *Type de données et algorithmes*

Leçon 923
Analyses lexicale et syntaxique. Applications.

Rapport du jury :

Cette leçon ne doit pas être confondue avec la 909, qui s'intéresse aux seuls langages rationnels, ni avec la 907, sur l'algorithmique du texte.

Si les notions d'automates finis et de langages rationnels et de grammaires algébriques sont au cœur de cette leçon, l'accent doit être mis sur leur utilisation comme outils pour les analyses lexicale et syntaxique. Il s'agit donc d'insister sur la différence entre langages rationnels et algébriques, sans perdre de vue l'aspect applicatif : on pensera bien sûr à la compilation. Le programme permet également des développements pour cette leçon avec une ouverture sur des aspects élémentaires d'analyse sémantique.

Questions possibles :

- Calculer la fonction Premier pour la grammaire suivante $G = (\Sigma, \mathcal{N}, \mathcal{T}, S, \mathcal{R})$ où $\Sigma = \{a, b, c, d\}$, $\mathcal{N} = \{S, A, B, C\}$, $\mathcal{T} = \Sigma$ et $\mathcal{R}$ est décrit par

$$\begin{aligned} S &\to AB \mid Ca \\ A &\to aAb \mid \varepsilon \\ B &\to bB \mid b \\ C &\to cC \mid d. \end{aligned}$$

- Donner la table d'analyse syntaxique de la grammaire précédente.
- Donner une grammaire qui n'est pas LL(1).
- Calculer la fonction Suivant pour la grammaire suivante $G = (\Sigma, \mathcal{N}, \mathcal{T}, S, \mathcal{R})$ où $\Sigma = \{a, b\}$, $\mathcal{N} = \{S\}$, $\mathcal{T} = \Sigma$ et $\mathcal{R}$ est décrit par

$$S \to \varepsilon \mid aSb.$$

Motivations :

Quand un ordinateur compile un programme dans un certain langage, il passe par trois étapes avant la compilation : l'analyse lexicale, l'analyse syntaxique et l'analyse sémantique. On va présenter les deux premiers. L'analyse lexicale permet de regrouper les caractères en des groupes de caractères appelés « lexèmes », cette analyse permet de renvoyer une erreur si le programme contient des caractères que le langage informatique ne reconnait pas (par exemple ¿ou ±). L'analyse syntaxique permet de vérifier que le programme est une succession de lexèmes qui est un mot de la grammaire qui engendre le langage utilisé, cette analyse permet de renvoyer une erreur si le programme contient des successions invalides de lexèmes (par exemple, le symbole « + » doit être entre deux lexèmes de type « entiers », sinon cela déclenche une erreur syntaxique).

Plan détaillé :

I - Langages rationnels et algébriques [CAR14]

1) Langage rationnel

Définition

Automate

Exemple automate du motif (utilité dans l'analyse lexicale)

Expression régulière

Théorème de Kleene

2) Langage algébrique

Définition grammaire

Définition dérivation

Arbre de dérivation

Lemme de factorisation

Exemples de grammaire préfixe et postfixe (utilité dans l'analyse syntaxique)

II - Analyse lexicale [LS15]

But : transformer un texte en liste de lexèmes

Définitions règles lexicales

Algorithme d'analyse lexicale en liste de lexèmes

III - Analyse syntaxique [LS15]

But : savoir si un texte est engendré par une grammaire et construire l'arbre de dérivation

1) Algorithme générique

Approche néïve

Cocke-Younger-Kasami

2) Analyse descndante

Grammaire $LL(1)$

Fonctions PREMIER, SUIVANT

Caractérisation de PREMIER pour l'analyse $LL(1)$

Présentation de l'algorithme

3) Analyse ascendante

Grammaire $LR(0)$

En annexe :

- Exemples de grammaires $LL(1)$

Développements :

- Cocke-Younger-Kasami
- Caractérisation de PREMIER pour l'analyse $LL(1)$

Références :

♥♥♥♥♥♥♥ - [LS15] Romain LEGENDRE et François SCHWARZENTRUBER, *Compilation : Analyse Lexicale et Syntaxique du Texte à sa Structure en Informatique*

♥♥ - [CAR14] Olivier CARTON, *Langages Formels : Calculabilité et complexité*

Leçon 924
Théories et modèles en logique du premier ordre. Exemples.

Rapport du jury :

Le jury s'attend à ce que la leçon soit abordée dans l'esprit de l'option informatique, en insistant plus sur la décidabilité/indécidabilité des théories du premier ordre que sur la théorie des modèles.

Il est attendu que le candidat donne au moins un exemple de théorie décidable (respectivement complète) et un exemple de théorie indécidable.

Le jury appréciera naturellement si des candidats connaissent l'existence du premier théorème d'incomplétude mais est bien conscient que la démonstration va au-delà du programme.

Questions possibles :

- Montrer que si T est récursive, alors $T-$valid est dans RE.
- Montrer que si T est complète et récursive, alors $T-$valid est dans R.
- Comment montrer le théorème de compacité à partir du théorème de correction et complétude ?
- Donner des applications du théorème de compacité.

Motivations :

La logique du premier ordre peut être vue comme une extension de la logique propositionnelle, cependant l'approche classique est une nouvelle structure syntaxique comprenant des symboles de fonctions et de prédicats, ensuite quand on ajoute la sémantique, les interprétations des fonctions seront des fonctions (mathématiques) prenant en argument des éléments du domaine et renvoyant un élément du domaine tandis que les interprétations des prédicats seront des fonctions prenant en argument des éléments du domaine et renvoyant un booléen True ou False. La donnée de modèles (le penchant de ce qu'on appelle « valuations » en logique propositionnelle) qui correspond à un domaine et des interprétations de tous les symboles de fonctions et de prédicats permettra de dire si une formule est satisfiable ou valide. On définit des théories en ce donnant un ensemble clos par conséquence logique de formules closes. Certaines théories sont axiomatisables, c'est-à-dire que la théorie sera l'ensemble des formules qui sont conséquence logique des axiomes.

Plan détaillé :

I - Logique du premier ordre [DNR04]

1) Syntaxe

Définition de signature

Définition de terme

Définition de formules

Définition de variables libre et liée

Définition formule close

2) Modèles

Définition de structure

Définition de valuation

Définition d'interprétation

Définition de modèle

Définition de validité

3) Théories

Définition de théorie

Définition de modèle d'une théorie

Définition de théorie cohérente/contradictoire

$T \models F$ si et seulement si $T \cup \{\neg F\}$ contradictoire

Définition de $T-$validité

Définition de théorie complète

Définition de théorie décidable

Indécidabilité de la validité d'une formule du premier ordre en disant que la théorie vide est indécidable

II - Résolution

1) Méthode de la résolution

Forme prénexe

Skolémisation

Unificateur principal

Règle de coupure et de factorisation

2) Théorème de correction et complétude

Modèle de Herbrand

$T \cup \{\neg F\}$ contradictoire si et seulement si $T \cup \{\neg F\} \vdash \bot$

3) Conséquences [DNR04]

Théorème de compacité

Théorème de Lowenheim Skolem

Définition théorie récursive

Si T est récursive, alors $T-$valid est dans RE

Si T est complète et T est récursive, alors $T-$valid est dans R

III - Théories arithmétiques

1) Arithmétique de Presburger

Définition de la théorie de Presburger

$\textsc{Tpres} \models F$ si et seulement si $\mathbb{N} \models F$

Décidabilité de Presburger

2) Arithmétique de Peano

Définition de la théorie de Peano

$\textsc{Tpeano}$ est indécidable

Théorème d'incomplétude de Gödel : Si T est récursive, cohérente et contient $\textsc{Tpeano}$, alors T n'est pas complète.

Développements :

- Indécidabilité de la validité d'une formule du premier ordre
- Décidabilité de Presburger

Références :

♥♥♥♥♥ - [DNR04] René DAVID, Karim NOUR et Christophe RAFFALLI, *Introduction à la logique : Théorie de la démonstration*

♥♥♥♥ - [LAL00] René LALEMENT, *Logique, Réduction, Résolution*

♥♥♥ - [LDR93] Richard LASSAIGNE et Michel DE ROUGEMONT, *Logique et fondements de l'informatique logique du 1er ordre, calculabilité et lambda-calcul*

Leçon 925
Graphes : représentations et algorithmes.

Rapport du jury :

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

Questions possibles :

- Faire tourner les algorithmes présents dans le plan.
- Pourquoi 2Col est dans P ?

Plan détaillé :

I - Généralité et cadre
- Définition de graphe, sommet, arête
- Définition de adjacence, voisins
- Définition de orienté
- Définition chemin, cycle, clique
- Définition de connexe
- Définition de poids
- Représentation des graphes en machine

II - Parcours
- Parcours en largeur
- Exemple du plus court chemin (voir partie 4)
- Parcours en profondeur
- Exemple des composante fortement connexe
- Tri topologique

III - Arbres couvrants minimaux
- Définition
- Explication algorithme de Prim
- Explication algorithme de Kruskal

IV - Plus court chemin
- Explication algorithme de Dijkstra
- Explication algorithme de Floyd-Warshall

V - Problèmes NP-complets (voir appendice)
- 3-Coloration d'un graphe
- Cycle Hamiltonien
- Problème du voyageur de commerce

En annexe :

- Dessins de Graphe
- Parcours en largeur et en profondeur
- Composantes fortement connexe
- Arbre couvrant
- Prim et Kruskal

Développements :

- 3-Coloration d'un graphe
- Tri topologique

Références :

♥♥♥♥ - [CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST et Clifford STEIN, *Algorithmique*

♥♥♥♥ - [FGS90] Christine FROIDEVAUX, Marie-Claude GAUDEL et Michèle SORIA , *Type de données et algorithmes*

♥♥♥ - [GJ79] Michael GAREY et David JOHNSON, *Computers and Intractability : A Guide to the Theory of Np-Completeness*

Leçon 926
Analyse des algorithmes : complexité. Exemples.

Rapport du jury :

Il s'agit ici d'une leçon d'exemples. Le candidat prendra soin de proposer l'analyse d'algorithmes portant sur des domaines variés, avec des méthodes d'analyse également variées : approche combinatoire ou probabiliste, analyse en moyenne ou dans le pire cas.

Si la complexité en temps est centrale dans la leçon, la complexité en espace ne doit pas être négligée. La notion de complexité amortie a également toute sa place dans cette leçon, sur un exemple bien choisi, comme union find (ce n'est qu'un exemple).

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Généralité et cadre
- Définitions
- Notation de Landau
- Différentes approches (au pire, moyenne, ...)

II - Premières méthodes de calcul de complexité
- Calcul direct
- Complexité moyenne vu comme une espérance
- Résolution de récurrence
- masterthrm

III - Complexité amortie
- Exemple filé sur le tableau dynamique

1) Agrégat
   - Expliquer sur le tableau dynamique
2) Comptable
   - Définir les coûts et dépenses
3) Potentiel
   - Exprimer la valeur du potentiel dans l'exemple

IV - Amélioration de la complexité
- Borne inférieure pour les tris par comparaison
- Tri par tas
- Amélioration de la structure de donnée
- Exemple entre Morris-Pratt et Knuth-Morris-Pratt
- Compromis entre espace et temps
- Exemple de Fibonacci

Développements :

- Tri par tas
- Master Theorem

Références :

♥♥♥♥ - [CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST et Clifford STEIN, *Algorithmique*

♥♥♥♥ - [FGS90] Christine FROIDEVAUX, Marie-Claude GAUDEL et Michèle SORIA , *Type de données et algorithmes*

♥♥♥ - [AK98] Luc ALBERT et Daniel KROB, *Cours et exercices d'informatique*

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

Rapport du jury :

Le jury attend du candidat qu'il traite des exemples d'algorithmes récursifs et des exemples d'algorithmes itératifs.

En particulier, le candidat doit présenter des exemples mettant en évidence l'intérêt de la notion d'invariant pour la correction partielle et celle de variant pour la terminaison des segments itératifs.

Une formalisation comme la logique de Hoare pourra utilement être introduite dans cette leçon, à condition toutefois que le candidat en maîtrise le langage. Des exemples non triviaux de correction d'algorithmes seront proposés. Un exemple de raisonnement type pour prouver la correction des algorithmes gloutons pourra éventuellement faire l'objet d'un développement.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Terminaison
- 1) Définitions
  - Exemples de Syracuse
  - Problème de l'arrêt
- 2) Ensemble bien fondé et algo récursif
  - Exemple de PGCD et Ackermann
- 3) Variant de boucle et algo itératif
  - Définition Variant de boucle
  - Théorème de terminaison
  - Exemple de la division euclidienne

II - Correction
- 1) Définitions
  - Différence entre partiel et total
  - Tri topologique
- 2) Algorithmes récursifs
  - Exemple PGCD et tri par insertion
- 3) Algorithmes itératifs
  - Définition invariant de boucle
  - Théorème pour la correction
  - Exemple Dijkstra

III - Logique de Hoare (voir appendice)
- 1) Langage IMP
  - Définitions
- 2) Sémantique naturelle (ou opérationnelle à grands pas)

Règles

Propriétés de langage déterministe

3) Triplets de Hoare (partiel)

Définition

Règles

Théorème de correction

Théorème de Complétude de la logique de Hoare

Développements :

- Tri topologique
- Complétude de la logique de Hoare

Références :

♥♥♥♥ - [CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST et Clifford STEIN, *Algorithmique*

♥♥♥♥ - [FGS90] Christine FROIDEVAUX, Marie-Claude GAUDEL et Michèle SORIA , *Type de données et algorithmes*

♥♥♥ - [AK98] Luc ALBERT et Daniel KROB, *Cours et exercices d'informatique*

♥♥♥ - [NN07] Hanne Riis NIELSON et Flemming NIELSON, *Semantics with applications*

Leçon 928
Problèmes NP-complets : exemples et réduction.

Rapport du jury :

L'objectif ne doit pas être de dresser un catalogue le plus exhaustif possible ; en revanche, pour chaque exemple, il est attendu que le candidat puisse au moins expliquer clairement le problème considéré, et indiquer de quel autre problème une réduction permet de prouver sa NP-complétude.

Les exemples de réduction polynomiale seront autant que possible choisis dans des domaines variés : graphes, arithmétique, logique, etc. Si les dessins sont les bienvenus lors du développement, le jury attend une définition claire et concise de la fonction associant, à toute instance du premier problème, une instance du second ainsi que la preuve rigoureuse que cette fonction permet la réduction choisie et que les candidats sachent préciser comment sont représentées les données.

Un exemple de problème NP-complet dans sa généralité qui devient P si on contraint davantage les hypothèses pourra être présenté, ou encore un algorithme P approximant un problème NP-complet.

Questions possibles :

- Donner un exemple de problème dans NP dont on ne sait pas s'il est dans P ou NP-dur.
- Donner un exemple de problème qui est NP-dur mais pas dans NP.
- Montrer l'une des réductions du plan.
- Comment passe-t-on de CnfSat à 3Sat ?

Motivations :

On a classifié les problèmes décidables et indécidables durant la leçon 914. Ensuite on a étudié les problèmes décidables durant la leçon 915 en hiérarchisant les problèmes afin de déterminer leur complexité (liée au modèle de calcul : machine de Turing). Une classe particulière de cette hiérarchie est la classe des problèmes NP-complets. Ces problèmes sont dans la classe NP et ont la particularité que tout problème de NP peut être réduit à lui. Autrement dit, si on sait résoudre de manière efficace un problème NP-complet, on pourra résoudre tous les autres problèmes NP. Une grande question en informatique est de savoir si $\mathsf{P} = \mathsf{NP}$ ou si $\mathrm{P} \neq \mathsf{NP}$. Tous les problèmes ci-dessous sont détaillés dans l'appendice sur les problèmes NP-complets.

Plan détaillé :

I - Définitions et outils

1) Les classes P et NP

Définition de P

Exemple de CYK

Définition de NP

Exemple de Sat

2) Réduction polynomiale

Définition

Exemple

3) NP-complétude

Définition de la NP-complétude

Théorème de Cook

II - Quelques problèmes NP-complets

1) Logique

SAT est NP-complet par le théorème de Cook

Réduction à CNFSAT par la Transformation de Tseitin

Réduction à 3SAT

2) Graphes

3-Coloration d'un graphe

Réduction de 3SAT à VERTEXCOVER

Équivalence entre VERTEXCOVER, INDEPENDANTSET et CLIQUE

Réduction de VERTEXCOVER à HAMCIRC

Réduction à PVC

3) Paquets

Réduction de 3SAT à SUBSETSUM

Réduction de SUBSETSUM à BINPACKING

Réduction de SUBSETSUM à PARTITION

Réduction de PARTITION à SACÀDOS

III - Que faire en cas de NP-difficulté ?

1) Restreindre les entrées

Le problème 2SAT est dans P

Le problème HORNSAT est dans P

Le problème 2COL est dans P

2) Approximation (on va parler de problème d'optimisation ici)

Définition d'un problème d'optimisation

2-approximation de VERTEXCOVER

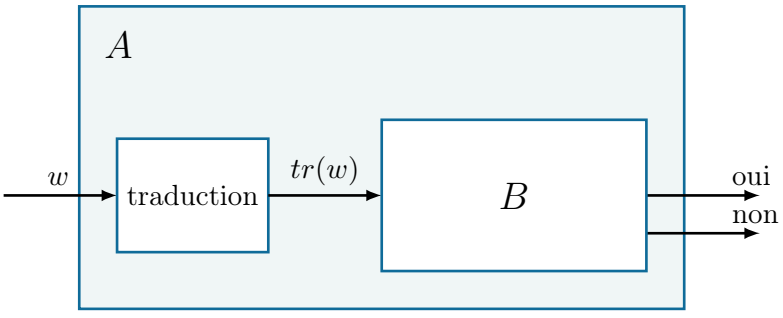
2-approximation du problème du voyageur de commerce euclidien

Remarques :

Pour la deuxième partie, j'écris dans le plan les définitions des problèmes avec entrée et sortie comme c'est montré dans l'appendice des problèmes NP-complets.

En annexe :

- un schéma de réduction



- un arbre des réductions des problèmes NP-complet (voir appendice)
- un exemple de graphe pour les problèmes VertexCover, IndependantSet et HamCirc
- un exemple de graphe biparti pour le problème 2Col

Développements :

- 3-Coloration d'un graphe
- Théorème de Cook
- Transformation de Tseitin

Remarques :
Il n'est sans doute pas très judicieux de mettre seulement le théorème de Cook et la transformation de Tseitin car ce sont tous les deux des développements sur la logique propositionnelle.

Références :

♥♥♥♥ - [GJ79] Michael GAREY et David JOHNSON, *Computers and Intractability : A Guide to the Theory of Np-Completeness*

♥♥♥♥ - [CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST et Clifford STEIN, *Algorithmique*

♥♥♥ - [PAP93] Christos PAPADIMITRIOU, *Computational Complexity*

Leçon 929
Lambda-calcul pur comme modèle de calcul. Exemples.

Rapport du jury :

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

Questions possibles :

- Donner un terme qui n'a pas de forme normale
- Expliquer if_then_else
- Expliquer la fonction prédécesseur sur les entiers de Barendregt
- Expliquer l'équivalence avec les machines de Turing

Points essentiels :

- les subtilités de la substitution
- théorèmes de Church Rosser
- lien avec les autres modèles de calcul

J'ai fait un résumé des bases du λ-calcul dans l'appendice sur le λ-calcul.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Syntaxe
- Termes
- Sous-termes
- Longueur
- Substitution
- α-équivalence

II - β-réduction
- β-réduction
- Exemples
- Théorème de Church Rosser I
- β-équivalence
- Formes normales
- Théorème de Church Rosser II

III - Représentations de données

booléens

$T := \lambda xy.x$

$F := \lambda xy.y$

if_then_else

Listes

Paires

Entiers de Church

Opérations sur ces entiers

Entiers de Barendregt

Opérations sur ces entiers

IV - Modèles de calcul

Thèse de Church

1) Fonctions μ-récursives

Définitions

μ-recursif $\implies$ λ-définissable

Théorème de Scott–Curry

2) Machine de Turing

équivalence

Développements :

- Théorème de Scott–Curry
- μ-recursif $\implies$ λ-définissable

Références :

♥♥♥ - [LDR93] Richard LASSAIGNE et Michel DE ROUGEMONT, *Logique et fondements de l'informatique logique du 1er ordre, calculabilité et lambda-calcul*

♥♥♥♥ - [BAR12] Henk BARENDREGT, *The Lambda Calculus*

♥♥♥♥ - [HS08] Roger HINDLEY et Jonathan SELDIN, *Lambda-Calculus and combinators, an introduction*

Leçon 930
Sémantique des langages de programmation. Exemples.

Rapport du jury :

L'objectif est de formaliser ce qu'est un programme : introduction des sémantiques opérationnelle et dénotationnelle, dans le but de pouvoir faire des preuves de programmes, des preuves d'équivalence, des preuves de correction de traduction.

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

Questions possibles :

- Montrer que les instructions while b do S et if b then S; while b do S else skip sont équivalentes pour la sémantique opérationnelle à grands pas.
- Écrire des règles de sémantique à grands et petits pas pour gérer les instructions repeat S until b, et montrer que l'équivalence est préservée.
- Montrer que le langage IMP muni de la sémantique opérationnelle à petits pas (ou à grands pas) est déterministe, *i.e.* il y a unicité de l'état sortant s' après exécution d'une instruction S à partir d'un état s.

Motivations :

Une sémantique d'un langage de programmation est une fonction $\mathcal{S}$ qui à une instruction S et un état mémoire s associe un état mémoire s'. Ce dernier état mémoire est interprété comme un état mémoire sortant après exécution de l'instruction S sur l'état mémoire initial s. On peut définir une fonction de sémantique $\mathcal{S}$ de différentes manières. Nous verrons deux manières différentes :

- la sémantique « opérationnelle », qui décrit la suite des pas de calcul pendant l'exécution du programme.
- la sémantique « dénotationnelle », qui décrit le programme informatique comme une fonction au sens mathématique du terme.

On va étudier trois sémantiquesdifférentes (deux sémantiques opérationnelleset une sémantique dénotationnelled'un langagede programmation « jouet » dénoté IMP pour langage « IMPératif ».

J'ai fait un résumé des bases de sémantiques des langages de programmation dans l'appendice sur la sémantique.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Le langage IMP
- 1) Syntaxe de IMP
  - Nombres
  - Variables
  - Expressions Arithmétiques
  - Expressions booléennes
  - Instructions
- 2) Sémantique dénotationnelle des expressions
  - $\mathbb{N}$, Var, $\mathcal{A}$, $\mathcal{B}$

II - Sémantique opérationnelle
- 1) A grands pas
  - Règles
  - Langage déterministe
  - Définition de la fonction sémantique
  - Définition d'instructions équivalentes sémantiquement
- 2) A petits pas
  - Règles
  - Langage déterministe
  - Définition de la fonction sémantique
  - Définition d'instructions équivalentes sémantiquement
  - Petites propriétés liées à cette sémantique
- 3) Équivalence des sémantiques
  - Équivalence entre sémantiques opérationnelles

III - Sémantique dénotationnelle
- 1) Fonction sémantique
  - Définition
- 2) Théorie de point fixe
  - CPO
  - Point fixe
- 3) Équivalence des sémantiques
  - Théorème : Équivalence entre sémantique dénotationnelle et à petits pas
  - Corollaire : Équivalence entre sémantique dénotationnelle et à grands pas

IV - Logique de Hoare
- 1) Triplets de Hoare
  - Définition
  - Précondition et postcondition
- 2) Règles de Hoare
  - Règles
- 3) Correction et complétude
  - Théorème de correction
  - Théorème de Complétude de la logique de Hoare

Développements :

- Équivalence entre sémantiques opérationnelles
- Complétude de la logique de Hoare

Références :

♥♥♥♥♥ - [NN07] Hanne Riis NIELSON et Flemming NIELSON, *Semantics with applications*

Leçon 931
Schémas algorithmiques. Exemples et applications.

Rapport du jury :

Cette leçon permet au candidat de présenter différents schémas algorithmiques, en particulier "diviser pour régner", programmation dynamique et approche gloutonne. Le candidat pourra choisir de se concentrer plus particulièrement sur un ou deux de ces paradigmes. Le jury attend du candidat qu'il illustre sa leçon par des exemples variés, touchant des domaines différents et qu'il puisse discuter les intérêts et limites respectifs des méthodes. Le jury ne manquera pas d'interroger plus particulièrement le candidat sur la question de la correction des algorithmes proposés et sur la question de leur complexité, en temps comme en espace.

Questions possibles :

- Donner d'autres paradigmes de programmation.
  Réponse : back tracking, branch and bound, ...
- Est-ce qu'on peut utiliser les trois paradigmes que je présente pour faire des algos d'approximation ?
  Réponse : oui, sac à dos avec programmation dynamique, vertex cover avec algorithmie gloutonne, TSPE avec diviser pour régner

J'ai dressé une liste non exhaustive de différents algorithmes suivant les 3 paradigmes que je présente dans mon plan dans l'appendice sur les schémas algorithmiques.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Diviser pour régner
- Master Theorem
- Tri fusion
- Tri Rapide
- Dichotomie
- Strassen
- Fibonacci

II - Programmation dynamique
- Découpe de barre
- Plus longue sous séquence commune
- Fibaonacci
- Triangle de Pascal
- Cocke-Younger-Kasami
- Floyd Warshall

III - Algorithmie gloutonne
- Problème du sac à dos
- Prim
- Kruskal
- Codage de Huffman

Développements :

- Cocke-Younger-Kasami
- Master Theorem

Références :

♥♥♥♥ - [CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST et Clifford STEIN, *Algorithmique*

♥♥♥ - [BBC92] Danièle BEAUQUIER, Jean BERSTEL et Philippe CHRETIENNE , *Éléments d'algorithmique*

Leçon 932
Fondements des bases de données relationnelles.

Rapport du jury :

Le cœur de cette nouvelle leçon concerne les fondements théoriques des bases de données relationnelles : présentation du modèle relationnel, approches logique et algébrique des langages de requêtes, liens entre ces deux approches.

Le candidat pourra ensuite orienter la leçon et proposer des développements dans des directions diverses : complexité de l'évaluation des requêtes, expressivité des langages de requête, requêtes récursives, contraintes d'intégrité, aspects concernant la conception et l'implémentation, optimisation de requêtes...

Questions possibles :

- Montrer l'indécidabilité du problème RelEqu.

  Réponse : voir commentaires de Indécidabilité de la satisfiabilité d'une requête

Motivations :

Une base de données est une structure qui permet d'organiser un grand nombre de données. Elles seront répertoriées par catégorie, appelée *attribut*, dans différents tableaux, appelés *relations*, ce qui formera la *base de données*. Cette dernière permettra de faire des liens entre les différentes informations qui y sont présentes. On va présenter différents moyens de récupérer des informations dans ces bases de données ainsi que les avantages et inconvénients de chaque moyen.

J'ai fait un résumé de ce qu'il faut savoir sur les bases de données dans l'appendice sur les bases de données.

J'ai rédigé le plan de cette leçon (voir ici)

Plan détaillé :

I - Formalisme

Définitions de variable, attribut, domaine, schéma de relations

Définition d'arité

Définition de schéma de relation

Définition de schéma de base de données

Définition de tuple

Définition de relation

Définition d'une base de données

II - Requêtes conjonctives

1) Règles conjonctives

Définition d'un tuple libre

Définition d'une règle conjonctive

Définition d'une valuation

Définition de la sémantique d'une règle conjonctive

Définition du domaine actif

Propriété : $adom(q(\mathcal{I})) \subset adom(q) \cup adom(\mathcal{I})$

2) Calcul conjonctif

Définition d'une formule de calcul conjonctif

Définition d'une requête en calcul conjonctif

Définition d'une valuation

Définition de la sémantique d'une requête de calcul conjonctif

Théorème de Codd(1) : Le calcul conjonctif et les règles conjonctives sont équivalentes.

III - Algèbre SPC

Définitions de la sélection, la projection et le produit carthésien qui forment l'algèbre SPC

Prop : on peut effectuer la joointure naturelle, l'intersection avec les trois opérations

Remarque : il existe des requêtes insatisfiables

Théorème de Codd (2) : Il y a équivalence entre les requêtes par règles conjonctives, le calcul conjonctif et les requêtes satisfiables de l'algèbre SPC

IV - Calcul et algèbre relationnelle

1) Ajout de l'union

Définition de l'union U

Ajout du $\vee$ dans le calcul conjonctif

Définition d'une requête sûre

2) Ajout de la négation

Définition de la différence ensembliste D

Ajout du $\neg$ dans le calcul conjonctif

Restreint au domaine actif, l'algèbre relationnelle SPCUD et le calcul relationnnel sont équivalents

Indécidabilité de la satisfiabilité d'une requête

V - Optimisation

1) Stockage

Définition d'un B-arbre

B-arbres

2) Optimisation locale des requêtes SPC

Ordre des opérations pour minimiser les requêtes et le nombre de données que l'on manipule

En annexe :

- deux relations qui forment une base de données
- un B-arbre avec $t = 2$

Développements :

- B-arbres
- Indécidabilité de la satisfiabilité d'une requête

Références :

♥♥♥♥ - [AHV95] Serge ABITEBOUL, Richard HULL et Victor VIANU, *Foundations of Databases*

♥ - [CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST et Clifford STEIN, *Algorithmique*

2.6 Les plans que j'ai rédigés

Voici ci-dessous les plans que j'ai rédigés durant mon année d'agrégation. Je précise la date à laquelle je les ai rédigés, avec qui je les ai concoctés et le cadre pendant lequel ils ont été réalisés puisque cela fait varier leur pertinence (notamment les plans rédigés en début d'année manquent parfois de recul et donc ne sont pas forcément les plus fidèles à ce qui est demandé à l'agrégation), leur objectif (une présentation devant la classe n'a pas le même but que la rédaction seule ou la rédaction pendant les oraux blancs), le temps de rédaction (temps limité ou non), la langue dans laquelle ils ont été écrit [1] et sans doute d'autres facteurs...

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

J'ai écrit ce plan tout seul durant le mois de décembre. Je ne suis pas très fier de cette version. J'ai eu beaucoup de mal à faire un plan qui me plaise, d'ailleurs cette version ne me plait pas. J'ai donc changé le plan plus tard dans l'année (voir métaplan **106**). Je trouve que les différents résultats sur les corps finis sont trop séparés.

— Leçon 123 : Corps finis. Applications. (plan manuscrit)

Je suis passé en leçon devant la classe avec Maxence Brévard avec qui j'ai écrit ce plan durant le mois de novembre. Nous étions encadrés par Agnès David. Je n'ai pas gardé la partie sur la transformée de Fourier rapide car je n'étais pas assez à l'aise sur cette notion à mon goût. Le plan final que j'ai fait est celui-ci : métaplan **123**.

— Leçon 126 : Exemples d'équations en arithmétique. (plan manuscrit)

J'ai écrit ce plan seul durant le mois de mai. Ma version finale (voir métaplan **126**) est restée très proche de ce plan.

— Leçon 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications. (plan manuscrit)

J'ai écrit ce plan seul durant le mois d'octobre. Ma version finale (voir métaplan **141**) est restée très proche de ce plan.

— Leçon 152 : Déterminant. Exemples et applications. (plan manuscrit)

J'ai écrit ce plan pour les oraux blancs de juin. Je suis passé devant Karine Beauchard, Jeremy Leborgne et Antoine Mouzard. J'aurai du me placer dans un cadre plus large que juste $\mathbb{R}$ ou $\mathbb{C}$, rien que pour définir le polynôme caractéristique correctement. J'ai modifié légèrement mon plan ensuite (voir métaplan **152**).

— Leçon 153 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications. (plan manuscrit)

J'ai écrit ce plan tout seul durant le mois de septembre. C'est le premier plan que j'ai écrit et donc il faut faire très attention avant de s'y référer car comme je l'ai rédigé très tot dans l'année je n'avais pas forcément le recul nécessaire. Cependant, je n'ai pas énormément modifié mon plan final (voir métaplan **153**). Toutefois, j'ai beaucoup trop développé la trigonalisabilité et la diagonalisabilité. J'aurais voulu mettre la décomposition de Frobenius avec les invariants de similitudes.

1. *# leçon d'anglais (243)*

— Leçon 156 : Exponentielle de matrices. Applications. (plan manuscrit)

Je suis passé en leçon devant la classe avec Emilie Tezenas avec qui j'ai écrit ce plan durant le mois de mai. Nous étions encadrés par Lionel Fourqueaux. J'ai gardé un plan très similaire à celui-ci (en même temps on était en mai déjà). Le plan final que j'ai fait est celui-ci : métaplan **156**.

— Leçon 159 : Formes linéaires et dualité en dimension finie. Exemples et applications. (plan manuscrit)

J'ai écrit ce plan tout seul durant le mois de novembre. J'ai gardé un plan très similaire (voir métaplan **159**).

— Leçon 214 : Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie. (plan manuscrit)

Je suis passé en leçon devant la classe avec Maxence Brévard avec qui j'ai écrit ce plan durant le mois de janvier. Nous étions encadrés par Bachir Bekka. J'ai gardé un plan très similaire à celui-ci. J'ai juste enlevé la dernière partie sur les groupes de Lie et le théorème de Cartan Von Neumann que je ne maitrisais pas du tout. Le plan final que j'ai fait est celui-ci : métaplan **214**.

— Leçon 223 : Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications. (plan manuscrit)

Je suis passé en leçon devant la classe avec Maxence Brévard avec qui j'ai écrit ce plan durant le mois de octobre. Nous étions encadrés par Arnaud Poinas. J'ai finalement changé l'agencement de mes parties car je n'aimais plus la partie applications importantes. Le plan final que j'ai fait est celui-ci : métaplan **223**.

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

J'ai écrit ce plan pour les oraux blancs de janvier. Je suis passé devant Karel Pravda-Starov, Jeremy Leborgne et Angelo Rosello. Finalement, j'ai plus ou moins gardé le même plan par la suite (voir métaplan **226**).

— Leçon 233 : Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples. (plan manuscrit)

J'ai écrit ce plan tout seul durant le mois de décembre. J'ai modifié un peu ce plan en déplaçant le développement du gradient à pas optimal (voir métaplan **233**).

— Leçon 243 : Power series : convergence and properties. Examples and applications. (plan manuscrit)

J'ai écrit ce plan avec Maxence Brévard, Thomas Cavallazzi et François Ernoult durant le mois de février. On a écrit ce plan dans le cadre des cours d'anglais que l'on avait. J'ai gardé à peu près le même plan, en enlevant la partie probabilité de la fin (voir métaplan **243**).

— Leçon 265 : Exemples d'études et d'applications de fonctions usuelles et spéciales. (plan manuscrit)

J'ai écrit ce plan tout seul durant le mois de mai. J'ai gardé le même plan (voir métaplan **265**). Comme c'était une leçon toute neuve de notre année, je voulais l'écrire entièrement. De plus, comme c'est une leçon qui est très personnelle, puisque chacun choisit les fonctions spéciales dont il a envie de parler.

— Leçon 913 : Machines de Turing. Applications. (plan manuscrit)

J'ai écrit ce plan pour les oraux blancs d'informatique d'avril. Je suis passé devant François Schwarzentruber, Nathalie Bertrand et Gilles Lesventes. J'ai modifié très légèrement mon plan ensuite (voir métaplan **913**).

— Leçon 914 : Décidabilité et indécidabilité. Exemples. (plan manuscrit)

Je suis passé en leçon devant la classe avec David Xu avec qui j'ai écrit ce plan durant le mois de décembre. Nous étions encadrés par Nicolas Markey. J'ai modifié légèrement mon plan ensuite (voir métaplan **914**).

— Leçon 916 : Formules du calcul propositionnel : représentation, formes normales, satisfiabilité. Applications. (plan manuscrit)

Je suis passé en leçon devant la classe avec Maxence Brévard avec qui j'ai écrit ce plan durant le mois de janvier. Nous étions encadrés par Sophie Pinchinat. Si je refaisais cette leçon, j'essayerais d'être plus concis sur la première partie. J'ai modifié légèrement mon plan ensuite (voir métaplan **916**).

— Leçon 926 : Analyse des algorithmes : complexité. Exemples. (plan manuscrit)

Je suis passé en leçon devant la classe avec Rémi Cornillet avec qui j'ai écrit ce plan durant le mois de novembre. Nous étions encadrés par Loïc Hélouët. J'ai modifié légèrement mon plan ensuite (voir métaplan **926**).

— Leçon 927 : Exemples de preuve d'algorithme : correction, terminaison. (plan manuscrit)

Je suis passé en leçon devant la classe avec Clarence Kineider avec qui j'ai écrit ce plan durant le mois de avril. Nous étions encadrés par Nicolas Markey. J'ai globalement gardé le même plan (voir métaplan **927**).

— Leçon 929 : Lambda-calcul pur comme modèle de calcul. Exemples. (plan manuscrit)

Je suis passé en leçon devant la classe avec Bastien Jean avec qui j'ai écrit ce plan durant le mois de juin. Nous étions encadrés par David Pichardie. J'ai gardé le même plan par la suite (voir métaplan **929**).

— Leçon 930 : Sémantique des langages de programmation. Exemples. (plan manuscrit)

Je suis passé en leçon devant la classe avec Julie Parreaux avec qui j'ai écrit ce plan durant le mois de avril. Nous étions encadrés par David Pichardie. J'ai gardé le même plan par la suite (voir métaplan **930**).

— Leçon 931 : Schémas algorithmiques. Exemples et applications. (plan manuscrit)

J'ai écrit ce plan pour les oraux blancs d'informatique non officiel de juin que l'on a organisé avec mes camarades. J'ai gardé le même plan par la suite (voir métaplan **931**).

— Leçon 932 : Fondements des bases de données relationnelles. (plan manuscrit)

J'ai écrit ce plan tout seul durant le mois de juin. J'ai gardé le même plan (voir métaplan **932**). Comme c'était une leçon toute neuve de notre année, je voulais l'écrire entièrement. De plus, comme c'est une leçon qui n'est connexe à aucune autre leçon d'informatique, je voulais tester si mon plan pouvait être écrit en 3h sur 3 pages.

106 — Groupe linéaire d'un espace vectoriel de dimension finie E. Sous-groupes de GL(E)

I Groupe linéaire en algèbre linéaire

a) Cadre et généralités

E espace vectoriel de dimension n sur $\mathbb{K}$ où $\mathbb{K}$ est un corps

Def 1 : On appelle groupe linéaire de E, les automorphismes $\mathbb{K}$-linéaires de E muni de la loi de composition $\circ$. On le note $GL(E)$

Ex 2 : l'identité Id appartient à $GL(E)$

2) Isomorphisme avec les matrices

Def 3 : On appelle groupe linéaire matriciel, l'ensemble des matrices inversibles (de taille n) muni de la multiplication. On le note $GL_n(\mathbb{K})$

Rmq 4 : Par l'isomorphisme entre matrices et applications linéaires, on a aussi un isomorphisme entre $GL(E)$ et $GL_n(\mathbb{K})$

Def 5 : On dit que deux matrices A et B de $\mathcal{M}_n(\mathbb{K})$ sont équivalentes s'il existe P et Q dans $GL_n(\mathbb{K})$ telles que $A = PBQ^{-1}$

Prop 6 : Si A et B sont équivalentes, elles ont le même rang

Def 7 : On dit que deux matrices A et B de $\mathcal{M}_n(\mathbb{K})$ sont semblables s'il existe P dans $GL_n(\mathbb{K})$ telle que $A = PBP^{-1}$

Prop 8 : Deux matrices semblables représentent la même application linéaire dans des bases différentes.

Ex 9 : $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -3 & 8 \\ -2 & 5 \end{pmatrix}$ sont semblables où $P = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$

Def 10 : On appelle matrice de permutation une matrice P_σ de $\mathcal{M}_n(\mathbb{K})$ obtenue en permutant les colonnes de I_n selon σ, où $\sigma \in \mathfrak{S}_n$.

Prop 11 : $\forall \sigma \in \mathfrak{S}_n$, $P_\sigma^{-1} = P_{\sigma^{-1}}$.

Prop 12 : Pour tout $\sigma \in \mathfrak{S}_n$, $\det(P_\sigma) = \varepsilon(\sigma)$ où ε est le morphisme signature.

Ex 13 : $\det \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = -1 = \varepsilon((1\,3))$

Lorsque $\mathbb{K}$ est un corps fini, on peut dénombrer $GL_n(\mathbb{K})$

Prop 14 : Si $\mathbb{K} = \mathbb{F}_q$ où $q = p^k$ avec p premier on a $|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$

Appli 15 : On utilise ce résultat pour dénombrer les matrices diagonalisables sur $\mathbb{F}_q$

DEV 1

3) Topologie du groupe linéaire

Prop 16 : $GL_n(\mathbb{C})$ et $GL_n(\mathbb{R})$ sont ouverts dans l'espace des matrices

(Utilisation du déterminant pour le prouver)

Prop 17 : $GL_n(\mathbb{C})$ et $GL_n(\mathbb{R})$ sont denses dans l'espace des matrices.

Appli 18 : Différentielle du déterminant.

Prop 19 : $GL_n(\mathbb{C})$ est connexe alors que $GL_n(\mathbb{R})$ ne l'est pas

(Utilisation du déterminant car $\mathbb{R}^*$ n'est pas connexe)

II Générateurs de $GL(E)$ et $SL(E)$

Def 20 : On appelle groupe spécial linéaire de E le noyau du déterminant

$$SL_n(\mathbb{K}) = \{ A \in GL_n(\mathbb{K}) \,/\, \det A = 1 \}$$

On veut trouver des générateurs de $SL(E)$ et $GL(E)$.

Def 21 : Soit $u \in GL(E)$. On dit que u est une dilatation si dans une base convenable, u a pour matrice $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$ avec $\lambda \in \mathbb{K}^*$ et $\lambda \neq 1$

Prop 22 : Soit H un hyperplan de E, soit $u \in GL(E)$ tel que $u_{|H} = id_H$

Il y a équivalence entre :
(i) u est une dilatation
(ii) $\det u = \lambda \neq 1$ (i.e. $u \notin SL(E)$)
(iii) u admet une valeur propre $\lambda \neq 1$ et est diagonalisable
(iv) $\mathrm{Im}(u - Id) \notin H$.

Illustration 23 : voir annexe

Def 24 : Soit $u \in GL(E)$. On dit que u est une transvection si dans une base convenable, u a pour matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ & & \ddots \\ & & & 1 \end{pmatrix}$

Prop 25 : Soit H hyperplan d'équation $f \in E^*$, soit $u \in GL(E)$, $u \neq id$ tel que $u_{|H} = id_H$

Il y a équivalence entre :
(i) u est une transvection
(ii) $\det u = 1$
(iii) u n'est pas diagonalisable
(iv) $D = \mathrm{Im}(u - Id) \subset H$
(v) $\exists a \in H$, $a \neq 0$ / $\forall x \in E$, $u(x) = x + f(x)a$.

voir annexe

Application 26 : Pivot de Gauss

Thm 27 : Les transvections et dilatations engendrent $GL(E)$

Thm 28 : Les transvections engendrent $SL(E)$

Prop 29 : Le centre de $GL(E)$ est formé des homothéties de E de rapport non nul.

Prop 30 : Le centre de $SL(E)$ est formé des homothéties de E dont le rapport est une racine $n$ième de l'unité de $\mathbb{K}$

Application 31 : définition de $PGL(E)$ et $PSL(E)$ les groupes projectifs de $GL(E)$ et $SL(E)$ en quotientant par leur centre respectif

Pour les corps finis on peut à nouveau dénombrer ces groupes :

Prop 32 :
$$|SL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-2})q^{n-1} = N$$
$$|PGL_n(\mathbb{F}_q)| = N$$
$$|PSL_n(\mathbb{F}_q)| = \frac{N}{pgcd(n, q-1)}$$

Appli 33 : isomorphismes exceptionnels
* $GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$
* $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ $PSL_2(\mathbb{F}_3) \simeq \mathcal{A}_4$
* $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathcal{A}_5$
* $PGL_2(\mathbb{F}_7) \simeq \mathfrak{S}_5$ $PSL_2(\mathbb{F}_7) \simeq \mathcal{A}_5$

III Groupe orthogonal

Def 34 : Soit E muni d'un produit scalaire réel. u est une transformation orthogonale si $\forall x, y \in E$, $\langle u(x), u(y) \rangle = \langle x, y \rangle$

Def 35 : On appelle groupe orthogonal, l'ensemble des transformations orthogonales. On le note $O(E)$

Prop 36 : $O(E)$ est isomorphe à $O_n(\mathbb{R})$
où $O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) / {}^tAA = I_n\}$

Prop 37 : $O_n(\mathbb{R})$ est un sous groupe compact maximal pour l'inclusion de $GL_n(\mathbb{R})$

Thm 38 : Soit $A \in GL_n(\mathbb{R})$, alors il existe un unique couple $(O,S) \in O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ tel que $A = OS$ où $S_n^{++}(\mathbb{R})$ est l'ensemble des matrices symétriques définies positives.

Def 39 : On appelle groupe spécial orthogonal, les transformations orthogonales de déterminant 1. On le note $SO(E)$

Appli 40 : Etude de $O(p,q)$ DEV2

Thm 41 : $O(q)$ est engendré par les réflexions orthogonales, plus précisément par au plus n réflexions pour $u \in O(q)$

Thm 42 : Pour $n \geq 3$, $SO(E)$ est engendré par les renversements. Plus précisément par au plus n renversements pour $u \in SO(q)$

Cas de la dimension 2 et 3 :

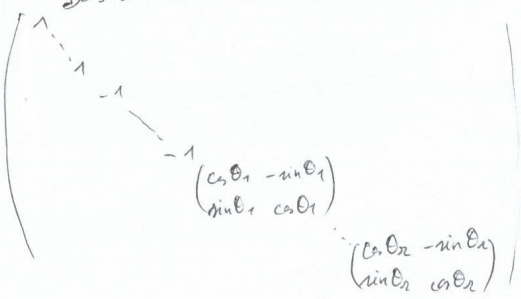
$$O_2(\mathbb{R}) = \left\langle \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \theta \in \mathbb{R}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$$

$$SO_2(\mathbb{R}) = \left\langle \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \theta \in \mathbb{R} \right\rangle$$

$$O_3(\mathbb{R}) = \left\langle \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}, \theta \in \mathbb{R} \right\rangle$$

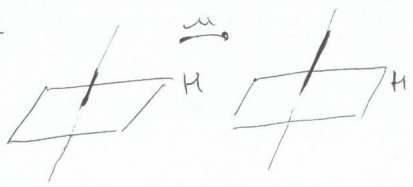
$$SO_3(\mathbb{R}) = \left\langle \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}, \theta \in \mathbb{R} \right\rangle$$

Thm 43 : Soit $u \in G(E)$
Dans une base convenable u est de la forme

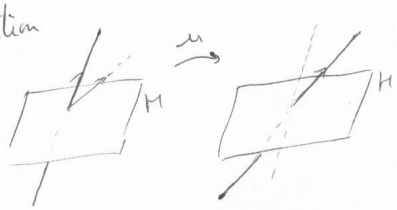


où $\theta_i \in [0; 2\pi[$, et $\theta_i \neq 0, \pi$.

dilatation



transvection



123 Corps finis. Applications [Perrin]

Motivations : Cryptographie / Transformée de Fourier discrète / Codes correcteurs.

I Corps finis

1) Construction des corps finis

K est un corps.

Def 1 : La caractéristique de K est le générateur de $\ker\varphi$ où $\varphi : \mathbb{Z} \to K$, $n \mapsto n.1 = \underbrace{1+1+\dots+1}_{n \text{ fois}}$. On notera $\mathrm{char}(K)$

Prop 2 : La caractéristique d'un corps K est nulle ou un entier p premier.

Prop 3 : $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ n est premier

Ex 4 : $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p / $\mathbb{Q}$ est de caractéristique 0

Def prop 5 : Le sous corps premier de K est le plus petit sous corps de K (contenant 1). Il vaut $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ si $\mathrm{char}(K) = p$ / $\mathbb{Q}$ si $\mathrm{char}(K) = 0$

Ex 6 : $\mathbb{F}_p(X)$ a pour sous corps premier $\mathbb{F}_p$
$\mathbb{R}$ et $\mathbb{C}$ ont pour sous corps premier $\mathbb{Q}$.

Corollaire 7 : Tout corps fini K est une extension de $\mathbb{F}_p$
Si $n = \dim_{\mathbb{F}_p}(K) = [K : \mathbb{F}_p]$, alors $|K| = p^n$

Def 8 : Le morphisme de Frobenius est $F : K \to K$, $x \mapsto x^p$ pour $p = \mathrm{char}(K)$

Prop 9 : F est un automorphisme (pour K fini), injectif + même cardinal au départ et à l'arrivée
F est l'identité sur $\mathbb{F}_p$ (petit théorème de Fermat)

Ex 10 : Pour tout x dans $\mathbb{F}_q$, $x^q = x$.

Thm Def 11 : Soit $q = p^n$, il y a existence et unicité à isomorphisme (non unique) près du corps à q éléments. On le note $\mathbb{F}_q$.
- $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$
- $\mathbb{F}_q$ est l'ensemble des racines de $X^q - X$ sur une clôture algébrique de $\mathbb{F}_p$

Prop 12 : Soit P un polynôme irréductible de degré n sur $\mathbb{F}_p$. Le corps $\mathbb{F}_q$ est alors le corps de rupture de P sur $\mathbb{F}_p$

Ex 13 : $\mathbb{F}_4 = \frac{\mathbb{F}_2[X]}{(X^2+X+1)}$ cf. annexe Attention $\mathbb{F}_4 \not\simeq \mathbb{Z}/4\mathbb{Z}$

Prop 14 : On a $(\mathbb{F}_q, +) \simeq (\mathbb{Z}/p\mathbb{Z})^n$ en tant que groupe abélien fini

Ex 15 : $\mathbb{F}_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Thm 16 : On a $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ si et seulement si $n \mid m$

Ex 17 : Diagramme d'inclusions pour $p = 2$ en annexe

2) Dénombrement et géométrie sur les corps finis

→ comme produit cartésien d'ensemble fini : $|(\mathbb{F}_q)^N| = q^N$
→ en faisant agir $\mathbb{F}_q^*$ sur $(\mathbb{F}_q)^n \setminus \{0\}$: $|P^n(\mathbb{F}_q)| = 1 + q + \dots + q^n$
→ en comptant les bases de $(\mathbb{F}_q)^n$: $|GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$
→ en quotientant $GL_n(\mathbb{F}_q)$ par les homothéties $|PGL_n(\mathbb{F}_q)| = \frac{1}{q^n-1}|GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}$
→ en utilisant le morphisme déterminant : $|SL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}$
→ en quotientant $SL_n(\mathbb{F}_q)$ par son centre : $|PSL_n(\mathbb{F}_q)| = \frac{1}{\mathrm{pgcd}(q-1,n)}|SL_n(\mathbb{F}_q)|$
car $|\mu_n(\mathbb{F}_q)| = \mathrm{pgcd}(q-1, n)$

Prop 18 : On a les isomorphismes exceptionnels suivants :
(i) $GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_2) \simeq PGL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$
(ii) $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$, $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$
(iii) $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$
(iv) $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$, $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$

3) Etude des carrés sur les corps finis

Def 19 : $\mathbb{F}_q^{*2}$ est l'ensemble des carrés de $\mathbb{F}_q$: $\{x \in \mathbb{F}_q / \exists a \in \mathbb{F}_q\ x = a^2\}$
$\mathbb{F}_q^{*2}$ est l'ensemble des carrés de $\mathbb{F}_q^*$: $\{x \in \mathbb{F}_q^* / \exists a \in \mathbb{F}_q^*\ x = a^2\}$

Ex 20 : Les carrés de $\mathbb{F}_7^*$ sont 1, 2 et 4

[NH2G2] [Perrin]

Prop 21 : $\mathbb{F}_q^*$ et $\mathbb{F}_q^{*2}$ sont des groupes cycliques

Rmq 22 : En pratique, il n'est pas facile de trouver un générateur de ces groupes

Ex 23 : 2 est un générateur de $(\mathbb{Z}/11\mathbb{Z})^*$
$\overline{x}$ est un générateur de $(\mathbb{F}_4)^*$
a est un générateur de $(\mathbb{Z}/11\mathbb{Z})^{*2}$

Prop 24 : Pour $p > 2$, x est un carré dans $\mathbb{F}_q^* \Leftrightarrow x^{\frac{q-1}{2}} = 1$

Corollaire 25 : -1 est un carré dans $\mathbb{F}_q \Leftrightarrow q \equiv 1\ [4]$

Application 26 : Théorème des deux carrés (cas p premier)

Application 27 : Classification des formes quadratiques sur $\mathbb{F}_q$ par le discriminant

Def 28 : Le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut $\begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p \\ 0 & \text{si } a = 0 \\ -1 & \text{sinon} \end{cases}$

Ex 29 : $\left(\frac{-1}{3}\right) = -1$ et $\left(\frac{2}{3}\right) = 1$

Prop 30 : pour a, b entiers on a $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}\ [p]$; $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
$\left(\frac{-1}{p}\right) = 1$ ssi $p \equiv 1\ [4]$ $\quad \left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1\ [3] \\ -1 & \text{si } p \equiv 2\ [3] \end{cases}$

Thm 31 : Loi de réciprocité quadratique
Soient p, q premiers impairs distincts, on a $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

[Perrin] [Dan] [Dem]

II Irréductibilité des polynômes sur $\mathbb{F}_q[X]$

La connaissance d'un polynôme irréductible de degré n sur $\mathbb{F}_p$ valide la construction alternative de $\mathbb{F}_q$ proposée en 12

a) Critère d'irréductibilité

Prop 32 : Soit $P \in \mathbb{F}_q[X]$ de degré n. P est irréductible sur $\mathbb{F}_q$ si et seulement si P n'a pas de racine dans les extensions de $\mathbb{F}_q$ de degré inférieur ou égal à $n/2$

Ex 33 : Pour montrer que X^4+X+1 est irréductible sur $\mathbb{F}_2$, il suffit de montrer qu'il n'a pas de racine dans $\mathbb{F}_2$ ni $\mathbb{F}_4$

Prop 34 : Soit $P \in \mathbb{F}_q[X]$ irréductible de degré n, soit K une extension de degré m avec $\mathrm{pgcd}(m, n) = 1$. Alors P est irréductible sur K

Ex 35 : X^3+X+1 n'a pas de racines dans $\mathbb{F}_2$, donc est irréductible sur $\mathbb{F}_{2^n}$ si $3 \nmid n$. Par contre il est réductible sur $\mathbb{F}_8$.

Prop 36 : (critère d'Eisenstein) Soit $P = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$, on suppose qu'il existe p premier tel que
(i) $\forall 0 \le k \le n-1$ $p \mid a_k$ (ii) $p \nmid a_n$ (iii) $p^2 \nmid a_0$
Alors P est irréductible dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$

Ex 37 : $P(X) = X^4+1$ est irréductible car $P(X+1)$ l'est avec $p = 2$

Prop 38 : Soit $P \in \mathbb{Z}[X]$, soit p premier, on pose $\overline{P}$ la réduction de P dans $\mathbb{F}_p[X]$, on suppose que $\overline{a_n} \neq 0$. Alors, si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, on a P irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$

Ex 39 : $P(X) = X^3+4X^2-5X+7 = X^3+X+1\ [2]$ irréductible sur $\mathbb{F}_2$
Donc P est irréductible sur $\mathbb{Z}$

Réciproque fausse 40 : X^4+1 est réductible sur tous les $\mathbb{F}_p$ mais irréductible sur $\mathbb{Z}$.

[Gou] [Perrin]

2) Les polynômes cyclotomiques

Intérêt 41 : étude des irréductibles de $X^N - 1$ sur $\mathbb{F}_q$
On fixe N et $q = p^n$, tels que $\mathrm{pgcd}(N, p) = 1$

Def 42 : On considère $K_{N,p}$ le corps de décomposition de $X^N - 1$ sur $\mathbb{F}_p$. On pose $\Phi_N(X) = \prod_{\omega \in \mu_N^*(K_{N,p})} (X - \omega)$
où $\mu_N^*(K_{N,p})$ est l'ensemble des racines primitives $N^{ième}$ de l'unité sur $K_{N,p}$
ce sont les polynômes cyclotomiques

Ex 43 : $\Phi_2, \mathbb{F}_3(X) = X+1$ car $\mu_2^*(K_{2,3}) = \{-1\}$

Prop 44 : On a $X^N - 1 = \prod_{d \mid N} \Phi_{d,p}(X)$

Utilisation 45 : On peut calculer les polynômes cyclotomiques récursivement grâce à cette propriété voir annexe.

Prop 46 : On suppose $\mathrm{pgcd}(N, q) = 1$ ($\Leftrightarrow p \nmid N$). Soit r l'ordre de q dans le groupe $(\mathbb{Z}/N\mathbb{Z})^*$. Alors $\Phi_{N,p}$ se décompose dans $\mathbb{F}_q[X]$ en produit de polynômes irréductibles, de degré r, tous différents.

[Perrin] [Peyr]

[Dem]

3) Déterminer automatiquement si un polyn est irréductible

Alg. 47: Algorithme de Berlekamp
Cet algorithme permet de trouver la décomposition en facteurs irréductibles d'un polynôme sur $\mathbb{F}_q$.

DEV 2 Max

III Applications au monde réel

1) Trouver des nombres premiers très très grands

Def 48: Un nombre de Mersenne s'écrit 2^q-1 pour q premier impair, on le note M_q.

Thm 49: M_q premier $\iff (2+\sqrt{3})^{2^{q-1}} \equiv -1 \ [M_q]$

DEV 2 Pierre

[Sau]

Algo 50: Test de Lehmer-Lucas
Soit $(L_n)_{n\geq 0}$ la suite de $\mathbb{Z}/n\mathbb{Z}$ définie par $L_0 = 4$ et $L_{n+1} = L_n^2 - 2 \ [M_q]$

Alors M_q premier $\iff L_{q-2} \equiv 0 \ [M_q]$

Appli 51: → Système RSA.
→ Donne le plus grand nombre premier qu'on connaisse

2) Transformée de Fourier Rapide (TFR)

[Dem] [Peyr]

Def 52: (Transformée de Fourier Discrète TFD) Soit $N \in \mathbb{N}^*$
Pour ω une racine $N^{ième}$ primitive de l'unité dans $\mathbb{F}_q$
on pose $\mathcal{F}$: $(\mathbb{F}_q)^N \to (\mathbb{F}_q)^N$, $(a_i)_1^N \mapsto \left(\sum_{k=0}^{N-1} a_k \omega^{-kj}\right)_{j=1}^N$ la TFD

et $\overline{\mathcal{F}}$: $(\mathbb{F}_q)^N \to (\mathbb{F}_q)^N$, $(a_j)_1^N \mapsto \left(\sum_{k=0}^{N-1} a_k \omega^{kj}\right)_{j=1}^N$ la TFD inverse

Prop 53: On a $\mathcal{F}(\overline{\mathcal{F}}(a)) = Na$ et $\overline{\mathcal{F}}(\mathcal{F}(a)) = Na \quad \forall a \in (\mathbb{F}_q)^N$

Prop 54: (Convolution) $\mathcal{F}(a*b) = \mathcal{F}(a).\mathcal{F}(b)$ et $\overline{\mathcal{F}}(a*b) = \overline{\mathcal{F}}(a).\overline{\mathcal{F}}(b)$
avec $a.b$ le produit terme à terme de a et b $(a,b \in (\mathbb{F}_q)^N)$

Prop 55: (TFR) Etant donnée une racine primitive $N^{ième}$ de l'unité dans $\mathbb{F}_q$, on peut calculer récursivement la TFD en $\mathcal{O}(N \log N)$

Appli 56: Multiplication des grands polynômes/grand entiers en $\mathcal{O}(N \log N)$ (schéma en annexe)

3) Codes correcteurs

Def 57: Un code linéaire C de taille N et de dimension m est un sous espace vectoriel de dimension m de $(\mathbb{F}_q)^N$.

Def 58: Un code linéaire est cyclique s'il est stable par décalage circulaire (i.e. si $a_0 \dots a_{n-1} \in C$ alors $a_{n-1} a_0 a_1 \dots a_{n-2} \in C$)

On peut le voir comme multiplication par X via l'isomorphisme $(\mathbb{F}_q)^N \xrightarrow{\sim} \mathbb{F}_q[X]/(X^N-1)$, $(a_i)_0^{N-1} \mapsto \sum_{i=0}^{N-1} a_i X^i$, ainsi C est stable par multiplication par tout polynôme donc c'est un idéal de $\mathbb{F}_q[X]/(X^N-1)$, il est isomorphe à un idéal (principal) de $\mathbb{F}_q[X]$ contenant X^N-1 (par la correspondance des idéaux)

Donc un code cyclique est engendré par un unique facteur irréductible P de X^N-1 sur $\mathbb{F}_q$.

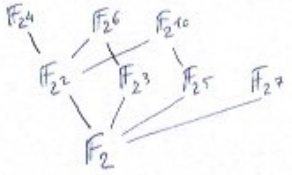
Ex 59: Les codes BCH utilisent la cyclotomie pour générer des codes de distance minimale fixée. Leur décodage s'effectue efficacement par TFR.

[Dem] [Peyr] [Sau]

Annexe 1: table de $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(1+X+X^2)$ multiplicative

	0	1	$\bar{x}$	$1+\bar{x}$
0	0	0	0	0
1	0	1	$\bar{x}$	$1+\bar{x}$
$\bar{x}$	0	$\bar{x}$	$1+\bar{x}$	1
$1+\bar{x}$	0	$1+\bar{x}$	1	$\bar{x}$

Annexe 2: Diagramme des inclusions des $\mathbb{F}_{2^k}$



Annexe 4: $N = 2^n$ $N \geq \deg P + \deg Q + 1$

$(P,Q) \in \mathbb{F}_q^N \times \mathbb{F}_q^N \xrightarrow{TRR_\omega} (\mathcal{F}P, \mathcal{F}Q) \in \mathbb{F}_q^N \times \mathbb{F}_q^N$

$\mathcal{O}(N)$ | produit terme à terme

$(P \times Q) \in \mathbb{F}_q^N \xleftarrow{TFR_{\omega^{-1}}} \mathcal{F}P.\mathcal{F}Q = \mathcal{F}(P \times Q)$ $\quad \mathcal{O}(N \log N)$

Annexe 3: pour $p = 11$

n	$\Phi_{n,p}(X)$
1	$X-1$
2	$X+1$
3	X^2+X+1
4	X^2+1
5	$X^4+X^3+X^2+X+1$
6	X^2-X+1
7	$X^6+X^5+X^4+X^3+X^2+X+1$
8	X^4+1

Références:

[Per] Daniel Perrin, Cours d'algèbre

[Peyr] Gabriel Peyré, L'algèbre discrète de la transformée de Fourier

[Sau] Sam Ricart-Ramon, Cours de Calcul formel, corps finis systèmes polynomiaux applications

[NH2G2] Caldero-Germoni NH2G2 Tome 2

[Dem] Michel Demazure, Cours d'algèbre

[Gou] Xavier Gourdon, Algèbre

126 Exemples d'équations en arithmétiques

[Gourdon Algèbre] [Lamarche Arithmétique p. 336] [Lamartin modulaire p163] [Hindry p. 81] [Lamartin algébrique] [Landreau Rédaction]

Idée: Résoudre des équations sur $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$

I Equations linéaires et arithmétique

1) Equations diophantiennes linéaires (sur $\mathbb{Z}$)

Def 1: Soient $a, b \in \mathbb{Z}$, on dit que a divise b s'il existe $n \in \mathbb{Z}$ tel que $b = an$. On note $a \mid b$ (dans le cas contraire $a \nmid b$)

Prop 2: Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < b$

Def 3: Soient $a_1, \dots, a_n \in \mathbb{Z}$. Il existe un unique $d \in \mathbb{N}$ tel que $a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$, on appelle d le pgcd de $a_1 \dots a_n$. On note $\text{pgcd}(a_1, \dots, a_n)$

Def 4: Si $\text{pgcd}(a_1 \dots a_n) = 1$ on dit que les a_i sont premiers entre eux

Thm 5: Des entiers $a_1, \dots, a_n$ ont leur ensemble ssi il existe des entiers $u_1 \dots u_n$ tels que $\sum_{i=1}^{n} a_i u_i = 1$

Ex 6: 12 et 35 sont premiers entre eux et $3 \times 12 - 35 = 1$

Rmq 7: L'algorithme d'Euclide qui utilise des divisions euclidiennes (Prop 2), successives permet de trouver le pgcd de deux nbrs et les coefficients de Bézout (Thm 5)

Prop 8: L'équation diophantienne linéaire $ax + by = c$ admet une solution ssi $\text{pgcd}(a, b) \mid c$

Méthode 9: Pour trouver les solutions on divise a et b par $d = \text{pgcd}(a, b)$, on a $au + bv = 1$ (Bézout) puis $auc' + bvc' = c'$, on a une solution particulière puisque $aX + bY = 0$ admet comme solution $-bk, ak$ on a finalement $uc' - bk$ et $vc' + ak$, $k \in \mathbb{Z}$ comme ensemble de solutions. $c' = c/\text{pgcd}(a,b)$.

Ex 10: $35x + 11y = 149$ admet comme solutions $x = -745 + 11k$ $y = 2384 - 35k$ $k \in \mathbb{Z}$

$6x + 15y = 56$ n'a pas de solution.

Thm 11: Soit $A \in \mathcal{M}_{n,m}(\mathbb{Z})$ $n, m \geq 0$. Le système $AX = 0$ admet une solution dans $\mathbb{N}^m$ ssi $0_{\mathbb{R}^n} \in \text{Conv}(A_1, \dots A_m)$ où A_i sont les colonnes de A. DEV

2) Equations linéaires aux congruences (sur $\mathbb{Z}/n\mathbb{Z}$)

Def 12: On appelle équation linéaire aux congruences une équation du type $ax \equiv b\ [p]$ où x est l'inconnue et a, b, p sont des entiers connus

Thm 13: $ax \equiv 1\ [n]$ admet une solution $a, n \geq 2$ ssi a et n sont premiers entre eux.

Ex 14: $3x \equiv 1\ [4]$ admet pour solution $x \equiv 3\ [4]$

$6x \equiv 1\ [9]$ n'admet pas de solution.

Thm 15 (chinois des restes): Soient $m_1, \dots m_r$ strictement positifs et premiers entre eux 2 à 2. Alors $\begin{cases} x \equiv a_1\ [m_1] \\ \vdots \\ x \equiv a_r\ [m_r] \end{cases}$ admet une unique solution x modulo $M = \prod_{i=1}^{r} m_i$

qui est $x \equiv a_1 M_1 y_1 + \dots + a_r M_r y_r$

$M_i = M/m_i$ $\quad y_i \Pi_i \equiv 1\ [m_i]$

Ex 16: $x \equiv 1\ [2]$, $x \equiv 2\ [3]$, $x \equiv 4\ [5]$ a pour solution $x \equiv 29\ [30]$

II Méthodes plus poussées

1) Réduction modulaire

Thm 17: Si une équation linéaire admet une solution sur $\mathbb{Z}$, alors en plongeant dans les coefficients dans $\mathbb{Z}/n\mathbb{Z}$, l'équation a une solution dans $\mathbb{Z}/n\mathbb{Z}$ $\forall n \in \mathbb{Z}$

Appli 18: Si une équation (E) n'a pas de solution dans $\mathbb{Z}/n\mathbb{Z}$, alors elle n'en a pas dans $\mathbb{Z}$.

Ex 19: $3x + 6y = 5$ n'a pas de solution car modulo 3 on a $0 \neq 2$

2) Utilisation de l'analyse

Idée 20: Pour certaines équations (E), on peut les résoudre sur $\mathbb{R}$ explicitement, si aucune solution n'est entière alors l'équation (E) n'admet pas de solution sur $\mathbb{Z}$.

Ex 21: $x^2 + 3x = 4$ n'admet pas de solution car les solutions sont $\frac{-3 \pm \sqrt{17}}{2}$.

solution de $ax^2 + bx = c$ [FGN/Alg 1]

III L'équation de Fermat

But 22: Résoudre $x^n + y^n = z^n$

Def 23: On dit que $(a, b, c) \in \mathbb{Z}^3$ est un triplet pythagoricien si $a^2 + b^2 = c^2$. Si a, b, c sont premiers entre eux, on dit que le triplet est irréductible

Ex 24: $(6, 8, 10)$ est un triplet pythagoricien

$(5, 12, 13)$ est un triplet pythagoricien irréductible

Thm 25: Si m et n sont deux entiers premiers entre eux et de parité distinctes, alors $(2mn, m^2 - n^2, m^2 + n^2)$ est pythagoricien

Réciproquement, tout triplet pythagoricien irréductible (a, b, c) peut être décrit sous la forme $a = m^2 - n^2$ $b = 2mn$ $c = m^2 + n^2$

Ex 26: pour $(5, 12, 13)$ on a $m = 3$ et $n = 2$

Principe 27: "Descente infinie" de Fermat

si (x, y, z) vérifie $x^4 + y^4 = z^2$ avec $xyz \neq 0$ alors il existe (x_1, y_1, z_1) une autre solution avec $0 < z_1 < z$

ABSURDE car les suites décroissantes de $\mathbb{N}$ stationnent [Lamartin algébrique]

Thm 28: L'équation $x^4 + y^4 = z^2$ n'a pas de solutions entières avec $xyz \neq 0$

Corollaire 29: L'équation $x^4 + y^4 = z^n$ n'a pas de solutions entières avec $xyz \neq 0$.

Thm 30 (Fermat, Wiles) (admis): pour tout $n \geq 3$ l'équation $x^n + y^n = z^n$ n'a pas de solution entières avec $xyz \neq 0$

Thm 31 (Fermat modulaire): pour tout $n \in \mathbb{N}^*$, il existe un rang n tel que pour tout p premier supérieur à n $x^n + y^n = z^n$ a une solution non triviale dans $\mathbb{Z}/p\mathbb{Z}$ DEV

IV Les carrés de $\mathbb{F}_p$

But 32: Résoudre $x^2 + py = a$

Prop 33: Soit $\mathbb{K}$ un corps de cardinal fini.
Alors la caractéristique de $\mathbb{K}$ est un nbr premier p
(générateur du noyau de $\mathbb{Z} \to \mathbb{K}$, $n \mapsto \underbrace{1+\dots+1}_{n \text{ fois}}$)

Prop 34: Un corps fini est de cardinal une puissance d'un nombre premier.

Prop 35: Si p est un nombre premier, $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$

Question 36: quels sont les carrés de $\mathbb{F}_p$? (pour p premier impair)

Prop 37: Si p premier impair, on a
x est un carré de $\mathbb{F}_p^\times$ ssi $x^{\frac{p-1}{2}} = 1$

Def 38: On définit le symbole de Legendre pour $a \in \mathbb{Z}$ et p premier comme
$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \text{ est divisible par } p \\ 1 \text{ si } a \text{ est un carré de } \mathbb{F}_p \\ -1 \text{ sinon} \end{cases}$$

Corollaire 39: $\left(\frac{a}{p}\right) = 1$ ssi $a^{\frac{p-1}{2}} = 1$

Prop 40: $\left(\frac{-1}{p}\right) = 1$ ssi $p \equiv 1 [4]$

Corollaire 41: un nombre premier p est somme de 2 carrés ssi $p = 2$ ou $p \equiv 1 [4]$.

Prop 42: pour tout a, b entiers, p premier on a
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \; ; \; \left(\frac{1}{p}\right) = 1 \; ; \; \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Thm 43: Loi de Réciprocité quadratique
Si p, q premiers distincts impairs, on a
$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)}{4}\frac{(q-1)}{4}}$$

DEV 2

[Perrin] [Samuel Liret]

II Théorie algébrique des nombres

But 44: Résoudre $x^2 - d y^2 = \pm 1$ (Pells Fermat)

Def 45: Un corps de nombre est une extension finie sur $\mathbb{Q}$

Ex 46: $\mathbb{Q}(\sqrt{2})$ est un corps de nombre
$\mathbb{Q}(\pi e)$ ne l'est pas.

Def 47: Un corps quadratique est un corps de nombre de degré 2.

Ex 48: $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$ est un corps quadratique

Prop 49: Un corps quadratique K peut toujours s'écrire comme $\mathbb{Q}(\sqrt{d})$ où d n'a pas de facteurs carrés ($d \in \mathbb{Z}$)

Def 50: Un anneau d'entiers d'un corps de nombres K sont les éléments de K qui sont solution d'un polynôme unitaire à coefficients entiers. On le note $\mathcal{O}_K$

Ex 51: $\phi = \frac{1+\sqrt{5}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ car $\phi^2 - \phi - 1 = 0$ et $\phi \in \mathbb{Q}(\sqrt{5})$

Thm 52: Si $d \in \mathbb{Z}$ sans facteurs carrés
si $d \neq 1 [4]$ $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$
si $d \equiv 1 [4]$ $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

Def 53: On définit $N(a + b\sqrt{d}) = a^2 - db^2$
pour $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$

Ex 54: $N(1 + 2\sqrt{3}) = 1 - 3 \times 4 = -11$
$N(2 - \sqrt{-5}) = 4 + 5 \times 1 = 9$

Prop 55: Les inversibles de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ sont les éléments $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ tels que $N(\alpha) = \pm 1$

Thm 56 (admis): Si $d > 0$ sans carré, il existe $(x_n, y_n) \in \mathbb{N}^* \times \mathbb{N}^*$ à l'équation $x^2 - dy^2 = \pm 1$ telle que toutes solutions $x_n + \sqrt{d} y_n$ s'écrivent $\pm(x_1 + \sqrt{d} y_1)^n$.

[Strent Tall] p63

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

I Polynômes irréductibles — $\mathbb{K}$ un corps

1) Définitions

Déf 1 : Soit A un anneau commutatif unitaire. On appelle polynôme à une indéterminée à coefficients dans A toute suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A tous nuls à partir d'un certain rang

Rmq 2 : Soit P un polynôme sur A, on le représente de la manière suivante : $P(X) = \sum_{i=0}^{n} a_i X^i$ où $n+1$ est le rang à partir duquel $(a_i)_{i\geq n+1}$ est nulle. On appelle n son degré.

Ex 3 : $P(X) = X^2 + 3X + 1$ est un polynôme de degré 2 sur $\mathbb{Z}$.
$P(X) = X^3 + \sqrt{2}X - \pi$ est un polynôme de degré 3 sur $\mathbb{R}$

Prop 4 : Si $A = \mathbb{K}$ un corps. Alors l'ensemble des polynômes sur $\mathbb{K}$ noté $\mathbb{K}[X]$ a une structure d'anneau euclidien.

Thm 5 : Soit $A, B \in \mathbb{K}[X]$, $B \neq 0$
Alors il existe un unique couple $(Q,R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$

Corollaire 6 : $\mathbb{K}[X]$ est principal.

Ex 7 : $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ sont principaux

Ex 8 : $\mathbb{Z}[X]$ ne l'est pas car $\langle 2, X\rangle$ n'est pas monogène

Rmq 9 : $\mathbb{K}[X]$ a la même structure que les entiers de $\mathbb{Z}$

Déf 10 : Soient $P, Q \in \mathbb{K}[X]$, on dit que P divise Q noté $P \mid Q$ si il existe un polynôme $R \in \mathbb{K}[X]$ tel que $RP = Q$.

Ex 11 : $X+1 \mid X^2 - 1$ car $(X+1)(X-1) = X^2 - 1$

Déf 12 : Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible dans $\mathbb{K}[X]$ si P n'est pas constant et si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les constantes non nulles et les polynômes associés à P.

Ex 13 : $X - 3$ est irréductible sur $\mathbb{Q}$.

Thm 14 : Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Alors P se décompose de manière unique à l'ordre près sous la forme $P = \lambda P_1^{a_1} \dots P_k^{a_k}$ où $\lambda \in \mathbb{K}^\times$, $a_i \in \mathbb{N}^*$ et P_i sont distincts, unitaires et irréductibles sur $\mathbb{K}$.

Ex 15 : $X^4 - 1 = (X^2+1)(X+1)(X-1)$ sur $\mathbb{Q}$

2) Critère d'irréductibilité

Thm 16 : (Eisenstein) Soit A un anneau factoriel et $K = Fr(A)$. Soit $P = \sum_{i=0}^{n} a_i X^i$ avec $a_i \in A$
Soit $p \in A$ irréductible. Si :
(i) $p \nmid a_n$ (ii) $p \mid a_i$ $\forall i \in \{0, \dots, n-1\}$ (iii) $p^2 \nmid a_0$
Alors P est irréductible dans $K[X]$

Ex 17 : $X^4 + 3X^2 - 6X + 3$ est irréductible sur $\mathbb{Q}$ avec $p=3$

Thm 18 : (réduction modulaire) Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$
Soit p premier. On note $\overline{P}$ la réduction de P modulo p
on impose que $\overline{a_n} \neq 0$
Alors si $\overline{P}$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$, alors P est irréductible sur $\mathbb{Q}$ (et sur $\mathbb{Z}$ si polynôme unitaire)

Ex 19 : $X^2 + 3X + 1$ est irréductible sur $\mathbb{Q}$ car X^2+1 l'est sur $\mathbb{Z}/3\mathbb{Z}$

Réciproque fausse 20 : $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais réductible sur tout $\mathbb{Z}/p\mathbb{Z}$.

Prop 21 : Un polynôme P de degré inférieur à 3 est irréductible sur $\mathbb{K}$ ssi P n'a pas de racines dans $\mathbb{K}$

Ex 22 : $X^2 - 3$ est irréductible sur $\mathbb{Q}$

Contre exemple 23 : $X^4 + 1$ n'a pas de racine dans $\mathbb{R}$ mais $X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$

II Extensions de corps

1) Cadre

Déf 24 : Soit $\mathbb{K}$ un corps, on appelle extension de $\mathbb{K}$ tout corps $\mathbb{L}$ contenant un sous corps isomorphe à $\mathbb{K}$.

Prop 25 : Soit $\mathbb{L}/\mathbb{K}$ une extension de $\mathbb{K}$, $\mathbb{L}$ a une structure d'espace vectoriel sur $\mathbb{K}$

Ex 26 : La plus petite extension de $\mathbb{Q}$ contenant $\sqrt{2}$ noté $\mathbb{Q}(\sqrt{2})$ est un $\mathbb{Q}$-ev de dimension 2 sur $\mathbb{Q}$: $\mathbb{Q}(\sqrt{2}) = \{a + \sqrt{2}b, a, b \in \mathbb{Q}\}$

Déf 27 : La dimension de cet espace vectoriel est appelé degré de l'extension $\mathbb{L}/\mathbb{K}$ (il peut être fini ou infini) noté $[\mathbb{L} : \mathbb{K}]$

Ex 28 : $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

Thm 29 : (Base télescopique). Quelles que soient les extensions de corps $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$, on a
$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$

Ex 30 : $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$
d'où $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

$[\mathbb{Q}(\pi, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\pi, \sqrt{2}) : \mathbb{Q}(\pi)][\mathbb{Q}(\pi) : \mathbb{Q}]$
d'où $[\mathbb{Q}(\pi, \sqrt{2}) : \mathbb{Q}] = \infty$ car $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$

Appli 31 : Construction à la règle et au compas

2) Corps de rupture, corps de décomposition

Déf 32 : Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ irréductible.
L'extension $\mathbb{L}/\mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ si $\mathbb{L}$ possède une racine de P et pour tout autre corps $\mathbb{M}$ qui contient une racine de P alors $\mathbb{M}$ est une extension de $\mathbb{L}$.

Ex 33 : $\mathbb{C}$ peut être vu comme corps de rupture de X^2+1 sur $\mathbb{R}$.

Appli 34 : Critère de primalité des nombres de Mersenne
n_q premier $\Leftrightarrow (2+\sqrt{3})^{q-1} \equiv -1 \ [n_q]$

DEV 1

Thm 35 : Soit $P \in \mathbb{K}[X]$ irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme près.

Ex 36 : $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[X]/(X^2-2)$

Déf 37 : Soit $P \in \mathbb{K}[X]$. On appelle corps de décomposition de P sur $\mathbb{K}$ une extension $\mathbb{L}$ de $\mathbb{K}$ qui vérifie :
- P est produit de facteurs de degré 1 dans $\mathbb{L}[X]$
- Si $\mathbb{M}$ vérifie cela, alors $\mathbb{M}$ est une extension de $\mathbb{L}$.

Rmq 38 : P n'est pas forcément irréductible

Ex 39 : $\mathbb{Q}$ est un corps de décomposition de X^4+1 sur $\mathbb{R}$

Thm 40 : Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près. On le note $D_{\mathbb{K}}(P)$.

Ex 41 : $D_{\mathbb{Q}}(X^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, i)$

III Théorie algébrique des nombres

1) Extensions algébriques

Def 42 : Soit $\alpha \in \mathbb{L}/\mathbb{K}$, α est dit algébrique sur $\mathbb{K}$ s'il existe un polynôme P sur $\mathbb{K}$, tel que $P(\alpha)=0$
Dans le cas contraire on dit que α est transcendant sur $\mathbb{K}$

Ex 43 : $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ car X^2-2 annule $\sqrt{2}$
i est algébrique sur $\mathbb{Q}$ car x^2+1 annule i
π est transcendant sur $\mathbb{Q}$ (admis)

Thm 44 : Soit α algébrique sur $\mathbb{K}$, il existe un unique polynôme P annulateur de α, unitaire, irréductible sur $\mathbb{K}$ tel que $\mathbb{K}(\alpha) = \mathbb{K}[X]/(P)$
De plus on a $[\mathbb{K}(\alpha):\mathbb{K}] =$ degré de P
P est le polynôme minimal de α sur $\mathbb{K}$.

Rmq 45 : $\mathbb{K}(\alpha)$ est le corps de rupture de P sur $\mathbb{K}$.

Def 46 : Une extension $\mathbb{L}/\mathbb{K}$ est algébrique sur $\mathbb{K}$, si tout élément de $\mathbb{L}/\mathbb{K}$ est algébrique sur $\mathbb{K}$.

Thm 47 : Toute extension $\mathbb{L}/\mathbb{K}$ de degré fini est algébrique sur $\mathbb{K}$

Ex 48 : $\mathbb{Q}(\sqrt{2})$ est algébrique car $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$
$\mathbb{Q}\left(\left(e^{i\frac{2\pi}{n}}\right)_{n\in\mathbb{N}}\right)$ est algébrique mais n'est pas de degré fini

Def 49 : Un corps $\mathbb{K}$ est dit algébriquement clos si tout polynôme non constant de $\mathbb{K}[X]$ a au moins une racine dans $\mathbb{K}$.

Thm 50 : Le corps $\mathbb{C}$ est algébriquement clos

Rmq 51 : Tout polynôme sur $\mathbb{C}$ est produit de facteurs de degré 1.

Def 52 : On appelle clôture algébrique d'un corps $\mathbb{K}$, toute extension $\mathbb{L}$ de $\mathbb{K}$ telle que
(i) $\mathbb{L}$ est algébrique sur $\mathbb{K}$
(ii) $\mathbb{L}$ est un corps algébriquement clos.

Ex 53 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ mais pas de $\mathbb{Q}$

2) Corps de nombre et corps cyclotomiques

Def 54 : Un corps de nombres est une extension $\mathbb{K}$ de $\mathbb{Q}$ de degré fini.

Ex 55 : $\mathbb{Q}(\sqrt{2})$ est un corps de nombre ($\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt[3]{2})$ aussi)

Def 56 : Un corps quadratique est un corps de nombre de degré 2

Prop 57 : Tout corps quadratique s'écrit $\mathbb{Q}(\sqrt{d})$ avec d sans facteur carré.

Ex 58 : $\mathbb{Q}(\sqrt{3})$ est un corps quadratique

Def 59 : Pour ω_n une racine primitive $n^{ième}$ de l'unité on dit que $\mathbb{Q}(\omega_n)$ est une extension cyclotomique de $\mathbb{Q}$

Prop 60 : $[\mathbb{Q}(\omega_n):\mathbb{Q}] = \varphi(n)$ avec φ l'indicatrice d'Euler

Ex 61 : $[\mathbb{Q}(e^{i\frac{2\pi}{5}}):\mathbb{Q}] = 4$ car $\varphi(5)=4$

Def 62 : Le polynôme $\Phi_n(X) = \prod_{\omega\in\Omega_n}(X-\omega)$ où Ω_n est l'ensemble des racines primitives $n^{ième}$ de l'unité
est appelé $n^{ième}$ polynôme cyclotomique

Thm 63 : Pour tout n, les polynômes Φ_n sont irréductibles sur $\mathbb{Q}$ DEV2

Ex 64 : $\Phi_1(X) = X-1$ $\Phi_2(X) = X+1$ $\Phi_3(X) = X^2+X+1$
$\Phi_4(X) = X^2+1$ $\Phi_5(X) = X^4+X^3+X^2+X+1$

Prop 65 : Pour p premier, $\Phi_p(X) = X^{p-1}+X^{p-2}+\dots+X+1$

Déterminant. Exemples et applications

152

Cadre : E un $\mathbb{K}$ espace vectoriel de dimension finie
$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$

(I) L'application déterminant

1) Formes n-linéaires alternées

Def 1 : $f : E_1 \times \dots \times E_n \to \mathbb{K}$ est forme n-linéaire si elle est linéaire selon chacune de ses variables.

Ex 2 : Si $\varphi_i \in E^*$ $\forall i$ $\Phi : (x_1, \dots, x_n) \mapsto \prod_{i=1}^{n} \varphi_i(x_i)$ $E^n \to \mathbb{K}$ est n-linéaire

Def 3 : Soit f une forme n-linéaire sur E (abus pour E^n)
f est alterné si $f(x_1, \dots, x_p) = 0$ dès que deux vecteurs parmi les x_i sont égaux
f est antisymétrique si l'échange de deux vecteurs dans $(x_1, \dots, x_p)$ change le signe de f.

Prop 4 : f antisymétrique $\iff$ f alterné

Thm 5 : L'ensemble des formes n-linéaires alternés sur E est un $\mathbb{K}$ ev de dimension 1. De plus, il existe une et une seule forme n-linéaire alternée prenant la valeur 1 sur une base donnée de E.

Def 6 : Soit $\mathcal{B} = (e_1, \dots, e_n)$ base de E, on appelle déterminant dans la base $\mathcal{B}$ la seule forme n-linéaire alternée valant 1 sur $(e_1, \dots, e_n)$
$$\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\, x_{1,\sigma(1)} x_{2,\sigma(2)} \dots x_{n,\sigma(n)}$$

Thm 7 : Soient $x_1, \dots, x_n \in E$. Il y a équivalence entre
(i) les vecteurs $x_1, \dots, x_n$ sont liés
(ii) Pour toute base $\mathcal{B}$ de E, $\det_{\mathcal{B}}(x_1, \dots, x_n) = 0$
(iii) il existe $\mathcal{B}$ telle que $\det_{\mathcal{B}}(x_1, \dots, x_n) = 0$

Def 8 : Soit $A \in \mathcal{M}_n(\mathbb{K})$, on appelle déterminant de A le déterminant des vecteurs colonnes de A dans la base canonique on l'écrit $\det(A) = \begin{vmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{vmatrix}$

Prop 9 : Soient $A, B \in \mathcal{M}_n(\mathbb{K})$ $\det(AB) = \det(A)\det(B)$
$\det(A) = \det({}^tA)$ $\det(A^{-1}) = \det(A)^{-1}$ si $A \in GL_n(\mathbb{K})$

2) Regularité du déterminant

Prop 10 : L'application $\det_n(\mathbb{R}) \to \mathbb{R}$, $A \mapsto \det(A)$ est C^∞ et $d\det(A) \cdot H = \mathrm{Tr}({}^t\mathrm{Com}(X)H)$ (on introduira la comatrice plus tard)

Application 11 : Par la continuité du déterminant, $GL_n(\mathbb{K})$ est ouvert

(II) Calcul du déterminant

Prop 12 : Si A est diagonale, $A = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$
$\det(A) = \prod_{i=1}^{n} \lambda_i$

Prop 13 : Si A est triangulaire, alors
$\det(A) = \prod_{i=1}^{n} a_{ii}$ où (a_{ij}) coefficient de A

Prop 14 : on ne change pas le déterminant d'une matrice A en ajoutant à une colonne une combinaison linéaire des autres colonnes

Prop 15 : Si $M = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$ matrice par blocs
$\det M = \det(A)\det B$

Def 16 : Soit $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{K})$
$\forall i, j \in \{1, \dots, n\}$ on appelle mineur de a_{ij} noté Δ_{ij} le déterminant de la matrice extraite de A en supprimant la $i$ème ligne et la $j$ème colonne de A
On appelle $(-1)^{i+j}\Delta_{ij}$ le cofacteurs de a_{ij}

Ex 17 : $A = \begin{pmatrix} -1 & 2 & 0 \\ 4 & 3 & 1 \\ 5 & 6 & 1 \end{pmatrix}$ $\Delta_{1,2} = \begin{vmatrix} 4 & 1 \\ 5 & 1 \end{vmatrix}$

Prop 18 : Soit $A \in \mathcal{M}_n(\mathbb{K})$ (annexe)
Le développement selon la $j$ème colonne donne $\det(A) = \sum_{i=1}^{n} (-1)^{i+j} \Delta_{ij} a_{ij}$
le développement selon la $i$ème ligne donne $\det(A) = \sum_{j=1}^{n} (-1)^{i+j} \Delta_{ij} a_{ij}$

Def 19 : Soit $A \in \mathcal{M}_n(\mathbb{K})$
On appelle comatrice de A noté $\mathrm{com}(A)$ la matrice des cofacteurs

Prop 20 : Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ alors $\det(A) = ad - bc$

Ex 21 : $\det \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = 2 \times 1 - 1 \times 1 = 1$

Prop 22 (Règle de Sarrus) : Si $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$
$\det(A) = aei + dhc + gbf - ceg - ffha - bdi$

Ex 23 : Annexe

Prop 24 (Vandermonde) : Si $A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_0 & a_1 & & a_{n-1} \\ \vdots & \vdots & & \vdots \\ a_0^{n-1} & a_1^{n-1} & & a_{n-1}^{n-1} \end{pmatrix}$
Alors $\det(A) = \prod_{i<j} (a_i - a_j)$

Prop 25 (déterminant circulant)
Si $A = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 \\ a_1 & \dots & a_{n-1} & a_0 \end{pmatrix}$, on pose $P(X) = \sum_{i=0}^{n-1} a_i X^i$ et $\omega = e^{\frac{2i\pi}{n}}$
Alors $\det(A) = \prod_{i=0}^{n-1} P(\omega^i)$

Application 26 : Soit $z^{(0)} = (z_1, \dots, z_n) \in \mathbb{C}^n$
La suite définie par $z^{(k+1)} = \left(\frac{z_1^{(k)} + z_2^{(k)}}{2}, \dots, \frac{z_{n-1}^{(k)} + z_n^{(k)}}{2}, \frac{z_n^{(k)} + z_1^{(k)}}{2} \right)$
converge vers l'isobarycentre de $z^{(0)}$

AEV 1

(III) Déterminant en algèbre linéaire

Def 27 : Soit $A \in \mathcal{M}_n(\mathbb{K})$ on appelle polynôme caractéristique de A noté χ_A, le polynôme de $\mathbb{K}[X]$ défini par
$\chi_A(X) = \det(X I_n - A)$

Prop 28 : λ est valeur propre de A ssi $\chi_A(\lambda) = 0$

Prop 29 : Si χ_A est scindé sur $\mathbb{K}$ et a toutes ses racines simples alors A est diagonalisable.

Ex 30 : $A = \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix}$ est diagonalisable sur $\mathbb{R}$ et $\mathbb{C}$.
Car $\chi_A = (X-1)(X-3) - 8 = (X-5)(X+1)$

Prop 31 : Si A est nilpotente alors $\chi_A = X^n$

Prop 32 : Si $A = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & 0 & \vdots \\ & & 1 & -a_{n-1} \end{pmatrix}$ on note $P = X^n + \sum_{i=0}^{n-1} a_i X^i$
Alors $\chi_A = P$

Thm 33 (Cayley Hamilton): Soit $A \in \mathcal{M}_n(\mathbb{K})$
Alors $\chi_A(A) = 0$

IV Le déterminant dans d'autres domaines

1) Changement de variables

Def 34 (Jacobien) Soit $\varphi : \mathbb{R}^d \to \mathbb{R}^d \in \mathcal{C}^1$
on appelle Jacobien de φ en u noté $J_\varphi(u)$
$\det\left(\frac{\partial \varphi_i(u)}{\partial x_j}\right)_{\substack{1 \le i \le n \\ 1 \le j \le n}}$ où φ_i sont les composantes de φ

Thm 35 : Soit φ un $\mathcal{C}^1$ difféomorphisme entre deux ouverts Δ et D de $\mathbb{R}^d$
Si $f : D \to \mathbb{K}$ λ intégrable sur D
alors $(f \circ \varphi)\,|J_\varphi|$ est λ intégrable sur Δ
et $\int_D f(x)\,dx = \int_\Delta f \circ \varphi(u)\,|J_\varphi(u)|\,du$

Exo 36 : $\int_0^{+\infty}\int_0^{+\infty} \left(\frac{t}{\delta}\right)^x \frac{1}{t} e^{-(t+\delta)}\,dt\,d\delta = \int_0^{+\infty}\int_0^{+\infty} \frac{u^{x-1}}{(u+1)^{x+1}} e^{-v}\,du\,dv$

2) Inégalité d'Hadamard

Rappel 37 (Thm des extrema liés) Soit U ouvert de $\mathbb{R}^n$
Soient $f, g_1, \dots, g_{n-k} \in \mathcal{C}^1(U, \mathbb{R})$
$\Gamma = \{x \in U,\ g_i(x) = 0\ \forall i \in \{1, \dots, n-k\}\}$
Si $f_{|\Gamma}$ admet un extremum local en x_0 et que la famille $dg_i(x_0)$ est libre
Alors il existe $(\lambda_i)_i^{n-k} \in \mathbb{R}^{n-k}$, $df(x_0) = \sum_{i=1}^{n-k} \lambda_i\, dg_i(x_0)$

Prop 38 : Si $x_1, \dots, x_n \in \mathbb{R}^n$
$|\det(x_1, \dots, x_n)| \le \|x_1\| \|x_2\| \dots \|x_n\|$

A ≥ 2

3) Volume

Thm 39 : L'aire $\mathcal{A}(v, w)$ du parallélogramme engendré par v et w des vecteurs de $\mathbb{R}^2$ est égale à la valeur absolue de $\det(v, w)$
ie. $\mathcal{A}(v, w) = |\det(v, w)|$

Thm 40 : Soient $v_1, \dots, v_n$ n vecteurs de $\mathbb{R}^n$
le volume du parallélépipède engendré par $v_1 \dots v_n$, ie l'ensemble
$\{z \in \mathbb{R}^n,\ z = \sum_{i=1}^n \lambda_i v_i \quad 0 \le \lambda_i \le 1\}$
et $\mathrm{vol}(v_1 \dots v_n) = |\det(v_1, \dots, v_n)|$

Annexe :

Prop 18 :

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1k} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nk} & \cdots & a_{nn} \end{pmatrix}$$

$$\Delta_{1,k} = \begin{vmatrix} a_{21} & \cdots & a_{2,k-1} & a_{2,k+1} & \cdots & a_{2n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n,k-1} & a_{n,k+1} & \cdots & a_{nn} \end{vmatrix}$$

Prop 22 : $\det\begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 1 \\ 4 & 5 & 2 \end{pmatrix}$

$= 2 \times 3 \times 2 + 1 \times 5 \times 1 + 4 \times 1 \times 1$
$\quad - 1 \times 3 \times 4 - 1 \times 5 \times 2 - 2 \times 1 \times 1$
$= 12 + 5 + 4 - 12 - 10 - 2$
$= -3$

I Polynômes d'endomorphismes

$\mathbb{K}$ désigne un corps (souvent $\mathbb{R}$ ou $\mathbb{C}$)
E désigne un $\mathbb{K}$-espace vectoriel de dimension finie

Def 1 Soit $f \in \mathcal{L}(E)$. Pour tout polynôme $P \in \mathbb{K}[X]$ de la forme $P(X) = \sum_{k=0}^{m} a_k X^k$, le polynôme d'endomorphisme $P(f)$ est défini par
$$P(f) = \sum_{k=0}^{m} a_k f^k$$
De même pour $A \in \mathcal{M}_n(\mathbb{K})$, on a $P(A) = \sum_{k=0}^{m} a_k A^k$

Exemple 2: pour $P = X^2+X+1$ on a $P(f)(x) = f^2(x) + f(x) + x$
et on a $P(A) = A^2+A+I_n$

Remarque 3: Il ne faut pas confondre avec $P(f(x))$

Def 4: L'algèbre des polynômes en $f \in \mathcal{L}(E)$ est définie comme l'image de $\varphi_f : \mathbb{K}[X] \to \mathcal{L}(E)$, $P \mapsto P(f)$ (morphisme de $\mathbb{K}$-algèbres)
De même pour $A \in \mathcal{M}_n(\mathbb{K})$, on a $\varphi_A : \mathbb{K}[X] \to \mathcal{M}_n(\mathbb{K})$, $P \mapsto P(A)$

Def 5: Soit $f \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$. Un polynôme P est annulateur de f si l'endomorphisme $P(f)$ est l'endomorphisme nul.
De même pour $A \in \mathcal{M}_n(\mathbb{K})$ on a $P(A) = 0$ si P annule A.

Exemple 6: $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $J^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $J^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ donc $P = X^4 - 1$ annule J c'est un polynôme annulateur

Prop 7 : En dimension finie, pour $f \in \mathcal{L}(E)$ donné, il existe toujours un polynôme annulateur

Contre exemple 8: $D : P \mapsto P'$ la dérivation n'admet pas de polynôme annulateur
Si on avait Q tel que $Q(D)(P) = 0 \ \forall P \in \mathbb{K}[X]$, pour $P = X^{\deg(Q)+1}$ on a $Q(D)(P) \neq 0$, contradiction.

Remarque 9: Le noyau de φ_f est l'ensemble des polynômes annulateurs de f, c'est un idéal de $\mathbb{K}[X]$ puisque c'est le noyau d'un morphisme.

Def 10: Soit $f \in \mathcal{L}(E)$. Le polynôme minimal de f est l'unique polynôme unitaire, noté μ_f, qui engendre l'idéal des polynômes annulateurs de f.
De même pour $A \in \mathcal{M}_n(\mathbb{K})$, on notera μ_A.

Remarque 11: $\mathbb{K}[X]$ étant un anneau principal (puisque $\mathbb{K}$ est un corps) ces idéaux sont $P\mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$, le noyau de φ_f s'écrit en fait $\ker(\varphi_f) = \langle \mu_f \rangle$

Exemple 12: $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $J^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ $J^2 + I_2 = 0$ et X^2+1 est le polynôme minimal de J car J n'est pas une homothétie.

Proposition 13: Un endomorphisme $f \in \mathcal{L}(E)$ est inversible si et seulement si 0 n'est pas racine de son polynôme minimal

Exemple 14: $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ $\mu_A = X(X-1)$ 0 est bien racine de μ_A

Application du polynôme minimal 15: Soit $f \in GL(E)$ avec son polynôme minimal μ_f, on a $\mu_f(0) \neq 0$. $\mu_f = \sum_{i=0}^{k} a_i X^i$ on a $\mu_f(f) = 0$
d'où $a_0 + \sum_{i=1}^{k} a_i f^i = 0$ donc $f \sum_{i=0}^{k-1} a_{i+1} f^i = -a_0$ $\mu_f(0) = a_0 \neq 0$
Ainsi $f \circ \left(-\frac{1}{a_0} \sum_{i=0}^{k-1} a_{i+1} f^i\right) = 1$
Donc $-\frac{1}{a_0} \sum_{i=0}^{k-1} a_{i+1} f^i$ est l'inverse de f.

Remarque 16: Maintenant que l'on a le polynôme minimal on peut comprendre l'isomorphisme $\mathbb{K}[f] \simeq \mathbb{K}[X]/\langle \mu_f \rangle$
En effet φ_f est un morphisme surjectif car $X(f) = f$
donc en utilisant le premier théorème d'isomorphisme avec $\langle \mu_f \rangle = \ker \varphi_f$, on a l'isomorphisme d'algèbres ci-dessus.

II Diagonalisabilité et Trigonalisabilité

E, E' deux espaces vectoriels de dimension finie

Def 17: Soit $f \in \mathcal{L}(E, E')$ et F un sous espace vectoriel de E
La restriction de f à F est l'application linéaire $f_{|F} : F \to E'$ définie par $f_{|F}(x) = f(x)$ pour tout $x \in F$

Exemple 18: Soit $A \in \mathcal{M}_{n,m}(\mathbb{K})$ $f : E \to E'$ avec $\dim E = m$, $\dim E' = n$
$F \subset E$ avec $\dim F = p \leq m$ $f_{|F} : F \to E'$
$$A_{|F} = \begin{pmatrix} & \\ & \end{pmatrix} \updownarrow n \in \mathcal{M}_{n,p}(\mathbb{K}) \quad \leftrightarrow p$$

Def 19: Soit f un endomorphisme d'un espace vectoriel E.
Un sous espace vectoriel F de E est stable par f si $f(F) \subset F$

Exemple 20: $A = \begin{pmatrix} \square & 0 \\ 0 & \square \end{pmatrix}$ $\dim F = p$, $F \subset E$; $\dim G = r$, $G \subset E$
F et G sont stables car les coordonnées sur leur supplémentaire sont nulles.

Remarque 21: Les espaces stables sont essentiels quand on veut obtenir une somme directe de E.

Def 22 : Si F est un sous espace stable d'un espace vectoriel E par un endomorphisme f, alors l'endomorphisme induit par f sur F est l'endomorphisme $f_F : F \to F$ défini par $f_F(x) = f(x)$ pour tout $x \in F$.

Exemple 23: $A = \begin{pmatrix} |F| & 0 \\ \hline 0 & \ddots \end{pmatrix} \updownarrow n$ $B = (F)$ est l'induit par A sur F.
$\overrightarrow{f}$, n

Def 24: Le polynôme caractéristique d'un endomorphisme f est le polynôme unitaire χ_f défini par
$\chi_f(X) = \det(X\mathrm{Id} - f)$
De même pour $A \in \mathcal{M}_n(\mathbb{K})$ $\chi_A(X) = \det(XI_n - A)$

Exemple 25: $A = \begin{pmatrix} 3 & 1 \\ 2 & 4 \end{pmatrix}$ $\chi_A = \begin{vmatrix} X-3 & -1 \\ -2 & X-4 \end{vmatrix} = (X-3)(X-4) - 2$
$= (X-5)(X-2) = \chi_A(X)$

Thm 26: (Cayley Hamilton)
Soit $f \in \mathcal{L}(E)$. Le polynôme caractéristique de f est annulateur de f : $\chi_f(f) = 0$
De manière équivalente, $\mu_f \mid \chi_f$.
DEV 1

Remarque 27: On a $\deg(\mu_f) \leq \deg(\chi_f) = n = \dim E$

Exemple 28: $A = \begin{pmatrix} 3 & 1 \\ 2 & 4 \end{pmatrix}$ $\chi_A = (X-5)(X-2)$ $(A - 5I_2)(A - 2I_2) = \begin{pmatrix} -2 & 1 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$B = I_2$ $\chi_B = \det(XI_n - I_n) = (X-1)^n$ on a bien $\mu_B \mid \chi_B$
$\mu_B = (X-1)$

Def 29 : Soit $f \in \mathcal{L}(E)$, on dit que f est nilpotente s'il existe un $r \in \mathbb{N}^*$ tel que $f^r = 0$
De même, pour $A \in \mathcal{M}_n(\mathbb{K})$ on aurait r tel que $A^r = 0$

Exemple 30: $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $N^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ donc N est nilpotente

Application 31 : on peut calculer des puissances grandes avec le binôme de Newton par exemple $(I - N)^3 = I_2 + 3N + 3N^2 + N^3 = I_2 + 3N = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$

Def 32 : Soit $f \in \mathcal{L}(E)$. On dit que f est diagonalisable si dans une certaine base la matrice de f est diagonale.
Pour $A \in \mathcal{M}_n(\mathbb{K})$, on dit que A est diagonalisable s'il existe $P \in GL_n(\mathbb{K})$ telle que $A = PDP^{-1}$ avec D diagonale (on dit que A est semblable à une matrice diagonale)

Exemple 33: * $A = \begin{pmatrix} 13 & -35 \\ 6 & 16 \end{pmatrix}$ est diagonalisable car $A = P^{-1}DP$ avec $P = \begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix}$ $P^{-1} = \begin{pmatrix} 5 & -7 \\ -2 & 3 \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$

* $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ n'est pas diagonalisable pour des raisons que l'on va voir après.

Proposition 34 : Soit $f \in \mathcal{L}(E)$. Si χ_f est scindé sur $\mathbb{K}$ et a toutes ses racines simples alors f est diagonalisable.

Exemple 35 : * $A = \begin{pmatrix} -13 & -35 \\ 6 & 16 \end{pmatrix}$ $\chi_A = (X-1)(X-2)$ donc A diagonalisable
* $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $\chi_B = (X-1)^2$ donc il est bien possible que B ne soit pas diagonalisable.

Thm 36 : Soit $f \in \mathcal{L}(E)$ Les propositions sont équivalentes :
(i) f est diagonalisable
(ii) μ_f est scindé à racines simples
(iii) il existe des valeurs propres $\lambda_1, \dots, \lambda_p$ de f vérifiant $E = E_{\lambda_1} \oplus \dots \oplus E_{\lambda_p}$

Application 37 : La diagonalisabilité d'une matrice permet de calculer plus facilement les puissances de matrice. $A = P^{-1}DP$
on a $A^k = (P^{-1}DP)^k = P^{-1}D^kP$ et si $D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_n \end{pmatrix}$ alors $D^k = \begin{pmatrix} \lambda_1^k & 0 \\ 0 & \lambda_n^k \end{pmatrix}$

Def 38: Soit $f \in \mathcal{L}(E)$. On dit que f est trigonalisable si dans une certaine base la matrice de f est triangulaire supérieure.
Pour $A \in \mathcal{M}_n(\mathbb{K})$, on dit que A est trigonalisable s'il existe $P \in GL_n(\mathbb{K})$ telle que $A = PTP^{-1}$ avec T triangulaire supérieure.

Exemple 39: $A = \begin{pmatrix} -3 & -10 \\ 2 & 6 \end{pmatrix}$ est trigonalisable car $A = P^{-1}TP$ avec $P = \begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix}$ $T = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$

Thm 40: Soit $f \in \mathcal{L}(E)$ les propositions sont équivalentes :
(i) f trigonalisable
(ii) μ_f est scindé
(iii) il existe un polynôme annulateur scindé

Exemple 41: $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ n'est pas trigonalisable sur $\mathbb{R}$ car $\mu_J = X^2+1$ non scindé sur $\mathbb{R}$
mais J est trigonalisable sur $\mathbb{C}$ car $\mu_J = (X-i)(X+i)$, scindé sur $\mathbb{C}$

III Décompositions d'endomorphismes.

Thm 42 (Décomposition des noyaux) : Soit $f \in \mathcal{L}(E)$ et $P = P_1 \dots P_k \in \mathbb{K}[X]$, les polynômes P_i étant premiers entre eux deux à deux.
Alors $\ker P(f) = \ker P_1(f) \oplus \dots \oplus \ker P_k(f)$

Exemple 43: Pour P un polynôme annulateur de f, $\ker P(f) = E$
donc si $(X+1)(X-2)$ annule f on a : $E = \ker(f+Id) \oplus \ker(f-2Id)$

Thm 44 (Décomposition de Jordan-Dunford) Soit $f \in \mathcal{L}(E)$ avec χ_f scindé
Alors il existe un unique couple $(d,n) \in \mathcal{L}(E)^2$ tel que
- $f = d+n$
- n, d commutent
- n nilpotent
- d diagonalisable

De plus, d et n sont des polynômes en f.

DEV

Exemple 45:
* $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{D} + \underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_{N}$ $DN = ND$ D diagonalisable et N nilpotent

* $A = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = D$ et $N = 0$ D est diagonalisable car $\chi_A = (X-1)(X-2)$

Application 46 :

Pour résoudre des systèmes différentiels, on a besoin parfois de calculer l'exponentielle de matrices. En ayant la décomposition de Dunford, le calcul devient plus simple.

$\exp(A) = \exp(D+N) = \exp(D)\exp(N)$ pour $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$\exp(D) = P^{-1}\exp(\tilde{D})P$ avec P la matrice inversible de changement de base et $\tilde{D}$ une matrice diagonale et $\exp\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_n \end{pmatrix} = \begin{pmatrix} e^{\lambda_1} & 0 \\ 0 & e^{\lambda_n} \end{pmatrix}$

ici $P = Id = \tilde{D} = D$

$\exp(I_2) = \sum_{k=0}^{+\infty} \frac{I_2^k}{k!} = I_2 \times e$ $\exp(N) = \sum_{k=0}^{+\infty} \frac{N^k}{k!} = I_2 + N$ car $N^i = 0 \ \forall i \geq 2$

Def 47: Un bloc de Jordan d'une matrice nilpotente de taille $m \in \mathbb{N}^*$ est la matrice $J_m \in \mathcal{M}_m(\mathbb{K})$ dont tous les coefficients sont nuls sauf ceux en position $(i,i+1)$ pour $i \in \{1,\dots,m-1\}$ qui valent 1, i.e $J_m = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$ (m)

Remarque 48: J_m est bien nilpotente car en itérant J_m on fait remonter la diagonale de 1 qui finit par disparaître.

Proposition 49: Soit f un endomorphisme nilpotent. Il existe des entiers $\deg \mu_f = d_r \geq d_{r-1} \geq \dots \geq d_1$ et une base dans laquelle la matrice de f est diagonale par blocs avec les blocs $J_{d_1}, \dots, J_{d_r}$.
Cette matrice est appelée réduite de Jordan de f.

Exemple 50: $N = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ alors $N = P\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}P^{-1}$ avec $P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 2 & 3 \end{pmatrix}$

Thm 51 (Réduction de Jordan) Soit f un endomorphisme dont le polynôme caractéristique est scindé, $\lambda_1, \dots, \lambda_m$ les valeurs propres de f.
Il existe des suites $d_{j,1} \geq \dots \geq d_{j,r_j}$ pour $j \in \{1,\dots,m\}$ telles que dans une certaine base, la matrice f soit diagonale par blocs avec les blocs

$\lambda_1 I_{d_{1,1}} + J_{d_{1,1}}, \dots, \lambda_1 I_{d_{1,r_1}} + J_{d_{1,r_1}}, \dots, \lambda_m I_{d_{m,1}} + J_{d_{m,1}}, \dots, \lambda_m I_{d_{m,r_m}} + J_{d_{m,r_m}}$

$A = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_m \end{pmatrix}$ avec $A_i = \begin{pmatrix} \lambda_1 I_{d_{i,1}} + J_{d_{i,1}} & & 0 \\ & \ddots & \\ 0 & & \lambda_1 I_{d_{i,r_i}} + J_{d_{i,r_i}} \end{pmatrix}$ pour tout $i \in \{1,\dots,m\}$

pas $\mathcal{C}^2$! Pas un Banach !

156 — Exponentielle de matrices. Applications

$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $n \in \mathbb{N}^*$, E un $\mathbb{K}$-ev de dim n.

I - Exponentielle de matrices

1 - Définition

Def-Prop 1 : Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, $\sum \frac{A^k}{k!}$ est absolument convergente.
On note $\exp(A) = \sum_{k=0}^{+\infty} \frac{A^k}{k!}$ sa somme, qui est donc continue.

Rq 2 : Pour toute norme $\|.\|$ sur $\mathcal{M}_n(\mathbb{K})$ on a $\|e^A\| \leq e^{\|A\|}$

Prop 3 : Pour tout $A \in \mathcal{M}_n(\mathbb{K})$ et $P \in GL_n(\mathbb{K})$,
$\exp(PAP^{-1}) = P\exp(A)P^{-1}$

Appli 4 : Deux matrices semblables ont des exponentielles semblables

Prop 5 : Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, ${}^t\exp(A) = \exp({}^tA)$.

Appli 6 : L'exponentielle d'une matrice symétrique est symétrique.

Prop 7 : Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, $\det(\exp(A)) = \exp(\mathrm{tr}(A))$

Cor 8 : Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, $\exp(A) \in GL_n(\mathbb{K})$.

Prop 9 : Soit A et $B \in \mathcal{M}_n(\mathbb{K})$ tq $AB = BA$. Alors
$\exp(A+B) = \exp(A)\exp(B) = \exp(B)\exp(A)$

C-ex 10 : $A = \begin{pmatrix}1&0\\0&2\end{pmatrix}$, $B = \begin{pmatrix}1&1\\0&1\end{pmatrix}$, $e^A = \begin{pmatrix}e&0\\0&e^2\end{pmatrix}$, $e^B = \begin{pmatrix}e&e\\0&e\end{pmatrix}$
$e^Ae^B = \begin{pmatrix}e^2&e^2\\0&e^2\end{pmatrix} \neq e^Be^A = \begin{pmatrix}e^2&e^3\\0&e^3\end{pmatrix}$

Prop 11 : Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, $\exp(A) \in \mathbb{K}[A]$

Cor 12 : $\exp(A)$ commute avec A et donc avec tout polynôme en A.

Ex 13 : $A = \begin{pmatrix}1&0\\0&2\end{pmatrix}$ $e^A = \begin{pmatrix}e&0\\0&e^2\end{pmatrix} = (2e-e^2)I_2 + (e^2-e)A$.

Cor 14 : $\forall A \in \mathcal{M}_n(\mathbb{K})$, $e^{A-A} = e^Ae^{-A} = Id$.
Donc $(e^A)^{-1} = e^{-A}$

2 - Calcul de l'exponentielle d'une matrice

Ex 15 : Si A est diagonale : $\exp\begin{pmatrix}\lambda_1&&0\\&\ddots&\\0&&\lambda_n\end{pmatrix} = \begin{pmatrix}e^{\lambda_1}&&0\\&\ddots&\\0&&e^{\lambda_n}\end{pmatrix}$

Ex 16 : Si $N \in \mathcal{M}_n(\mathbb{K})$ est nilpotente, Alors
$e^N = \sum_{k=0}^{p-1} \frac{N^k}{k!}$ où p est l'indice de nilp. de N.

Ex 17 : $\exp\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix} = I_3 + N + \frac{1}{2}N^2 = \begin{pmatrix}1&1&1/2\\0&1&1\\0&0&1\end{pmatrix}$

Ex 18 : Pour $a, b \in \mathbb{K}$, $\exp\begin{pmatrix}a&-b\\b&a\end{pmatrix} = e^a\begin{pmatrix}\cos b&-\sin b\\\sin b&\cos b\end{pmatrix}$

Th 19 : Décomposition de Dunford

Lemme 19.1 : Pour $u \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$ tel que $P(u) = 0$,
on note $P = \alpha \prod_{i=1}^{r} \pi_i^{\alpha_i}$ sa décomposition en irréductibles,
et $N_i = \ker \pi_i^{\alpha_i}(u)$ $\forall i \in [\![1, r]\!]$
Alors $E = \bigoplus_{i=1}^{r} N_i$ et $\forall i \in [\![1, r]\!]$, la projection sur N_i à $\bigoplus_{j \neq i} N_j$ est un polynôme en u.

Th 19.2 : Pour $u \in \mathcal{L}(E)$, tq χ_u est scindé sur $\mathbb{K}$, il existe un unique couple $(d, n) \in \mathcal{L}(E)$ tel que
- d diagonalisable
- n nilpotent
- d et $n \in \mathbb{K}[u]$
- $u = d + n$

Appli 20 : Soit $u \in \mathcal{M}_n(\mathbb{K})$, tel que χ_u scinde. On note p_i les projecteurs sur N_i à $\bigoplus_{j \neq i} N_j$, $\forall i \in [\![1, r]\!]$, $p_i = S_{\mathbb{K}[u]}(u)$
Alors $\exp(u) = \exp(d)\exp(n) = \sum_{i=1}^{r} e^{\lambda_i}\left(\sum_{k=0}^{\alpha_i - 1} \frac{(u - \lambda_i \mathrm{id})^k}{k!}\right) \circ p_i$

Ex 21 : cf Annexe 1

Def 22 : (Bloc de Jordan)
Pour $\lambda \in \mathbb{K}$ on note $J(\lambda) = \begin{pmatrix}\lambda&1&&0\\&\ddots&\ddots&\\&&\ddots&1\\0&&&\lambda\end{pmatrix} \in \mathcal{M}_m(\mathbb{K})$ avec $m \in [\![0, n]\!]$

A et B commutent ssi $\forall t$, $e^{tA}e^{tB} = e^{t(A+B)}$

Th 23 : Décomposition de Jordan.
Soit $u \in \mathcal{L}(E)$ tq χ_u scinde sur $\mathbb{K}$. Alors il existe une base de E dans laquelle la matrice de u est de la forme diagonale par blocs
$\mathrm{diag}(J_{r_1}(\lambda_1), \dots, J_{r_{n_1}}(\lambda_1), \dots, J_{r_1}(\lambda_n), \dots, J_{r_{n_n}}(\lambda_n))$
où $r_{ij} = \dim E_{ij}$ et $d_i = \dim E_{\lambda_i}$ $\dim \lambda_n$

Appli 24 : Calcul de l'exponentielle par blocs.

Appli 20 bis : $A \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable sur $\mathbb{K}$ si et seulement si e^A diagonalisable sur $\mathbb{K}$

II - Propriétés de la fonction exponentielle

1 - Régularité

Prop 25 : $\exp : \mathcal{M}_n(\mathbb{K}) \longrightarrow GL_n(\mathbb{K})$ est $\mathcal{C}^\infty$

Prop 26 : $\exp : \mathcal{M}_n(\mathbb{K}) \longrightarrow GL_n(\mathbb{K})$ est différentiable en 0 et $d(\exp)(0) = Id$.

Cor 27 : la fonction exponentielle est un $\mathcal{C}^1$-difféo au voisinage de 0.

Appli 28 : Les sous-groupes de $GL_n(\mathbb{K})$ arbitrairement petits sont triviaux ($= \mathcal{Z}_{GL_n}$).

Def 29 : Si $A \in B_{\|.\|}(I_n, 1) \subset \mathcal{M}_n(\mathbb{K})$ pour $\|.\|$ une norme matricielle, on pose $\log(A) = \sum_{k=1}^{+\infty} (-1)^{k+1} \frac{(A - I_n)^k}{k}$

Prop 30 : $\log : B_{\|.\|}(I_n, 1) \longrightarrow \mathcal{M}_n(\mathbb{K})$ est continue et $\forall A \in B_{\|.\|}(I_n, 1)$, $\exp(\log(A)) = A$

Ex 31 : $A = \begin{pmatrix}1/2&1/2\\0&1/2\end{pmatrix}$, $\|A\|_\infty = 1/2 < 1$, $\log(A) = \begin{pmatrix}-\ln 2&1\\0&-\ln 2\end{pmatrix}$

Prop 32 : On note $\mathcal{N}$ les endomorphismes nilpotents
$\mathcal{U}$ ——— unipotents

Alors $\exp : \mathcal{N} \longrightarrow \mathcal{U}$ est un homéomorphisme d'inverse le logarithme.

Ex 33 : $A = \begin{pmatrix}1&1\\0&1\end{pmatrix} \in \mathcal{U}$ $\log(A) = \begin{pmatrix}0&1\\0&0\end{pmatrix}$

2 - Injectivité et surjectivité

Rq 34 : l'exponentielle n'est pas injective :
- sur $\mathcal{M}_n(\mathbb{C})$ pour $n \geq 1$
- sur $\mathcal{M}_n(\mathbb{R})$ pour $n \geq 2$

Ex 35 : $\exp\begin{pmatrix}0&-2\pi\\2\pi&0\end{pmatrix} = \exp\begin{pmatrix}0&0\\0&0\end{pmatrix} = I_2$

Prop 36 : $\exp : \mathcal{D}_n(\mathbb{K}) \longrightarrow GL_n(\mathbb{K})$ est injective.

Th 37 : Pour $A \in GL_n(\mathbb{C})$, $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$
où $\mathbb{C}[A]^\times$: inversibles de l'anneau $\mathbb{C}[A]$

Coro 38 : $\exp(\mathcal{M}_n(\mathbb{C})) = GL_n(\mathbb{C})$

Coro 39 : $\exp(\mathcal{M}_n(\mathbb{R})) = \{A^2, A \in GL_n(\mathbb{R})\}$ DEV 1

C-ex 40 : exp non surjective dans $GL_n(\mathbb{R})$: $-I_n$ n'est pas une exponentielle de matrice.

Prop 41 : $\exp : \mathcal{A}_n(\mathbb{R}) \longrightarrow SO_n(\mathbb{R})$ est surjective

espace tangent de $SO_n(\mathbb{R})$ (ou $O_n(\mathbb{R})$)

Th 42 :
L'exponentielle induit un homéomorphisme entre $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{S}_n^{++}(\mathbb{R})$.

Cor 43 : $GL_n(\mathbb{R}) \simeq O_n(\mathbb{R}) \times \mathbb{R}^{\frac{n(n+1)}{2}}$

Rq 44 : on a les mêmes résultats sur $\mathbb{C}$:
$\exp : \mathcal{H}_n(\mathbb{C}) \longrightarrow \mathcal{H}_n^{++}(\mathbb{C})$ est un homéo
$GL_n(\mathbb{C}) \simeq U_n(\mathbb{C}) \times \mathbb{R}^{n^2}$

Appli 45 : On note pour $p,q \in \mathbb{N}$, **DEV 2**

$O(p,q) = \{M \in GL_{p+q}(\mathbb{R}) \text{ tq } {}^tM I_{p,q} M = I_{p,q}\}$

Alors $O(p,q) \simeq O_p(\mathbb{R}) \times O_q(\mathbb{R}) \times \mathbb{R}^{pq}$

Corollaire 46 : $O(p,q)$ est compact ssi $p=0$ ou $q=0$.

III - Application aux équations différentielles

1. Equations linéaires

Th 47 : Soit (E) : $Y' = AY + B(t)$ une équation différentielle linéaire à coefficients constants avec $Y \in \mathcal{C}^1(\mathbb{R}, \mathbb{R}^n)$, $A \in \mathcal{M}_n(\mathbb{R})$, $B \in \mathcal{C}(\mathbb{R}, \mathbb{R}^n)$

Alors (E) a ses solutions maximales définies sur $\mathbb{R}$.

Cor 46 : La solution au problème de Cauchy

(C) : $\begin{cases} Y' = AY \\ Y(t_0) = Y_0 \end{cases}$ est $Y(t) = e^{(t-t_0)A} Y_0 \quad \forall t \in \mathbb{R}$.

- avec second membre : (C') $\begin{cases} Y' = AY + B(t) \\ Y(t_0) = Y_0 \end{cases}$

est $Y(t) = e^{(t-t_0)A} Y_0 + \int_{t_0}^{t} e^{(t-u)A} B(u)\,du$

Ex 47 : $\begin{pmatrix} x \\ y \\ z \end{pmatrix}'(t) = \begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & -1 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}(t) + \begin{pmatrix} e^{2t} \\ 0 \\ e^{2t} \end{pmatrix}$.

Def 48 : On considère le système différentiel autonome $y' = f(y)$, $f \in \mathcal{C}^1(\mathbb{R}^d, \mathbb{R}^d)$

- $y_0 \in \mathbb{R}^d$ est un équilibre si $f(y_0) = 0$
- un équilibre y_0 est stable si $\forall \varepsilon > 0$, $\exists \delta > 0$ tel que si y est la solution du problème $\begin{cases} y' = f(y) \\ y(t_0) = y_1 \end{cases}$ avec $|y_1 - y_0| \leq \delta$, alors $\forall t \geq t_0$, $|y(t) - y_0| \leq \varepsilon$.
- un équilibre y_0 est asymptotiquement stable s'il est stable et que $\exists \delta_1 > 0$ tq si $|y_1 - y_0| \leq \delta_1$, alors $y(t) \xrightarrow[t \to \infty]{} y_0$.

Ex 49 : cf annexe 2

Th 50 : Soit $A \in \mathcal{M}_n(\mathbb{R})$. 0 est un équilibre de $y' = Ay$

- stable ssi $\forall \lambda \in Sp(A)$, $\begin{cases} Re(\lambda) < 0 \\ \text{ou} \\ Re(\lambda) = 0 \text{ et } \dim E_\lambda = \dim C_\lambda \end{cases}$
- asymptotiquement stable ssi $\forall \lambda \in Sp(A)$, $Re(\lambda) < 0$.

Ex 51 : Si $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, 0 n'est pas stable

si $A = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$, 0 est asymptotiquement stable

Th 52 (Liapunov) : Soit $y' = f(y)$ un système différentiel avec $f \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}^n)$ et $f(0) = 0$.

Alors 0 est un équilibre asymptotiquement stable si $Df(0)$ a ses valeurs propres de partie réelle strictement négative.

Ex 53 : Pendule avec frottement : $y'' + ky' + C\sin y = 0$ avec $C > 0$, $k > 0$. 0 est un équilibre asymptotiquement stable.

Annexe 1 : Décomposition de Dunford et Exponentielle

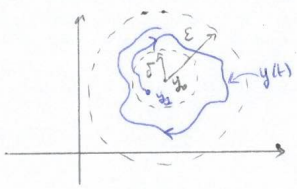
$$A = \begin{pmatrix} 8 & -1 & -5 \\ -2 & 3 & 1 \\ 4 & -1 & -1 \end{pmatrix}$$

$$D = \begin{pmatrix} 5 & -1 & -2 \\ 1 & 3 & -2 \\ 1 & -1 & 2 \end{pmatrix} \qquad N = \begin{pmatrix} 3 & 0 & -3 \\ -3 & 0 & 3 \\ 3 & 0 & -3 \end{pmatrix}$$

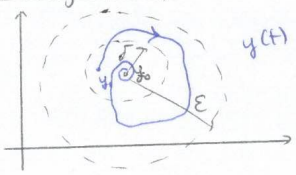
$$\exp(A) = \begin{pmatrix} \frac{-e^2+3e^4}{2} & \frac{e^2-e^4}{2} & e^2-4e^4 \\ \frac{-e^2-5e^4}{2} & \frac{e^2+e^4}{2} & e^2+2e^4 \\ \frac{-e^2+7e^4}{2} & \frac{e^2-e^4}{2} & e^2-3e^4 \end{pmatrix}$$

Annexe 2 :

Equilibre stable :



Equilibre asymptotiquement stable



Formes linéaires et dualité en dimension finie. Exo et Appli

159

Motivation : permet de dédoubler les résultats par dualité

I Formes linéaires et hyperplans

1) Définitions

E un espace vectoriel (sur un corps $\mathbb{K}$) de dim finie n.

Def 1 : On appelle forme linéaire sur E une application linéaire $\varphi : E \to \mathbb{K}$

Ex 2 : $\varphi(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} x_i$ où (e_i) est une base de E est une forme linéaire

Def 3 : On appelle noyau de φ, l'ensemble $\{x \in E / \varphi(x) = 0\}$ on le note $\ker \varphi$

Prop 4 : Si φ est une forme linéaire non nulle alors $\dim \ker(\varphi) = n-1$

Ex 5 : $\varphi(\sum_{i=1}^{n} x_i e_i) = x_1$ Ainsi $\ker \varphi = \mathrm{Vect}(x_2, \dots, x_n)$ de dim $n-1$.

Prop 6 : Le rang d'une forme linéaire non nulle est 1 i.e $\dim(\mathrm{Im}\,\varphi) = 1$

2) Lien avec les hyperplans

Def 7 : On appelle hyperplan H de E, un sous espace de E de dimension $n-1$.

Rmq 8 : On a donc vu que le noyau d'une forme linéaire non nulle est un hyperplan (Prop 4)

Prop 9 : Pour $e \notin \ker \varphi$ on a $E = \ker \varphi \oplus \mathbb{K}e$

Thm 10 : Tout hyperplan de E est le noyau d'une forme linéaire non nulle

Rmq 11 : On peut donc définir de manière cohérent $H = \{x \in E / \varphi(x) = 0\}$ par φ une forme linéaire non nulle

Ex 12 : $H = \{x \in E / x_1 = 2x_2\}$ est décrit par $\varphi(x) = 2x_2 - x_1$ en écrivant $x = \sum_{i=1}^{n} x_i e_i$

Prop 13 : Deux formes linéaires φ et $\tilde{\varphi}$ non nulles ont le même noyau SSi elles sont proportionnelles

II Dualité

1) Base duale

Def 14 : On appelle dual de E, l'ensemble des formes linéaires sur E, noté E^* (ou $\mathcal{L}(E, \mathbb{K})$)

Prop 15 : $\dim E = \dim E^*$ (puisqu'on est en dim finie)

Corollaire 16 : E et E^* sont isomorphes

Rmq 17 : L'isomorphisme n'est pas canonique, il dépend des bases choisies.

Def 18 : Soit $(e_i)_{i=1}^{n}$ une base de E, on appelle forme linéaire coordonnée d'indice i la forme linéaire e_i^* telle que $e_i^*(e_j) = \delta_{i,j}$.

Prop 19 : Soit $(e_i)_1^n$ base de E. Alors $(e_i^*)_1^n$ est une base de E^*, on l'appelle la base duale de $(e_i)_1^n$.

Ex 20 : La base duale de la base $\{e_1=(1,1,1), e_2=(1,0,-1), e_3=(0,1,1)\}$ de $\mathbb{R}^3$ est $\{\theta_1(x) = x_1 - x_2 + x_3, \theta_2(x) = x_2 - x_3, \theta_3(x) = -x_1 + 2x_2 - x_3\}$

Def 21 : On peut définir le bidual de E comme E^{**} $E^{**} := \{\varphi : E^* \to \mathbb{K}, \text{ linéaire}\}$

Thm 22 : Si $x \in E$, on note $\tilde{x} : E^* \to \mathbb{K}$, $\varphi \mapsto \varphi(x)$

On a $\tilde{x} \in E^{**}$ et $\Phi : E \to E^{**}$, $x \mapsto \tilde{x}$ est un isomorphisme (canonique)

Rmq 23 : Il ne dépend pas de bases choisies donc on peut identifier E et E^{**}.

Prop 24 : Soit $(\varphi_i)_1^n$ une base de E^*. Il existe une unique base $(e_i)_1^n$ de E telle que $e_i^* = \varphi_i$ $\forall i$

2) Orthogonalité

Def 25 : Pour $x \in E$, $\varphi \in E^*$, ils sont dits orthogonaux si $\varphi(x) = 0$

Ex 26 : $u = (1,0,0)$ $\varphi(x) = x_2 + x_3$ $\forall x \in E$ $\varphi(u) = 0$ donc φ et u sont dits orthogonaux

Def 27 : Si $A \subset E$, on note $A^\perp = \{\varphi \in E^* / \forall x \in A, \varphi(x) = 0\}$ $A^\perp \subset E^*$ est appelé orthogonal de A

Si $B \subset E^*$ on note $B^\circ = \{x \in E / \forall \varphi \in B \ \varphi(x) = 0\}$ $B^\circ \subset E$ est appelé orthogonal de B

Prop 28 : Si $A_1 \subset A_2 \subset E$, alors $A_2^\perp \subset A_1^\perp$

Si $B_1 \subset B_2 \subset E$, alors $B_2^\circ \subset B_1^\circ$

Si $A \subset E$, alors $A^\perp = (\mathrm{Vect} A)^\perp$

Si $B \subset E^*$, alors $B^\circ = (\mathrm{Vect} B)^\circ$

Thm 29 : Si F ssev de E, $\dim F + \dim F^\perp = \dim E$ et $F^{\perp\circ} = F$

Si G ssev de E^*, $\dim G + \dim G^\circ = \dim E$ et $G^{\circ\perp} = G$

Prop 30 : Soit H un hyperplan de E. L'ensemble $H^\perp$ des formes linéaires sur E qui s'annulent sur H est une droite de E^*

Appli 31 : Les morphismes d'algèbre de $\mathcal{C}(K, \mathbb{R})$ avec K compact sont les formes linéaires $f \mapsto f(x)$ $\forall x \in K$ ou l'application nulle (on se place ici en dimension infinie)

DEV 1

3) Transposées

Def 32 : Soit E, F des $\mathbb{K}$ev, soit $u \in \mathcal{L}(E,F)$. $\forall f \in F^*$ on a $f \circ u \in E^*$

On appelle $t_u : F^* \to E^*$, $f \mapsto f \circ u$ la transposée de u.

Prop 33 :
- $\mathrm{rg}(u) = \mathrm{rg}(t_u)$
- $\mathrm{Im}(t_u) = (\ker u)^\perp$
- $\ker(t_u) = (\mathrm{Im}\, u)^\perp$

Rmq 34 : Cela coïncide bien avec la notion de transposition des matrices.

III Utilisation en algèbre et en analyse

1) En analyse : différentielle

Def 35 : Soit E un $\mathbb{R}$-ev, U un ouvert de E, $a \in U$. $f : U \to \mathbb{R}$ est dite différentiable en a s'il existe $\varphi \in E'$ telle que $f(a+h) = f(a) + \varphi(h) + o(\|h\|)$ lorsque $h \to 0$. On appelle φ la différentielle en a de f, on la note df_a

Rmq 36 : On est ici en dimension infini, E' est le dual de E au sens des formes linéaires continues de E dans $\mathbb{R}$

Appli 37 : L'application $\det : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$ est différentiable en tout point $A \in \mathcal{M}_n(\mathbb{R})$ et $d\det_M(H) = (\det M)\,\mathrm{tr}(M^{-1}H)$.

Thm 38 (Extrema liés)
Soient $f, g_1, \dots, g_r : U \subset \mathbb{R}^n \to \mathbb{R} \in \mathcal{C}^1$ U ouvert de $\mathbb{R}^n$
$\Gamma = \{x \in U / g_1(x) = g_2(x) = \dots = g_r(x) = 0\}$
Si $f_{|\Gamma}$ admet un extremum relatif en a
et si les formes linéaires $dg_{1a} \dots dg_{ra}$ sont linéairement indépendantes, alors l'existe des réels $\lambda_1, \dots, \lambda_r$ tels que $df_a = \lambda_1 dg_{1a} + \dots + \lambda_r dg_{ra}$

REV 2

2) En algèbre linéaire : $\dim(E) = n$
On peut voir un système linéaire $AX = B$ ($B \in \mathcal{M}_{m,1}(\mathbb{R})$, $A \in \mathcal{M}_{m,n}(\mathbb{R})$)
comme une intersection d'hyperplans H_i $\forall i \in [\![1; m]\!]$
$H_i = \{x \in E / \sum_{j=1}^{n} a_{ij} x_j - b_i = 0\}$
On pose $\Lambda_i(x) = \sum_{j=1}^{n} a_{ij} x_j$ les m formes linéaires associées à A

Thm 39 : Soit $\varphi : E \to \mathbb{K}^m$, $v \mapsto \begin{pmatrix} \Lambda_1(v) \\ \vdots \\ \Lambda_m(v) \end{pmatrix}$
Alors $\operatorname{rg} \varphi = \operatorname{rg}(\Lambda_1, \dots, \Lambda_m)$

Corollaire 40 : si $\operatorname{rg}(\Lambda_1, \dots, \Lambda_m) = r$
Alors $\bigcap_{i=1}^{m} \ker \Lambda_i$ est de dimension $n - r$

Prop 41 : Soit $r \in [\![1; n]\!]$, V un sev de E de dimension $n - r$, Alors il existe une famille libre de r formes linéaires sur E dont l'intersection des noyaux coïncident avec V

Appli 42 : Calcul de la dimension d'une intersection d'hyperplans H_i
Soient $H_i := \ker \Lambda_i$
alors $\dim\left(\bigcap_{i=1}^{m} H_i\right) = n - \operatorname{rg}(\Lambda_1 \dots \Lambda_m)$
En notant $r = \operatorname{rg}(\Lambda_1 \dots \Lambda_m)$ et en supposant que les r premières formes linéaires sont indépendantes
alors $\bigcap_{i=1}^{m} H_i = \bigcap_{i=1}^{r} H_i$
On pourrait donc réduire le système $AX = O_m$ à $A'X = O_r$ avec A' la restriction de A aux r premières lignes.

214

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

Motivations : généraliser l'inversion des $f:\mathbb{R}\to\mathbb{R}$ ou d'applications linéaires

I Théorème d'inversion locale (TiL)

1) Enoncés et variantes (cadre : $n\in\mathbb{N}$, $p\in\mathbb{N}^*\cup\{\infty\}$)

Thm 1 : (TiL) Soit U un ouvert de $\mathbb{R}^n$, a un point de U et $f:U\to\mathbb{R}^n$ une application $\mathcal{C}^1$. Si $Df(a)$ est inversible
Alors il existe V un voisinage ouvert de a (dans U) et $W\in\mathcal{V}_{f(a)}(\mathbb{R}^n)$ tels que f est un $\mathcal{C}^1$-difféomorphisme de V sur W.

Rmq 2 : on peut se placer dans des Banach en supposant $df(a)$ bijective de E dans F

Rmq 3 : De plus, si $f\in\mathcal{C}^p(U,\mathbb{R}^n)$, alors f est un $\mathcal{C}^p$ difféo de V sur W

Ex 4 : $U=\mathbb{R}^2\setminus\{0,0\}$, $f:(x,y)\mapsto(x^2-y^2,2xy)$ est un $\mathcal{C}^1$ difféomorphisme local sur U

Contre-ex 5 :
- $f:\mathbb{R}\to\mathbb{R}$, $x\mapsto x+x^2\sin(\frac{1}{x})$ n'est pas un $\mathcal{C}^1$ difféo au voisinage de 0 car n'est pas $\mathcal{C}^1$.
- $f:\mathbb{R}\to\mathbb{R}$, $x\mapsto x^3$ n'est pas un $\mathcal{C}^1$ difféo au voisinage de 0, car $f^{-1}\notin\mathcal{C}^1$ il manque $Df(0)$ inversible.

Thm 6 : (Théorème d'inversion globale) Soit U ouvert de $\mathbb{R}^n$, $f\in\mathcal{C}^1(U,\mathbb{R}^n)$. Si f est injective sur U et que pour tout $x\in U$, $Df(x)$ est inversible
Alors $f(U)$ est un ouvert de $\mathbb{R}^n$ et f est un $\mathcal{C}^1$ difféomorphisme de U sur $f(U)$.

Contre ex 7 : Dans l'exemple 4, f est un $\mathcal{C}^1$ difféo local sur U mais pas global.

Thm 8 : (Théorème d'inversion holomorphe) Soit U ouvert connexe de $\mathbb{C}$ et $f:U\to\mathbb{C}$ fonction holomorphe on suppose f injective sur U.
Alors $f(U)$ est un ouvert de $\mathbb{C}$ et f est un biholomorphisme de U sur $f(U)$.

2) Applications en analyse

Thm 9 : (changement de coordonnées) Soient $f_1,\dots,f_n\in\mathcal{C}^1(\mathbb{R}^n,\mathbb{R})$
$\left(\begin{array}{l}u_1=f_1(x_1,\dots,x_n)\\ \dots\\ u_n=f_n(x_1,\dots,x_n)\end{array}\right.$ définissent un chgmt de variables au voisinage de $a\in\mathbb{R}^n$ $\left.\right)\iff\left(\det\left(\frac{\partial f_i}{\partial x_j}(a)\right)\neq 0\right)$

Ex 10 : (coordonnées polaires) $f:]0,\infty[\times]-\pi,\pi[\mapsto(r\cos\theta,r\sin\theta)\in\mathbb{R}^2\setminus(\mathbb{R}^-\times\{0\})$

Prop 11 : Les fonctions exp : $\mathcal{M}_n(\mathbb{R})\to GL_n(\mathbb{R})$, $\mathbb{C}\to\mathbb{C}$, $x\mapsto x^k$, inv : $GL_n(\mathbb{C})\to GL_n(\mathbb{C})$, $\mathcal{Z}(E)\to\mathcal{Z}(E)$, $u\mapsto u^{-1}$ sont resp. des $\mathcal{C}^1$ difféo local au voisinage des points resp. $0,1,I_n,Id$.

Prop 12 : (perturbation de l'identité) Soit E Banach, $g\in\mathcal{C}^1(E,E)$. Si pour tout $x\in E$ $\|d_xg\|_{\mathcal{L}(E)}\leq 1$
Alors, pour tout $\varepsilon\in]0,1[$, $f_\varepsilon=I_E+\varepsilon g$ est un $\mathcal{C}^1$ difféo de $E\to E$.

Prop 13 : Soit $n\geq 2$, $f:\mathbb{R}^{n*}\to\mathbb{R}^{n*}$ $\mathcal{C}^1$ telle que $\forall x\in\mathbb{R}^{n*}$ $Df(x)\in O_n(\mathbb{R})$ et $\|f(x)\|_2=\|x\|_2$
Alors f est surjective.

Thm 14 : (Lemme de Morse à deux variables) Soit U ouvert de $\mathbb{R}^2$ tels que $0\in U$, Soit $f:U\to\mathbb{R}$ $\mathcal{C}^3$
on suppose que la forme quadratique $D^2f(0,0)$ est non dégénérée.
si signature $(D^2f(0,0))=(2,0)$, il existe u et v tels que $f(x,y)-f(0,0)-df(0,0).(x,y)=u(x,y)^2+v(x,y)^2$
si signature $(D^2f(0,0))=(1,1)$, il existe u et v tels que $f(x,y)-f(0,0)-df(0,0).(x,y)=u(x,y)^2-v(x,y)^2$

Appli 15 : Etude locale d'une conique par rapport à son plan tangent (voir annexe)

Appli 16 : Méthode de la phase stationnaire : étudier le comportement en $+\infty$ de $I(\lambda)=\int e^{i\lambda\varphi(x)}a(x)dx$ où $\varphi\in\mathcal{C}^\infty(\mathbb{R}^n,\mathbb{R})$ et $a\in\mathcal{C}^\infty_c(\mathbb{R}^n,\mathbb{C})$

3) Applications en algèbre linéaire et en géométrie

Thm 17 : (D'Alembert Gauss) Tout polynôme de $\mathbb{C}[X]$ est scindé.

Prop 18 : Soit $n\geq 3$ impair, $SO_n(\mathbb{R})$ est simple.

Prop 19 : (Réduction des formes quadratiques) Soit $A_0\in\mathcal{S}_n\cap GL_n(\mathbb{R})$ il existe un voisinage V de A_0 dans $\mathcal{S}_n(\mathbb{R})$ et $\Psi:V\to GL_n(\mathbb{R})$ $\mathcal{C}^1$, $A\mapsto\Psi(A)$ tels que $A={}^t\Psi(A)\,A_0\,\Psi(A)$ $\forall A\in V$

Appli 20 : Lemme de Morse en dimension n.

Thm 21 : Si $A\in\mathcal{M}_n(\mathbb{C})$, alors $\exp(\mathbb{C}[A])=\mathbb{C}[A]^\times$

Corollaire 22 : $\exp:\mathcal{M}_n(\mathbb{C})\to GL_n(\mathbb{C})$ surjective
$\exp:\mathcal{M}_n(\mathbb{R})\to\{A^2,A\in GL_n(\mathbb{R})\}$ surjective

DEV1

Appli 23 : $GL_n(\mathbb{C})$ n'a pas de sous groupe arbitrairement petit.

II Théorème des fonctions implicites (TFi)

1) Enoncés

Thm 24 : Soit U ouvert de $\mathbb{R}^n\times\mathbb{R}^k$, $(a,b)\in U$, $f\in\mathcal{C}^1(U,\mathbb{R}^k)$
Si $f(a,b)=0$ et $D_yf(a,b)$ est inversible
Alors il existe $V\in\mathcal{V}_a(\mathbb{R}^n)$, $W\in\mathcal{V}_b(\mathbb{R}^k)$ avec $V\times W\subset U$ et $\varphi\in\mathcal{C}^1(V,W)$ telle que
$(x\in V, y\in W$ et $f(x,y)=0)\iff(x\in V,\ y=\varphi(x))$ (généralisable au cas holomorphe)

Rmq 25 : Si $f\in\mathcal{C}^p(U,\mathbb{R}^k)$, alors $\varphi\in\mathcal{C}^p(V,W)$ (du cas holomorphe)

Rmq 26 : De plus, il y a existence de $D\varphi(x)$ sur V et l'on peut la calculer explicitement.

Ex 27 :
- Le cercle $\{x^2+y^2=1\}$ peut être vu localement comme un graphe (sauf en $(\pm1,0)$)
- Folium de Descartes $\{x^3+y^3-3xy=0\}$ aussi sauf en $(0,0)$ et $(\frac{3}{2},\frac{3}{2})$

Rmq 28 : Historiquement, la première preuve du TFi utilise le théorème de Cauchy Lipschitz, on a en fait une équivalence entre
(Cauchy Lipschitz) $\iff$ (TiL) $\iff$ (TFi) $\iff$ (Point fixe de Picard)

2) Applications dans d'autres domaines

Thm 29 : Soit $P\in\mathbb{C}[X]$ de degré n, $P=\sum_{i=0}^n a_iX^i$. Soit x_0 une racine simple de P. Alors il existe $U\in\mathcal{V}_{x_0}(\mathbb{C})$, $V\in\mathcal{V}_{(a_0,\dots,a_n)}(\mathbb{C}^{n+1})$ et $\Psi:U\to V$ $\mathcal{C}^1$ tels que
$(x\in V,(b_0,\dots,b_n)\in U$ $\sum_{i=0}^n b_ix^i=0)\iff((b_0,\dots,b_n)\in V$ $x=\Psi(b_0,\dots,b_n))$

Cor 30 : $\{P\in\mathbb{C}[X]$ scindé simple$\}$ est un ouvert de $\mathbb{C}[X]$ donc les matrices diagonalisables de $\mathcal{M}_n(\mathbb{C})$ forment un ouvert de $\mathcal{M}_n(\mathbb{C})$

Appli 31 : Donner une solution approchée de la racine réelle de $x^7+0{,}99x-2{,}03=0$

Appli 32 : Trouver un développement asymptotique de $I(\varepsilon)=\int_{x_1(\varepsilon)}^{x_2(\varepsilon)}\frac{dx}{\sqrt{f(x,\varepsilon)}}$ où $f(x,\varepsilon)=(x-a)(b-x)+\varepsilon x^2$ $a<b$
et $x_1(\varepsilon)$, $x_2(\varepsilon)$ les deux premières racines de f.

Prop 33 : Soient Σ_1 et Σ_2 deux nappes régulières $\mathcal{C}^1$ à paramétrage injectif, soit $p\in\Sigma_1\cap\Sigma_2$. Si les plans tangents $T_p\Sigma_1$ et $T_p\Sigma_2$ en p sont distincts.
Alors, au voisinage de p, l'intersection $\Sigma_1\cap\Sigma_2$ est une courbe dont la tangente en p est d'intersection $T_p\Sigma_1\cap T_p\Sigma_2$ des deux plans tangents.

III Sous variétés (cadre : $n\in\mathbb{N}$, $p\in\mathbb{N}^*\cup\{\infty\}$, $k\in\mathbb{N}^*$)

1) Sous variétés et espaces tangents

Def 34 : (sous variété) $N\subset\mathbb{R}^n$ est une sous variété de dimension k et de classe $\mathcal{C}^p$ si pour tout $x_0\in N$, il existe $W\in\mathcal{V}_{\mathbb{R}^n}(x_0)$ et $\varphi:W\to\mathbb{R}^n$ un $\mathcal{C}^p$ difféomorphisme local tel que
$\varphi(N\cap W)=\varphi(W)\cap[\mathbb{R}^k\times\{0\}^{n-k}]$

Ex 35 : les ouverts de $\mathbb{R}^n$ sont des sous variétés, $GL_n(\mathbb{R})$ dans $\mathbb{R}^{n^2}$

Thm 36 : (des sous variétés) Il y a équivalence entre :

(i) (Carte locale) N est une sous variété de dim k de classe $\mathcal{C}^p$

(ii) (équation) pour tout $x_0 \in N$, il existe $W \in \mathcal{V}_{x_0}(\mathbb{R}^n)$ et $F : W \to \mathbb{R}^{n-k}$ $\mathcal{C}^p$ tels que $dF(x)$ soit surjective $\forall x \in W$ et $N \cap W = F^{-1}(\{0\})$

(iii) (graphe) pour tout $x_0 \in N$, il existe $W \in \mathcal{V}_{x_0}(\mathbb{R}^n)$, $U \in \mathcal{V}_{(x_{0,1}, \dots x_{0,k})}(\mathbb{R}^k)$ et $u : U \to \mathbb{R}^{n-k}$ de classe $\mathcal{C}^p$ tels que $W \cap N = \{ A(x, u(x)),\ x \in U \}$ avec A une matrice de changement de base

(iv) (nappe paramétrée) pour tout $x_0 \in N$, il existe $W \in \mathcal{V}_{x_0}(\mathbb{R}^n)$, $U \in \mathcal{V}_0(\mathbb{R}^k)$ et $j : U \to \mathbb{R}^n$ $\mathcal{C}^p$ tel que $j(0) = x_0$ $dj(x_0)$ injective et j est une bijection bicontinue de U vers $N \cap W$

Ex 37 : La parabole $y = x^2$ est une $\mathcal{C}^\infty$ sous variété de dimension 1
Le cercle $x^2 + y^2 = 1$ est une $\mathcal{C}^\infty$ sous variété de dimension 1
Le cône $x^2 + y^2 = z^2$ est une $\mathcal{C}^\infty$ sous variété de dimension 2

Def 38 (espace tangent) Soit N une sous variété, soit $x_0 \in N$
l'espace tangent est l'espace vectoriel de dimension k

$$T_{x_0}N = \{ v \in \mathbb{R}^n \text{ tel qu'il existe } \gamma : I \to \mathbb{R}^n \text{ avec } 0 \in \overset{\circ}{I},\ \gamma(I) \subset N,\ \gamma(0) = x_0 \text{ et } \gamma'(0) = v \}$$

Rmq 39 : Parfois on parle d'espace affine tangent qui est $x_0 + T_{x_0}N$.

Thm 40 : on peut caractériser l'espace tangent comme ci-dessous

(i) (Carte locale) $T_{x_0}N = d\varphi(x_0)^{-1} \cdot [\mathbb{R}^k \times \{0\}^{n-k}]$

(ii) (équation) $T_{x_0}N = \ker(dF(x_0))$

(iii) (graphe) $T_{x_0}N = \{A(h, du(z_0).h),\ h \in \mathbb{R}^k\}$ avec $z_0 / x_0 = A(z_0, u(z_0))$

(iv) (nappe paramétrée) $T_{x_0}N = dj(0)(\mathbb{R}^k)$

Ex 41 : Soit q une forme quadratique sur $\mathbb{R}^n$ et $x_0 \in C_0(q)$
Alors $\{x_0\}^\perp$ est l'espace tangent en x_0 de la sous variété $C_0(q)$

2) Théorème des extrema liés

Thm 42 : (extrema liés) Soit $U \in \mathbb{R}^n$, $f, g_1, \dots g_{n-k} \in \mathcal{C}^1(U, \mathbb{R})$
on pose $\Gamma = \{ x \in U,\ g_1(x) = g_2(x) = \dots = g_{n-k}(x) = 0 \}$
Si $f_{|\Gamma}$ admet un extremum local en $x_0 \in U$ et que la famille $dg_i(x_0)$ est libre
Alors il existe $(\lambda_i)_1^{n-k} \in \mathbb{R}^{n-k}$ tels que

$$df(x_0) = \sum_{i=1}^{n-k} \lambda_i\, dg_i(x_0)$$

DEV 2

Appli 43 : pour tout $u_1, \dots, u_n \in \mathbb{R}^n$ (inégalité d'Hadamard)

$$|\det(u_1, \dots, u_n)| \leq \prod_{i=1}^{n} \|u_i\|_2$$

Appli 44 : pour tout $x_1, \dots, x_n \in \mathbb{R}^+$ (inégalité arithmético-géométrique)

$$\left(\prod_{i=1}^{n} x_i \right)^{1/n} \leq \frac{\sum_{i=1}^{n} x_i}{n}$$

Appli 45 : pour tout $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{R}^+$ (inégalité de Hölder)

$$\sum_{i=1}^{n} a_i b_i \leq \left(\sum_{i=1}^{n} a_i^p \right)^{1/p} \left(\sum_{i=1}^{n} b_i^q \right)^{1/q} \quad \text{où } \frac{1}{p} + \frac{1}{q} = 1,\ p > 1,\ q > 1$$

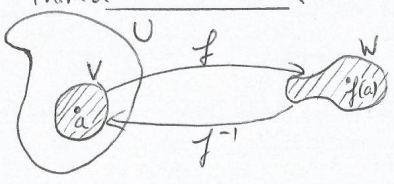
3) Application à l'étude des sous groupes de $GL_n(\mathbb{R})$

Thm 46 : (Cartan – Von Neumann)
Tout sous groupe fermé de $GL_n(\mathbb{R})$ est une sous variété de $\mathbb{R}^{n^2}$

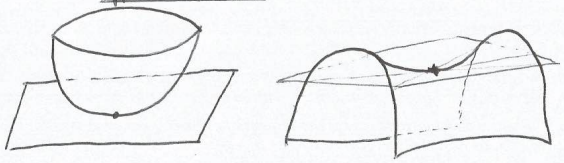
DEV 3

Ex 47 : On peut illustrer ce théorème grâce au tableau en annexe regroupant les résultats pour les sous groupe fermés de $GL_n(\mathbb{R})$ suivants
$GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$, $O_n(\mathbb{R})$, $Sp_{2n}(\mathbb{R})$ et $O(p,q)$

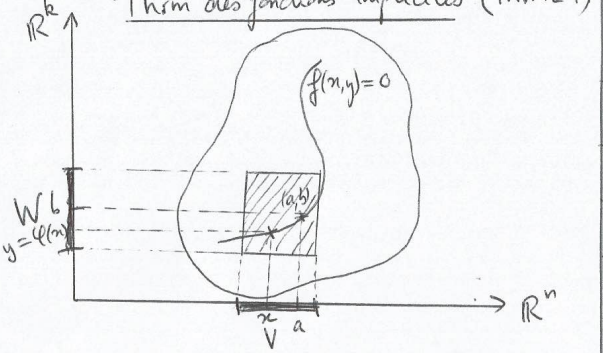
Thm d'inversion locale (Thm 1)



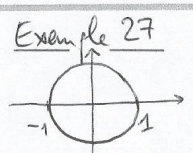
Application 15



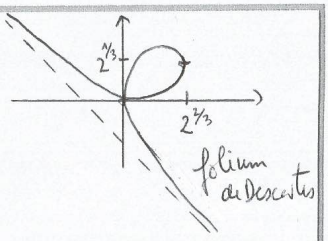
Thm des fonctions implicites (Thm 24)



Exemple 27



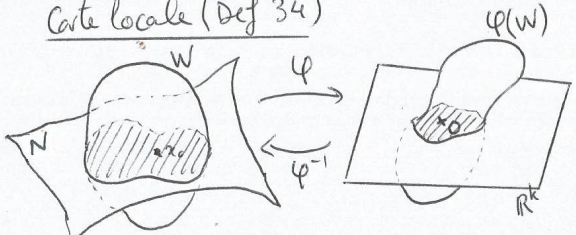
cercle



folium de Descartes

sous variétés.

Carte locale (Def 34)



Ex 47 : Illustration de Cartan Von Neumann

ssgp fermé de $GL_n(\mathbb{R})$ G	submersion F tq $G = F^{-1}(\{0\})$	différentielle de F dF_{I_n}	espace tangent en I_n $T_{I_n}G$	dimension
$GL_n(\mathbb{R})$	0	0	$\mathcal{M}_n(\mathbb{R})$	n^2
$SL_n(\mathbb{R})$	$\det - 1$	tr	$\mathfrak{sl}_n(\mathbb{R}) = \{\mathrm{tr}M = 0\}$	$n^2 - 1$
$O_n(\mathbb{R})$	$F(M) = {}^tMM - I_n$	$dF_{I_n}.H = H + {}^tH$	$\mathfrak{o}_n(\mathbb{R}) = \mathcal{A}_n(\mathbb{R})$	$\frac{n(n-1)}{2}$
$Sp_{2n}(\mathbb{R})$	$F(M) = {}^tMJM - J$	$dF_{I_n}.H = JH + {}^tHJ$	$\mathfrak{sp}_{2n}(\mathbb{R}) = {}^tJ\mathcal{S}_{2n}(\mathbb{R})$	$\frac{2n(2n+1)}{2}$
$O(p,q)$	$F(M) = {}^tMI_{pq}M - I_{pq}$	$dF_{I_n}.H = I_{pq}H + {}^tHI_{pq}$	$\mathfrak{o}_{p,q} = \{I_{pq}H + {}^tHI_{pq} = 0\}$	$\frac{(p+q)(p+q-1)}{2}$

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

Motivations : La notion d'itération est utilisée par Archimède pour approcher la valeur de π. Gauss et Cauchy (XIX°siècle) formalisent les concepts de suite, de limite, et de convergence.

Cadre : Sauf précision contraire, les suites considérées sont à valeurs dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I) Convergence

Déf 1 : une suite réelle $(u_n)_{n\in\mathbb{N}}$ est dite **convergente** vers $\ell \in \mathbb{R}$ si :

$$\forall \varepsilon > 0,\ \exists n_0 \in \mathbb{N} \ /\ \forall n \geq n_0,\ |u_n - \ell| < \varepsilon$$

- une suite complexe $(z_n)_{n\in\mathbb{N}}$ converge vers $x+iy$, $(x,y)\in\mathbb{R}^2$ si
  (i) $z_n = x_n + i y_n$ où $(x_n)_{\mathbb{N}}$ et $(y_n)_{\mathbb{N}}$ sont des suites réelles.
  (ii) $(x_n)_{n\in\mathbb{N}}$ converge vers x.
  (iii) $(y_n)_{n\in\mathbb{N}}$ converge vers y.

ex 2 : $\left(u_n = \frac{1}{n}\right)_{n\in\mathbb{N}^*}$ converge vers 0 ; $\left(u_n = e^{in}\right)_{n\in\mathbb{N}}$ ne converge pas.

prop 3 : Si $(u_n)_{n\in\mathbb{N}}$ converge vers $\ell \in K$ et $f : K \to K$ est continue en ℓ, alors la suite $(f(u_n))_{n\in\mathbb{N}}$ converge vers $f(\ell)$.

ex 4 : $f : x \mapsto x^2$ est continue en zéro donc $\left(f(u_n) = \frac{1}{n^2}\right)_{n\in\mathbb{N}^*}$ converge vers $f(0) = 0$.

prop 5 : L'espace des suites convergentes dans $\mathbb{K}$ est un espace vectoriel sur $\mathbb{K}$.

Déf 6 :
- une suite réelle $(u_n)_{n\in\mathbb{N}}$ est dite **monotone** si, pour tout $n \in \mathbb{N}$, $(u_{n+1} - u_n)$ est du même signe que $(u_{n+2} - u_{n+1})$.
- une suite $(z_n)_{n\in\mathbb{N}}$ est **bornée** s'il existe $M > 0$ tel que $\forall n \in \mathbb{N},\ |z_n| \leq M$.

Prop 7 : une suite réelle monotone bornée est convergente.

prop 8 : Soient $(a_n)_{\mathbb{N}}$ et $(b_n)_{\mathbb{N}}$ deux suites réelles > 0 telles que :
(i) $\forall n \in \mathbb{N},\ \frac{a_{n+1}}{a_n} \leq \frac{b_{n+1}}{b_n}$.
(ii) (b_n) est convergente.
Alors (a_n) est convergente.

ex 9 : $(n)_{\mathbb{N}}$ est monotone, non-bornée ; $\left((-1)^n\right)_{\mathbb{N}}$ est bornée, non-monotone.

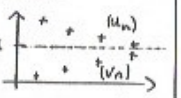
Déf 10 : $(u_n)_{\mathbb{N}}$ est de **Cauchy** dans $\mathbb{K}$ si

$$\forall \varepsilon > 0,\ \exists n_0 \in \mathbb{N} \ /\ \forall p,q \geq n_0,\ |u_p - u_q| < \varepsilon$$

prop 11 : Toute suite de Cauchy dans $\mathbb{K}$ converge.

Déf 12 : Deux suites réelles $(u_n)_{\mathbb{N}}$ et $(v_n)_{\mathbb{N}}$ sont **adjacentes** si :
(i) $(u_n)_{\mathbb{N}}$ est décroissante et $(v_n)_{\mathbb{N}}$ est croissante.
(ii) $|u_n - v_n| \underset{n\to\infty}{\longrightarrow} 0$

ex 13 : $\left(1+\frac{1}{n}\right)_{\mathbb{N}^*}$ et $\left(1-\frac{1}{n}\right)_{\mathbb{N}^*}$ sont adjacentes.



prop 14 : Deux suites adjacentes convergent vers la même limite.

App 15 : critère spécial des séries alternées.

Déf 16 : Soient $(u_n)_{\mathbb{N}}$ et $(v_n)_{\mathbb{N}}$ deux suites réelles
- $u_n \sim v_n \iff u_n - v_n \underset{n\to\infty}{\longrightarrow} 0$
- $u_n = o(v_n) \iff v_n > 0$ et $\frac{u_n}{v_n} \underset{n\to\infty}{\longrightarrow} 0$
- $u_n = O(v_n) \iff v_n > 0$ et $\exists C \geq 0 \ /\ \forall n \in \mathbb{N},\ \left|\frac{u_n}{v_n}\right| \leq C$

ex 17 : $\frac{1}{n+(-1)^n} \sim \frac{1}{n}$

App 18 : Formule de Stirling $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$

App 19 : Convergence géométrique dans le théorème de point fixe de Picard : $|x_n - \ell| = O(k^n)$

II) Valeurs d'adhérence.

Déf 20 : la **borne supérieure** d'une suite réelle est le plus petit de ses majorants $\sup_{n\geq 0}(u_n) \in \mathbb{R} \cup \{+\infty\}$

la **borne inférieure** d'une suite réelle est le plus grand de ses minorants. $\inf_{n\geq 0}(u_n) \in \mathbb{R} \cup \{-\infty\}$

ex 21 : $\sup_{n\geq 0}(n) = +\infty$; $\inf_{n\geq 0}\left((-1)^n\right) = -1$

Déf 22 :
- $\liminf_{n\to\infty}(u_n) := \sup_{k\in\mathbb{N}} \inf_{n\geq k}(u_n) \in \mathbb{R} \cup \{\pm\infty\}$
- $\limsup_{n\to\infty}(u_n) := \inf_{k\in\mathbb{N}} \sup_{n\geq k}(u_n) \in \mathbb{R} \cup \{\pm\infty\}$

ex 23 : $u_0 = -4$; $u_{n\geq 1} = \frac{1}{n}$. Alors $\liminf_{n\to\infty}(u_n) = -4$; $\limsup_{n\to\infty}(u_n) = 0$

prop 24 : $\liminf_{n\to\infty}(u_n) \leq \limsup_{n\to\infty}(u_n)$ et l'égalité caractérise la convergence.

Déf 25 : une **sous-suite** de (u_n) est une suite $(u_{\varphi(n)})$ où $\varphi : \mathbb{N} \to \mathbb{N}$ est strictement croissante.

ex 26 : La suite (u_{2n}) est une sous-suite de (u_n)

App 27 : Critère d'Hadamard pour les séries entières $\frac{1}{R} = \limsup_{n\to\infty} |a_n|^{\frac{1}{n}}$

Déf 28 : une **valeur d'adhérence** est la limite d'une sous-suite $(u_{\varphi(n)})$

ex 30 : $\mathrm{Adh}\left((-1)^n\right) = \{-1, +1\}$; $\mathrm{Adh}\left(e^{in}\right) = \mathbb{U}$

$\liminf_{n\to\infty}(u_n)$, $\limsup_{n\to\infty}(u_n) \in \mathrm{Adh}(u_n)$

prop 31 : Si $u_n \underset{n\to\infty}{\longrightarrow} \ell$, Alors $\mathrm{Adh}(u_n) = \{\ell\}$

Rq 32 : la réciproque est fausse, sauf pour une suite de Cauchy.
Contre-exemple : $u_n = n + (-1)^n n$

Thm 33 : (Bolzano-Weierstrass). De toute suite bornée de $\mathbb{K}$ on peut extraire une sous-suite convergente.

App 34 : Principe des compacts décroissants.

III) Applications importantes

* Quelques familles de suites classiques :

- **Suites arithmétiques.** $u_{n+1} = u_n + a$, $a \in \mathbb{K}$.
On a alors $u_n = u_0 + n.a$ pour $n \in \mathbb{N}$.
- **Suites géométriques.** $u_{n+1} = q.u_n$, $q \in \mathbb{K}$.
On a alors $u_n = q^n.u_0$. $|q| < 1 \Rightarrow u_n \underset{n\to\infty}{\longrightarrow} 0$

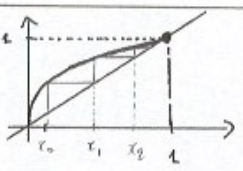
Déf 35 : **suites récurrentes d'ordre 1** $u_{n+1} = f(u_n)$

prop 36 : Si une suite récurrente (u_n) converge vers une limite $\ell \in \mathbb{K}$, alors ℓ est un point fixe de f : $f(\ell) = \ell$.

prop 37 : Si $I \subseteq \mathbb{R}$ est un intervalle stable pour f et que $u_0 \in I$,
(i) Si f est croissante, $(u_n)_{\mathbb{N}}$ est monotone.
(ii) Si f est décroissante, $(u_{2n})_{\mathbb{N}}$ et $(u_{2n+1})_{\mathbb{N}}$ sont monotones, de monotonie opposée.

ex 38 : $f : x \mapsto \sqrt{x}$

$I = [0;1]$. Alors $x_n \xrightarrow[n\to\infty]{} 1$



App 39 : Méthode de Newton

$I = [c;d]$. $x_0 \in I$. $x_{n+1} = x_n - \dfrac{f(x_n)}{f'(x_n)}$

(i) On suppose que $f \in C^2(I,\mathbb{R})$, $f(a)=0$ et $f'(a) \neq 0$. Alors il existe $\eta > 0$ tel que pour $|a - x_0| < \eta$, la suite $(x_n)_{\mathbb{N}}$ converge vers a hypergéométriquement : il existe $k \in [0;1[$ tq :

$$x_n = a + O(k^{2^n})$$

(ii) On suppose, de plus, f convexe sur I.
Alors le résultat est vrai pour tout $x_0 \in [a;d]$

DVP 1

IV] Convergence au sens de Césàro

Thm 40 : (Cesàro)

Si $u_n \xrightarrow[n\to\infty]{} \ell$, alors $\frac{1}{n}\sum_{k=1}^{n} u_k \xrightarrow[n\to\infty]{} \ell$

Rq 41 : le résultat est vrai pour $\ell = \pm\infty$

ex 42 : $u_n = (-1)^n$ converge en moyenne vers 0.

Thm 43 : (réciproque partielle)

Si la suite $(u_n)_{\mathbb{N}^*}$ converge en moyenne vers ℓ, et que $u_n = \sum_{k=1}^{n} a_n$, avec $a_n = O(\frac{1}{n})$

Alors $u_n \xrightarrow[n\to\infty]{} \ell$

DVP 2

App 44 : Soit $a_n > 0$ une suite réelle tq :

$$\frac{a_{n+1}}{a_n} \xrightarrow[n\to\infty]{} \ell$$

Alors $\sqrt[n]{a_n} \xrightarrow[n\to\infty]{} \ell$

App 45 : Régularisation du noyau de Dirichlet

- $\|D_N\|_{L^2} \xrightarrow[N\to\infty]{} +\infty$ et $\|K_N\|_{L^2} = 1$
- si $f \in C^0_{2\pi}$ et que sa série de Fourier converge simplement, alors $f = \sum_{n\in\mathbb{Z}} c_n(f)\, e^{int}$

Références :
- Gourdon - Analyse (voir le Thm taubérien de Hardy - problème 22 page 289).
- Cassini Analyse 1 (réciproque partielle de Cesàro)
- Rombaldi (Méthode de Newton).
- Combes - suites et séries.

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

I Suites récurrentes : cadre

1) Définitions

Def 1 : Soient (E,d) un espace métrique, $h \in \mathbb{N}^*$
Une suite $(u_n)_{n\in\mathbb{N}}$ à valeurs dans E est dite récurrente d'ordre h si on peut écrire
$\forall n \geq h$, $u_n = f(u_{n-1}, u_{n-2}, \dots, u_{n-h})$
où f est une application de E^h dans E

Ex 2 : La suite de Fibonacci $u_0 = 1$ $u_1 = 1$
$u_{n+2} = u_{n+1} + u_n$ $\forall n \in \mathbb{N}$ est récurrente d'ordre 2

Prop 3 : Dans le même cadre, si $(u_n)_{n\in\mathbb{N}}$ converge vers ℓ et que f est continue au point $(\ell, \ell, \dots, \ell)$
alors on a $\ell = f(\ell, \ell, \dots, \ell)$
on dit que ℓ est un point fixe de f

Contre-ex 4 : pour $f(x) = -x$ sur $[-1;1]$
$u_0 \neq 0$ la suite $u_{n+1} = f(u_n)$ est divergente

Rmq 5 : Pour toute suite récurrente d'ordre h on peut se ramener à une suite récurrente vectorielle d'ordre 1.
$\forall n \geq h$ $X_n = \begin{pmatrix} u_{n-h+1} \\ u_{n-h+2} \\ \vdots \\ u_n \end{pmatrix}$ avec $\tilde{f} : E^h \to E^h$, $(u_{n-h+1}, \dots, u_n) \mapsto (u_{n-h+2}, \dots, u_n, f(u_{n-h+1}, \dots, u_n))$

Ex 6 : La suite de Fibonacci peut s'écrire
$X_n = A X_{n-1}$ où $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ $X_n = \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix}$

Prop 7 : I intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$ avec $f(I) \subset I$
Soit $u_{n+1} = f(u_n)$ $\forall n \in \mathbb{N}$ avec $u_0 \in I$
- Si f est croissante, $(u_n)_{n\in\mathbb{N}}$ est monotone et son sens est donné par le signe de $u_1 - u_0$
- Si f est décroissante, $(u_{2n})_{n\in\mathbb{N}}$ et $(u_{2n+1})_{n\in\mathbb{N}}$ sont de monotonie opposée.

Ex 8 : $f(x) = x+1$ (u_n) est croissante $u_0 = 0$

2) Exemples de suites classiques sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$

- **arithmétique** : pour $f(x) = x + a$ $a \in \mathbb{K}$
on a $u_{n+1} = u_n + a$ $\forall n \in \mathbb{N}$ d'où $u_n = u_0 + na$ $\forall n \in \mathbb{N}$
- **géométrique** : pour $f(x) = qx$ $q \in \mathbb{K}$
on a $u_{n+1} = q u_n$ d'où $u_n = q^n u_0$ $\forall n \in \mathbb{N}$
Si $|q| < 1$ il y a convergence de (u_n)
Si $|q| > 1$ il y a divergence de (u_n)
Si $q = 1$ il y a convergence car constante $= 1$.
- **récurrente linéaire à coefficients constants** :

Def 9 : (u_n) est une suite récurrente linéaire d'ordre h à coefficients constants si
$\forall n \geq h$ $u_n = a_1 u_{n-1} + a_2 u_{n-2} + \dots + a_h u_{n-h}$ $(a_i \in \mathbb{K})$ $i \leq h$

Rmq 10 : On peut se ramener à une suite vectorielle récurrente d'ordre 1
de la forme $X_n = A X_{n-1}$ où $A \in \mathcal{M}_h(\mathbb{K})$

Ex 11 : Convergence de polygône vers l'isobarycentre
voir annexe 1

3) Théorèmes du point fixe.

Thm 12 : Si f est une fonction croissant de $I = [a,b]$ dans I, elle admet alors au moins un pt fixe $\alpha \in I$.

Thm 13 : Une fonction continue de $[a;b]$ dans $[a;b]$ admet au moins un point fixe

Thm 14 : Soit E un espace de Banach
et $f : E \to E$ contractante (k constante de Lipschitz)
Alors f admet un unique point fixe dans E
et pour tout $u_0 \in E$ la suite définie par $u_{n+1} = f(u_n)$ converge vers a géométriquement, i.e
$\forall n \in \mathbb{N}$ $\|x_n - a\| \leq \frac{k^n}{1-k} \|x_0 - a\|$

Rmq 15 : Si E est compact et que l'on a $\|f(x) - f(y)\| < \|x - y\|$ $\forall x, y \in E$
on a aussi unicité et existence du point fixe.

Appli 16 : Thm de Cauchy Lipschitz pour les équations différentielles

II Recherche de zéros d'une fonction

1) Dichotomie

Thm 17 : Soit $f \in \mathcal{C}(I, \mathbb{R})$ telle que f ne s'annule qu'une seule fois en a sur I. Alors on peut approcher a par dichotomie.

Algo 18 : tant que $|a_n - b_n| > \varepsilon$
$c = \frac{a_n + b_n}{2}$
si $f(a_n) f(c) < 0$: $b_{n+1} = c$, $a_{n+1} = a_n$
si $f(b_n) f(c) < 0$: $a_{n+1} = c$, $b_{n+1} = b_n$
sinon $a_{n+1} = b_n = c$
$b_{n+1} = c$

voir Annexe 2

convergence en $\ln(n)$

2) Méthode de Newton

voir Annexe 3

Thm 19 : Si $f \in \mathcal{C}^2(I)$, $a \in \mathring{I}$ / $f(a) = 0$ et $f'(a) \neq 0$, alors pour tout u_0 "assez proche" de a, la suite
$u_{n+1} = g(u_n) = u_n - \frac{f(u_n)}{f'(u_n)}$
converge vers a quadratiquement.

Thm 20 : Si, de plus, f est convexe et $f'(a) > 0$
alors (u_n) converge quadratiquement $\forall u_0 \in]a, r_0[\cap I$

DEV 1

Ex 21 : On peut approcher la racine p-ième d'un réel $\alpha > 0$ en utilisant $f(x) = x^p - \alpha$
et $u_0 > 0$ $u_{n+1} = \frac{1}{p}\left((p-1)u_n + \frac{\alpha}{u_n^{p-1}}\right)$

Rmq 22 : on peut appliquer Newton en dimension supérieure
avec $g(X_n) = X_n - (df(x_n))^{-1} \circ f(X_n)$

III Recherche de solutions de $AX = B$

Soit $A \in GL_n(\mathbb{R})$, $B \in \mathbb{R}^n$
On veut décomposer A comme $M - N$ avec M inversible
on pose $M X_{k+1} = N X_k + B$ pour $X_0 \in \mathbb{R}^n$ $\forall k \in \mathbb{N}$

Rmq 23 : Si (X_k) converge vers $\bar{X}$ alors $\bar{X}$ est solution du système $AX = B$

Thm 24 : Il y a équivalence entre :
$\rho(M^{-1}N) < 1$ où ρ est le rayon spectral
et (X_k) converge quelque soit $X_0 \in \mathbb{R}^n$

$A = D - E - F$ où D est la diagonale de A
E est l'opposé de la partie strictement inférieur
F est l'opposé de la partie strictement supérieur

- **Méthode de Jacobi**
  $M = D$ et $N = E + F$
- **Méthode de Gauss Seidel**
  $M = D - E$ et $N = F$
- **Méthode de relaxation**
  Soit $\omega \in \mathbb{R}^+$ $M = \frac{D}{\omega} - E$ et $N = \frac{1-\omega}{\omega} D + F$

2) Méthode du gradient à pas optimal

Thm 25 : $A\bar{X} = B \iff \bar{X}$ minimise la fonctionnelle $f : \mathbb{R}^n \to \mathbb{R}$, $X \mapsto \frac{1}{2}\langle AX, X\rangle - \langle B, X\rangle$

Algo 26 : pour X_0, on note $R_0 = AX_0 - B$
tant que $\frac{\|R_k\|}{\|R_0\|} > \varepsilon$ faire

- $\alpha_{k+1} = \frac{\|R_k\|^2}{\|R_k\|_A^2}$ où $\|X\|_A^2 = \langle AX, X\rangle$
- $X_{k+1} = X_k - \alpha_{k+1} R_k$
- $R_{k+1} = AX_{k+1} - B$

Thm 27 : Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$, $X_0 \in \mathbb{R}^n$
La suite (x_k) définie par l'algo 26 converge vers $\bar{X}$ solution de $AX = B$
et $\forall k \in \mathbb{N}$ $\|X_k\| \leq \sqrt{\text{cond}_2(A)} \left(\frac{\text{cond}(A)-1}{\text{cond}(A)+1}\right)^k \|X_0 - \bar{X}\|$

DEV 2

IV Recherche de solutions approchées d'équations différentielles.

1) Schéma d'Euler explicite

Soit (E) $\begin{cases} y' = f(t,y) \\ y(t_0) = y_0 \end{cases}$ une équation différentielle avec conditions initiales sur $[t_0, t_0+T]$

On discrétise $[t_0, t_0+T]$ en notant $h = \frac{T}{m}$ le pas
on a $t_i = t_0 + ih$ avec $t_m = t_0 + T$.
On approche la solution de (E) par la suite (y_n) définie par

$$y_{n+1} = y_n + h f(t_n, y_n)$$

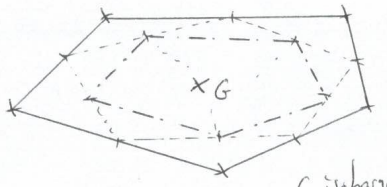
2) Schéma d'Euler implicite

Dans le même cadre, on posera

$$\tilde{y}_{n+1} = \tilde{y}_n + h f(t_{n+1}, \tilde{y}_{n+1}) \quad \forall n \in \mathbb{N}$$

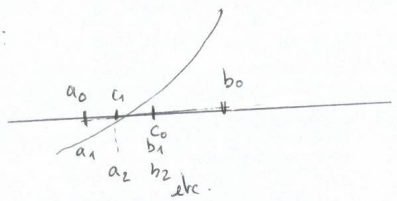
Le schéma d'Euler implicite est plus proche de la solution réelle (l'erreur est moins grande) mais on a une équation à résoudre à chaque itération car dans l'expression de $\tilde{y}_{n+1}$, $\tilde{y}_{n+1}$ apparaît.

Annexe 1 :

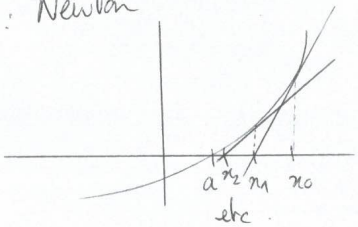


G isobarycentre

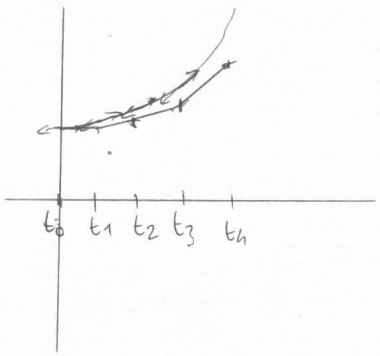
Annexe 2 :



Annexe 3 : Newton



Annexe 4 : Euler explicite



Analyse numérique matriciel : résolution approchée de systèmes linéaires. Recherche de vecteurs propres. Applications

233

I Outils matriciels

Def 1 : Soit $\|.\|$ une norme sur $\mathcal{M}_n(\mathbb{K})$. On dit que c'est une norme matricielle si elle vérifie
$\forall A,B \in \mathcal{M}_n(\mathbb{K}) \quad \|AB\| \leq \|A\|\|B\|$

Exo 2 : La norme de Frobenius $\|A\|_F = \sqrt{\sum_{i,j}(a_{ij})^2}$ est une norme matricielle.

Contre exemple 3 : $\|A\| = \max_{1\leq i,j\leq n} |a_{ij}|$ n'est pas matricielle.

Def 4 : Soit $\|.\|$ une norme sur $\mathbb{K}^n$. On lui associe sa norme subordonnée définie par
$$\|A\| = \sup_{\substack{x\neq 0 \\ x\in\mathbb{K}^n}} \frac{\|Ax\|}{\|x\|}$$

Prop 5 : Une norme subordonnée est une norme matricielle

Rmq 6 : il existe des normes matricielles non subordonnée comme $\|.\|_F$.

Def 7 : Soit A une matrice dans $\mathcal{M}_n(\mathbb{C})$. On appelle rayon spectral de A (noté $\rho(A)$), le maximum des modules des valeurs propres de A.

Prop 8 : On a $\rho(A) = \lim_{k\to+\infty} (\|A^k\|)^{1/k}$ pour $\|.\|$ une norme matricielle.

Def 9 : Pour une norme matricielle subordonnée $\|.\|$, on appelle conditionnement de $A \in \mathcal{M}_n(\mathbb{C})$, la valeur
$$\text{cond}_{\|.\|}(A) = \|A\|\,\|A^{-1}\|$$

Prop 10 : Soit $A \in \mathcal{M}_n(\mathbb{C})$
(i) $\text{cond}(A) = \text{cond}(A^{-1}) = \text{cond}(\alpha A) \quad \forall \alpha \neq 0$
(ii) $\text{cond}_2(A) = \rho(A)\rho(A^{-1}) = \frac{|\lambda_{max}(A)|}{|\lambda_{min}(A)|}$

II Systèmes linéaires

On veut résoudre $Ax = b$ avec $A \in \mathcal{M}_n(\mathbb{K})$, $b \in \mathbb{K}^n$

1) Méthode directe

* Pivot de Gauss

Thm 11 : Pour A matrice carrée, il existe au moins une matrice inversible M telle que $T = MA$ soit triangulaire supérieure.

Rmq 12 : On peut trouver T en appliquant des dilatations et des transvections aux lignes de A.

Pour résoudre $Ax = b$ il suffit ensuite de remonter les égalités car $Tx = Mb$ $\left(\begin{array}{|c|}\hline \square \\ \hline \end{array}\right)\left(\begin{array}{|c|}\hline x \\ \hline \end{array}\right) = \left(\begin{array}{|c|}\hline \\ \hline \end{array}\right)$

* Méthode LU

Thm 13 : Soit $A \in \mathcal{M}_n(\mathbb{K})$ dont toutes les sous matrices diagonales d'ordre k soient inversibles. Il existe un unique couple de matrices (L, U) avec U triangulaire supérieure et L triangulaire inférieure tel que $A = LU$

Rmq 14 : on doit résoudre $LUx = b$ on trouve déjà y tel que $Ly = b$ puis on résout $Ux = y$ pour avoir x

* Méthode QR

Thm 15 : Soit A réelle inversible. Il existe un unique couple (Q,R) où Q est une matrice orthogonale et R une matrice triangulaire supérieure dont tous les éléments diagonaux sont tous positifs tel que $A = QR$

Rmq 16 : on doit résoudre $QRx = b$ or $Q^{-1} = Q^*$ d'où $Rx = Q^*b$ et R triangulaire donc comme pour le pivot on remonte les égalités.

2) Problème des moindres carrés

On veut trouver une solution x la plus fidèle possible à un problème $Ax = b$ qui n'a pas de solution.

Problème de minimisation : (voir Annexe 1)

$$(*) \quad \|b - Ax\|_n = \min_{y\in\mathbb{R}^p} \|b - Ay\|_n \quad \text{pour } A \in \mathcal{M}_{n,p}(\mathbb{R})$$

Prop 17 : Il existe un solution $x \in \mathbb{R}^p$ du problème $(*)$ ssi x satisfait $A^*Ax = A^*b$

Thm 18 : Pour tout $A \in \mathcal{M}_{n,p}(\mathbb{R})$, il existe toujours au moins une solution à $A^*Ax = A^*b$
De plus, elle est unique ssi $\ker A = \{0\}$ et $x = (A^*A)^{-1}A^*b$.

3) Méthodes itératives

Def 20 : Soit A inversible, on appelle décomposition régulière de A un couple de matrices (M,N) avec M inversible tel que $A = M - N$

L'idée générale est de construire la suite
$$Mx^{(k+1)} = Nx^{(k)} + b \quad \forall k \text{ avec } x_0 \in \mathbb{R}^n \quad (**)$$
donc il faut (dans la pratique) que M soit beaucoup plus facile à inverser que A.
Par passage à la limite on a $(M-N)x = b$.

Def 21 : On dit qu'une méthode itérative converge si $\forall x_0 \in \mathbb{R}^n$ la suite (x_k) converge vers la solution exacte x.

Thm 22 : La méthode $(**)$ converge ssi $\rho(M^{-1}N) < 1$.

* Méthode de Jacobi

On associe $M = D$ diagonale de A et $N = D - A$

Avantage : M^{-1} est facile à calculer

Inconvénient : pour calculer $x^{(k+1)}$ il faut toutes les composantes de $x^{(k)}$

* Méthode de Gauss-Seidel

On associe $M = D - E$ où $-E$ est la partie inférieure (triangulaire) de A et $N = F$ la partie triangulaire supérieure de A

Avantage : $x^{(k+1)}$ se calcule sans utiliser toutes les composantes de $x^{(k)}$ à chaque fois

Inconvénient : Π^{-1} moins facile à calculer (mais grand même triangulaire)

* Méthode de relaxation

Soit $\omega \in \mathbb{R}^+$ on associe $M = \frac{D}{\omega} - E$
$$N = \frac{1-\omega}{\omega}D + F$$

Remarque 23 : pour $\omega = 1$ on retrouve Gauss Seidel

Thm 24 : Soit A une matrice hermitienne définie positive Alors $\forall \omega \in]0;2[$, la méthode de relaxation converge

Thm 25 : Pour tout A, la méthode de relaxation ne converge que si $\omega \in]0;2[$.

III Recherche de valeurs propres.

Méthode la puissance

Thm 26 : Soit A diagonalisable de valeurs propres réelles $(\lambda_1 - \lambda_n)$ / $|\lambda_1| \leq |\lambda_2| \leq \ldots \leq |\lambda_{n-1}| < \lambda_n$
Alors pour tout $x_0 \in \mathbb{R}^n$ / $\|x_0\| = 1$, l'algorithme suivant

Pour $k \geq 1$ et $\|x_k - x_{k-1}\| \leq \varepsilon$
$y_k = A x_{k-1}$
$x_k = y_k / \|y_k\|$
$a = \|y_k\|$

Entrée : A
Sortie : $a \simeq \lambda_n$, $x_k \simeq e_n$

converge, et ainsi $\lim_{k \to +\infty} \|y_k\| = \lambda_n$ et $\lim x_k = x_\infty$

où $x_\infty = \pm e_n$ vecteur propre associé à λ_n.

Rmq 27 : On peut adapter l'algorithme pour trouver la valeur propre de plus petit module en considérant A^{-1}.
On appelle cela la méthode de la puissance inverse.

IV Analyse fonctionnelle

1) Optimisation d'une fonctionnelle

* Méthode du gradient à pas optimal

On veut trouver un minimum d'une fonctionnelle J, $J : \mathbb{R}^n \to \mathbb{R}$
on veut donc résoudre

$$\begin{cases} J(u_k) - \rho(u_k) \nabla J(u_k) = \inf_{\rho \in \mathbb{R}} J(u_k - \rho \nabla J(u_k)) \\ u_{k+1} = u_k - \rho(u_k) \nabla J(u_k) \end{cases}$$

Thm 28 : Si J est elliptique, i.e. $\exists \alpha > 0, \langle \nabla J(u) - \nabla J(v), u - v \rangle \geq \alpha \|u - v\|^2 \quad \forall u, v \in \mathbb{R}^n$
Alors la méthode du gradient à pas optimal converge.

Rmq 29 : Toutes les méthodes de type gradient
i.e. $u_{k+1} = u_k - \rho_k \nabla J(u_k)$
veulent résoudre : Trouver $u \in \mathbb{R}^n$ tel que $J(u) = \inf_{v \in \mathbb{R}^n} J(v)$

2) Résolution approchée d'équations différentielles.

On veut approcher la solution de l'équation différentielle

$$\begin{cases} y' = f(t, y) \text{ sur } I \text{ borné} \\ y(t_0) = y_0 \end{cases} \quad (***)$$

* Schéma d'Euler explicite

Soit $t_0 < t_1 < \dots < t_m$ une subdivision de I
on pose la suite $\begin{cases} \tilde{y}_0 = y_0 \\ \tilde{y}_{n+1} = \tilde{y}_n + (t_{n+1} - t_n) f(t_n, \tilde{y}_n) \end{cases}$

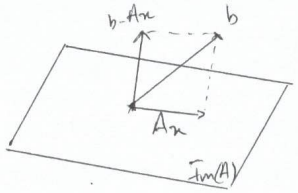
Thm 30 : Soit y la solution de $(***)$ telle que $y \in C^2(I)$
Supposons qu'il existe $\varepsilon > 0$, $L \in \mathbb{R}$ tels que
$\forall t \in I$, $\forall \tilde{y} \in \mathbb{R}^m$ avec $|\tilde{y} - y(t)| \leq \varepsilon$, $|f(t, \tilde{y}) - f(t, y(t))| \leq L |\tilde{y} - y(t)|$
Alors il existe $h^* > 0$ tel que $\forall 0 < h \leq h^*$ et $\forall n \in [\![0, m]\!]$
on ait $|y(t_n) - \tilde{y}_n| \leq h \int_{t_0}^{t_n} e^{L(t_n - s)} |y''(s)| \, ds$.

* Schéma d'Euler implicite

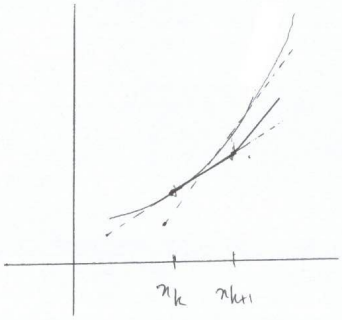
La suite que l'on pose est :

$$\begin{cases} \tilde{y}_0 = y_0 \\ \tilde{y}_{n+1} = \tilde{y}_n + (t_{n+1} - t_n) f(t_{n+1}, \tilde{y}_{n+1}) \end{cases}$$

Rmq 31 : plus difficile à calculer en pratique
mais une meilleure majoration de l'erreur.



Annexe 1 : moindres carrés



Annexe 2 : Euler explicite

243: Power Series : convergence and properties. Examples and Applications.

* Motivations : generalize polynomials, show smoothness, solve ODE, generating function..

I] Definition and first properties.

1) Convergences : the radius of convergence.

def 1 : a power series is a formal series $\sum_{n\in\mathbb{N}} a_n z^n$ where $(a_n)_{\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ and the variable $z \in \mathbb{C}$.

def-thm 2 : the radius of convergence of a power series $\sum_{n\in\mathbb{N}} a_n z^n$ is defined equivalently by :

- $R = \sup\{r \geq 0 \ / \$ the sequence $|a_n| r^n$ is bounded$\}$
- $R = \sup\{r \geq 0 \ / \sum_{n\in\mathbb{N}} a_n z^n$ converges absolutely for $|z| \leq r\}$
- $R = \sup\{r \geq 0 \ / \sum_{n\in\mathbb{N}} a_n z^n$ converges normally on $B(0,r)\}$
- $R = \inf\{r \geq 0 \ / \ \forall |z| > r, \sum_{n\in\mathbb{N}} a_n z^n$ diverges$\}$

ex 3 : polynomials are power series with radius $R = +\infty$.
$\sum_{n\in\mathbb{N}} z^n$ has radius 1 ; $\sum_{n\in\mathbb{N}} n!\, z^n$ has radius 0.

prop 4 : (d'Alembert, Cauchy-Hadamard)

- ratio test : if $\lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right| = \lambda$, the radius of $\sum_{n\in\mathbb{N}} a_n z^n$ is $\frac{1}{\lambda}$.
- n^{th}-root test : if $\lim_{n\to\infty} \sqrt[n]{|a_n|} = \lambda$, the radius of $\sum_{n\in\mathbb{N}} a_n z^n$ is $\frac{1}{\lambda}$.

ex 5 : $\sum_{n\in\mathbb{N}} \frac{z^n}{n!}$ has radius $+\infty$. We define $\exp(z) = \sum_{n=0}^{+\infty} \frac{z^n}{n!}$

$\forall \alpha \in \mathbb{R}$, $\sum_{n\in\mathbb{N}} n^\alpha z^n$ has radius 1.

⚠ The sequence should not satisfy [$u_n = 0$ infinitely often] → we cannot compute the radius of $\sum_{n\in\mathbb{N}} z^{n^2}$ with these tests.

Rq 6 : If the series $\sum_{n\in\mathbb{N}} a_n z^n$ satisfies the ratio-test, then so does it for the n-th root test. The converse is false.

ex 7 : $u_n = \begin{cases} 1/3^n & \text{if } n \text{ is even} \\ 1/3^n & \text{if } n \text{ is odd} \end{cases}$ satisfies $\sqrt[n]{u_n} \to \frac{1}{3} < 1$ but $\frac{u_{n+1}}{u_n} = \begin{cases} 1/3 & \text{(even)} \\ 1/2 & \text{(odd)} \end{cases}$

Rq 8 : To compute usual power series, we use the integral Taylor-Lagrange formula (cf Annex : usual power series).

2) Algebraic operations on power series.

prop 9 : let $\sum_{n\in\mathbb{N}} a_n z^n$ and $\sum_{n\in\mathbb{N}} b_n z^n$ two power series with radius $R, R' > 0$ and sum f, g. Then :

- $\sum_{n\in\mathbb{N}} (a_n + b_n) z^n$ is a power series with radius $R'' \geq \min(R, R')$ and sum $f+g$.
- $\sum_{n\in\mathbb{N}} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) z^n$ is a power series with radius $R'' \geq \min(R, R')$ and sum $f \times g$
- For any $\alpha \in \mathbb{C}^*$, $\sum_{n\in\mathbb{N}} (\alpha a_n) z^n$ is a power series with radius R and sum $\alpha \times f$.
- If $g(0) = 0$, $f \circ g$ has a power series expansion with radius $R'' > 0$.
- If $f(0) \neq 0$, $\frac{1}{f}$ has a power series expansion with radius $R'' > 0$.

ctrex 10 : $\sum_{n\in\mathbb{N}} z^n$ and $\sum_{n\in\mathbb{N}} (-1) z^n$ has radius 1, but their sum satisfies $R'' = +\infty$.

ctrex 11 : Define $u_n = \begin{cases} 2 \text{ if } n = 0 \\ z^n \text{ if } n \geq 1 \end{cases}$ / $v_n = \begin{cases} -1 \text{ if } n = 0 \\ 1 \text{ if } n \geq 1 \end{cases}$
$\sum_{\mathbb{N}} u_n z^n$ has radius $\frac{1}{2}$; $\sum_{\mathbb{N}} v_n z^n$ has radius 1 but the product has infinite radius.

3) Tauberian theorem

Th 12 Let $f(z) = \sum_{n\geq 0} a_n z^n$, with a radius 1 such that $\sum_{n\geq 0} a_n$ converges.
Let $\Theta_0 \in [0, \pi/2[$, we set $\Delta_{\Theta_0} = \{z \in \mathbb{C} : |z| < 1 \} \cap \{1 - \rho e^{i\Theta} ; \rho > 0, \Theta \in]\Theta_0, \Theta_0[\}$.
Then $S(z) \xrightarrow[z\in\Delta_{\Theta_0}]{z\to 1} \sum_{n=0}^{\infty} a_n$.

Cor 13 $\sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} = \pi/4$ and $\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = \ln(2)$

Th 14 Let $f(z) = \sum_{n\geq 0} a_n z^n$, with a radius 1, and we assume there exists $S \in \mathbb{C}$ s.t $f(x) \xrightarrow[x\to 1]{} S$. If $a_n = o(\frac{1}{n})$, then $\sum_{n\geq 0} a_n$ converges and $S = \sum_{n=0}^{\infty} a_n$.

Rq 15 : If the series $\sum_{n\in\mathbb{N}} a_n z^n$ satisfies the ratio-test, then so does it for the n-th root test. The converse is false.

ex 16 : $u_n = \begin{cases} 1/3^n & \text{if } n \text{ is even} \\ 1/4^n & \text{if } n \text{ is odd} \end{cases}$ satisfies $\sqrt[n]{u_n} \to \frac{1}{3} < 1$ but $\frac{u_{n+1}}{u_n} = \begin{cases} 1/3 & \text{(even)} \\ 1/12 & \text{(odd)} \end{cases}$

Rq 17 : To compute usual power series, we use the integral Taylor-Lagrange formula (cf Annex : usual power series).

2) Algebraic operations on power series.

prop 18 : let $\sum_{n\in\mathbb{N}} a_n z^n$ and $\sum_{n\in\mathbb{N}} b_n z^n$ two power series with radius $R, R' > 0$ and sum f, g. Then :

- $\sum_{n\in\mathbb{N}} (a_n + b_n) z^n$ is a power series with radius $R'' \geq \min(R, R')$ and sum $f+g$.
- $\sum_{n\in\mathbb{N}} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) z^n$ is a power series with radius $R'' \geq \min(R, R')$ and sum $f \times g$
- For any $\alpha \in \mathbb{C}^*$, $\sum_{n\in\mathbb{N}} (\alpha a_n) z^n$ is a power series with radius R and sum $\alpha \times f$.
- If $g(0) = 0$, $f \circ g$ has a power series expansion with radius $R'' > 0$.
- If $f(0) \neq 0$, $\frac{1}{f}$ has a power series expansion with radius $R'' > 0$.

ctrex 19 : $\sum_{n\in\mathbb{N}} z^n$ and $\sum_{n\in\mathbb{N}} (-1) z^n$ has radius 1, but their sum satisfies $R'' = +\infty$.

ctrex 20 : Define $u_n = \begin{cases} 2 \text{ if } n = 0 \\ z^n \text{ if } n \geq 1 \end{cases}$ / $v_n = \begin{cases} -1 \text{ if } n = 0 \\ 1 \text{ if } n \geq 1 \end{cases}$
$\sum_{\mathbb{N}} u_n z^n$ has radius $\frac{1}{2}$; $\sum_{\mathbb{N}} v_n z^n$ has radius 1 but the product has infinite radius.

3) Tauberian theorem

Th 21 Let $f(z) = \sum_{n\geq 0} a_n z^n$, with a radius 1 such that $\sum_{n\geq 0} a_n$ converges.
Let $\Theta_0 \in [0, \pi/2[$, we set $\Delta_{\Theta_0} = \{z \in \mathbb{C} : |z| < 1 \} \cap \{1 - \rho e^{i\Theta} ; \rho > 0, \Theta \in]\Theta_0, \Theta_0[\}$.
Then $S(z) \xrightarrow[z\in\Delta_{\Theta_0}]{z\to 1} \sum_{n=0}^{\infty} a_n$.

Cor 22 $\sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} = \pi/4$ and $\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = \ln(2)$

Th 23 Let $f(z) = \sum_{n\geq 0} a_n z^n$, with a radius 1, and we assume there exists $S \in \mathbb{C}$ s.t $f(x) \xrightarrow[x\to 1]{} S$. If $a_n = o(\frac{1}{n})$, then $\sum_{n\geq 0} a_n$ converges and $S = \sum_{n=0}^{\infty} a_n$.

II] Smoothness of the sum and the holomorphic point of view

1) Continuity, derivative and antiderivative

Theorem 24 : The function $z \mapsto \sum_{n=0}^{+\infty} a_n z^n$ is continuous on the convergence disc $\{z \in \mathbb{C}, |z| < R\}$

Example 25 : $z \mapsto \exp(z) = \sum_{n=0}^{+\infty} \frac{z^n}{n!}$ is continuous on $\mathbb{C}$ because $R = +\infty$

Thm 26 : The function $f :]-R;R[\to \mathbb{C}$, $x \mapsto \sum_{n=0}^{+\infty} a_n x^n$ is continuously differentiable

$\sum_{n=1}^{+\infty} n a_n x^{n-1}$ has the same radius than $\sum_{n=0}^{+\infty} a_n x^n$
and $f'(x) = \sum_{n=1}^{+\infty} n a_n x^{n-1}$

Example 27 : $\frac{1}{(1-x)^2} = \sum_{n=0}^{+\infty} (n+1) x^n \quad \forall x \in]-1;1[$

Corollary 28 : The same f is, in fact, infinitely differentiable and all the derivatives have the same radius.
Also $\forall p \in \mathbb{N}$ $a_p = \frac{f^{(p)}(0)}{p!}$ then $\forall z \in \mathbb{C}$ $f(z) = \sum_{p=0}^{+\infty} \frac{f^{(p)}(0)}{p!} z^p$

Thm 29 The function $F :]-R;R[\to \mathbb{C}$, $x \mapsto \sum_{n=0}^{+\infty} \frac{a_n}{n+1} x^{n+1}$ is a primitive of $f :]-R;R[\to \mathbb{C}$, $x \mapsto \sum_{n=0}^{+\infty} a_n x^n$ and F has the same radius R than f.

Example 30 : $-\ln(1-x) = \sum_{n=0}^{+\infty} \frac{x^{n+1}}{n+1} \quad \forall x \in]-1;1[$

2) Real analytic function.

Def 31 Let I be an open interval containing $a \in \mathbb{R}$ and $f : I \to \mathbb{R}$ $\mathcal{C}^\infty$
The power series around the point a given by $\sum_{k=0}^{+\infty} \frac{f^{(k)}(a)}{k!} (x-a)^k$ is called the Taylor series of f around a.

Rmk 32 The Taylor series of f around a converges to $f(a)$ but it may not converge to $f(x)$ for other point $x \in I$ and may be divergent.

Example 33 $f(x) = |x|$ around 1 gives $1 + (x-1)$ not equal to $f(x)$ when $x < 0$

- $f(x) = \begin{cases} e^{-\frac{1}{x^2}} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$ $f^{(k)}(0) = 0 \ \forall k \in \mathbb{N}$ but $f \neq 0$

Def 34 If the Taylor series of f around each point of I converges to $f(x)$ for every $x \in I$ then f is said to be a real analytic function on I.

Example 35
- $f(x) = \exp(x)$ is a real analytic function on $\mathbb{R}$
- $f(x) = \begin{cases} e^{-\frac{1}{x^2}} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$ is not.

3) Links with the holomorphic functions

Thm 36 : $f : D(0,R) \to \mathbb{C}$, $z \mapsto \sum_{n=0}^{+\infty} a_n z^n$ is holomorphic on $D(0,R)$
and analytic on $D(0,R)$
$a \in D(0,R)$, $|z-a| < R - |a| \Rightarrow z \in \Omega$ and $f(z) = \sum_{k=0}^{+\infty} \frac{f^{(k)}(a)}{k!} (z-a)^k$

Thm 37 Let $f(z) = \sum_{n=0}^{+\infty} a_n z^n$ be a power series. If there exists $(z_p)_{\in\mathbb{C}^{\mathbb{N}}}$ such that $z_p \xrightarrow[p\to+\infty]{} 0$ and $f(z_p) = 0$ for all p in $\mathbb{N}$.
Then $a_n = 0$ for all n in $\mathbb{N}$.

Corollary 38 Two power series that are equal on a neighbourhood of zero have the same coefficients.

Thm 39 Let $f(z) = \sum a_n z^n$ be a power series of radius $R > 0$
Then $\forall r \in]0,R[$, $\forall n \in \mathbb{N}$ $2\pi r^n a_n = \int_0^{2\pi} f(re^{i\theta}) e^{-ni\theta} d\theta$

III) Applications.

1) Ordinary differential equations.

App31: The function $f: x \in]-1,1[\mapsto (\text{Arcsin}\, x)^2$ has a power series expansion with positive radius. It satisfies the following equation:

$$(1-x^2) f'(x)^2 = 4 f(x)$$

Then for any $x \in]-1,1[$, $f(x) = \sum_{n=0}^{+\infty} a_n x^n$ with:

$$a_{2n+1} = 0 \quad , \quad a_{2n} = \frac{2^{2n-2}((n-1)!)^2}{n(2n-1)!}$$

Similarly, for any $x \in]0,1[$, $\frac{\text{Arcsin}\sqrt{x}}{\sqrt{x(1-x)}} = \sum_{n=0}^{+\infty} \frac{2^{2n}(n!)^2}{(2n+1)!} x^n$

1st DEV

App32: (Bessel function). Let $J_0 : x \in \mathbb{R} \mapsto \frac{1}{\pi}\int_0^\pi \cos(x \sin\theta)\, d\theta$. Then:

(i) $J_0(x) = \sum_{n=0}^{+\infty} \frac{(-1)^n}{4^n (n!)^2} x^{2n}$

(ii) J_0 is solution of the equation (B) $xy'' + y' + xy = 0$ on $\mathbb{R}$.

(iii) The solutions of (B) on $I_\alpha =]0,\alpha[$ where $\alpha > 1$ and $J_0 \neq 0$ on I satisfy: $\exists C, D \in \mathbb{R} / \forall x \in I_\alpha,\ y(x) = C J_0(x) \int_1^x \frac{dt}{t (J_0(x))^2} + D J_0(x)$

(iv) $\int_1^x \frac{dt}{t(J_0(x))^2} = \ln x + \frac{x^2}{4} + o(x^2)$

thm33: The closure of the sets of polynomials on $\overline{B_c(0,1)}$ with respect to uniform convergence is the set of continuous functions f on $\overline{B_c(0,1)}$ having a power series expansion on $B_c(0,1)$.

2) Combinatorics.

App34: Let $n \in \mathbb{N}$ and D_n be the number of fixed-point-free permutations of $[\![1,n]\!]$. Then: $D_n = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor$

App35: The number of valid parentheses expressions of length $n \in \mathbb{N}$ is $C_n = \frac{1}{n}\binom{2n-2}{n-1}$

App36: (Bell numbers) Let $n \in \mathbb{N}$ and B_n the number of partitions of $[\![1,n]\!]$. Then: $B_n = \frac{1}{e}\sum_{k=0}^{+\infty} \frac{k^n}{k!}$

2nd DEV

3) Power Series in Probability.

Let X be a random variable on $(\Omega, \mathcal{F}, \mathbb{P})$ such that $X(\Omega) \subset \mathbb{N}$.

Def37: The generating function of X is the power series: $G_X(z) = \sum_{n=0}^{\infty} \mathbb{P}(X=n) z^n = \mathbb{E}(z^X)$, with radius ≥ 1.

Prop38: G_X characterises the law of X: $\mathbb{P}_X$.

Prop39: Let $X_1, \dots, X_n$ be independent random variables. Then $G_{X_1+\dots+X_n} = \prod_{k=1}^{n} G_{X_k}$.

Ex40. $X \sim \mathcal{B}(1,p)$: $G_X(z) = 1-p+pz$.

$X \sim \mathcal{B}(n,p)$: $G_X(z) = (1-p+pz)^n$.

$X \sim \mathcal{P}(\lambda)$: $G_X(z) = e^{\lambda(z-1)}$.

Prop41: Let (X,Y) be a random variable with law $\mathcal{P}(\lambda) \otimes \mathcal{P}(\mu)$. Then $X+Y \sim \mathcal{P}(\lambda+\mu)$.

Thm42: $\mathbb{E}(|X|) < \infty$ if and only if G_X has a left-hand derivative at 1^-. In this case: $\mathbb{E}(X) = G_X'(1^-)$.

Thm43: Let $(X_n)_{n\geq 0}$ be iid random variables and N be a random variable independent of $(X_n)_{n\geq 0}$. Let S_N be: $S_N := \sum_{k=0}^{N} X_k$. Then we have: $G_{S_N}(z) = G_N \circ G_{X_1}(z)$.

Prop44: Let $(X_n)_n$ be iid with $X_n \sim \mathcal{B}(1,p)$ and $N \sim \mathcal{P}(\lambda)$ independent of $(X_n)_{n\geq 0}$. Then $S_N = \sum_{k=1}^{N} X_k \sim \mathcal{P}(\lambda p)$.

Thm45: Let $\mu_k := \mathbb{E}(|X|^k)$. If $\limsup_k \frac{(\mu_k)^{1/k}}{k} < \infty$, then the law $\mathbb{P}_X$ is characterized by its moments: $(\mathbb{E}(X^k))_{k\geq 1}$.

Ex46: $\mathcal{N}(0,1)$ is characterized by its moments.

Appendix: Usual power series

$\forall x \in \mathbb{R}$ $e^x = 1 + x + \frac{x^2}{2!} + \dots + \frac{x^n}{n!} + \dots = \sum_{k=0}^{+\infty} \frac{x^k}{k!}$

$\forall x \in \mathbb{R}$ $\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} + \dots + (-1)^p \frac{x^{2p+1}}{(2p+1)!} + \dots = \sum_{k=0}^{+\infty} (-1)^k \frac{x^{2k+1}}{(2k+1)!}$

$\forall x \in \mathbb{R}$ $\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \dots + (-1)^p \frac{x^{2p}}{(2p)!} + \dots = \sum_{k=0}^{+\infty} (-1)^k \frac{x^{2k}}{(2k)!}$

$\forall x \in \mathbb{R}$ $\text{sh}(x) = x + \frac{x^3}{3!} + \frac{x^5}{5!} + \dots + \frac{x^{2p+1}}{(2p+1)!} + \dots = \sum_{k=0}^{+\infty} \frac{x^{2k+1}}{(2k+1)!}$

$\forall x \in \mathbb{R}$ $\text{ch}(x) = 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \dots + \frac{x^{2p}}{(2p)!} + \dots = \sum_{k=0}^{+\infty} \frac{x^{2k}}{(2k)!}$

$\forall x \in]-1,1[$ $(1+x)^\alpha = 1 + \frac{\alpha}{1!}x + \frac{\alpha(\alpha-1)}{2!}x^2 + \dots + \frac{\alpha(\alpha-1)(\alpha-2)\dots(\alpha-n+1)}{n!}x^n + \dots$

In particular:

$$\frac{1}{1-x} = 1 + x + x^2 + \dots + x^n + \dots = \sum_{k=0}^{+\infty} x^k$$

$$\frac{1}{1+x} = 1 - x + x^2 + \dots + (-1)^n x^n + \dots = \sum_{k=0}^{+\infty} (-1)^k x^k$$

$$\sqrt{1+x} = 1 - \frac{1}{2}x + \frac{1\times 3}{2\times 4}x^2 + \dots + (-1)^n \frac{1\times 3 \times \dots \times (2n-1)}{2\times 4 \times \dots \times (2n)} x^n + \dots$$

$\forall x \in]-1,1[$ $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \dots + (-1)^{n-1}\frac{x^n}{n} + \dots = \sum_{k=1}^{+\infty} (-1)^{k-1}\frac{x^k}{k}$

$\forall x \in \mathbb{R}$ $\text{arctan}(x) = x - \frac{x^3}{3} + \frac{x^5}{5} + \dots + (-1)^n \frac{x^{2n+1}}{2n+1} + \dots = \sum_{k=0}^{+\infty} (-1)^k \frac{x^{2k+1}}{2k+1}$

$\forall x \in]-1,1[$ $\text{argth}(x) = x + \frac{x^3}{3} + \frac{x^5}{5} + \dots + \frac{x^{2n+1}}{2n+1} + \dots = \sum_{k=0}^{+\infty} \frac{x^{2k+1}}{2k+1}$

$\forall x \in]-1,1[$ $\text{arcsin}(x) = x + \frac{1}{2\times 3}x^3 + \dots + \frac{1\times 3 \times \dots \times (2n-1)}{2\times 4 \times \dots \times (2n)(2n+1)} x^{2n+1} + \dots$

$\forall x \in]-1,1[$ $\text{argsh}(x) = x - \frac{1}{2\times 3}x^3 + \dots + (-1)^n \frac{1\times 3 \times \dots \times (2n-1)}{2\times 4 \times \dots \times (2n)(2n+1)} x^{2n+1} + \dots$

[Amar Matheron] p. 72 [Jolissaint] p. 23

265 Exemples d'études et d'applications de fonctions usuelles et spéciales

I Fonctions usuelles et variable complexe

1) Exponentielle, sinus et cosinus.

Def 1: On définit l'exponentielle complexe comme $\forall z \in \mathbb{C}$ $e^z = \sum_{n=0}^{+\infty} \frac{z^n}{n!}$ converge normalement sur tout compact de $\mathbb{C}$.

Rmq 2: si $z = x+iy$ où $x, y \in \mathbb{R}$
$e^z = e^x e^{iy} = e^x(\cos y + i \sin y)$

Prop 3: La fonction exponentielle complexe est holomorphe sur $\mathbb{C}$ et $(e^z)' = e^z$.

Prop 4: $\forall z_1, z_2 \in \mathbb{C}$ $e^{z_1+z_2} = e^{z_1} e^{z_2}$
$\forall z \in \mathbb{C}$ $e^z \neq 0$
$\forall z \in \mathbb{C}^*$ $\exists y$ $e^y = z$
$\forall z \in \mathbb{C}$ $e^z = 0 \iff z \in 2i\pi\mathbb{Z}$.

Rmq 5: on peut définir l'exponentielle dans une algèbre de Banach, exemple: exponentielle de matrices.

Def 6: On définit le sinus complexe et le cosinus complexe par $\sin(z) = \frac{e^{iz} - e^{-iz}}{2i}$ et $\cos(z) = \frac{e^{iz} + e^{-iz}}{2}$ $\forall z \in \mathbb{C}$

Prop 7: exp, sin, cos coïncident avec leur définition réelle sur $\mathbb{R}$

Prop 8: $\forall z \in \mathbb{C}$ $\cos(z) = \sum_{n=0}^{+\infty} \frac{z^{2n}}{(2n)!}$ et $\sin(z) = \sum_{n=0}^{+\infty} \frac{z^{2n+1}}{(2n+1)!}$

Rmq 9: $\forall y \in \mathbb{R}$ $\cos(iy) = \mathrm{ch}(y)$ et $\sin(iy) = i\,\mathrm{sh}(y)$ où ch et sh sont les cosinus et sinus hyperboliques

2) Logarithme et détermination.

Def 10: Si $z \in \mathbb{C}^*$ on dit qu'un nombre complexe w est un logarithme de z si $e^w = z$ et que $\theta \in \mathbb{R}$ est un argument de z si $z = |z| e^{i\theta}$.

Ex 11: $z = 1+i$ $\theta = \frac{\pi}{4}$ est un argument de z
$\frac{1}{2}\ln(2) + i\frac{9\pi}{4}$ est un logarithme de z

Rmq 12: il y a une infinité de log et d'argument pour un z fixé

Prop 13: Si θ est un argument de z alors $\ln(|z|) + i\theta$ est un logarithme de z
Si $\log(z)$ est un logarithme de z alors $\mathrm{Im}(\log(z))$ est un argument de z

Def 14: La détermination principale du logarithme est telle que
$\mathrm{Log}(z) = \log(re^{i\theta}) = \ln(r) + i\theta$
où $r \in \mathbb{R}^{+*}$ et $\theta \in]-\pi; \pi[$

Rmq 15: sur $[0; +\infty[$ Log coïncide avec ln.

Prop 16: La fonction Log est holomorphe sur $\mathbb{C} \setminus \mathbb{R}^-$ et $\mathrm{Log}'(x) = \frac{1}{z}$.

Application 17: on peut définir la puissance grâce au Log $z^x = e^{x\log(z)} = e^{x(\ln(r)+i\theta)}$
$= r^x e^{xi\theta}$.

[Gourdon Saulbat] p. 101 [Jolissaint] p. 159

Prop 18: Sur le disque $D(0,1)$ ouvert, on a
$\mathrm{Log}(1-h) = -\sum_{i=1}^{+\infty} \frac{h^i}{i}$ qui converge normalement sur tout compact.

3) Indice et théorème des résidus

Def 19: Soit γ un lacet, et $\Omega = \mathbb{C} \setminus \gamma$
$\forall z \in \Omega$, l'indice de z par γ est $\mathrm{Ind}_\gamma(z) = \frac{1}{2i\pi} \int_\gamma \frac{d\zeta}{\zeta - z}$

Prop 20: Sous les mêmes hypothèses, $\mathrm{Ind}_\gamma \in \mathcal{H}(\Omega)$ à valeurs dans $\mathbb{Z}$ et $\mathrm{Ind}_\gamma(z) = 0$ pour tout z dans la composante non bornée de Ω.

Ex 21: voir annexe

Thm 22 (de Cauchy): Soit Ω un ouvert étoilé, soit $f \in \mathcal{H}(\Omega)$ et soit γ un lacet dans Ω. Alors on a pour tout $z \in \Omega \setminus \gamma$:
$\mathrm{Ind}_\gamma(z) f(z) = \frac{1}{2i\pi} \int_\gamma \frac{f(\zeta)}{\zeta - z} d\zeta$

Application 23 Calcul d'intégrales (calculs de Dirichlet par exemple)

[Jolissaint] p. 41

Thm 24 (des résidus): Soit γ un lacet de $\Omega \setminus A$ (A : pôles de f)
Alors $\frac{1}{2i\pi} \int_\gamma f(z) dz = \sum_{a \in A} \mathrm{Res}_a(f) \mathrm{Ind}_\gamma(a)$

Application 25: Calcul d'intégrales pour des fonctions ayant des pôles dans le contour qu'on considère.

I La fonction Gamma Γ

Def 26: $\forall z \in \mathbb{C}$ tel que $\mathrm{Re}(z) > 0$ on pose
$\Gamma(z) = \int_0^{+\infty} e^{-t} t^{z-1} dt$
on appelle cette fonction la fonction Gamma

Prop 27: $\forall z \in \mathbb{C}$ tel que $\mathrm{Re}(z) > 0$
$\Gamma(z+1) = z\,\Gamma(z)$

Rmq 28: En particulier, comme $\Gamma(1) = 1$
on a $\Gamma(n) = (n-1)!$ $\forall n \in \mathbb{N}^*$

Prop 29: La fonction Γ est holomorphe sur $\mathcal{B}_0 = \{z \in \mathbb{C}, \mathrm{Re}(z) > 0\}$

Prop 30 (Formule des compléments)
$\forall z \in \mathbb{C}$ tel que $0 < \mathrm{Re}(z) < 1$
$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}$

DEV 1

Application 31: $\Gamma(1/2) = \sqrt{\pi}$

Prop 32: La fonction Γ se prolonge en une fonction méromorphe sur $\mathbb{C}$. Ses pôles sont les entiers négatifs et $\forall k \in \mathbb{N}$
$\mathrm{Res}_{-k}(\Gamma) = \frac{(-1)^k}{k!}$
On continuera de noter Γ

Prop 33 (Formule de Gauss) $\forall z \in \mathbb{C} \setminus (\mathbb{Z}^-)$
$\Gamma(z) = \lim_{n \to +\infty} \frac{n!\, n^z}{z(z+1)\cdots(z+n)}$

Prop 34 (Formule de Weierstrass) $\forall z \in \mathbb{C}$
$\frac{1}{\Gamma(z)} = z e^{\gamma z} \prod_{n=1}^{+\infty} \left(1 + \frac{z}{n}\right) e^{-z/n}$
γ constante d'Euler

Parler loi Gamma ?

[Jolissaint] p. 167

II Fonction Zeta de Riemann ζ et Theta de Jacobi Θ

Def 35 : $\forall z \in \mathbb{C}$ tel que $\mathrm{Re}(z) > 1$, on pose
$$\zeta(z) = \sum_{n=1}^{+\infty} \frac{1}{n^z} = \sum_{n=1}^{+\infty} e^{-z\log(n)}$$
on appelle cette fonction, la fonction Zéta de Riemann

Rmq 36 : La série converge absolument car $\mathrm{Re}(z) > 1$ et converge normalement sur tout demi plan fermé $\{z \in \mathbb{C} ; \mathrm{Re}(z) \geq a\}$ où $a > 1$

Prop 37 : La fonction ζ est holomorphe sur $\mathcal{B}_1 = \{z \in \mathbb{C}, \mathrm{Re}(z) > 1\}$

Ex 38 : Pour z entier strictement positifs on reconnait $\zeta(1)$ la série harmonique, $\zeta(2) = \sum_{n\geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$ etc...

Thm 39 (lien avec les nombres premiers) :
$\forall z \in \mathcal{B}_1$, on a
$$\zeta(z) = \prod_{p \in \mathcal{P}} (1 - p^{-z})^{-1}$$
où $\mathcal{P}$ est l'ensemble des nombres premiers

Rmq 40 : $\prod_{p\in\mathcal{P}}$: $\lim_{n\to+\infty} \prod_{\substack{p\leq n \\ p \text{ premier}}}$ et la série converge uniformément sur les demi plan $\{z \in \mathbb{C} \ \mathrm{Re}(z) \geq a\}$ $(a > 1)$

Def 41 : $\forall z \in \mathbb{C}$ tel que $\mathrm{Re}(z) > 0$, on pose
$$\Theta(z) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 z}$$ fonction Theta de Jacobi

Prop 42 : Si $f \in \mathcal{C}^1(\mathbb{R}, \mathbb{C})$ telle que $f = \overline{O}_{\pm\infty}(\frac{1}{x^2})$ et $f' = \overline{O}_{\pm\infty}(\frac{1}{x^2})$
Alors $\forall x \in \mathbb{R} \ \sum_{k\in\mathbb{Z}} f(x + 2\pi k) = \frac{1}{2\pi} \sum_{k\in\mathbb{Z}} \hat{f}(k) e^{ikx}$ $\hat{f}$ transformation de Fourier

Thm 43 : $\forall u > 0$
$$\Theta(u) = \frac{1}{\sqrt{u}} \Theta\left(\frac{1}{u}\right)$$

Formule Sommatoire de Poisson

Def 44 : $\forall u > 0$, on pose
$$\Theta_1(u) = \frac{1}{2}(\Theta(u) - 1) = \sum_{n=1}^{+\infty} e^{-\pi n^2 u}$$

Lemme 45 : (1) $\forall u > 0$ $\Theta_1(\frac{1}{u}) = \sqrt{u}\,\Theta_1(u) + \frac{1}{2}(\sqrt{u} - 1)$

(2) il existe $C > 0$ tel que
(a) $\Theta_1(u) \leq C e^{-\pi u}$ $\forall u \geq 1$
(b) $\Theta_1(u) \leq \frac{C}{\sqrt{u}}$ $\forall u \in]0;1]$

Thm 46 : $\forall z \in \mathbb{C} \setminus \{0,1\}$, on pose
$$\xi(z) = \frac{1}{z(z-1)} + \int_1^{+\infty} \Theta_1(y)\left(y^{\frac{z}{2}-1} + y^{-\frac{z+1}{2}}\right) dy$$
qui est holomorphe sur $\mathbb{C} \setminus \{0,1\}$
et on a $\xi(z) = \frac{\xi(z)\,\pi^{z/2}}{\Gamma(z/2)}$ $\forall z$ tel que $\mathrm{Re}(z) > 1$

Prop 47 : La fonction ξ se prolonge en une fonction holomorphe dans $\mathbb{C} \setminus \{1\}$ avec un pôle simple en 1 de résidu $\mathrm{Res}_1(\xi) = 1$.

Application 48 : Les zéros "triviaux" de ζ sont les entiers pairs strictement négatifs ie $\zeta(2k) = 0$ $\forall k \in \mathbb{N}^*$

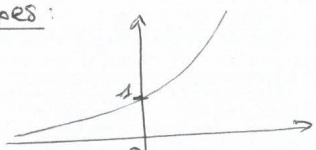
Conjecture de Riemann 49 : Les autres zéros de ζ sont sur la droite de partie réelle valant $\frac{1}{2}$ verticale

Thm 50 (admis) (Thm des nombres premiers) :
Pour tout $x > 0$, on pose
$$\pi(x) = \sum_{p \leq x} 1 = \#\{p \in \mathcal{P}, p \leq x\}$$
Alors $\pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\log(x)}$

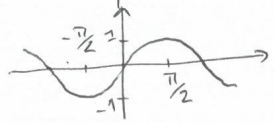
[Jolissaint] p. 43

Annexes :

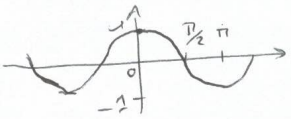
① exp — fonction exponentielle sur $\mathbb{R}$



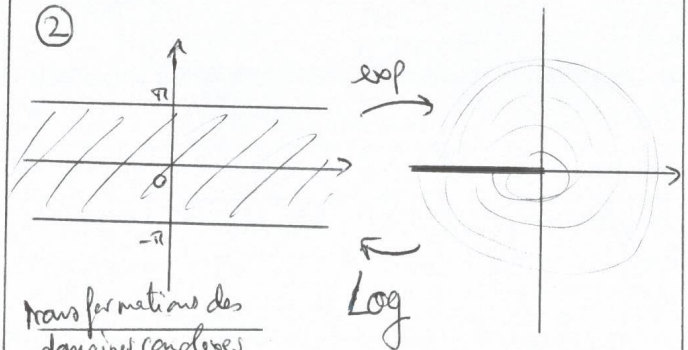
sin — sinus sur $\mathbb{R}$



cos — cosinus sur $\mathbb{R}$



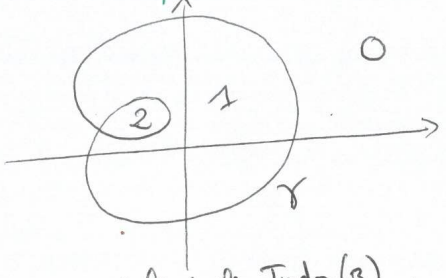
② exp → Log



transformations des domaines complexes

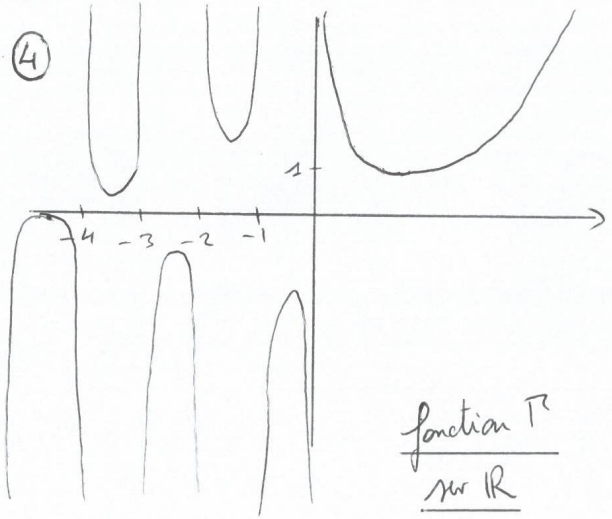
[Amar Rathera] p. 80

③



valeurs de $\mathrm{Ind}_\gamma(z)$

④



fonction Γ sur $\mathbb{R}$

[Gourx Soulat] p. 109

913 — Machines de Turing. Applications

Motivations : étendre le pouvoir de calcul des automates, trouver un autre modèle de calcul.

I Machines de Turing

1) Définitions :

Description : Une machine de Turing déterministe est composée :
- d'un ruban infini à droite divisé en cases.
- une tête de lecture
- un ensemble fini d'états (avec un état initial et des états acceptants)
- une fonction de transition

Formellement : Une machine de Turing déterministe est décrite par un heptuplet

$M = (Q, \Gamma, \Sigma, q_0, S, *, \delta)$ ← fonction de transition
Q : états ; Γ : alphabet d'écriture ; Σ : alphabet de lecture ; q_0 : état initial ; S : états acceptants ; $*$: symbole blanc $\in \Gamma$

où $\delta : Q \times \Gamma \to Q \times \Gamma \times \{\leftarrow, \rightarrow\}$ et $\Sigma \subsetneq \Gamma$, $* \notin \Sigma$, $* \in \Gamma$

Ex 2 : voir annexe.

Def 3 : Une configuration est l'état global de la machine à un instant donné
ie. l'état de la machine $\in Q$
le contenu du ruban $\in \Gamma^*$
la position de la tête de lecture sur le ruban.

Ex 4 : $(g, q, d') \in \Gamma^* \times Q \times \Gamma^*$ est une configuration

Def 5 : Une étape de calcul d'une machine de Turing est une paire (C, C') de configurations notée $C \to C'$ telle que C' soit la configuration après exécution de 1 sur C.

Ex 6 : $00q_111 \to 000q_11$ est une étape de calcul de l'exemple 2.

Def 7 : On appelle exécution une suite de configurations successives. Elle est dite acceptante si la première configuration est initiale et si la dernière est dans un état acceptant.

Def 8 : On dit que la machine M bloque sur w, si lors de l'exécution, une configuration n'a pas de configuration suivante (qui n'est pas dans un état acceptant).

2) Variantes

Def 9 : Une machine de Turing à ruban bi-infini est composée d'un ruban infini à droite et à gauche

Def 10 : Une machine de Turing à k rubans dispose de k rubans chacun avec une tête de lecture indépendante et $\delta : Q \times \Gamma^k \to Q \times \Gamma^k \times \{\leftarrow, \rightarrow\}^k$

Def 11 : Une machine de Turing non déterministe ne possède pas de fonction de transition mais d'une relation de transition $\subseteq Q \times \Gamma^k \times Q \times \Gamma^k \times \{\leftarrow, \rightarrow\}^k$ laissant plusieurs choix possibles de configurations suivantes

Thm 12 : Toutes ces variantes de machines de Turing sont équivalentes (elles ont la même expressivité de calcul.)

II Décidabilité et indécidabilité

1) Langages R et RE

Def 13 : on dit qu'un mot $w \in \Sigma^*$ est accepté par $\mathcal{M}$ s'il existe une exécution acceptante partant du mot w
On appelle $L(\mathcal{M})$ les mots acceptés par $\mathcal{M}$.

Def 14 : Un langage $L \subseteq \Sigma^*$ est récursivement énumérable (RE) s'il existe $\mathcal{M}$ telle que $L = L(\mathcal{M})$

Prop 15 : L'ensemble des langages récursivement énumérables RE est stable par union et intersection.

Def 16 : Un langage $L \subseteq \Sigma^*$ est décidable ($\in R$) si il existe $\mathcal{M}$ sans exécution infinie telle que $L = L(\mathcal{M})$.

Prop 17 : L'ensemble des langages décidables R est stable par union, intersection et complémentaire

Def 18 : On dit que $L \subseteq \Sigma^*$ est dans co-RE si son complémentaire est dans RE.

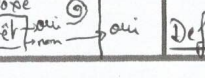
Prop 19 : $coRE \cap RE = R$.

Prop 20 : Le langage $L_U = \{ \langle M, w \rangle / w \in L(M) \} \in RE$
Une machine $\mathcal{M}_U$ telle que $L(\mathcal{M}_U) = L_U$ est dite universelle.

2) Problèmes indécidables.

Pb 21 : ARRET
entrée : une machine de Turing $\mathcal{M}$, w un mot
sortie : oui si l'exécution de $\mathcal{M}$ sur w s'arrête
non sinon

ARRET est dans RE mais est indécidable par construction d'une machine paradoxale



Def 22 : Une fonction $f : \Sigma^* \to \Gamma^*$ est dite calculable si il existe $\mathcal{M}$ telle que pour toute entrée w, $\mathcal{M}$ s'arrête sur $f(w)$ sur le ruban.

Def 23 : Soient 2 problèmes A et B,
Une réduction de A à B est une fonction calculable $f : \Sigma_A^* \to \Sigma_B^*$ telle que $w \in L_A \Leftrightarrow f(w) \in L_B$.
(voir annexe)

Thm 24 : (Rice) Pour toute propriété P telle que $\emptyset \subsetneq P \subsetneq RE$
le problème de savoir si $L(\mathcal{M})$ (où $\mathcal{M}$ est en entrée) vérifie P est indécidable.
(par réduction de Arrêt à ce problème)

Prop 23 bis : Si A se réduit à B
- A indécidable $\Rightarrow$ B indécidable
- B décidable $\Rightarrow$ A décidable

Pb 25 : Les problèmes suivants sont indécidables.

Accept :
entrée : $\mathcal{M}$ et w
sortie : oui si $\mathcal{M}$ accepte w

POST :
entrée : ensemble fini de tuiles $\left[\frac{u_i}{v_i}\right]$ où $u_i, v_i \in \Sigma^*$
sortie : oui si il existe une concaténation de tuiles formant le même mot en haut et en bas.

VALID :
entrée : une formule Φ close en logique du 1er ordre
sortie : oui, si Φ est valide non sinon.

III Modèles de calcul

Thèse de Church 26 : Les fonctions calculables par une procédure effective sont celles calculables par une machine de Turing.

Def 27 : calculable par machine de Turing (voir def 22)

1) Fonctions récursives

Def 28 : Les fonctions primitives récursives sont le plus petit ensemble contenant la fonction zéro, la fonction successeur et la projection π_i^n qui est clos par composition et par récursion primitive contenu dans $\{\mathbb{N}^k \to \mathbb{N}, k>0\}$

Ex 29 : l'addition est primitive récursive :

$$plus(n,k) = \begin{cases} n \text{ si } k=0 \\ succ(plus(n,k-1)) \text{ si } k>0 \end{cases}$$

Def 30 : On ajoute la minimisation non bornée

$$(\mu_i(q(\vec{n},i))) = \begin{cases} \text{le plus petit } i \text{ tel que } q(\vec{n},i)=1 \\ 0 \text{ si un tel } i \text{ n'existe pas} \end{cases}$$

aux fonctions primitives récursives pour ainsi obtenir les fonctions μ-récursives

Thm 31 : Toute fonction μ-récursive est calculable par une machine de Turing.

Thm 32 : Toute fonction (totale) calculable par une machine de Turing est μ-récursive

DEV1

2) λ-calcul

Def 33 : L'ensemble $\mathcal{L}$ des termes de λ-calcul est le plus petit ensemble tel que :

- les variables $x, y, z \ldots$ sont des termes
- si u et v sont des termes, (uv) est un terme
- si x est une variable et t un terme, $\lambda x.t$ est un terme.

Thm 34 : Une fonction est calculable par une machine de Turing si et seulement si elle est représentable par un terme de λ-calcul.

IV) Classes de complexité

Def 35 : La classe de problèmes P regroupe tous les problèmes décidés par une machine de Turing déterministe en temps polynomial.

Ex 36 : L'accessibilité dans un graphe est dans P

Def 37 : La classe de problèmes NP regroupe tous les problèmes décidés par une machine de Turing non déterministe en temps polynomial.

Prop 38 : $P \subseteq NP$

Def 39 : La réduction de A à B dans ce cadre nécessite une fonction $f : \Sigma_A^* \to \Sigma_B^*$ calculable en temps polynomial.

Def 40 : Un problème est NP-dur si tout problème NP peut se réduire à lui

Def 41 : Un problème est dit NP-complet si il est dans NP et est NP-dur.

Thm 42 : Le problème SAT est NP complet

SAT : entrée : une formule Ψ du calcul propositionnel ; sortie : oui si Ψ est satisfiable, non sinon

DEV2

Pb 43 : Les problèmes suivants sont NP-complets

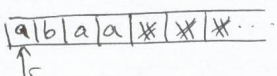
CNFSAT : entrée : Ψ en forme normale conjonctive ; sortie : oui si Ψ est satisfiable, non sinon

3 COL : entrée : un graphe $G=(S,A)$ non orienté ; sortie : oui si G est 3-coloriable, non sinon

VERTEX COVER : entrée : un graphe $G=(S,A)$ non orienté, un entier k ; sortie : oui si il existe $S' \subseteq S$, $|S'| \leq k$ et $\forall (u,v) \in A$, $u \in S'$ ou $v \in S'$

Description 1 :

$\Sigma = \{a,b\}$

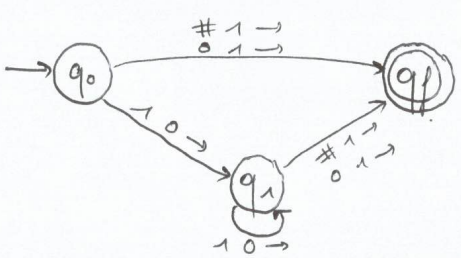


Exemple 2 : successeur pour un nombre écrit en binaire poids faible à gauche

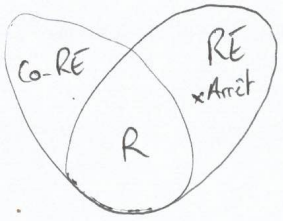
$Q = \{q_0, q_1, q_f\}$ $A = \{q_f\}$

$\Sigma = \{0,1\}$ $\Gamma = \{0,1,*\}$

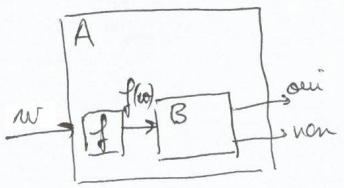
$$\delta = \{ (q_0,0) \to (q_f,1,\to) \quad (q_0,1) \to (q_1,0,\to) \quad (q_0,*) \to (q_f,1,\to) \quad (q_1,0) \to (q_f,1,\to) \quad (q_1,1) \to (q_1,0,\to) \quad (q_1,*) \to (q_f,1,\to) \}$$



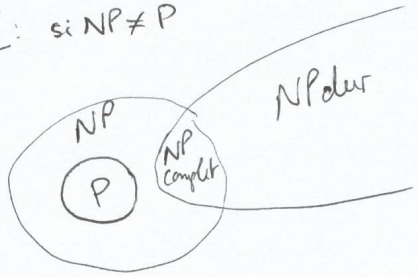
Prop 19 :



Def 23 :



Partie IV : si $NP \neq P$



Décidabilité et indécidabilité. Exemples.

3.14

I. Généralités et cadre

1. Classes R et RE

Déf 1: Une machine de Turing est un heptuplet $(Q, \Gamma, \Sigma, \delta, q_0, \#, F)$ où
- Q est un ensemble fini d'états;
- Γ est l'alphabet de ruban;
- $\Sigma \subseteq \Gamma$ est l'alphabet d'entrée;
- $q_0 \in Q$ est l'état initial;
- $F \subseteq Q$ est l'ensemble des états acceptants;
- $\# \in \Gamma \setminus \Sigma$ est le symbole blanc;
- $\delta : Q \times \Gamma \to Q \times \Gamma \times \{\leftarrow, \rightarrow\}$ est la fonction de transition.

Déf 2: Un problème de décision est une question dont la réponse est soit "oui", soit "non".

Ex 3: Étant donné un graphe G, "est-ce que G est connexe ?" est un problème de décision.

Déf 4: Un mot $w \in \Sigma^*$ est accepté par une machine de Turing M si l'exécution de M avec la configuration initiale $q_0 w$ mène à une configuration uqv où $q \in F$. Le langage accepté par une machine M est l'ensemble des mots de Σ^* acceptés par M. On le note $\mathcal{L}(M)$.

Déf 5: L'ensemble des langages récursivement énumérables, RE, est l'ensemble des langages acceptés par une machine de Turing, i.e. les langages L pour lesquels il existe une machine de Turing M telle que $L = \mathcal{L}(M)$.

Ex 6: Le problème ARRET:
| entrée: machine de Turing M, mot w
| sortie: oui si $M(w)$ s'arrête, non sinon

est dans RE.

Déf 7: L'ensemble des langages récursifs, R, est l'ensemble des langages décidés par une machine de Turing, i.e. les langages L pour lesquels il existe une machine de Turing M sans calcul infini telle que $L = \mathcal{L}(M)$.

Ex 8: Le problème CONNEXE:
| entrée: graphe G
| sortie: oui si G est connexe, non sinon

est dans R car on peut exhiber un algorithme qui décide si G est connexe.

Déf 9: Un énumérateur est une machine de Turing qui énumère des mots de Σ^*, i.e. qui écrit sur une bande de sortie des mots de Σ^* séparés par un symbole qui n'est pas dans Σ.

Prop 10: $L \in RE$ ssi il existe un énumérateur qui énumère exactement les mots de L.

Déf 11: On définit co-RE $= \{A \mid \bar{A} \in RE\}$ où
$\bar{A}$:
| entrée: une instance de A, w
| sortie: oui si $w \notin A$, non sinon

Prop 12: $R = RE \cap$ co-RE. En particulier, $R \subseteq RE$.

Prop 13: R et RE sont stables par union et intersection. De plus, R est stable par complémentaire.

2. Fonctions calculables et réduction

Jusqu'à présent, nous avons considérés les machines de Turing comme des automates acceptant un langage. Mais les machines de Turing peuvent aussi calculer des fonctions :

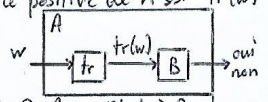
Déf 14: Une machine de Turing calcule une fonction $f : \Sigma^* \to \Sigma^*$ si pour tout mot d'entrée w, elle s'arrête toujours dans une configuration où $f(w)$ se trouve sur le ruban. Une fonction f est calculable s'il existe une machine de Turing qui la calcule.

Thm 15: Les fonctions μ-récursives sont exactement celles calculables par une machine de Turing.

Thm 16: Soit $A \subseteq \mathbb{N}$, les assertions suivantes sont équivalentes:
(i) $A \in RE$
(ii) $A = \pi_2^2(B)$ où $B \subseteq \mathbb{N}^2$ est primitif récursif
(iii) $A = \emptyset$ ou A est l'image d'une fonction primitive récursive
(iv) A est l'image d'une fonction μ-récursive.

DEV 1

Déf 17: Une réduction d'un problème A à un problème B est une fonction calculable tr telle que pour toute instance w de A, w est une instance positive de A ssi $tr(w)$ est une instance positive de B.



Prop 18: Si A se réduit à B, alors : $B \in R \Rightarrow A \in R$
$A \notin R \Rightarrow B \notin R$

1/3

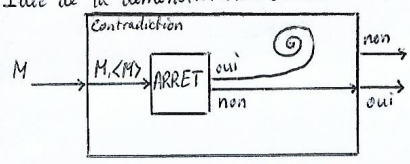
II. Techniques pour prouver l'indécidabilité

Rmq 19: Pour prouver qu'un problème est décidable, il suffit de trouver un algorithme effectif qui décide le problème, ou bien on peut le réduire à un problème que l'on sait décidable d'après la proposition 18. On s'intéresse ici aux problèmes indécidables.

1. Le problème ARRET

Thm 20: ARRET $\notin R$.

Idée de la démonstration : construire la machine "Contradiction".



Donner "Contradiction" en entrée à "Contradiction" donne une contradiction.

2. Utilisation de la réduction pour prouver l'indécidabilité

Déf 21: On définit le problème de l'acceptation d'un mot par une machine de Turing
ACCEPTATION:
| entrée: machine de Turing M, mot w
| sortie: oui si M accepte w, non sinon

Thm 22: ACCEPTATION est indécidable.
(Par réduction d'ARRET à ACCEPTATION.)

Déf 23: Problèmes de correspondances de Post :
POST:
| entrée: alphabet fini Σ, famille de tuiles $(u_1, v_1), \dots, (u_N, v_N)$
| sortie: oui s'il existe $i_1, \dots, i_p \in \{1, \dots, N\}$ tels que $p \geq 1$ et $u_{i_1} \dots u_{i_p} = v_{i_1} \dots v_{i_p}$, non sinon

$\text{POST}_{\text{marqué}}$:
| entrée: alphabet fini Σ, famille de tuiles $(u_1, v_1), \dots, (u_N, v_N)$
| sortie: oui s'il existe $i_1, \dots, i_p \in \{1, \dots, N\}$ tels que $p \geq 1$ et $u_1 u_{i_2} \dots u_{i_p} = v_1 v_{i_2} \dots v_{i_p}$, non sinon

Thm 24: $\text{POST}_{\text{marqué}}$ est indécidable (par réduction de ACCEPTATION à $\text{POST}_{\text{marqué}}$). Et POST est indécidable (par réduction de $\text{POST}_{\text{marqué}}$ à POST).

III. Décidabilité et indécidabilité de différents problèmes.

1. Machines de Turing

Rmq 25: On a déjà vu que les problèmes ARRET et ACCEPTATION sont indécidables.

Thm 26 (de Rice): Soit $\mathcal{P}$ telle que $\emptyset \subsetneq \mathcal{P} \subsetneq RE$.
Alors le problème
$P_{\mathcal{P}}$:
| entrée: machine de Turing M
| sortie: oui si $\mathcal{L}(M) \in \mathcal{P}$, non sinon

est indécidable.

Appli 27: Le problème du langage vide
VIDE :
| entrée: machine de Turing M
| sortie: oui si $\mathcal{L}(M) = \emptyset$, non sinon

est indécidable (appliquer le théorème de Rice à $\mathcal{P} = \{\emptyset\}$).

2. Automates finis

Thm 28: Le problème ACCEPTATION pour les automates finis est décidable.

Prop 29: Le problème VIDE pour les automates finis est décidable.

Prop 30: Le problème du langage universel pour les automates finis
UNIV:
| entrée: langage L sur un alphabet Σ
| sortie: oui si $L = \Sigma^*$, non sinon

est décidable.

3. Grammaires algébriques

Thm 31: Le problème ACCEPTATION pour les langages algébriques est décidable via l'algorithme de Cocke-Younger-Kasami.

Prop 32: Le problème VIDE pour les langages algébriques est également décidable.

2/3

Prop 33: Le problème
INTERSECTION:
| entrée: G, G' deux grammaires algébriques
| sortie: oui si $L(G) \cap L(G') = \emptyset$, non sinon
est indécidable.

Prop 34: Le problème
EGAL:
| entrée: G, G' deux grammaires algébriques
| sortie: oui si $L(G) = L(G')$, non sinon
est indécidable.

Cor 35: Le problème UNIV pour les langages algébriques est aussi indécidable.

4. Logique

Déf 36: On définit le problème
VALIDE:
| entrée: formule close φ
| sortie: oui si φ est valide, non sinon

Prop 37: Le problème VALIDE pour le calcul propositionnel est décidable.

Thm 38: En logique du premier ordre, le problème VALIDE est indécidable. DEV 2

Déf 39: L'arithmétique de Presburger est la théorie du premier ordre des entiers munis de l'addition mais pas de la multiplication.
C'est le langage L engendré par $\{0, 1, +, =\}$ où
- 0 et 1 sont des symboles de constantes
- $+$ est un symbole de fonction binaire
- $=$ est le prédicat binaire de l'égalité.

Prop 40: Le problème
PRES
| entrée: formule close φ de L
| sortie: oui si $\mathbb{N} \models \varphi$, non sinon
est décidable.

Déf 41: Si on ajoute à L le symbole de fonction $\times$ et aux axiomes de l'arithmétique de Presburger ceux relatifs à la multiplication sur les entiers, on obtient la théorie de l'arithmétique de Peano.

Thm 42: La théorie de Peano n'est pas décidable.
(Admis)

Références:

- Autebert, *Calculabilité et décidabilité, une introduction*
- Carton, *Langages formels, calculabilité et complexité*
- Cori-Lascar, *Logique mathématique, tome II*.
- Sipser, *Introduction to the theory of computation*
- Wolper, *Introduction à la calculabilité*

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

* Motivations : Problèmes d'emploi du temps, coloriage d'un graphe

I) Syntaxe.

1) le langage de la logique propositionnelle (LP).

déf 1 : l'ensemble des variables propositionnelles est un ensemble de symboles $VAR = \{p, q, r, \dots, p_1, p_2, p_3, \dots\}$

déf 2 : le langage $\mathcal{F}$ de la LP est le langage sur l'alphabet $\Sigma = VAR \cup \{\bot, \neg, \wedge, (,)\}$ défini par induction par :

- $VAR \cup \{\bot\} \subseteq \mathcal{F}$
- $\forall \varphi \in \mathcal{F}$, $\neg\varphi \in \mathcal{F}$
- $\forall \varphi, \psi \in \mathcal{F}$, $(\varphi \wedge \psi) \in \mathcal{F}$

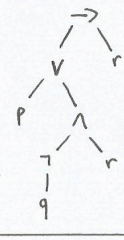
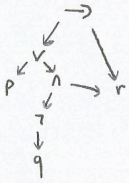
ex 3 : $(\neg p \wedge (q \wedge (\neg \bot \wedge p)))$ est une formule de la LP.

thm 4 (lecture unique) :
Soit $\varphi \in \mathcal{F}$. Alors un et un seul des trois cas suivants se présente :
(i) $\varphi \in VAR$
(ii) Il existe $\psi \in \mathcal{F}$ tq $\varphi = \neg\psi$
(iii) Il existe $(\psi_1, \psi_2) \in \mathcal{F}^2$ tq $\varphi = (\psi_1 \wedge \psi_2)$

Rq 5 : on s'autorisera, pour tout $\varphi, \psi \in \mathcal{F}$, l'écriture de :
- $(\varphi \vee \psi)$ à la place de $\neg(\neg\varphi \wedge \neg\psi)$
- $(\varphi \to \psi)$ à la place de $(\neg\varphi \vee \psi)$
- $(\varphi \leftrightarrow \psi)$ à la place de $((\varphi \to \psi) \wedge (\psi \to \varphi))$
- $\top$ à la place de $\neg\bot$

ex 6 : on considérera donc que ceci est une formule de la LP :
$$\varphi_1 = ((p \vee (\neg q \wedge r)) \to r)$$

2) Représentations

formule (mot)	arbre	DAG
φ_1		

Rq 7 : le DAG économise de l'espace en mémoire.

3) Résolution par réfutation.

déf 8 : un littéral est une formule de la forme p ou $\neg p$, avec $p \in VAR$. une clause est une disjonction ($\vee$) de littéraux.

déf 9 : une formule est sous forme normale conjonctive (CNF) si elle s'écrit sous la forme :

$$\varphi = \bigwedge_{i \in I} \bigvee_{j \in J} l_{ij}$$

pour I, J finis et l_{ij} littéral

déf 10 : règles de résolution :

coupure $\dfrac{(\neg p \vee l_1 \vee \dots \vee l_n) \quad (p \vee l'_1 \vee \dots \vee l'_m)}{(l_1 \vee \dots \vee l_n \vee l'_1 \vee \dots \vee l'_m)}$

Redondance $\dfrac{l \vee l \vee l_1 \vee \dots \vee l_n}{l \vee l_1 \vee \dots \vee l_n}$

→ Une dérivation d'une formule φ en CNF vers une formule ψ en CNF est une suite de règles de résolutions à partir de l'ensemble des clauses de φ aboutissant à l'ensemble des clauses de ψ.

déf 11 : Une preuve de la réfutation de $\varphi \in \mathcal{F}$ en FNC est une dérivation de φ à $\bot$.

ex 12 : $\varphi_2 = (((p \vee \neg q) \wedge (r \vee \neg p)) \wedge ((q \vee r) \wedge \neg r))$ [cf Annexe]

II) Sémantique

1) Valuation et table de vérité.

déf 13 : une valuation est une fonction $\nu : VAR \to \{0,1\}$

prop-déf 14 : Soit $\nu \in \{0,1\}^{VAR}$ une valuation. On étend ν de manière unique en une fonction $\tilde{\nu} : \mathcal{F} \to \{0,1\}$ par :
- $\tilde{\nu}(p) = p$
- $\tilde{\nu}(\neg\phi) = 1 - \tilde{\nu}(\phi)$
- $\tilde{\nu}(\bot) = 0$
- $\tilde{\nu}(\phi \wedge \varphi) = \tilde{\nu}(\phi) \times \tilde{\nu}(\varphi)$

Rq 15 : on obtient également :
- $\tilde{\nu}(\top) = 1$
- $\tilde{\nu}(\varphi \to \psi) = 1 - \tilde{\nu}(\varphi) + \tilde{\nu}(\varphi)\tilde{\nu}(\psi)$
- $\tilde{\nu}(\varphi \vee \psi) = \tilde{\nu}(\varphi) + \tilde{\nu}(\psi) - \tilde{\nu}(\varphi)\tilde{\nu}(\psi)$
- $\tilde{\nu}(\varphi \leftrightarrow \psi) = 1 - \tilde{\nu}(\varphi) - \tilde{\nu}(\psi) + 2\tilde{\nu}(\varphi)\tilde{\nu}(\psi)$

→ Désormais, on note ν et on appelle valuation cette extension.

ex 16 : si $\nu(p) = \nu(q) = \nu(r) = 0$, $\nu(\varphi_1) = 1$ et $\nu(\varphi_2) = 0$.

déf 17 : une table de vérité est un tableau représentant, en colonnes, l'image de toutes les valuations possibles de formules données.

ex 18 : tables de vérité de φ_1 et φ_2 [cf Annexe].

Pb 19 : EVAL (φ, ν)
Entrée : une formule $\varphi \in \mathcal{F}$ et une valuation $\nu \in \{0,1\}^{VAR}$.
Sortie : oui si $\nu(\varphi) = 1$; non sinon.

prop 20 : le problème EVAL est décidable en temps linéaire.

2) Validité et satisfiabilité.

déf 21 : une formule φ est valide si pour toute valuation $\nu \in \{0,1\}^{VAR}$, on a : $\nu(\varphi) = 1$.
Un ensemble de formules $\{\varphi_i, i \in I\}$ est valide si chaque φ_i est valide

déf 22 : une formule φ est satisfiable s'il existe une valuation $\nu \in \{0,1\}^{VAR}$ telle que $\nu(\varphi) = 1$.
Un ensemble de formules $\{\varphi_i, i \in I\}$ est satisfiable s'il existe une valuation ν telle que $(\forall i \in I,\ \nu(\varphi_i) = 1)$.
on dit insatisfiable dans le cas contraire.

ex 23 : φ_1 est satisfiable mais non valide ; φ_2 est insatisfiable.

prop 24 : $\varphi \in \mathcal{F}$ est valide ssi $\neg\varphi$ est insatisfiable.

déf 25 : deux formules sont équisatisfiables si elles sont toutes les deux satisfiables ou toutes les deux insatisfiables.

thm 26 : (Compacité de la logique propositionnelle)
Un ensemble de formules $E \subseteq \mathcal{F}$ est satisfiable ssi toute partie finie de E est satisfiable.

DEV 1

Application 27 : un graphe G non-orienté est k-coloriable ssi tout sous-graphe fini $G' \subseteq G$ est k-coloriable.

Application 28 : Soit (H, V) des règles de pavage sur $\mathbb{Z}^2$. Alors
$\mathbb{Z}^2$ est (H,V)-pavable ssi pour tout $n \geq 0$, $[-n, n]^2$ est (H,V)-pavable.

3) Équivalence sémantique.

déf 29 : deux formules $\varphi, \psi \in \mathcal{F}$ sont sémantiquement équivalentes si la formule $(\varphi \leftrightarrow \psi)$ est valide. On notera alors $\varphi \sim \psi$.

ex 30 : (Lois de DE MORGAN)
$\neg(p \vee q) \sim (\neg p \wedge \neg q)$ $\quad$ $\neg(p \vee q) \sim (\neg p \wedge \neg q)$

prop 31 : deux formules équivalentes sont en particulier équisatisfiables.

4) Lien entre syntaxe et sémantique.

thm 32 : (complétude du calcul propositionnel) Soit $\varphi \in \mathcal{F}$ sous CNF.

Il existe une preuve de la réfutation de φ. ⟺ ($\Leftarrow$ complétude, $\Rightarrow$ correction) φ est insatisfiable.

III] Satisfiabilité et formes normales.

Pb 33 : SAT (φ)
{ Entrée : une formule $\varphi \in \mathcal{F}$.
{ Sortie : oui si φ est satisfiable (et une valuation ν tq $\nu(\varphi)=1$) ; non sinon.

thm 34 : (Cook, 1971) le problème SAT est NP-complet. DEV 2

1) Mise sous forme normale conjonctive.

Pb 35 : CNF_SAT (φ)
{ Entrée : une formule $\varphi \in \mathcal{F}$ sous CNF
{ Sortie : oui si φ est satisfiable (et $\nu \in \{0,1\}^{VAL}$ tq $\nu(\varphi)=1$) ; non sinon.

thm 36 : Pour toute formule $\varphi \in \mathcal{F}$, il existe une formule $\tilde{\varphi} \in \mathcal{F}$ en CNF sémantiquement équivalente à φ ($\tilde{\varphi} \sim \varphi$). La transformation est exponentielle.

ex 37 :
$$\begin{aligned}(\neg p \to \neg q) \to (p \to q) &\sim \neg(\neg\neg p \vee \neg q) \vee (\neg p \vee q) \\ &\sim (\neg\neg\neg p \wedge \neg\neg q) \vee (\neg p \vee q) \\ &\sim (\neg p \wedge q) \vee (\neg p \vee q) \\ &\sim (\neg p \vee \neg p \vee q) \wedge (q \vee \neg p \vee q)\end{aligned}$$

Cor 38 : le thm 32 est vrai pour toute formule $\varphi \in \mathcal{F}$.

thm 39 (Algorithme de Tseitin) : pour toute formule $\varphi \in \mathcal{F}$, il existe une formule $\tilde{\varphi} \in \mathcal{F}$ en CNF tq φ et $\tilde{\varphi}$ sont équisatisfiables. De plus, la transformation $tr : \varphi \mapsto \tilde{\varphi}$ est calculable en temps linéaire. DEV 3

Corollaire 40 : le problème CNFSAT est NP-complet.

Pb 41 : 3CNF_SAT(φ)
{ Entrée : $\varphi \in \mathcal{F}$ en CNF avec au plus 3 littéraux par clause.
{ Sortie : oui si φ est satisfiable (ν tq $\nu(\varphi)=1$) ; non sinon.

Thm 42 : Il existe une réduction polynômiale de CNF_SAT à 3CNF_SAT.

Corollaire 43 : le problème 3CNF_SAT est NP-complet.

Pb 44 : 2CNF_SAT
{ Entrée : $\varphi \in \mathcal{F}$ sous CNF avec au plus deux littéraux par clause.
{ Sortie : oui si φ est satisfiable (ν tq $\nu(\varphi)=1$) ; non sinon.

thm 45 : le problème 2CNF_SAT est décidable en temps polynômial.

Corollaire 46 : Il n'existe pas de réduction polynômiale du problème 3CNF-SAT au problème 2CNF_SAT.

2) D'autres formes normales à la rescousse !

def 47 : une formule est sous forme normale disjonctive (DNF) si elle s'écrit sous la forme :

$$\varphi = \bigvee_{i \in I} \bigwedge_{j \in J} p_{i,j}$$

pour I, J finis et $p_{i,j}$ littéraux

Pb 48 : DNF_SAT(φ)
{ Entrée : $\varphi \in \mathcal{F}$ sous DNF
{ Sortie : oui si φ est satisfiable (ν tq $\nu(\varphi)=1$) ; non sinon.

thm 49 : le problème DNF_SAT est calculable en temps linéaire.

prop 50 : Toute formule $\varphi \in \mathcal{F}$ est sémantiquement équivalente à une formule $\tilde{\varphi} \in \mathcal{F}$ sous DNF (il suffit de lire sa table de vérité).

Rq 51 : D'après le théorème de Cook, cette transformation ne peut pas être polynômiale. De plus, le thm 49 assure qu'il n'existe pas d'algorithme calculant en temps polynômial une transformation $tr : \varphi \mapsto \tilde{\varphi}$ tq φ et $\tilde{\varphi}$ soient équisatisfiables et $\tilde{\varphi}$ soit sous DNF.

déf 52 : une clause de Horn est une clause $\ell_1 \vee \dots \vee \ell_n$ où apparaît au plus un littéral positif $\ell_i = p \in VAR$ ($\forall j \neq i$, $\ell_j = \neg q, q \in VAR$)

Pb 53 : HORN_SAT (φ)
{ Entrée : $\varphi \in \mathcal{F}$ sous CNF avec uniquement des clauses de Horn.
{ Sortie : oui si φ est satisfiable (ν tq $\nu(\varphi)=1$) ; non sinon.

thm 54 : le problème HORN_SAT est décidable en temps linéaire.

ex 55 : la formule suivante est satisfiable pour la valuation $\begin{cases} p \to 0 \\ q \to 1 \\ r \to 0 \end{cases}$

$\varphi_3 = \underbrace{(p \vee \neg q \vee \neg r)}_{\text{clause de Horn stricte}} \wedge \underbrace{(q)}_{\text{positive}} \wedge \underbrace{(\neg p \vee \neg q)}_{\text{négative}}$

ANNEXE

ex 12 : $\varphi_2 = (((p \vee \neg q) \wedge (r \vee \neg p)) \vee ((q \vee r) \wedge \neg r))$

$$\dfrac{\dfrac{\dfrac{p \vee \neg q \qquad r \vee \neg p}{(F)}\ \neg q \vee r \qquad q \vee r}{(F)}\ r \vee r}{(R)}\ r \qquad \dfrac{\neg r}{(P)}\ \bot$$

ex 18 :

p	q	r	$\varphi_1 = ((p \vee (\neg q \wedge r)) \to r$	$\varphi_2 = (((p \vee \neg q) \wedge (r \vee \neg p)) \vee ((q \vee r) \wedge \neg r))$
0	0	0	1	0
0	0	1	1	0
0	1	0	0	0
0	1	1	1	0
1	0	0	0	0
1	0	1	1	0
1	1	0	0	0
1	1	1	1	0

926

Analyse des algorithmes : Complexité. Exemples.

Motivations : Calculer l'efficacité d'un algorithme A

I Cadre et généralités

1) Qu'est ce que la complexité ?

Def 1 : On appelle données d'entrées l'ensemble des variables externes à l'algorithme sur lequel on va exécuter l'algorithme.

Ex 2 : Un algorithme de tri d'un tableau doit prendre en entrée un tableau.

Def 3 : La taille de l'entrée x est un entier n qui est défini grâce à une fonction $f : \{\text{entrées}\} \to \mathbb{N}$

Ex 4 : Pour un mot $w = w_1 \dots w_n$, on peut dire $f(w) = n$, i.e. nbr de caractères
Pour un tableau T de taille n, on pourrait dire $f(T) = n$ mais aussi l'espace mémoire nécessaire pour mettre le tableau.

Def 5 : La complexité est une fonction φ qui à une donnée d'entrée x renvoie la consommation d'une certaine ressource
La ressource peut être le temps, l'espace mémoire, la chaleur dissipée lors de l'exécution, le nombre d'accès au disque dur externe, ...

Rmq 6 : En pratique pour la complexité temporelle, on compte le nombre d'opérations, de comparaisons, d'affectations ou d'appels récursifs par exemple.

Ex 7 : Tri Bulle en comptant le nombre de comparaisons
il y en a $\sum_{i=1}^{n-1} i = \frac{n(n+1)}{2}$ pour toutes les entrées possibles

2) Notation de Landau

Parfois, on ne peut pas calculer la complexité exacte mais on peut en donner un ordre de grandeur.

Def 8 : Soient $f, g : \mathbb{N} \to \mathbb{R}^+$
On note $\mathcal{O}(g) = \{f$ telle qu'il existe $C > 0$, $n_0 \in \mathbb{N}$ / $0 \le f(n) \le C g(n)$ $\forall n \ge n_0\}$
et $\Theta(g) = \{f$ telle qu'il existe $C_1, C_2 > 0$, $n_0 \in \mathbb{N}$ / $0 \le C_1 g(n) \le f(n) \le C_2 g(n)$ $\forall n \ge n_0\}$

Remarque 9 : On écrira $f = \mathcal{O}(g)$ ($resp = \Theta(g)$) pour $f \in \mathcal{O}(g)$ ($resp \in \Theta(g)$).

Proposition 10 : $[f = \mathcal{O}(g)$ et $g = \mathcal{O}(f)] \iff f = \Theta(g)$
$f = \Theta(g) \iff g = \Theta(f)$

Exemple 11 : $n^2 + n = \mathcal{O}(n^3)$ $\quad n^2 + n = \mathcal{O}(n^2)$
et $n^2 = \mathcal{O}(n^2 + n)$ d'où $n^2 + n = \Theta(n^2)$
mais $n^3 \neq \mathcal{O}(n^2 + n)$

Exemple 12 : Pour le tri bulle de l'exemple 7, on a une complexité en $\mathcal{O}(n^2)$

Prop 13 : L'ordre de croissance des $\mathcal{O}$ est :
$\mathcal{O}(1) ; \mathcal{O}(\log n) ; \mathcal{O}(n) ; \mathcal{O}(n \log n) ; \mathcal{O}(n^2) ; \mathcal{O}(n^k) ; \mathcal{O}(k^n) ; \mathcal{O}(n!)$

3) Différentes approches de complexité

Def 14 : Soit $\Omega_n = \{$entrées de taille n pour l'algorithme considéré$\}$
Soit φ la fonction de complexité définie à la définition 5
On a $C_{pire}(n) = \max_{x \in \Omega_n} \varphi(x)$ $\quad C_{mieux}(n) = \min_{x \in \Omega_n} \varphi(x)$
distribution uniforme $C_{moy}(n) = \frac{1}{|\Omega_n|} \sum_{x \in \Omega_n} \varphi(x)$ si $\varphi(x) = cste$ $\forall x \in \Omega_n$ on notera $C(n) = \text{Cste}$

II Premières techniques pour calculer la complexité

1) Calcul direct

On peut parfois calculer directement la complexité en dénombrant les opérations que l'on doit compter

Ex 15 : Recherche du maximum dans un tableau en comptant le nombre de comparaison
Pour un tableau de taille n, il y aura n comparaisons car une boucle for de taille n, $C(n) = \Theta(n)$

2) Complexité moyenne vue comme calcul d'espérance

Prop 16 : Soit p la distribution des données d'entrées
On a en fait $C_{moy} = \sum_{x \in \Omega} p(x) \varphi(x)$

Rmq 17 : Souvent on prend une distribution uniforme d'où la définition de C_{moy} à la Def 14.

Ex 18 : Pour le tri rapide, en comptant le nombre de comparaisons on a $C_{moy}(n) = \Theta(n \log n)$

3) Calcul par la résolution de récurrences

On peut parfois exprimer la complexité pour une donnée de taille n par rapport à la complexité pour une donnée de taille strictement inférieure et donc de résoudre l'équation obtenue pour avoir la complexité.

Prop 19 : Pour une suite récurrente linéaire d'ordre 1 $(u_n)_{n \in \mathbb{N}}$ avec $u_{n+1} = a u_n + b$ $\forall n \ge 0$ où $u_0 \in \mathbb{R}$, $a, b \in \mathbb{R}$
Alors $u_n = a^n (u_0 - \ell) + \ell$ où $\ell = \frac{b}{1-a}$ si $a \neq 1$
$u_n = b n + u_0$ si $a = 1$

Ex 20 : Pour l'algorithme de calcul du factoriel où l'on compte le nombre de multiplication
$C(n) = C(n-1) + 1$ donc $a = 1$, $b = 1$, $C(0) = 0$ d'où $C(n) = 1 \times n + 0 = n$

Prop 21 : Master theorem
Soit $t : \mathbb{N} \to \mathbb{R}^+$ croissante à partir d'un certain rang
$n_0 \ge 0$, $b \ge 2$ entiers
$k \ge 0$, $a, c, d > 0$ réels positifs.
tels que $\begin{cases} t(n_0) = d \\ t(n) = a\, t(\frac{n}{b}) + c n^k \end{cases}$ pour $\frac{n}{n_0}$ puissance de b
Alors on a $t(n) = \begin{cases} \Theta(n^k) & \text{si } a < b^k \\ \Theta(n^k \log_b(n)) & \text{si } a = b^k \\ \Theta(n^{\log_b(a)}) & \text{si } a > b^k \end{cases}$

Ex 22 : • Tri Fusion $C(n) = \Theta(n \log n)$
• Algorithme de Strassen pour la multiplication matricielle en $\Theta(n^{\log 7})$

DÉV 1

III Technique pour calculer la complexité amortie

Def 23 : Soit une suite de k opérations $op_1, \dots, op_k$
on appelle complexité amortie $C_{amo} = \max_{op_1 \dots op_k} \sum_{i=1}^{k} C(op_i)$

Rmq 24 : Le max veut simplement dire qu'on se place dans le pire cas

Exemple 25 : que l'on va suivre dans toute la suite de cette partie
Le tableau dynamique où l'on compte "allocations + écriture".
Pour ajouter un élément dans le tableau T_n de taille n :
→ Soit il n'est pas rempli et on met l'élément dans la 1ère case vide
→ Soit il est rempli et on crée un tableau T_{2n}, on copie les n éléments de T_n dans T_{2n} et on met notre élément dans la case $n+1$.

1) Agrégat

C'est un calcul direct : on considère une suite de k ajouts à T_1
Il faut doubler $\lceil \log_2(k) \rceil$ fois la taille du tableau
nbr d'opérations = k (écriture) + $\sum_{i=0}^{\lfloor \log_2(k) \rfloor} 2^i \le 3k$ (copie) ainsi $C_{amo} = 3$ (copie)

2) Comptable

On définit un crédit et une dépense pour chaque type d'opérations, en mettant des crédits plus forts aux opérations peu coûteuses pour rattraper les lourdes dépenses des opérations coûteuses, il faut nécessairement avoir $\sum_{i=1}^{k} cred(op_i) - \sum_{i=1}^{k} dép(op_i) \ge 0$. On a $C_{amo}(op) = C_{réel}(op) + cred(op) - dép(op)$
Dans notre exemple :
T non plein : $cred(op) = 2$; $dép(op) = 0$
T plein : $cred(op) = 2$; $dép(op) = |T|$
D'où $C_{amo}(op) = \begin{cases} 1 + 2 - 0 \\ (|T|+1) + 2 - |T| \end{cases} = 3$

3) Potentiel

Au lieu d'assigner des crédits à des opérations on va associer une énergie potentielle à la structure donnée elle-même (il faut que $\varphi(\text{structure vide}) = 0$ et $\varphi(T) \ge 0$ $\forall T$) on a alors
$C_{amo}(op) = C_{réel}(op) + \varphi(T') - \varphi(T)$ pour $T \leadsto T'$
Dans notre exemple : $\varphi(T) = 2 \times$ cases remplies $-$ # cases totales
$C_{amo}(op) = \begin{cases} 1 + 2 & \text{si pas de réallocation} \\ (|T|+1) + 2 - |T| & \text{sinon} \end{cases} = 3$

IV Amélioration de la complexité d'un algorithme

On peut parfois améliorer la complexité d'un algorithme en choisissant une structure de données plus adaptée. Cependant pour certain problème, il existe une complexité minimale. On ne pourra pas aller en dessous, donc on voudrait atteindre cette borne

1) Complexité minimale pour une classe d'algorithme

Prop 26 : Pour un algorithme de tri par comparaison la complexité est au moins $\Omega(n \log n)$

Ex 27 : Tri par insertion en $\Theta(n^2) \geq \Omega(n \log n)$

On peut trouver des algo de tri qui atteignent cette borne
- Tri fusion en $\Theta(n \log n)$
- Tri par tas en $\Theta(n \log n)$

2) Amélioration par des structures de données adaptées

Ex 28 : Pour le tri par tas on utilise une structure de tas pour obtenir un tri efficace.

Rmq 29 : La complexité peut dépendre de la façon d'implémenter la structure que l'on utilise

Ex 30 : Pour les algorithmes sur les graphes, on peut implémenter les graphes de différentes manières :
- liste de tous les couples (u,v) si il y a une arête de u à v dans le graphe
- liste d'adjacence
- matrice d'adjacence

Rmq 31 : En général, s'il y a beaucoup d'arêtes qui partent de chaque sommet, il est mieux d'utiliser des matrices d'adjacence, dans le cas contraire, les listes d'adjacence sont souvent plus performantes.

Ex 32 : Algorithme de Prim → liste d'adjacence
Algorithme de Floyd Warshall → matrice d'adjacence

On peut aussi ajouter une structure ou changer la structure pour améliorer la complexité.

Ex 33 : Amélioration de l'algo de Morris Pratt en Knuth Morris Pratt, en remplaçant le graphe des occurrences (qui prend une taille $m|\Sigma|$ où m est la taille du motif à rechercher et Σ l'alphabet) par un tableau des tailles des plus longs préfixes (de taille m)

Algorithme de Knuth Morris Pratt : Exemple et complexité

2v2

3) Compromis temps/espace

Souvent on peut améliorer la complexité spatiale au détriment de la complexité temporelle et réciproquement

Prop 34 : On peut parfois utiliser la programmation dynamique pour faire des économies de temps et d'espace

Ex 35 : Calculer les nombres de Fibonacci
- → Naïvement (récursif) en $\Theta(2^n)$ pour le temps et en $\Theta(1)$ pour l'espace si on compte le nombre de variables nécessaires
- → en utilisant 2 variables (pour calculer un seul nombre) en $\Theta(n)$ pour le temps, en $\Theta(1)$ pour l'espace
- → programmation dynamique pour calculer les n premiers nombres en $\Theta(n)$ pour le temps, en $\Theta(n)$ pour l'espace

Rmq 36 : Si on augmente trop la complexité spatiale, cela peut ralentir l'algorithme en pratique car l'accès à la mémoire sera plus long.

Exemples de preuves d'algorithmes : correction et terminaison

927

Def 1 : La spécification consiste à définir exactement les entrées sur lesquels l'algorithme doit tourner et quelles sorties il doit rendre.

(I) Terminaison.

Def 2 : On dit qu'un algorithme termine si son exécution s'arrête après un nombre fini d'étapes pour toute entrée conforme à sa spécification.

Ex 3 : Si l'algorithme A termine alors

```
for i=0 to n do
    A
done
```

termine aussi

```
while true do:
    skip
```

ne termine pas.

Ex 4 :

```
while n≠0
    n := n-1
```

termine ssi $n \geq 0$

Thm 5 : Le problème de l'arrêt

ARRET : { entrée : un algorithme A ; sortie : oui si A termine, non sinon }

est indécidable.

1) Ensemble bien fondé

Def 6 : $(E, \leq)$ est dit bien fondé s'il n'existe pas de suite infinie d'éléments de E strictement décroissante.

Ex 7 : $(\mathbb{N}, \leq)$ est bien fondé, $(\mathbb{Z}, \leq)$ ne l'est pas.

Prop 8 : $\mathbb{N}^2$ muni de l'ordre lexicographique est bien fondé

Prop 9 : Un ensemble $(E, \leq)$ est bien fondé ssi toute partie non vide de E admet un élément minimal

Thm 10 : Soit A un algo récursif, X l'ensemble de ses entrées, $\varphi : X \to E$ avec $(E, \leq)$ bien fondé.

Soit $Y = \{x \in X, \varphi(x) = \min \varphi(X)\} \subset X$

Si A(y) termine pour tout $y \in Y$ et que dans l'exécution de A(x) n'apparaissent, en nombre fini, que des appels à A(z) avec $\varphi(z) < \varphi(x)$, alors l'exécution de A(x) termine pour tout $x \in X$.

Ex 11 :

```
pgcd(a,b):
    if b=0:
        return a
    else
        return pgcd(b, a mod b)
```

{ entrée : $0 \leq b < a$; sortie : pgcd(a,b) } termine par l'ordre naturel sur le premier argument

Ex 12 :

```
ackermann(m,n):
    if m=0:
        return n+1
    elif n=0:
        return ackermann(m-1, 1)
    else:
        return ackermann(m-1, ackermann(m, n-1))
```

{ entrée : $m, n \in \mathbb{N}$; sortie : un entier }

termine en utilisant l'ordre lexicographique

2) Variant de boucle

Def 13 : Un variant de boucle est une quantité à valeur dans un ensemble $(E, \leq)$ bien fondé qui décroît strictement à chaque tour de boucle.

Thm 14 : Si une boucle (dont le corps termine) admet un variant de boucle, alors elle termine.

Ex 15 :

```
divis_euclid(a,b):
    q=0
    r=a
    while r≥b do
        r := r-b
        q := q+1
    done
    return (q,r)
```

{ entrée : $(a,b) \in \mathbb{N} \times \mathbb{N}^*$; sortie : $q, r \in \mathbb{N}$ tq $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$ }

Variant : $r \in \mathbb{N}$.

(II) Correction

Def 16 : Un algorithme est correct s'il est conforme à sa spécification. On parle de correction totale si l'algorithme termine, partielle sinon.

Ex 17 :

```
syracuse(n):
    if n=1:
        return 1
    elif n pair:
        return syracuse(n/2)
    else
        return syracuse(3×n+1)
```

{ entrée : $n \in \mathbb{N}^*$; sortie : 1 }

partiellement correct

Ex 20 : L'algorithme pgcd (Ex 11) est correct.

Ex 21 :

```
tri_inser(L):
    if L==[] then return []
    else return insere(tete(L), tri_inser(queue(L)))

insere(x, L):
    if L==[]:
        return [x]
    elif tete(L) ≥ x:
        return x::L
    else:
        return tete(L)::insere(x, queue(L))
```

tri_inser : { Entrée : Une liste L. ; Sortie : Une liste triée contenant les éléments de L. }

insere : { Entrée : Une liste triée d'éléments de $(E, \leq)$, $x \in E$. ; Sortie : Une liste triée contenant les éléments de L et x. }

L'algorithme tri_inser est correct

DEV 1 : Algorithme du tri topologique et correction

1) Correction des algorithmes récursifs

Prop 18 : Soit $(E, \leq)$ un ensemble bien fondé et p un prédicat sur les éléments de E. Si p est vérifié sur tous les éléments minimaux de E et si $\forall x \in E \left([\forall y < x, p(y)] \Rightarrow p(x) \right)$ alors $\forall x \in E$ p(x).

Thm 19 : Soit A un algorithme récursif, X l'ensemble de ses entrées, $\varphi : X \to E$ avec $(E, \leq)$ bien fondé.

Soit $Y = \{x \in X, \varphi(x) = \min \varphi(X)\} \subset X$ et p un prédicat sur les valeurs calculés par A.

Si p(y) est vérifié pour tout $y \in Y$ et si

$\forall z$ argument d'appel de A dans l'exécution de A(x), $\varphi(z) < \varphi(x)$

et $[\forall z\ p(z)] \Rightarrow p(x)$

Alors p est vérifié pour tout $x \in X$.

2) Correction des algorithmes itératifs

Def 22 : Un invariant de boucle est une propriété vraie au début de la première itération de la boucle et qui vérifie : si elle est vraie au début d'une itération de la boucle, alors elle est vraie à la fin de l'itération

TH 23 : Si une boucle admet un invariant I, alors I est vrai à la sortie de la boucle.

Ex 24 :

```
dijkstra(G, w, v):
    d = [∞, ..., ∞] de taille |V|
    d[v] = 0
    E = ∅
    F = V
    while F≠∅:
        u = Extraire_min(F)
        E = E ∪ {u}
        for s ∈ Adj(u)
            relacher(u, s, w)
    return d
```

{ Entrée : Un graphe $G=(V,E)$ $v \in E$, w un poids sur G ; Sortie : Un tableau d tel que $\forall u \in V$, $d[u] = d(v,u)$ }

Invariant de la boucle while : "$\forall u \in E$, $d[u] = d(v,u)$".

↳ L'algorithme dijkstra est correct.

(III) Logique de Hoare

1) Le langage IMP

Def 25 : On définit les expressions arithmétiques :
$a ::= n \in \mathbb{N} \mid x \in Var \mid a_1 + a_2 \mid a_1 * a_2 \mid a_1 - a_2$
On définit les expressions booléennes :
$b ::= true \mid false \mid a_1 = a_2 \mid a_1 \leq a_2 \mid \neg b_1 \mid b_1 \wedge b_2$
On définit un programmes :
$S ::= skip \mid x := a \mid S_1 ; S_2 \mid if\ b\ then\ S_1\ else\ S_2 \mid while\ b\ do\ S$

Ex 26 : Un programme de factorielle :
$i := 1 ; f := 1 ; while\ i \leq n\ do\ (f := f * i ; i := i + 1)$

2) Sémantique naturelle

L'état de la mémoire est représenté par une fonction $\delta : Var \to \mathbb{Z}$. On note $State = \mathbb{Z}^{Var}$.

Def 27 : On définit les règles de dérivation sygntaxique ci-dessous.
On note $\langle S, \delta \rangle \to \delta'$ s'il existe un arbre de dérivation pour $\langle S, \delta \rangle \to \delta'$

$$* \frac{}{\langle skip, \delta \rangle \to \delta}\ (skip) \qquad * \frac{}{\langle x := a, \delta \rangle \to \delta[x \mapsto a]}\ (affect)$$

$$* \frac{\langle S_1, \delta \rangle \to \delta'' \quad \langle S_2, \delta'' \rangle \to \delta'}{\langle S, \delta \rangle \to \delta'}\ (seq) \qquad * \frac{\langle S_1, \delta \rangle \to \delta'}{\langle if\ b\ then\ S_1\ else\ S_2, \delta \rangle \to \delta'}\ \text{si } [\![b]\!] = true\ (if_t)$$

$$* \frac{\langle S_2, \delta \rangle \to \delta'}{\langle if\ b\ then\ S_1\ else\ S_2, \delta \rangle \to \delta'}\ \text{si } [\![b]\!] = false\ (if_f) \qquad * \frac{\langle S, \delta \rangle \to \delta' \quad \langle while\ b\ do\ S, \delta' \rangle \to \delta''}{\langle while\ b\ do\ S, \delta \rangle \to \delta''}\ \text{si } [\![b]\!] = true$$

$$* \langle while\ b\ do\ S, \delta \rangle \to \delta \quad \text{si } [\![b]\!] = true$$

Th 28 : IMP est déterministe : $\forall S, \forall \delta, \begin{cases} \langle S, \delta \rangle \to \delta_1 \\ \langle S, \delta \rangle \to \delta_2 \end{cases} \Rightarrow \delta_1 = \delta_2$

Def 29 : On définit $\mathcal{Y}_{ns}[\![S]\!]_\delta = \begin{cases} \delta' \text{ si } \langle S, \delta \rangle \to \delta \\ \underline{undef} \end{cases}$

Ex 30 : L'arbre sémantique de "while true do skip" est infini, donc $\mathcal{Y}_{ns}[\![while\ true\ do\ skip]\!] = \underline{undef}$

3) Triplets de Hoare

Def 31 : On appelle triplet de Hoare un triplet de la forme $\{P\} S \{Q\}$ où P et Q sont des prédicats et S est un programme.

Def 32 : On définit les règles de dérivation suivantes :

$$* \frac{}{\{P\}\ skip\ \{P\}}\ (skip_H) \qquad * \frac{}{\{P[x \mapsto a]\}\ x := a\ \{P\}}\ (Aff_H)$$

$$* \frac{\{\ \}\ S_1\ \{Q\} \quad \{Q\}\ S_1\ \{R\}}{\{P\}\ S_1 ; S_2\ \{R\}}\ (seq_H) \qquad * \frac{\{[\![b]\!] \wedge P\}\ S_1\ \{Q\} \quad \{[\![\neg b]\!] \wedge P\}\ S_2\ \{Q\}}{\{P\}\ if\ b\ then\ S_1\ else\ S_2\ \{Q\}}\ (if_H)$$

$$* \frac{\{[\![b]\!] \wedge P\}\ S\ \{P\}}{\{P\}\ while\ b\ do\ S\ \{\neg [\![b]\!] \wedge P\}}\ (while_H) \qquad * \frac{\{P'\}\ S\ \{Q'\}}{\{P\}\ S\ \{Q\}}\ \text{si} \begin{cases} P \Rightarrow P' \\ Q' \Rightarrow Q \end{cases}\ (CSQ)$$

Def 33 : On note $\vdash \{P\} S \{Q\}$ s'il existe un arbre de dérivation pour $\{P\} S \{Q\}$
On note $\models \{P\} S \{Q\}$ si $(\forall \delta \in State$ tel que $\delta \models P,\ \mathcal{Y}_{ns}[\![S]\!]_\delta \models Q)$
(par convension, $\underline{undef} \models Q$ pour tout Q)

Th 34 : $(\vdash \{P\} S \{Q\}) \Rightarrow (\models \{P\} S \{Q\})$

DEV 2 : $(\models \{P\} S \{Q\}) \Rightarrow (\vdash \{P\} S \{Q\})$

Ex 35 : On a $\vdash \{x = n\}\ y := 1 ; while\ \neg(x = 1)\ do\ (y := y * x ; x := x - 1)\ \{y = n!\}$

Références :

* Cormen, Leiserson, Rivest, Stein, Introduction à l'algorithmique
* Albert, Cours et exercices d'informatique
* Froidevaux, Gaudel, Soria, Types de données et algorithmes
* Nielson, Nielson, Semantics with applications
* Winskel, The formal semantics of programming languages

929

Lambda calcul pur comme modèle de calcul. Exemples.

(*) M et N sont alors des sous termes de (MN) (**) M est alors un sous terme de (λx.M)

But : Avoir un modèle de calcul fonctionnel pour calculer des fonctions

I Termes de λ-calcul : syntaxe

Def 1 : On se donne un ensemble de variables VAR dénombrable $\{x, y, z, \dots\}$. On définit les termes de λ-calcul par induction
(i) Les variables sont des termes
(*) (ii) Si M et N sont des termes, alors (MN) est un terme
(**) (iii) Si M est un terme, alors (λx.M) est un terme où $x \in VAR$

Ex 2 : $(\lambda x.(xy))$; $((\lambda y.y)(\lambda x.(xy)))$ sont des termes
$(x(\lambda x))$ n'est pas un terme.

Rmq 3 : On notera MNP pour ((MN)P) où M,N,P termes
et λxy.M pour (λx.(λy.M)) où M terme et $x, y \in VAR$

Def 4 : La longueur d'un terme est définie par induction
$lg(x) = 1$ pour $x \in VAR$
$lg(MN) = lg(M) + lg(N)$ pour M, N termes
$lg(\lambda x.M) = 1 + lg(M)$ pour $x \in VAR$ et M un terme.

Def 5 : Dans un sous terme λx.M on dit que M et ses sous termes sont dans la portée de λx

Def 6 (lié) Une occurrence x est liée dans un terme P si x est un sous terme de P et x est dans la portée d'un λx qui est dans P.

Def 7 (libre) Une occurrence x est libre dans un terme P si elle n'est pas liée et qu'elle est dans le terme P

Ex 8 : λx.y on a y est libre
(x(λx.x)) la première occurrence de x est libre, la deuxième est liée
((λy.y)(λx.(xy))) le 1er y lié, le 2ème est libre, x est lié

Def 9 : Si un terme n'a pas de variable libre, il est dit clos.

Ex 10 : $I = \lambda x.x$ $K = \lambda xy.x$ $S = \lambda xyz.xz(yz)$ sont 3 termes clos.

Def 11 (Substitution) Soit M, N des termes, $x \in VAR$
La substitution de x par N dans M est le remplacement de chaque occurrence libre de x dans M par N en renommant si besoin les variables libres de N pour qu'elles restent libres dans [N/x]M où l'on a noté la substitution [N/x]M.
→ par des variables fraîches

Def 12 : On définit l'α-conversion comme la plus petite relation d'équivalence $\equiv_\alpha$ satisfaisant :
(i) $\lambda x.M \equiv_\alpha \lambda y.([y/x]M)$ si y n'est pas libre dans M
(ii) $\lambda x.M \equiv_\alpha \lambda x.N$ si $M \equiv_\alpha N$
(iii) $MN \equiv_\alpha PQ$ si $M \equiv_\alpha P$ et $N \equiv_\alpha Q$

Ex 13 : $\lambda xy.x(xy) \equiv_\alpha \lambda uv.u(uv)$

II β-réduction

Def 14 : La β-réduction est définie par induction sur les termes
- $(\lambda x.M)N \to_\beta [N/x]M$
- Si $M \to_\beta M'$, alors $\lambda x.M \to_\beta \lambda x.M'$
- Si $M \to_\beta M'$, alors $MN \to_\beta M'N$
- Si $N \to_\beta N'$, alors $MN \to_\beta MN'$

Ex 15 : $(\lambda xy.yx)uv \to_\beta (\lambda y.yu)v \to_\beta vu$
$(\lambda x.xxy)(\lambda y.yz) \to_\beta (\lambda y.yz)(\lambda y.yz)y$
$\to_\beta (\lambda y.yz)zy \to_\beta zzy$
(cf Annexe ①)

Def 16 (forme normale) Un terme M est sous forme normale si il ne peut plus être β-réduit.

Ex 17 : vu et zzy sont en forme normale
$(\lambda x.xx)(\lambda x.xx)$ n'a pas de forme normale

Thm 18 (Church-Rosser) Si $P \to_\beta^* M$ et $P \to_\beta^* N$ alors il existe T tel que $M \to_\beta^* T$ et $N \to_\beta^* T$ (cf Annexe ②a)

Corollaire 19 : Si P admet une forme normale, alors cette forme normale est unique (à $\equiv_\alpha$ près).

Def 20 (β-équivalence) M et N sont β-équivalents ($M =_\beta N$) Si il existe $M_1 \dots M_n$ avec $M_1 \equiv_\alpha M$ et $M_n \equiv_\alpha N$ et $\forall i \in \{1, \dots, n-1\}$ $M_i \to_\beta^* M_{i+1}$ ou $M_{i+1} \to_\beta^* M_i$
(C'est la clôture symétrique transitive de $\to_\beta$)

Thm 21 (Church Rosser) Si $M =_\beta N$, alors il existe T tel que $M \to_\beta^* T$ et $N \to_\beta^* T$ (cf Annexe ②b)

Ex 22 : $(\lambda xyz.xzy)(\lambda xy.x) =_\beta (\lambda xy.x)(\lambda x.x)$
$\downarrow_\beta$ $\lambda yz.[(\lambda xy.x)zy]$ $\downarrow_\beta$ $\lambda yx.x$
$\downarrow_\beta$ $\lambda yz.[\lambda y.z] \to_\beta \lambda yz.z$ et $\lambda yz.z \equiv_\alpha \lambda yx.x$

Def 23 : On dit que M est un combinateur de point fixe si M est clos et pour tout terme clos F :
$MF =_\beta F(MF)$

Ex 24 : $Y = \lambda f.(\lambda x.f(xx))(\lambda x.f(xx))$ est un combinateur de point fixe
$A = \lambda xy.y(xxy)$ $\Theta = AA$ est un combinateur de point fixe (Turing)
(cf Annexe ③)

III Représentation de données

A - Booléens :

$T := \lambda xy.x$ (Vrai) $F := \lambda xy.y$ (Faux)
si B alors M sinon $N := BMN$ (Conditionnelle)

B - Paires et listes :

$\langle M, N \rangle := \lambda x.xMN$ (paire) (liste)
$[M_1, \dots, M_n] := \langle M_1, \langle M_2, \dots \langle M_{n-1}, M_n \rangle \dots \rangle \rangle$
$hd := \lambda x.xT$ $tl := \lambda x.xF$
$\langle \pi_1, \dots, \pi_n \rangle := \lambda x.x\pi_1 \dots \pi_n$ (tuple)
$\pi_i^n := \lambda x.xU_i^n$ où $U_i^n = \lambda x_1 \dots x_n.x_i$ (projection)

C - Entiers de Church

(entiers) $\to [\![n]\!]_C := \lambda sz.s^n z$ où $s^n z = \underbrace{s(s \dots (sz) \dots)}_{n \text{ fois}}$
(successeur) $\to [\![succ]\!]_C := \lambda nsz.ns(sz)$
(is-zero) $\to [\![is\text{-}zero]\!]_C := \lambda n.n(\lambda x.F)T$
(addition) $\to [\![+]\!]_C := \lambda n_1 n_2.n_1 [\![succ]\!]_C n_2$

D - Entiers de Barendregt

(zero) $\to [\![0]\!]_B := \lambda x.x$
(entiers) $\to [\![n+1]\!]_B := \langle F, [\![n]\!]_B \rangle$
(successeur) $\to [\![succ]\!]_B := \lambda x.\langle F, x \rangle$
(prédécesseur) $\to [\![pred]\!]_B := \lambda x.xF$
(is-zero) $\to [\![is\text{-}zero]\!]_B := \lambda x.xT$

IV. Modèle de calcul

Def 25 : Une fonction $f : \mathbb{N}^p \to \mathbb{N}$ est dite λ-définissable s'il existe F en terme clos tel que
$\forall n_1, \dots, n_p \in \mathbb{N}$ $[\![f(n_1, \dots, n_p)]\!]_\beta = F\,[\![n_1]\!]_\beta \cdots [\![n_p]\!]_\beta$
On dit que F représente f.

Thèse de Church 27 : Les fonctions calculables par une procédure effective sont exactement les fonctions λ-définissables.

1) Lien avec les fonctions μ-récursives

Def 28 : Les fonctions primitives récursives sont définies par induction
- zero, succ, projections sont primitives récursives
- la composition de f.p.r est f.p.r
- si g et h sont des f.p.r alors le schéma de récursion $f(\vec{x}, k) = \begin{cases} h(\vec{x}) \text{ si } k = 0 \\ g(\vec{x}, k, f(\vec{x}, k-1)) \text{ sinon} \end{cases}$ est une fonction primitive récursive.

Def 29 : On appelle minimisation non bornée la fonction $\mu[\![F]\!]$ qui à x associe le plus petit indice i tel que $F(\vec{x}, i) \neq 0$

Def 30 : Les fonctions μ-récursives sont le plus petit ensemble contenant les fonctions primitives récursives et clos par minimisation non bornée.

Thm 31 : Les fonctions μrécursives sont λ-définissables — DÉV 1

Thm 32 : Les fonctions λ-définissables sont μ-récursives

Def 33 (Séparabilité) : $A, B \in \mathcal{P}(\mathbb{N})$ sont récursivement séparables s'il existe une fonction récursive totale φ telle que
$n \in A \Rightarrow \varphi(n) = 0$
$n \in B \Rightarrow \varphi(n) = 1$

Thm 34 (Scott Curry) : Aucune paire d'ensembles non vides de termes clos par β équivalence ne sont récursivement séparables. — DÉV 2

Corollaire 35 : Le problème
{entrée : un terme T du λ-calcul
sortie : oui si T a une forme normale, non sinon
est indécidable.

2) Lien avec les machines de Turing

Thm 36 : Les fonctions μ-récursives sont exactement les fonctions calculables par une machine de Turing.

Corollaire 37 : Le λ-calcul et les machines de Turing sont des modèles de calcul équivalents

Références : Barendregt, The Lambda Calculus its syntax and semantics
Hindley & Seldin, Lambda Calculus and combinators
Lassaigne & de Rougemont, Logique et fondements de l'informatique

---

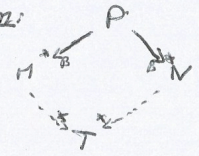
Annexes :

① β-réduction

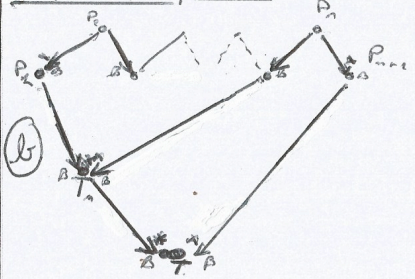
$(\lambda xyz.\, xz(yz))((\lambda xy.\, yx)u)((\lambda xy.\, yx)v)\,w$
$\to_\beta (\lambda xyz.\, xz(yz))(\lambda y.\, yu)(\lambda y.\, yv)\,w$
$\to_\beta (\lambda yz.\, (\lambda y.\, yu)z(yz))(\lambda y.\, yv)\,w$
$\to_\beta (\lambda yz.\, zu(yz))(\lambda y.\, yv)\,w$
$\to_\beta (\lambda z.\, zu((\lambda y.\, yv)z))\,w$
$\to_\beta (\lambda z.\, zu(zv))\,w$
$\to_\beta wu(wv)$

② Propriété de Church-Rosser

Version β-réduction :



Version β-équivalence



③ Combinateurs de point fixe.

$Y F \to_\beta (\lambda x.\, F(xx))(\lambda x.\, F(xx))$
$\to_\beta^* F((\lambda x.\, F(xx))(\lambda x.\, F(xx)))$
$_\beta\!\leftarrow F(YF)$

$\Theta F \to_\beta AAF$
$\to_\beta F(AAF) = F(\Theta F)$.

Sémantique des langages de programmation. Exemples.

J30

Motivations : * Raisonner sur le comportement attendu des programmes d'un langage de programmation via des modèles mathématiques (une sémantique).
* Plusieurs modèles mathématiques peuvent décrire un même langage de programmation.

I. Le langage IMP [1, p. 7]

A. Syntaxe du langage IMP

Définition 1 : On définit la syntaxe du langage IMP avec les ensembles :
* l'ensemble des entiers n noté Num ;
* l'ensemble des variables x noté Var ;
* l'ensemble des expressions arithmétiques a noté Aexp ;
* l'ensemble des expressions booléennes b noté Bexp ;
* l'ensemble des instructions S notée Stm.

et la grammaire associée :

$a ::= n \mid x \mid a_1 \oplus a_2 \mid a_1 \otimes a_2 \mid a_1 \ominus a_2$

$b ::= \text{True} \mid \text{False} \mid a_1 = a_2 \mid a_1 \leq a_2 \mid \neg b \mid b_1 \wedge b_2$

$S ::= x := a \mid \text{skip} \mid S_1 ; S_2 \mid \text{if } b \text{ then } S_1 \text{ else } S_2 \mid \text{while } b \text{ do } S$

Exemple 2 : Factorielle (n) : $i := 1$; rep := 1 ; while $i \leq n$ do (rep := rep $\otimes$ i ; $i := i \oplus 1$)

Fibonacci (n) : $x := 1$; $y := 1$; $i := 2$; while $i \leq n$ do ($y := x \oplus y$; $x := y \ominus x$; $i := i \oplus 1$)

Arbres de syntaxe en annexe (Figure 1).

B. Sémantique dénotationnelle des expressions.

Idée : Les sémantiques dénotationnelles modélisent le comportement par une fonction mathématique.

Définition 3 : On définit la sémantique des expressions du langage IMP par :
* $\mathcal{D} : \text{Bexp} \to (\text{State} \to \{\text{tt}, \text{ff}\})$
* $\mathcal{A} : \text{Aexp} \to (\text{State} \to \mathbb{Z})$

$\mathcal{A}[\![n]\!]_\sigma = \mathcal{N}[\![n]\!]$

$\mathcal{A}[\![x]\!]_\sigma = \sigma(x)$

$\mathcal{A}[\![a_1 \oplus a_2]\!]_\sigma = \mathcal{A}[\![a_1]\!]_\sigma + \mathcal{A}[\![a_2]\!]_\sigma$

$\mathcal{A}[\![a_1 \ominus a_2]\!]_\sigma = \mathcal{A}[\![a_1]\!]_\sigma - \mathcal{A}[\![a_2]\!]_\sigma$

$\mathcal{A}[\![a_1 \otimes a_2]\!]_\sigma = \mathcal{A}[\![a_1]\!]_\sigma \times \mathcal{A}[\![a_2]\!]_\sigma$

avec $\sigma \in \text{State}$.

* $\text{State} : \text{Var} \to \mathbb{Z}$
* $\mathcal{N} : \text{Num} \to \mathbb{Z}$, $\mathcal{N}[\![n]\!] = n$

$\mathcal{D}[\![\text{True}]\!]_\sigma = \text{tt}$

$\mathcal{D}[\![\text{False}]\!]_\sigma = \text{ff}$

$\mathcal{D}[\![a_1 = a_2]\!]_\sigma = \begin{cases} \text{tt} & \text{si } \mathcal{A}[\![a_1]\!]_\sigma = \mathcal{A}[\![a_2]\!]_\sigma \\ \text{ff} & \text{sinon} \end{cases}$

$\mathcal{D}[\![a_1 \leq a_2]\!]_\sigma = \begin{cases} \text{tt} & \text{si } \mathcal{A}[\![a_1]\!]_\sigma \leq \mathcal{A}[\![a_2]\!]_\sigma \\ \text{ff} & \text{sinon} \end{cases}$

$\mathcal{D}[\![\neg b]\!]_\sigma = \begin{cases} \text{tt} & \text{si } \mathcal{D}[\![b]\!]_\sigma = \text{ff} \\ \text{ff} & \text{sinon} \end{cases}$

$\mathcal{D}[\![b_1 \wedge b_2]\!]_\sigma = \begin{cases} \text{tt} & \text{si } \mathcal{D}[\![b_1]\!]_\sigma = \mathcal{D}[\![b_2]\!]_\sigma = \text{tt} \\ \text{ff} & \text{sinon} \end{cases}$

Remarque 4 : On suppose que la fonction State est totale. On la représentera par une liste finie.

Exemple 5 : On pose $\sigma = [x \mapsto 3]$. On calcule :

$\mathcal{A}[\![x \oplus 1]\!]_\sigma = \mathcal{A}[\![x]\!]_\sigma + \mathcal{A}[\![1]\!]_\sigma = \sigma(x) + \mathcal{N}[\![1]\!] = 3 + 1 = 4$

$\mathcal{D}[\![x = 1]\!]_\sigma = \begin{cases} \text{tt} & \text{si } \sigma(x) = \mathcal{N}(1) \\ \text{ff} & \text{sinon} \end{cases} = \begin{cases} \text{tt} & \text{si } 3 = 1 \\ \text{ff} & \text{sinon} \end{cases} = \text{ff}$

Remarque 6 : Les fonctions $\mathcal{A}$ et $\mathcal{D}$ sont totales, mais elles ne le seraient pas en présence d'un opérateur Binaire de division.

II. Sémantiques opérationnelles.

Idée : Les sémantiques opérationnelles modélisent le comportement par un système de transitions dont les règles $\langle S, \sigma \rangle \to \sigma'$ modélisent le fait "l'exécution de S sur l'état σ termine dans l'état σ'".

A. Sémantique à grands pas [1, p. 20]

Définition 7 : On définit inductivement la sémantique à grands pas des instructions du langage IMP à l'aide de règles de la forme $\langle S, \sigma \rangle \to \sigma'$ pour $\sigma, \sigma' \in \text{State}$.

$[\text{ass}_{NS}]$ $\langle x := a, \sigma \rangle \to \sigma[x \mapsto \mathcal{A}[\![a]\!]_\sigma]$ $\quad [\text{skip}_{NS}]$ $\langle \text{skip}, \sigma \rangle \to \sigma$

$[\text{comp}_{NS}]$ $\dfrac{\langle S_1, \sigma \rangle \to \sigma' \quad \langle S_2, \sigma' \rangle \to \sigma''}{\langle S_1 ; S_2, \sigma \rangle \to \sigma''}$

$[\text{if}^{\text{tt}}_{NS}]$ $\dfrac{\langle S_1, \sigma \rangle \to \sigma'}{\langle \text{if } b \text{ then } S_1 \text{ else } S_2, \sigma \rangle \to \sigma'}$ si $\mathcal{D}[\![b]\!]_\sigma = \text{tt}$

$[\text{if}^{\text{ff}}_{NS}]$ $\dfrac{\langle S_2, \sigma \rangle \to \sigma'}{\langle \text{if } b \text{ then } S_1 \text{ else } S_2, \sigma \rangle \to \sigma'}$ si $\mathcal{D}[\![b]\!]_\sigma = \text{ff}$

$[\text{while}^{\text{tt}}_{NS}]$ $\dfrac{\langle S, \sigma \rangle \to \sigma' \quad \langle \text{while } b \text{ do } S, \sigma' \rangle \to \sigma''}{\langle \text{while } b \text{ do } S, \sigma \rangle \to \sigma''}$ si $\mathcal{D}[\![b]\!]_\sigma = \text{tt}$

$[\text{while}^{\text{ff}}_{NS}]$ $\langle \text{while } b \text{ do } S, \sigma \rangle \to \sigma$ si $\mathcal{D}[\![b]\!]_\sigma = \text{ff}$

Définition 8 : On appelle arbre de dérivation la succession d'applications des règles et des axiomes.

Exemple 9 : L'arbre de dérivation de la factorielle (Figure 2 en annexe).

Proposition 10 : Un langage est déterministe sous la sémantique à grands pas si et seulement si pour tout $S, \sigma, \sigma', \sigma''$, ($\langle S, \sigma \rangle \to \sigma'$ et $\langle S, \sigma \rangle \to \sigma''$) implique $\sigma' = \sigma''$.

Application 11 : Le langage IMP est déterministe sous la sémantique à grands pas.

Contre-exemple 12 : Le langage IMP muni d'une nouvelle instruction choix $S_1 \square S_2$ dont la sémantique est donnée par les règles : $\dfrac{\langle S_1, \sigma \rangle \to \sigma' \quad \langle S_2, \sigma \rangle \to \sigma''}{\langle S_1 \square S_2, \sigma \rangle \to \sigma'}$ et $\dfrac{\langle S_1, \sigma \rangle \to \sigma' \quad \langle S_2, \sigma \rangle \to \sigma''}{\langle S_1 \square S_2, \sigma \rangle \to \sigma''}$ est un langage non-déterministe sous la sémantique à grands pas.

Définition 13 : La sémantique à grands pas peut s'écrire sous la forme d'une fonction telle que $\mathcal{G}_{NS} : \text{Stm} \to (\text{State} \hookrightarrow \text{State})$ et $\mathcal{G}_{NS}[\![S]\!]\sigma = \begin{cases} \sigma' \text{ si } \langle S, \sigma \rangle \to \sigma' \\ \text{undef sinon} \end{cases}$

Exemple 14 : $\mathcal{G}_{NS}[\![\text{while true do skip}]\!]_\sigma = \text{undef}$

Définition 15 : Deux instructions S_1 et S_2 sont sémantiquement équivalentes si pour tout $\sigma, \sigma' \in \text{State}$, $\langle S_1, \sigma \rangle \to \sigma'$ si et seulement si $\langle S_2, \sigma \rangle \to \sigma'$.

Exemple 16 : Les instructions (while b do S) et (if b then (S; while b do S) else skip) sont sémantiquement équivalentes.

Contre-exemple 17 : Les instructions $x := 3$; $x := x \oplus 1$ et $x := x \oplus 1$; $x := 3$ ne sont pas équivalentes sémantiquement.

Limite : La sémantique à grands pas ne permet pas d'exprimer la terminaison.

B. Sémantique à petits pas [1, p. 33]

Idée : La sémantique à petits pas est plus fine que la précédente : elle se concentre sur les étapes de l'exécution : les affectations et les tests.

Définition 18 : On définit inductivement la sémantique à petits pas des instructions du langage IMP à l'aide de règles du type $\langle S, \sigma \rangle \Rightarrow \gamma$ où $\sigma \in \text{State}$ et γ est de la forme $\langle S', \sigma' \rangle$ ou σ' avec $\sigma' \in \text{State}$ et $S' \in \text{Stm}$.

$[\text{ass}_{SOS}]$ $\langle x := a, \sigma \rangle \Rightarrow \sigma[x \mapsto \mathcal{A}[\![a]\!]_\sigma]$ $\quad [\text{skip}_{SOS}]$ $\langle \text{skip}, \sigma \rangle \Rightarrow \sigma$

$[\text{comp}^1_{SOS}]$ $\dfrac{\langle S_1, \sigma \rangle \Rightarrow \langle S_1', \sigma' \rangle}{\langle S_1 ; S_2, \sigma \rangle \Rightarrow \langle S_1' ; S_2, \sigma' \rangle}$ $\quad [\text{comp}^2_{SOS}]$ $\dfrac{\langle S_1, \sigma \rangle \Rightarrow \sigma'}{\langle S_1 ; S_2, \sigma \rangle \Rightarrow \langle S_2, \sigma' \rangle}$

$[\text{if}^{\text{tt}}_{SOS}]$ $\langle \text{if } b \text{ then } S_1 \text{ else } S_2, \sigma \rangle \Rightarrow \langle S_1, \sigma \rangle$ si $\mathcal{D}[\![b]\!]_\sigma = \text{tt}$

$[\text{if}^{\text{ff}}_{SOS}]$ $\langle \text{if } b \text{ then } S_1 \text{ else } S_2, \sigma \rangle \Rightarrow \langle S_2, \sigma \rangle$ si $\mathcal{D}[\![b]\!]_\sigma = \text{ff}$

$[\text{while}_{SOS}]$ $\langle \text{while } b \text{ do } S, \sigma \rangle \Rightarrow \langle \text{if } b \text{ then } (S ; \text{while } b \text{ do } S) \text{ else skip}, \sigma \rangle$

Définition 19 : Une séquence de dérivations pour $S \in \text{Stm}$ et $\sigma \in \text{State}$ est soit une séquence finie $\gamma_0 \Rightarrow \cdots \Rightarrow \gamma_k$ avec $\gamma_0 = \langle S, \sigma \rangle$ et γ_k une configuration finale, soit une séquence infinie $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \cdots$ où $\gamma_0 = \langle S, \sigma \rangle$.

Exemple 20 : Une séquence de dérivations de la factorielle (Figure 3)

Proposition 21 : Un langage est déterministe sous la sémantique à petits pas si et seulement si pour tout $S \in \text{Stm}$, $\sigma \in \text{State}$, γ et γ', $\langle S, \sigma \rangle \Rightarrow \gamma$ et $\langle S, \sigma \rangle \Rightarrow \gamma'$ implique que $\gamma = \gamma'$.

Application 22 : Le langage IMP est déterministe sous la sémantique à petits pas.

Définition 23 : La fonction sémantique à petits pas est telle que :

$\mathcal{G}_{SOS} : \text{Stm} \to (\text{State} \hookrightarrow \text{State})$ et $\mathcal{G}_{SOS}[\![S]\!]\sigma = \begin{cases} \sigma' \text{ si } \langle S, \sigma \rangle \Rightarrow^* \sigma' \\ \text{undef sinon} \end{cases}$

Proposition 24 : Si $\langle S_1 ; S_2, \sigma \rangle \Rightarrow^k \sigma''$ alors il existe $\sigma' \in \text{State}$ et $k_1, k_2 \in \mathbb{N}$ tels que $\langle S_1, \sigma \rangle \Rightarrow^{k_1} \sigma'$ et $\langle S_2, \sigma' \rangle \Rightarrow^{k_2} \sigma''$ avec $k_1 + k_2 = k$.

Proposition 25 : Si $\langle S_1, \sigma \rangle \Rightarrow^k \sigma'$ alors $\langle S_1 ; S_2, \sigma \rangle \Rightarrow^k \langle S_2, \sigma' \rangle$.

Définition 26 : Deux instructions S_1 et S_2 sont sémantiquement équivalentes si et seulement si :
* $\exists \sigma'' \in \text{State}$, $\langle S_1, \sigma \rangle \Rightarrow^* \sigma''$ et $\langle S_2, \sigma \rangle \Rightarrow^* \sigma''$
ou
* $\forall k \in \mathbb{N}, \exists \gamma_1, \gamma_2$, $\langle S_1, \sigma \rangle \Rightarrow^k \gamma_1$ et $\langle S_2, \sigma \rangle \Rightarrow^k \gamma_2$

Exemple 27 : Les instructions (while b do S) et (if b then (S; while b do S) else skip) sont sémantiquement équivalentes.

C. Equivalence de ces deux sémantiques [1, p. 41]

Théorème 28 (Equivalence des sémantiques)
Pour toute instruction S du langage IMP, on a $\mathcal{G}_{NS}[\![S]\!] = \mathcal{G}_{SOS}[\![S]\!]$

DEV1

III. Sémantique dénotationnelle [1, p. 91]

Idée : On définit la sémantique dénotationnelle pour les instructions du langage IMP (modélisation par des fonctions). On utilise alors la théorie du point fixe afin de définir la sémantique du while.

Remarque 29 : On commence par définir la sémantique pour l'ensemble des instructions. Puis on montre que cette sémantique est bien définie en détaillant la théorie du point fixe.

Définition 30 : On définit la sémantique dénotationnelle des instructions du langage IMP par la fonction sémantique $\mathcal{G}_{DS} : \text{Stm} \to (\text{State} \hookrightarrow \text{State})$ définie par : $\mathcal{G}_{DS}[\![x := a]\!]\sigma = \sigma[x \mapsto \mathcal{A}[\![a]\!]_\sigma]$ $\quad \mathcal{G}_{DS}[\![\text{skip}]\!] = id$

$\mathcal{G}_{DS}[\![S_1 ; S_2]\!] = \mathcal{G}_{DS}[\![S_2]\!] \circ \mathcal{G}_{DS}[\![S_1]\!]$ $\quad \mathcal{G}_{DS}[\![\text{if } b \text{ then } S_1 \text{ else } S_2]\!] = \text{cond}(\mathcal{D}[\![b]\!], \mathcal{G}_{DS}[\![S_1]\!], \mathcal{G}_{DS}[\![S_2]\!])$

$\mathcal{G}_{DS}[\![\text{while } b \text{ do } S]\!] = \text{Fix } F$

avec $F(g) = \text{cond}(\mathcal{D}[\![b]\!], g \circ \mathcal{G}_{DS}[\![S]\!], id)$ $\quad \text{cond}(p, g_1, g_2)\sigma = \begin{cases} g_1\sigma \text{ si } p\sigma = \text{tt} \\ g_2\sigma \text{ sinon} \end{cases}$

Fix : $((\text{State} \hookrightarrow \text{State}) \to (\text{State} \hookrightarrow \text{State})) \to (\text{State} \hookrightarrow \text{State})$
qui se lit "le plus petit point fixe".

Exercice 31 : while $\neg(x = 0)$ do skip possède plusieurs points fixes.

$\mathcal{G}_{DS}[\![\text{while } \neg(x=0) \text{ do skip}]\!] = (F\,g)\sigma = \begin{cases} g\sigma \text{ si } \neg(\sigma x = 0) \\ \sigma \text{ sinon} \end{cases}$. On pose $g_0\sigma = \sigma$ et $g_\sigma\sigma = \begin{cases} \text{undef sinon} \\ \sigma \text{ si } \sigma(x) = 0 \end{cases}$ qui sont des points fixes pour cette instruction.

Définition 32 : Deux instructions S_1 et S_2 sont sémantiquement équivalentes si et seulement si $\mathcal{G}_{DS}[\![S_1]\!] = \mathcal{G}_{DS}[\![S_2]\!]$.

Exemple 33 : (S; skip) et (S) sont sémantiquement équivalentes.

A. Théorie du point fixe

Définition 34 : On introduit un ordre partiel $\sqsubseteq$ sur $(\text{State} \hookrightarrow \text{State})$: $g_1 \sqsubseteq g_2$ si et seulement si $g_1\sigma = \sigma' \Rightarrow g_2\sigma = \sigma'$.

Définition 35 : Etant donné $(D, \sqsubseteq)$, $C \subseteq D$ est une chaîne si $\forall d_1, d_2 \in C$ $d_1 \sqsubseteq d_2$ ou $d_2 \sqsubseteq d_1$.

Exemple 36 : On définit $\forall n \in \mathbb{N}$, $g_n\sigma = \begin{cases} \text{undef si } x > n \\ \sigma[x \mapsto 1] \text{ si } 0 \leq x \leq n \\ \sigma \text{ sinon} \end{cases}$

$\{g_i\}$ est une chaîne pour $(\text{State} \hookrightarrow \text{State}, \sqsubseteq)$.

Définition 37 : $(D, \sqsubseteq)$ est un CCPO (chain complete partial order) si et seulement si pour toute chaîne Y, Y a une borne inférieure $\sqcup Y$.

Proposition 38 : $(\text{State} \hookrightarrow \text{State}, \sqsubseteq)$ est un CCPO de borne inférieure $\perp$ où $\perp$ est la fonction partielle $\perp\sigma = \text{undef}$ $\forall \sigma$.

Définition 39 : Soient $(D, \sqsubseteq)$, $(D', \sqsubseteq')$ deux CCPO et $f : D \to D'$ une fonction :
* f est monotone si et seulement si $\forall d_1, d_2 \in D$, $d_1 \sqsubseteq d_2 \Rightarrow f(d_1) \sqsubseteq' f(d_2)$
* f est continue si et seulement si elle est monotone et pour toute chaîne de D (non vide) $\sqcup' \{f(d), d \in Y\} = f(\sqcup Y)$.

Proposition 40 : La fonction $F(g) = \text{cond}(\mathcal{D}[\![b]\!], g \circ \mathcal{G}_{DS}[\![S]\!], id)$ est une fonction continue.

Théorème 41: Soit f une fonction continue de $D \to D$. Fix$(f) = \bigsqcup \{f^n(\perp) \mid n \geq 0\}$ est un élément de D et se lit "le plus petit point fixe".
Conséquence: La sémantique dénotationnelle de l'instruction while est bien définie.

C - Équivalence des sémantiques

Théorème 42: Pour toute instruction S du langage IMP, on a $\mathcal{S}_{SOS}[\![S]\!] = \mathcal{S}_{DS}[\![S]\!]$
Corollaire 43: Pour toute instruction S du langage IMP, on a $\mathcal{S}_{DS}[\![S]\!] = \mathcal{S}_{NS}[\![S]\!]$

IV - Sémantique axiomatique (Hoare partielle) [1, p.212]

Idée: Cette sémantique facilite la preuve de programme et son automatisation. On se base sur les systèmes de déduction en logique que nous sommes capable de bien manipuler.
Correction partielle: on donne des garanties que si le programme termine.

A - Triplet de Hoare.

Définition 44: On définit le langage des prédicats :
$P ::= b \mid P \wedge P \mid P \vee P \mid \neg P \mid P[x \mapsto a] \mid P[[a]] \mid P \Rightarrow P$
avec $b \in \mathbb{B}exp$, $a \in Aexp$ et $x \in Var$.
Définition 45: On définit la sémantique des prédicats : pour tout $\sigma \in State$
* $b\ \sigma$ si et seulement si $\mathcal{B}[\![b]\!]_\sigma = tt$
* $(P_1 \wedge P_2)_\sigma$ si et seulement si $P_1\ \sigma$ et $P_2\ \sigma$
* $(P_1 \vee P_2)_\sigma$ si et seulement si $P_1\ \sigma$ ou $P_2\ \sigma$
* $(\neg P)_\sigma$ si et seulement si $\neg(P\ \sigma)$
* $(P[x \mapsto a][[a]])_\sigma$ si et seulement si $P(\sigma[x \mapsto \mathcal{A}[\![a]\!]_\sigma])$
* $(P_1 \Rightarrow P_2)_\sigma$ si et seulement si $P_1\ \sigma$ implique $P_2\ \sigma$.

Définition 46: Un triplet de Hoare est la donnée d'une précondition P, d'une instruction S et d'une postcondition Q avec P et Q des prédicats. On la note $\{P\}\ S\ \{Q\}$.
Exemple 47: Un triplet de Hoare pour la factorielle
$\{n \geq 0\}\ y := 1;$ while $\neg(x = 0)$ do $(y := y \otimes x;\ x := x \ominus 1)\ \{y = n!\}$
Définition 48 (validité pour la sémantique à grands pas)
$\vdash_p \{P\}\ S\ \{Q\}$ si et seulement si $\forall \sigma\ P\sigma = tt$, si $\langle S, \sigma\rangle \to \sigma'$ alors $Q\sigma' = tt$
Exemple 49: $\vdash_p \{n \geq 0\}\ x := n;\ x := 1\ \{x = 1\}$
Définition 50: Deux instructions S_1 et S_2 sont sémantiquement équivalentes si et seulement si pour tout prédicat P, Q, $\vdash_p \{P\}\ S_1\ \{Q\}$ est équivalent à $\vdash_p \{P\}\ S_2\ \{Q\}$.
Exemple 51: $(S;$ skip$)$ est sémantiquement équivalent à S.

B - Logique de Hoare partielle

Définition 52: On définit les règles d'inférences de la logique de Hoare partielle pour les instructions du langage IMP par :

$$[\text{ass}_p]\ \{P[x \mapsto a][[a]]\}\ x := a\ \{P\} \qquad [\text{skip}_p]\ \{P\}\ \text{skip}\ \{P\}$$

$$[\text{comp}_p]\ \frac{\{P\}\ S_1\ \{Q\} \quad \{Q\}\ S_2\ \{R\}}{\{P\}\ S_1; S_2\ \{R\}} \qquad [\text{cons}_p]\ \frac{\{P'\}\ S\ \{Q'\}}{\{P\}\ S\ \{Q\}}\ \text{si}\ P \Rightarrow P'\ \text{et}\ Q' \Rightarrow Q$$

$$[\text{if}_p]\ \frac{\{\mathcal{B}[\![B]\!] \wedge P\}\ S_2\ \{Q\} \quad \{\neg\mathcal{B}[\![B]\!] \wedge P\}\ S_2\ \{Q\}}{\{P\}\ \text{if } B \text{ then } S_1 \text{ else } S_2\ \{Q\}}$$

$$[\text{while}_p]\ \frac{\{\mathcal{B}[\![B]\!] \wedge P\}\ S\ \{P\}}{\{P\}\ \text{while } B \text{ do } S\ \{\neg\mathcal{B}[\![B]\!] \wedge P\}}$$

Exemple 53: On montre que $\{True\}$ while True do skip $\{False\}$ à l'aide de la logique de Hoare (figure 4)
Définition 54: On note $\vdash_p \{P\}\ S\ \{Q\}$ s'il existe une preuve donnée par un arbre d'inférence tel que $\{P\}\ S\ \{Q\}$ soit à la racine et que toutes ses feuilles soient des axiomes.
Exemple 55: $\vdash_p \{True\}$ while True do skip $\{False\}$
Proposition 56: Pour toute instruction S et prédicat P, on a $\vdash_p \{P\}\ S\ \{True\}$
Définition 57: Deux instructions S_1 et S_2 sont prouvées équivalentes si et seulement si pour tout prédicat P et Q, $\vdash_p \{P\}\ S_1\ \{Q\}$ est équivalent à $\vdash_p \{P\}\ S_2\ \{Q\}$.
Exemple 58: $(S;$ skip$)$ est prouvée équivalente à S.

C - Correction et complétude.

Théorème 59 (Correction): La logique de Hoare est correcte.
Pour tous prédicats P, Q et instruction S, $\vdash_p \{P\}\ S\ \{Q\}$ implique $\vdash_p \{P\}\ S\ \{Q\}$
Définition 60: La précondition la plus faible est un prédicat défini tel que $wlp(S, Q)\sigma = tt$ si et seulement si $\forall \sigma' \in State$, si $\langle S, \sigma\rangle \to \sigma'$ alors $Q\sigma' = tt$
Lemme 61: $\vdash_p \{wlp(S, Q)\}\ S\ \{Q\}$
Lemme 62: $\vdash_p \{P\}\ S\ \{Q\}$ implique $P \Rightarrow wlp(S, Q)$

Théorème 63 (Complétude). La logique de Hoare est complète.
Pour tous prédicats P, Q et instruction S, $\vdash_p \{P\}\ S\ \{Q\}$ implique $\vdash_p \{P\}\ S\ \{Q\}$ [DEV 2]

Ouverture :
* Les sémantiques offrent de nombreuses applications :
  + Certification de compilateur : compiler notre langage IMP dans un langage à pile simple
  + Vérifier la sécurité de programme : présence ou non d'interruption de programme, leur communication, confidentialité des données, ...
* Il existe d'autres sémantiques dont on ne parle pas ici, comme la sémantique opérationnelle à petit pas de la continuation qui permet de simplifier la règle de la séquence

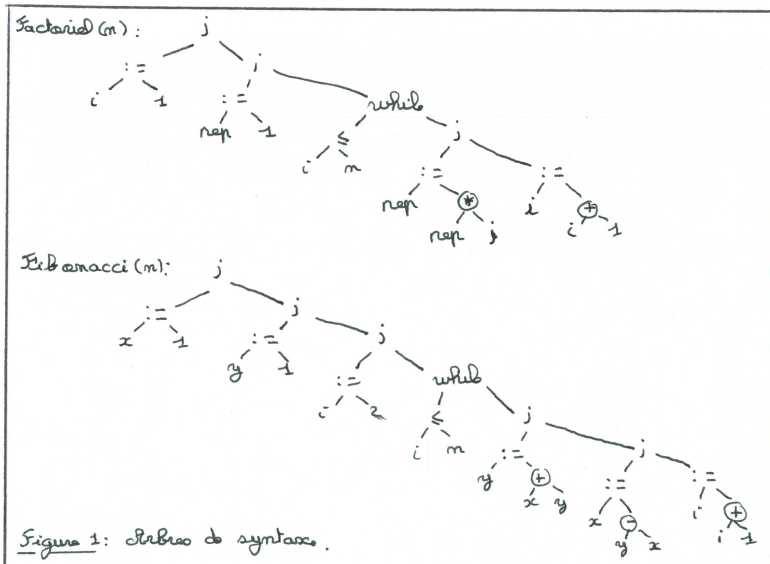


Figure 1 : Arbres de syntaxe.

$$[\text{ass}_{NS}]\ \langle y := 1, [x \mapsto 2]\rangle \to \overbrace{[x \mapsto 2, y \mapsto 1]}^{\sigma_1} \qquad [\text{while}^{tt}_{NS}]\ \frac{\vdots}{\langle \text{while } \neg(x=1) \text{ do } (\dots), \sigma_1\rangle \to [x \mapsto 1, y \mapsto 2]}$$

$$[\text{comp}_{NS}]\ \langle y := 1;\ \text{while } \neg(x=1) \text{ do } (y := y \otimes x;\ x := x \ominus 1), [x \mapsto 2]\rangle \to [x \mapsto 1, y \mapsto 2]$$

Figure 2 : Arbre de dérivation (sémantique à grands pas) pour factorielle 2.

$$[\text{comp}^2_{SOS}]\ \frac{\langle y := 1, [x \mapsto 2]\rangle \Rightarrow [x \mapsto 2, y \mapsto 1] \qquad \langle \text{while } \neg(x=1) \text{ do } (y := y \otimes x;\ x := x \ominus 1), [x \mapsto 2, y \mapsto 1]\rangle \Rightarrow}{\langle y := 1;\ \text{while } \neg(x=1) \text{ do } (y := y \otimes x;\ x := x \ominus 1), [x \mapsto 2]\rangle \Rightarrow}$$

(σ_1 : $y := 1$; σ_2 : while ... ; σ' : $[x \mapsto 2, y \mapsto 1]$; S : while ... ; S_2 : $(S;$ while ...$)$)

$$[\text{while}_{SOS}]\ \frac{\langle \text{while } \neg(x=1) \text{ do } (y := y \otimes x;\ x := x \ominus 1), [x \mapsto 2, y \mapsto 1]\rangle \Rightarrow}{\langle \text{if } \neg(x=1) \text{ then } (S; \text{while } B \text{ do } S) \text{ else skip}, [x \mapsto 2, y \mapsto 1]\rangle \Rightarrow}$$

...

Figure 3 : Séquence de dérivation pour factorielle 2 (sémantique à petit pas).

$$\frac{}{\{True\}\ \text{skip}\ \{True\}}\ [\text{skip}_p]$$

$$\frac{\{True\}\ \text{skip}\ \{True\}}{\{True \wedge True\}\ \text{skip}\ \{True\}}\ [\text{cons}_p]$$

$$\frac{\{True \wedge True\}\ \text{skip}\ \{True\}}{\{True\}\ \text{while True do skip}\ \{False \wedge True\}}\ [\text{while}_p]$$

$$\frac{\{True\}\ \text{while True do skip}\ \{False \wedge True\}}{\{True\}\ \text{while True do skip}\ \{False\}}\ [\text{cons}_p]$$

Figure 4 : Preuve par la logique de Hoare de $\{True\}$ while True do skip $\{False\}$.

Références :
[1] H.R. Nielson et F. Nielson, Semantics with applications.

931 — Schémas algorithmiques. Exemples et applications.

Motivations : Trouver des paradigmes de programmation qui permettront d'utiliser les mêmes procédés pour résoudre des algorithmes ou du moins améliorer leur complexité.

(I) Diviser pour régner

But 1 : traiter des instances plus petites du même problème puis les combiner pour avoir la solution cherchée.

Ex 2 : Algorithme de DICHOTOMIE — entrée : T est trié, $0 \leq a < b \leq n$, $n = T.\text{taille}$; sortie : indice d'une occurrence de x si $x \in T$, NIL sinon. Complexité : $O(\lg(n))$

```
Dicho(T, a, b, x):
  si a=b et T[a]=x :
    renvoie a
  si a=b et T[a]≠x :
    renvoie NIL
  si x > T[⌊(a+b)/2⌋] :
    renvoie dicho(T, ⌊(a+b)/2⌋+1, b, x)
  sinon
    renvoie dicho(T, a, ⌊(a+b)/2⌋, x)
```

Thm 3 (MASTER THEOREM) : Soit $T : \mathbb{N} \to \mathbb{R}_+$ fonction croissante à partir d'un certain rang. $n_0 \geq 1$, $b \geq 2$ des entiers, $k \geq 0$, $a > 0$, $c > 0$, $d > 0$ des réels tels que $T(n_0) = d$ et $T(n) = aT(n/b) + cn^k$ pour $n = n_0 b^p$, $p \in \mathbb{N}$.

Alors $T(n) = \begin{cases} \Theta(n^k) & \text{si } a < b^k \\ \Theta(n^k \log_b(n)) & \text{si } a = b^k \\ \Theta(n^{\log_b(a)}) & \text{si } a > b^k \end{cases}$

(I) DEV

Appli 4 : TRI FUSION en $O(n \log_2(n))$ — $a=2$ $b=2$ $k=1$, $n_0=1$ $d=1$ $c=1$

Rmq 5 : Ce théorème 3 ne permet pas de donner la complexité de tout algorithme utilisant le paradigme diviser pour régner.

Ex 6 : Le TRI RAPIDE ne peut pas être traité par le Master Thm car on divise notre entrée en des parts de tailles qui diffèrent.

Ex 7 : La multiplication de matrices par la METHODE de STRASSEN permet de passer de $O(n^3)$ (algo naïf) à $O(n^{\log_2(7)})$ (Strassen) $(\log_2(7) \simeq 2{,}81)$

Limite 8 : Tous les algorithmes qui utilisent diviser pour régner ne sont pas forcément efficace.

Ex 9 : Pour calculer le $n^{\text{ième}}$ nombre de FIBONACCI, calculer récursivement le $(n-1)^{\text{ième}}$ et le $(n-2)^{\text{ième}}$ et les ajouter n'est pas efficace.

```
FiBo(n)                                  (1)
  si n=0 ou n=1
    renvoie 1
  sinon renvoie
      FiBo(n-1)
    + FiBo(n-2)
```
Complexité : $\Theta(\varphi^n)$

```
FiBo(n)                                  (2)
  S ← 1
  T ← 1
  pour i allant de 2 à n
    U ← S
    S ← T
    T ← S+U
  renvoie T
```
Complexité : $O(n)$

Notation 14bis : $X_i = \langle x_1, \dots, x_i \rangle$ et $Y_j = \langle y_1, \dots, y_j \rangle$

(II) Programmation dynamique

But 10 : mémoriser les solutions des sous problèmes (mémoïsation) pour résoudre le problème global.

Ex 11 :

```
FiBo(n)                                  (3)
  T = [1,1,0,...,0] (de taille n+1)
  pour i allant de 2 à n
    T[i] ← T[i-1] + T[i-2]
  renvoie T[n]
```
Complexité : $O(n)$ (temporelle) ; $O(n)$ (spatiale)

Rmq 12 : La mémoïsation nécessite de la mémoire en plus mais ne recalcule pas de sous problèmes déjà calculés.

Ex 13 : Algorithme COCKE YOUNGER KASAMI résolvant le problème du mot polynomialement en utilisant la programmation dynamique

(II) DEV

Ex 14 : PLUS LONGUE SOUS SEQUENCE COMMUNE

Soient deux séquences $X = \langle x_1, \dots, x_m \rangle$ et $Y = \langle y_1, \dots, y_n \rangle$

On veut trouver le plus grand $k \in \{0, \dots, \min(n,m)\}$ tel qu'il existe $i_1, \dots i_k \in \{1, \dots, m\}$ croissant strictement et $j_1, \dots j_k \in \{1, \dots, n\}$ croissant strictement et $x_{i_\ell} = y_{j_\ell}$ $\forall \ell \in \{1, \dots, k\}$ on note $z_\ell = x_{i_\ell}$

On dira que $\langle z_1, \dots, z_k \rangle$ est une plus longue sous séquence commune à X et Y, notée PLSC(X,Y)

Thm 15 : Soient X, Y deux séquences et Z une PLSC(X, Y)

1) Si $x_m = y_n$ alors $z_k = x_m = y_n$ et Z_{k-1} est une PLSC(X_{m-1}, Y_{n-1})
2) Si $x_m \neq y_n$ alors $z_k \neq x_m \Rightarrow Z$ est une PLSC(X_{m-1}, Y)
3) Si $x_m \neq y_n$ alors $z_k \neq y_n \Rightarrow Z$ est une PLSC(X, Y_{n-1})

Corollaire 16 : En notant $c[i,j]$ la longueur d'une PLSC(X_i, Y_j)

ana $c[i,j] = \begin{cases} 0 & \text{si } i=0 \text{ ou } j=0 \\ c[i-1,j-1]+1 & \text{si } i,j>0 \text{ et } x_i = y_j \\ \max(c[i,j-1], c[i-1,j]) & \text{si } i,j>0 \text{ et } x_i \neq y_j \end{cases}$

annexe

Ex 17 : Pour calculer la distance d'édition entre deux mots, on peut utiliser la programmation dynamique

Ex 18 : L'algorithme de FLOYD-WARSHALL utilise le paradigme de la programmation dynamique.

$d_{ij}^{(k)} = \begin{cases} w_{ij} & \text{si } k = 0 \\ \min(d_{ij}^{(k-1)}, d_{ik}^{(k-1)}, d_{kj}^{(k-1)}) & \text{si } k \geq 1 \end{cases}$

```
FLOYD-WARSHALL(W)  graphe pondéré sans cycle de poids négatif
  n = W.lignes
  D(0) = W
  pour k allant de 1 à n
    soit D(k) nouvelle matrice n×n
    pour i allant de 1 à n
      pour j allant de 1 à n
        d_ij(k) = min(d_ij(k-1), d_ik(k-1), d_kj(k-1))
  renvoie D(n)
```
Complexité : $O(n^3)$ (temporelle)

PLUS COURT CHEMIN ENTRE TOUTES LES PAIRES DE SOMMETS

III Algorithmie gloutonne

But ig: Faire des choix localement optimaux pour obtenir une solution globalement optimale.

Rmq 20: Attention tout algorithme glouton ne redonne pas forcément une solution globalement optimale

Ex 21: L'algorithme glouton de rendu de monnaie en un minimum de pièces n'est pas toujours optimale (cela dépend de la valeur des pièces)

Ex 22: Les algorithmes de PRIM et KRUSKAL sont deux algorithmes gloutons qui renvoient des solution optimales.

ARBRE COUVRANT MINIMAL

```
KRUSKAL(G=(S,A), w)
    E = ∅
    pour v ∈ S
        create(v)
    trier A par ordre croissant de poids w
    pour (u,v) ∈ A (pris par ordre croissant)
        si FIND(u) ≠ FIND(v)
            E = E ∪ {(u,v)}
            UNION(u,v)
    renvoie E
```

G non orienté connexe
$w : A \to \mathbb{R}$

complexité
$O(|A| \log |A| + |A| \alpha(|S|) + |S|)$ (temporelle)

utilisation de UNION FIND

ARBRE COUVRANT MINIMAL

```
PRIM(G=(S,A), w, r)
    pour u ∈ S
        u.clé = ∞
        u.π = NIL
    r.clé = 0
    F = S
    tant que F ≠ ∅
        u = Extraire_min(F)
        pour v ∈ Adj(u)
            si v ∈ F et w(u,v) < v.clé
                v.π = u
                v.clé = w(u,v)
    renvoie π
```

G non orienté connexe
$w : A \to \mathbb{R}$
$r \in S$

complexité: $O(|S| \log |S| + |A| \log |S|)$ (temporelle)

utilisation d'une file de priorité

Annexe:

y_j		B	D	C	A	B	A
x_i	0	0	0	0	0	0	0
A	0	↑ 0	↑ 0	↑ 0	↖ 1	← 1	↖ 1
B	0	↖ 1	← 1	← 1	↑ 1	↖ 2	← 2
C	0	↑ 1	↑ 1	↖ 2	← 2	↑ 2	↑ 2
B	0	↖ 1	↑ 1	↑ 2	↑ 2	↖ 3	← 3
D	0	↑ 1	↖ 2	↑ 2	↑ 2	↑ 3	↑ 3
A	0	↑ 1	↑ 2	↑ 2	↖ 3	↑ 3	↖ 4
B	0	↖ 1	↑ 2	↑ 2	↑ 3	↖ 4	↑ 4

Fondements des bases de données relationnelles

932

I Formalisme

Def 1 : On se donne des ensembles dénombrables distincts de variables VAR = {x, y, z, ...}, d'attributs att, de domaine dom et de noms de schéma de relation Relname

on considère la fonction :
sort : relname → $\mathcal{P}_f$(att)
qui à R ∈ relname associe un nombre fini d'attributs.

Def 2 : on dira que, pour R ∈ relname, |sort(R)| est l'arité de R

Def 3 (schème de relation) Un élément R ∈ relname est un schème de relation.
on notera R[U] où U = sort(R)

Def 4 (schème de base de données) c'est un nombre fini de schèmes de relation
on notera $\mathcal{R} = \{R_1[U_1], \dots R_n[U_n]\}$

Ex 5 : $\mathcal{R}$ { Films [Titre, Réal, Acteur], Séances [cinéma, horaires, Titres] } est un schème de base de données.

Def 6 (tuple) Un tuple sur un schème de relation R[U] est une fonction u : U → dom
on notera < U_1 : u(U_1), ..., U_n : u(U_n) >

Ex 7 : < Titre : Dune, Réal : A. Chabat, Acteur : A. Chabat > est un tuple de FILMS
on pourra écrire < Dune, A. Chabat, A. Chabat >

Def 8 : Une relation I sur un schème de relation R[U] est un nombre fini de tuple pour R[U].

Ex 9 : FILMS est une relation.

Def 10 : Une base de données I sur $\mathcal{R}$ est un ensemble de relation, où une relation I est sur un schéma R[U] ∈ $\mathcal{R}$.

Ex 11 : voir annexe 1

II Requêtes conjonctives

1) Règles conjonctives

Def 12 : Un tuple libre d'un schème de relation R[U] est un tuple pouvant avoir des variables
u : U → dom ∪ VAR.

Ex 13 : < x, A. Chabat, y > est un tuple libre.

Def 14 : Une règle conjonctive sur $\mathcal{R}$ est une expression de la forme $ans(u) \leftarrow R_1(u_1), \dots, R_n(u_n)$
où $u, u_1, \dots, u_n$ sont des tuples libres, $R_i \in \mathcal{R}$

Ex 15 : $ans(x) \leftarrow Films(x, A.Chabat, y)$ $ans \notin \mathcal{R}$
est une règle conjonctive.

Def 16 : Une valuation ν sur VAR est une fonction
ν : VAR → dom
prolongée aux tuples libres en les tuples $(\nu|_{dom} = id_{dom})$

Def 17 : La sémantique d'une règle conjonctive q pour I sur $\mathcal{R}$ est donnée par

$$q(I) = \{ \nu(u) \mid \nu \text{ valuation sur VAR}(q) \text{ et } \nu(u_i) \in I(R_i) \ \forall i \in 1..n \}$$

Ex 18 : L'exemple 15 a pour sémantique
< Dune, A. Chabat, A. Chabat >
< Astérix, A. Chabat, E. Baer >
Cette règle répond à la question
Q_1 Quels films ont été réalisés par A. Chabat ?

Def 19 : Le domaine actif de I, adom(I) est l'ensemble des constantes présentes dans I. Celui de q, adom(q) est l'ensemble des constantes présentes dans q.

Prop 20 : On a adom(q(I)) ⊆ adom(q) ∪ adom(I)

Ex 21 : Q_2 Dans quels cinémas peut-on voir un film d'A. Chabat ?
$ans(x) \leftarrow Séances(x, y, z), Films(z, A.Chabat, t)$

2) Calcul conjonctif

Def 22 : Soit $\mathcal{R}$, une formule du calcul conjonctif (CC) est de la forme
(i) R(u) pour R[U] ∈ $\mathcal{R}$ et u un tuple libre
(ii) φ ∧ ψ où φ, ψ sont des formules du CC
(iii) ∃x φ où x ∈ VAR et φ une formule du CC

Def 23 : On définit l'ensemble des variables libre FV(φ) comme en logique du premier ordre.

Def 24 : Une requête du CC sur $\mathcal{R}$ est une expression de la forme $\{e_1, \dots, e_n \mid \varphi\}$ où < $e_1, \dots, e_n$ > tuple libre et FV(φ) = {$e_1, \dots, e_n$} φ formule du CC

Def 25 : Pour $\mathcal{R}$, φ du CC sur $\mathcal{R}$, ν valuation sur FV(φ), I satisfait φ sous ν, noté $I \models \varphi[\nu]$, si
(i) φ = R(u), ν(u) ∈ I(R) ou
(ii) φ = ψ ∧ Φ, $I \models \psi[\nu|_{FV(\psi)}]$ et $I \models \Phi[\nu|_{FV(\Phi)}]$ ou
(iii) φ = ∃x ψ, ∃c ∈ dom I, $I \models \psi[\nu \cup \{x \mapsto c\}]$

Def 26 : La sémantique d'une requête q du CC est donnée par
$q(I) = \{ \nu(< e_1, \dots, e_n >) \mid I \models \varphi[\nu] \text{ et } \nu \text{ valuation sur } FV(\varphi) \}$

Ex 27 : on exprime Q_1 par $\{ x \mid \exists y, Films(x, A.Chabat, y) \}$
et Q_2 par $\{ x \mid \exists y, z, t, Séances(x, y, z) \wedge Films(z, A.Chabat, t) \}$

Thm 28 : Le calcul conjonctif et les règles conjonctives sont équivalents.

III L'algèbre SPC

Def 29 : On définit des opérations sur I ∈ $\mathcal{I}$ qui forment l'algèbre SPC.

* **sélection** : $\sigma_{j=a}(I) = \{ t \in I, t(j) = a \}$.
avec j attribut, a ∈ dom, t un tuple.
$\sigma_{j=k}(I) = \{ t \in I, t(j) = t(k) \}$
avec j, k attributs, t un tuple.

* **projection** : $\Pi_{j_1, \dots, j_n}(I) = \{ < t(j_1), \dots, t(j_n) > , t \in I \}$.
avec $j_1, \dots, j_n$ des attributs de I.

* **produit cartésien** : $I \times J = \{ < t(1), \dots, t(n), s(1), \dots, s(m) > , t \in I, s \in J \}$
avec n = arité(I), m = arité(J)

Def 30 : La sémantique liée à ces opérations est naturelle puisque l'on effectue les opérations sur les relations.

Ex 31 : Q_1 est exprimée par $\Pi_{titre} \sigma_{Réal = A.Chabat}(Films)$
Q_2 est exprimée par $\Pi_{cinéma} \sigma_{Réal = A.Chabat} \sigma_{Titre_{Film} = Titre_{Séances}}(Films \times Séances)$

Prop 32 : On peut effectuer une jointure naturelle (union de deux relations où l'on fait correspondre les éléments communs) avec les trois opérations

Ex 33 : Dans l'exemple on a fait une jointure naturelle

Prop 34 : On peut exprimer aussi l'intersection grâce aux 3 opérations de SPC.

Rmq 35 : Il existe des requêtes insatisfiables.

Ex 36 : Q_3 $\Pi_A(\sigma_{A=0}(\sigma_{A=1}(table)))$ est insatisfiable.

Rmq 37 : C'est une grande différence avec les requêtes conjonctives qui sont toujours satisfiables.

Thm 38 : Il y a équivalence entre les requêtes par règles conjonctives, le calcul conjonctif et les requêtes satisfiables de l'algèbre SPC.

Limite 39 : On ne peut pas encore répondre aux questions : Quels sont les films réalisés par A. Chabat ou par Q. Dupieux ? (Q4)

Quels sont les films de Q. Dupieux dans lesquels A. Chabat ne joue pas ? (Q5)

IV L'algèbre relationnelle et le calcul relationnel

1) Ajout de l'union

Def 40 : On autorise dorénavant la sélection avec $\delta_{j=a \vee j=b}$ (avec le "ou" logique) muni de sa sémantique naturelle → Algèbre SPCU

Ex 41 : (Q4) $T_{titre}\,\delta_{réal=A.Chabat \text{ ou } réal=Q.Dupieux}(Films)$

Def 42 : On ajoute le $\vee$ aux formules du CC

Problème 43 : On peut avoir des requêtes infinies

Ex 44 : $\{x_1, y \mid R(x_1) \vee R(y)\}$ si $R(x_2)=1$ et donc infini $\forall y \in dom\ R(x_1) \vee R(y) = 1$

Def 45 : On dit qu'une requête est sûre si $|q(I)| < +\infty$ $\forall I \in R$

Problème 46 : savoir si une requête est sûre est indécidable.

2) Ajout de la négation :

Def 47 : On ajoute la différence ensembliste ce qui donne l'algèbre SPCUD.

Ex 48 : (Q5) $T_{titre}\left(\delta_{réal=Q.Dupieux}(Films) \setminus \delta_{acteur=A.Chabat}(Films)\right)$

Def 49 : On ajoute le $\neg$ aux formules pour obtenir le calcul relationnel et $\forall$

Problème 50 : On a de nouveau des requêtes infinies

Ex 51 : $\{\langle\rangle \mid \neg R(x_1)\}$ si le domaine est infini c'est une requête infinie.

Solution 52 : Pour une relation I sur R, on peut restreindre le domaine au domaine actif, ainsi pour une requête et une relation, la requête sera finie.

Thm 53 : Restreint au domaine actif, l'algèbre relationnelle SPCUD et le calcul relationnel (FO) sont équivalents.

Thm 54 : Le problème
REL SAT : entrée : une requête du calcul relationnel sur R
sortie : oui s'il existe $I \in R$ tq $q(I) \neq \emptyset$, non sinon
est indécidable.

DEV 1

Rq 55 : Savoir si deux requêtes q, q' sont équivalentes est aussi indécidable.

V Optimisation

1) Stockage

Def 56 : (B-arbres) Un B-arbre est un arbre tel que il existe t degré minimal de T
1) chaque nœud x contient $x.n$ clés, notés $x.clé_1, \dots, x.clé_n$ stockées par ordre croissant, un booléen $x.feuille$, $n+1$ pointeurs vers ses fils $x.c_1 \dots x.c_{n+1}$
2) les clés et valeurs k_i des fils sont telles que $k_0 \leq x.clé_1 \leq k_1 \leq x.clé_2 \dots \leq x.clé_n \leq k_n$
3) toutes les feuilles ont même profondeur, h.
4) $\forall x \quad t-1 \leq x.n \leq 2t-1$

Thm 57 : Soit T un B-arbre à n éléments, de degré minimal $t \geq 2$ Alors sa hauteur h vérifie $h \leq \log_t\left(\frac{n+1}{2}\right)$

Algorithme de recherche et exemple d'insertion.

DEV 2

Annexe : $R = \{FILMS, Séances\}$

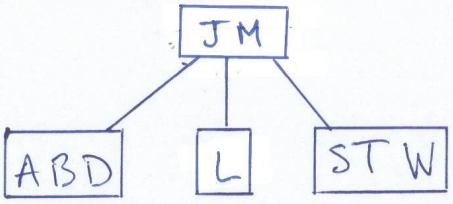
FILMS

Titre	Réal	Acteur
Didier	A. Chabat	A. Chabat
Au poste	Q. Dupieux	G. Ludiq
Réalité	Q. Dupieux	A. Chabat
Astérix	A. Chabat	E. Baer

Séances

Cinéma	Horaire	Titre
UGC	12^h00	Au poste
Gaumont	20^h30	Didier
Pathé	13^h30	Réalité
Pathé	16^h30	Didier

B-arbre : $t = 2$



CHAPITRE 3

DÉVELOPPEMENTS

3.1 Conseils

— Le développement doit tenir entre 15 minutes
— S'entrainer suffisamment pour être serein et qu'il soit bien calibré
— Faire des dessins dès que c'est possible (convergence des polygones, méthode de Newton, etc...)
— Présenter entre vous des développements est très formateur, car chacun arrive à trouver des petites améliorations, etc.
— Sinon, on peut aussi se filmer ce qui permet de se rendre compte de notre performance
— En s'entrainant, on peut écrire le développement sur une feuille en parlant à voix haute
— Savoir donner les étapes principales de chaque développement.

J'ai commencé une liste de questions qu'il faut se poser sur chaque développement pour être sûr qu'il soit le plus parfait possible :

— Où utilise-t-on chacune des hypothèses ?
— Le résultat est-il vrai dans un cadre plus général ?
— Sais-tu justifier tous les résultats admis ?
— Où vivent les objets que l'on manipule ?
— Y-a-t'il des problèmes d'indice ?
— À quoi ce développement peut servir ? Quelles sont les applications ?
— Est-ce qu'on utilise cela en pratique ?
— Existe-t-il d'autres preuves qui rendent le résultat trivial ?
— Quelles sont les grandes étapes de ce développement ?
— Quelle est la justification de l'interversion somme-intégrale ? de ce Fubini ? etc.

3.2 Ma liste des développements de mathématiques

— **Primalité des nombres de Mersenne** : 120 ; 121 ; 123 ; 141
— **Isométries du cube et du tétraèdre** : 101 ; 104 ; 105 ; 108 ; 183
— **Dénombrement des matrices diagonalisables de $\mathbb{F}_q$** : 101 ; 104 ; 106 ; 190
— **Loi de réciprocité quadratique** : 121 ; 123 ; 126 ; 170 ; 190
— **Décomposition de Dunford** : 153 ; 157
— **Image de l'exponentielle** : 153 ; 156 ; 214
— **Convergence de polygones vers l'isobarycentre** : 152 ; 182 ; 226
— **Banach–Steinhaus** : 208 ; 246
— **Méthode de Newton** : 219 ; 223 ; 226 ; 228 ; 229
— **Réciproques partielles de Césaro** : 223 ; 230
— **Formule des compléments** : 236 ; 239 ; 265
— **Cauchy Lipschitz et lemme de Gronwall** : 203 ; 208 ; 220
— **Translatés d'une fonction $\mathcal{C}^1$** : 151 ; 159 ; 221 ; 228
— **Méthode de gradient à pas optimal** : 162 ; 219 ; 226 ; 229 ; 233
— **Nombres de Bell** : 190 ; 230 ; 243
— **Formule d'inversion de la fonction caractéristique** : 236 ; 239 ; 250 ; 260 ; 264
— **Théorème des extrema liés** : 152 ; 159 ; 214 ; 219
— **Nombres de zéros des solutions d'une équation différentielle** : 220 ; 221 ; 224
— **Morphismes d'algèbre de $\mathcal{C}(K, \mathbb{R})$ sur $\mathbb{R}$** : 159 ; 203
— **Théorème Central Limite** : 260 ; 264
— **Générateurs de $SL_2(\mathbb{Z})$** : 108 ; 182 ; 183
— **Automorphismes de $\mathfrak{S}_n$** : 104 ; 105 ; 108
— **Etude du groupe $O(p, s)$** : 106 ; 156 ; 170
— **Théorème de Carathéodory** : 126 ; 151
— **Théorème de Fermat modulaire** : 120 ; 121 ; 126 ; 190
— **Méthode QR** : 157 ; 162 ; 233
— **Irréductibilité des polynômes cyclotomiques** : 141
— **Formule de Poisson et Shannon** : 239 ; 246 ; 250
— **Formule de Poisson et équivalent Θ** : 224 ; 243 ; 246
— **Formule de Poisson et fonction Θ** : 246 ; 265

3.3 Ma liste des développements d'informatique

— **Tri par tas** : 901 ; 903 ; 926
— **Master Theorem** : 926 ; 931
— **Indécidabilité de la validité d'une formule du premier ordre** : 914 ; 924
— **Machine de Turing $\Longrightarrow$ μ-recursif** : 912 ; 913
— **Transformation de Tseitin** : 916 ; 928
— **Théorème de Cook** : 913 ; 915 ; 916 ; 928
— **B-arbres** : 901 ; 921 ; 932
— **Cocke-Younger-Kasami** : 907 ; 915 ; 923 ; 931
— **Tri topologique** : 903 ; 925 ; 927
— **Automate des occurrences** : 907 ; 909 ; 921
— **3-Coloration d'un graphe** : 915 ; 925 ; 928
— **μ-recursif $\Longrightarrow$ λ-définissable** : 912 ; 929
— **Décidabilité de Presburger** : 909 ; 914 ; 924
— **Équivalence entre sémantiques opérationnelles** : 930
— **Complétude de la logique de Hoare** : 927 ; 930
— **Théorème de Scott–Curry** : 929
— **Caractérisation de *premier* pour l'analyse $LL(1)$** : 923
— **Indécidabilité de la satisfiabilité d'une requête** : 914 ; 932

3.4 Développements de mathématiques

Primalité des nombres de Mersenne

Leçons : 120 ; 121 ; 123 ; 141

Références : SAUX PICART–RANNOU, *Cours de Calcul Formel, Corps finis, Systèmes polynomiaux Applications* (p.80)[SPR02]

Prérequis :

- le symbole de Legendre et la propriété $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$
- la Loi de Réciprocité Quadratique (voir le développement)
- le théorème chinois
- le morphisme de Frobenius
- corps de rupture

Introduction :

Un nombre de Mersenne est un nombre de la forme $M_q = 2^q - 1$ avec $q \in \mathbb{N}^*$. On veut trouver les nombres de Mersenne qui sont premiers. Si q n'est pas premier, $q = ab$ et

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$$

est divisible par $2^a - 1$ non inversible dans $\mathbb{Z}$ (ainsi le cas q non premier ne donnera jamais de M_q premier). Pour $q = 2$, $M_q = 2^2 - 1 = 3$ qui est premier. On se restreint donc à q premier impair.

Remarques :

Tous les nombres de Mersenne ne sont pas premiers, par exemple, $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$, et l'on ne sait pas aujourd'hui s'il existe une infinité de nombres de Mersenne qui sont premiers, ni s'il existe une infinité de nombres de Mersenne qui ne sont pas premiers. Aujourd'hui, les plus grands nombres premiers que l'on connaisse sont des nombres de Mersenne.

Le théorème ci-dessous nous donne donc un critère de primalité des nombres de Mersenne pour q premier impair.

Théorème 1. Pour q premier impair, on a

$$M_q \text{ est premier } \iff (2+\sqrt{3})^{2^{q-1}} \equiv -1 \ [M_q]$$

Remarques :

Tout d'abord, il faut comprendre où l'on se place pour dire cela, en effet il faut comprendre le sens de $\sqrt{3}$. Si 3 est un carré dans $\mathbb{Z}/M_q\mathbb{Z}$, on peut se placer dans $\mathbb{Z}/M_q\mathbb{Z}$, sinon on se placera dans une extension de corps de $\mathbb{Z}/M_q\mathbb{Z}$ qui contient une racine de 3, un corps de rupture de $X^2 - 3$ par exemple. Cela dit dans la première implication, on prouvera que 3 n'est jamais un carré dans $\mathbb{Z}/M_q\mathbb{Z}$ donc on se placera forcément dans $\mathbb{Z}/M_q\mathbb{Z}[X]/(X^2-3)$. De plus, le deuxième membre de l'équivalence n'a de sens que si on est dans $\mathbb{Z}/M_q\mathbb{Z}$, ainsi dans le cas où il faut se placer dans $\mathcal{A} = \mathbb{Z}/M_q\mathbb{Z}[X]/(X^2-3)$, il faut comprendre que l'on veut juste l'égalité dans $\mathcal{A}$.

Démonstration :

$\boxed{\Longrightarrow}$ Pour le sens direct :

Étape 1 : *Condition nécessaire pour que 3 soit un carré modulo p avec p premier.*

On utilise la loi de réciprocité quadratique [1] avec 3 et p.

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$$

On suppose que 3 est un carré modulo p. Donc $\left(\frac{3}{p}\right) = 1$.

Ainsi si $p \equiv 1\ [3]$, on a $\left(\frac{p}{3}\right) = 1$ donc nécessairement, on a $\frac{p-1}{2}$ qui doit être pair, d'où $p \equiv 1\ [4]$. Par le lemme chinois [2], on a $p \equiv 1\ [12]$.

Et si $p \equiv 2\ [3]$, on a $\left(\frac{p}{3}\right) = -1$ donc nécessairement, on a $\frac{p-1}{2}$ qui doit être impair, d'où $p \equiv 3\ [4]$. Par le lemme chinois [3], on a $p \equiv -1\ [12]$.

Donc si 3 est un carré modulo p, on a nécessairement $p \equiv \pm 1\ [12]$.

Étape 2 : *3 n'est pas un carré modulo M_q.*

On va prouver par récurrence sur les q impairs (pour $q \geqslant 3$) que $M_q \equiv 7\ [12]$.

Initialisation : pour $q = 3$, on a $M_3 = 2^3 - 1 = 7 \equiv 7\ [12]$

Hérédité : on suppose que $M_{2k+1} \equiv 7\ [12]$, on veut prouver que $M_{2(k+1)+1} \equiv 7\ [12]$.

$M_{2(k+1)+1} = 2^{2k+3} - 1 = 4 \times 2^{2k+1} - 1 = 4(2^{2k+1} - 1) + 3 \equiv 4 \times 7 + 3 \equiv 24 + 7 \equiv 7\ [12]$.

Donc pour tout q impair premier, on a $M_q \equiv 7\ [12]$, ainsi par l'étape 1, on sait que 3 n'est pas un carré modulo M_q.

Étape 3 : *2 est un carré modulo M_q.*

Il suffit de faire un court calcul : $2(2^q - 1) \equiv 0\ [M_q]$ d'où $2^{q+1} \equiv 2\ [M_q]$, donc comme $q+1$ est pair, on a $(2^{\frac{q+1}{2}})^2 \equiv 2\ [M_q]$. Donc 2 est bien un carré modulo M_q. On notera désormais $\sqrt{2}$ pour $2^{\frac{q+1}{2}}$.

Étape 4 : *Calcul de $(2+\sqrt{3})^{2^{q-1}}$ dans un corps approprié.*

Comme 3 n'est pas un carré modulo M_q, le polynôme $X^2 - 3$ est irréductible sur $\mathbb{Z}/M_q\mathbb{Z}$. Donc on peut se placer dans le corps $\mathcal{A} = \mathbb{Z}/M_q\mathbb{Z}[X]/(X^2-3)$. On notera désormais $\sqrt{3}$ pour la classe de X dans $\mathcal{A}$. On pose $\rho = \dfrac{1+\sqrt{3}}{\sqrt{2}}$ et $\bar{\rho} = \dfrac{1-\sqrt{3}}{\sqrt{2}}$. On veut prouver que $(2+\sqrt{3})^{2^{q-1}} = -1$ dans $\mathcal{A}$.

$$\begin{aligned}(2+\sqrt{3})^{2^{q-1}} &= (\rho^2)^{2^{q-1}} = \rho^{2^q} \\ &= \rho\Big(\frac{1+\sqrt{3}}{\sqrt{2}}\Big)^{M_q} \\ &= \rho\Big(\Big(\frac{1}{\sqrt{2}}\Big)^{M_q} + \Big(\frac{\sqrt{3}}{\sqrt{2}}\Big)^{M_q}\Big) \text{ car } \mathcal{A} \text{ est de caractéristique } M_q\end{aligned}$$

Or $\sqrt{2}^{M_q} = \sqrt{2}$ dans $\mathcal{A}$ car 2 est un carré modulo M_q. Et $\sqrt{3}^{M_q} = \sqrt{3} \times (\sqrt{3})^{M_q-1} = \sqrt{3}.3^{\frac{M_q-1}{2}} = -\sqrt{3}$ car 3 n'est pas un carré modulo M_q [4].

Donc $(2+\sqrt{3})^{2^{q-1}} = \rho\Big(\Big(\frac{1}{\sqrt{2}}\Big) - \Big(\frac{\sqrt{3}}{\sqrt{2}}\Big)\Big) = \rho\bar{\rho} = -1$ dans $\mathcal{A}$.

1. Connaitre la loi de réciprocité quadratique, c'est un développement classique donc ça peut aider.
2. Savoir expliquer rapidement comment trouver que $p \equiv 1\ [12]$
3. Même chose avec $p \equiv -1\ [12]$.
4. Savoir que pour x un carré modulo p, $x^{\frac{p-1}{2}} \equiv 1\ [p]$ et pour un non carré, $x^{\frac{p-1}{2}} \equiv -1\ [p]$.

$\boxed{\Longleftarrow}$ Pour le sens indirect : De nouveau, il faut comprendre comment interpréter $\sqrt{3}$ dans l'hypothèse, donc on se place

— soit dans $\mathcal{A} = \mathbb{Z}/M_q\mathbb{Z}$ si 3 est un carré dans $\mathbb{Z}/M_q\mathbb{Z}$,

— soit dans $\mathcal{A} = \mathbb{Z}/M_q\mathbb{Z}[X]/(X^2-3)$ si 3 n'est pas un carré dans $\mathbb{Z}/M_q\mathbb{Z}$.

On prend $p > 1$ un facteur premier de M_q. Donc p est un diviseur de zéro dans $\mathcal{A}$, car $p \times \frac{M_q}{p} = 0$ dans $\mathcal{A}$. Ainsi p n'est pas inversible. Donc on peut considérer $\mathcal{M}$ un idéal maximal de $\mathcal{A}$ qui contient p [5].

On se place dans $\mathcal{A}/\mathcal{M}$ qui est un corps (car $\mathcal{M}$ est maximal) de caractéristique p car p est premier et $\underbrace{1+\cdots+1}_{p \text{ fois}} = 0$ dans $\mathcal{A}/\mathcal{M}$.

On pose α (resp. β) la classe de $2+\sqrt{3}$ (resp. $2-\sqrt{3}$), $\alpha^{2^{q-1}} = -1$ dans $\mathcal{A}/\mathcal{M}$ donc l'ordre de α est 2^q comme expliqué dans la note [6].

On considère le polynôme $Q(X) = (X-\alpha)(X-\beta) = X^2 - 4X + 1$ dans $\mathcal{A}/\mathcal{M}$. Or puisque $\mathcal{A}/\mathcal{M}$ est de caractéristique p, α^p est aussi zéro de Q [7] car α l'est. Donc $\alpha^p = \alpha$ ou $\alpha^p = \beta$.

Dans le premier cas, $\alpha^p = \alpha$, comme α est inversible car $\alpha^{2^q} = 1$, on a alors $\alpha^{p-1} = 1$ donc 2^q divise $p-1$ or on sait que p divise $2^q - 1$ ce qui est absurde.

Dans le deuxième cas, $\alpha^p = \beta$, or $\alpha^p = \beta = \alpha^{-1} = \alpha^{M_q}$ [8]. Donc 2^q divise $M_q - p$, ce qui implique que $p = M_q$ [9]. Ainsi M_q est bien premier.

□

Remarques :

En pratique cette méthode n'est pas applicable directement car pour chercher des nombres premiers extrêmement grand, on va avoir un q très grand et donc le calcul $(2+\sqrt{3})^{2^{q-1}}$ est difficilement faisable. Cependant, on se sert de ce résultat pour le test de Lehmer–Lucas :
On définit la suite $(L_n) \in (\mathbb{Z}/M_q\mathbb{Z})^{\mathbb{N}}$ par $L_0 = 4$ et $L_{n+1} \equiv L_n^2 - 2\ [M_q]$, on a alors M_q premier $\iff L_{q-2} \equiv 0\ [M_q]$
Complexité en $\mathcal{O}(q^3)$.

Théorème 2 (Test de Lehmer–Lucas)**.** Soit la suite $(L_n) \in (\mathbb{Z}/M_q\mathbb{Z})^{\mathbb{N}}$ définie par

$$L_0 = 4 \quad \text{et} \quad L_{n+1} \equiv L_n^2 - 2\ [M_q]$$

On a alors :

$$M_q \text{ est premier} \iff L_{q-2} \equiv 0\ [M_q]$$

Démonstration. On pose $\omega = 2+\sqrt{3}$ et $\tilde{\omega} = 2-\sqrt{3}$. On a $\omega^{2^n} + \tilde{\omega}^{2^n} \in \mathbb{Z}/M_q\mathbb{Z}$ car les parties en $\sqrt{3}$ se compensent et $\omega^{2^n} + \tilde{\omega}^{2^n} = L_n$ (par récurrence).
Initialisation : $n = 0$, $\omega^{2^0} + \tilde{\omega}^{2^0} = \omega + \tilde{\omega} = 4 = L_0 \in \mathbb{Z}/M_q\mathbb{Z}$.
Hérédité : On suppose que le résultat est vrai pour $k \in \mathbb{N}$, on veut prouver le résultat au rang $k+1$.

$\omega^{2^{k+1}} + \tilde{\omega}^{2^{k+1}} \equiv (\omega^{2^k} + \tilde{\omega}^{2^k})^2 - 2\omega^{2^k}\tilde{\omega}^{2^k} \equiv L_n^2 - 2\ [M_q]$ par hypothèse de récurrence et car $a^2+b^2 = (a+b)^2 - 2ab$ et $\omega^{2^k}\tilde{\omega}^{2^k} = 1$ puisque $\omega\tilde{\omega} = 1$.
Conclusion : Donc $\omega^{2^n} + \tilde{\omega}^{2^n} = L_n$ pour tout $n \in \mathbb{N}$.

5. car $\mathcal{A}$ est fini, donc on peut ajouter des éléments dans l'idéal tant que l'idéal n'est pas $\mathcal{A}$ tout entier
6. Bien comprendre pourquoi, l'ordre est forcément une puissance de 2 par hypothèse, puis par la même hypothèse, on a forcément que 2^q est l'ordre car $\alpha^{2^{q-1}} = -1$ puisque la caractéristique p est impaire donc $1 \neq -1$
7. Comprendre pourquoi (morphisme de Frobenius)
8. Bien comprendre d'où vient chaque égalité
9. Car $2^q - 1 - p = 2_q k$ implique en fait que $k = 0$ d'où le résultat

Ainsi on a

$$\begin{aligned} L_{q-2} \equiv 0\ [M_q] &\iff \omega^{2^{q-2}} + \tilde{\omega}^{2^{q-2}} \equiv 0\ [M_q] \\ &\iff \omega^{2^{q-2}} \equiv -\tilde{\omega}^{2^{q-2}}\ [M_q] \\ &\iff (\omega^{2^{q-2}})^2 \equiv -1\ [M_q] \text{ toujours car } \omega^{2^k}\tilde{\omega}^{2^k} = 1 \\ &\iff (\omega^{2^{q-1}}) \equiv -1\ [M_q] \\ &\iff M_q \text{ est premier, par le théorème précédent} \end{aligned}$$

□

Astuces de l'agrégatif :

Pour les différentes leçons, je ne fais pas toujours la même chose,

— pour la 120, j'utilise la notation $\mathbb{Z}/M_q\mathbb{Z}$, je mets en lumière le lemme chinois

— pour la 123, j'utilise la notation $\mathbb{F}_{M_q}$, je parle de corps fini, je mets en lumière la loi de réciprocité quadratique

— pour la 141, je mets en lumière la construction du corps de rupture.

— pour la 121, j'utilise un moyen plus court pour prouver que 3 n'est pas un carré dans $\mathbb{Z}/M_q\mathbb{Z}$ et je fais la réciproque qui est la partie plus intéressante car cela nous donne une caractérisation des nombres de Mersenne qui sont premiers.

Moyen plus court pour prouver que 3 n'est pas un carré dans $\mathbb{Z}/M_q\mathbb{Z}$:

$$\begin{aligned} \left(\frac{3}{M_q}\right) &\overset{(1)}{=} \left(\frac{M_q}{3}\right)(-1)^{\frac{M_q-1}{2}} = \left(\frac{2^q-1}{3}\right)(-1)^{\frac{2^q-2}{2}} \\ &\overset{(2)}{=} \left(\frac{(-1)^q-1}{3}\right)(-1)^{2^{q-1}-1} \overset{(3)}{=} -\left(\frac{(-1-1}{3}\right) = -\left(\frac{1}{3}\right) = -1 \end{aligned}$$

(1) Loi de réciprocité quadratique

(2) car $2 \equiv -1\ [3]$

(3) car $2^{q-1} - 1$ est impair et car q est impair

Isométries du cube et du tétraèdre

Leçons : 101 ; 104 ; 105 ; 108 ; 183

Références : CALDERO–GERMONI, *Nouvelles Histoires Hédonistes de Groupes et de Géométries Tome 2* (p.221) [CG18]

Prérequis :

- définitions des isométries d'un objet X [CG18, p.218]
- la géométrie affine (repère, isométrie)
- une isométrie préserve les barycentres, donc préserve les points extrémaux (*i.e.* les sommets) d'un polygone.
- définition de $\mathrm{Isom}^+(X)$

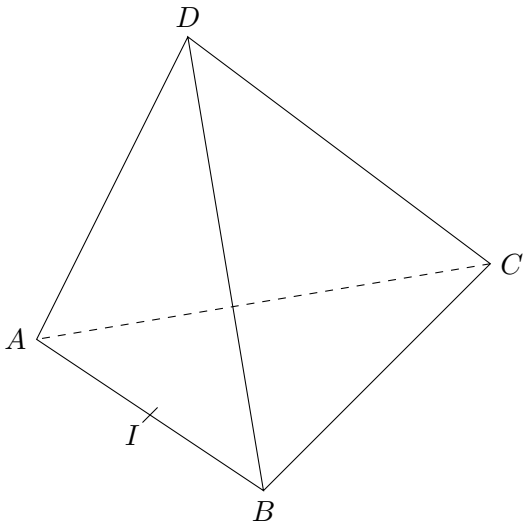
Introduction :

On va étudier les groupes des isométries et des isométries positives de 2 des 5 solides de Platon. On étudiera le tétraèdre et le cube. Cela nous permettra de mieux comprendre ces groupes car ils seront isomorphes à des groupes que l'on a l'habitude de manipuler. Ainsi, on pourra mieux comprendre les groupes symétriques et mieux comprendre le groupe des isométries en fonction de l'angle d'attaque que l'on se donne.

Théorème 1. Soit T un tétraèdre. On a alors

$$\mathrm{Isom}(T) \simeq \mathfrak{S}_4 \text{ et } \mathrm{Isom}^+(T) \simeq \mathfrak{A}_4$$

Démonstration. Commençons par dessiner le tétraèdre.



Les isométries préservent les sommets du tétraèdre car elles préservent les longueurs. Ainsi l'ensemble $S = \{A, B, C, D\}$ est stable par $\mathrm{Isom}(T)$. On peut donc faire agir $\mathrm{Isom}(T)$ sur S.

$$\varphi : \mathrm{Isom}(T) \to \mathfrak{S}_S \simeq \mathfrak{S}_4$$

On veut prouver que c'est un isomorphisme.

Étape 1 : *Montrons que φ est injective.*

Soit $f \in \ker(\varphi)$, f fixe les sommets du tétraèdre, donc en particulier f fixe le repère affine $(A, \overrightarrow{AB}, \overrightarrow{AC}, \overrightarrow{AD})$. Ainsi f fixe tout l'espace, donc f est l'identité. On obtient alors que φ est injective.

Étape 2 : *Montrons que φ est surjective.*

$\mathfrak{S}_4$ est engendré par les transpositions. Montrons que l'on peut trouver, pour chaque transposition t, une isométrie f telle que $\varphi(f) = t$. Soit la transposition (AB) qui échange les sommets A et B et laisse fixe C et D. On peut prendre la reflexion par rapport au plan (ICD) qui est le plan médiateur de $[AB]$. Ainsi, on a bien trouvé une isométrie qui échange A et B en laissant fixe C et D. Donc on peut obtenir toutes les transpositions sur le même principe. Ainsi φ est surjective.

En conclusion,

$$\mathrm{Isom}(T) \simeq \mathfrak{S}_4.$$

Étape 3 : *Regardons Isom$^+(T)$.*

$\det \circ \varphi^{-1} : \mathfrak{S}_4 \to \mathbb{C}^*$ est un morphisme non trivial donc c'est le morphisme signature [1]. Donc $\det = \varepsilon \circ \varphi$. Or $\mathrm{Isom}^+(T) = \ker(\det) \simeq \ker(\varepsilon) = \mathfrak{A}_4$ car φ est un isomorphisme [2]. Ainsi,

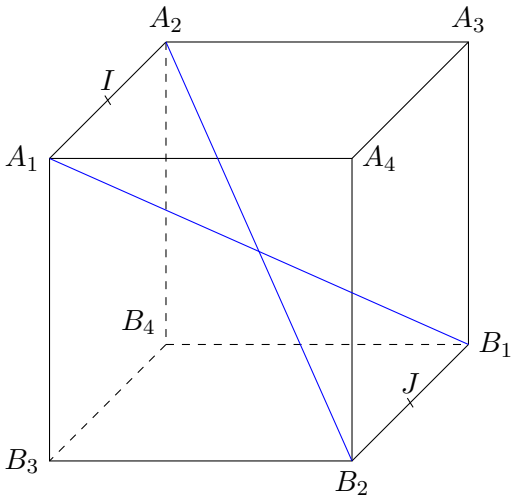
$$\mathrm{Isom}^+(T) \simeq \mathfrak{A}_4$$

□

Théorème 2. Soit C un cube. On a alors

$$\mathrm{Isom}(C) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z} \text{ et } \mathrm{Isom}^+(C) \simeq \mathfrak{S}_4$$

Démonstration. Commençons par dessiner le cube.



L'ensemble des 4 grandes diagonales D est stable par isométries du cube car les isométries préservent les longueurs (donc en particulier la plus grande longueur entre deux points du cube, c'est à dire les grandes diagonales). Ainsi on peut faire agir $\mathrm{Isom}(C)$ sur D par le morphisme suivant

$$\varphi : \mathrm{Isom}(C) \to \mathfrak{S}_D \simeq \mathfrak{S}_4$$

1. car il n'y a que deux morphismes de $\mathfrak{S}_n \to \mathbb{C}^*$ qui sont l'identité et la signature
2. on aurait pu dire aussi que $\mathrm{Isom}^+(T)$ est distingué d'indice 2 dans $\mathrm{Isom}(T)$ et que le seul groupe distingué d'indice 2 de $\mathfrak{S}_4$ est $\mathfrak{A}_4$

Étape 1 : *Étude du noyau de φ*

Soit $f \in \ker\varphi$. Par définition, f envoie chaque grande diagonale sur elle-même. Ainsi $f([A_1B_1]) = [A_1B_1]$, on a deux cas possibles :

— Si $f(A_1) = A_1$, on a donc $f(B_1) = B_1$ puis pour des questions de préservation des longueurs, f fixe tous les autres sommets du cube. Ainsi, f est l'identité que l'on notera Id.

— Si $f(A_1) = B_1$, on a donc $f(B_1) = A_1$ et de nouveau pour préserver les longueurs, il faut que f échange chaque sommet A_i avec B_i et vice versa pour tout $i \in \{1, 2, 3, 4\}$. Donc f est alors la symétrie centrale par rapport au centre du cube, on la notera $-Id$.

Ainsi $\ker\varphi = \{Id, -Id\}$.

Étape 2 : *Surjectivité de φ*

Comme pour le tétraèdre, on va prouver que l'on peut engendrer n'importe quelle transposition de $\mathfrak{S}_4$, et parce que les transpositions engendrent $\mathfrak{S}_4$, on aura la surjectivité de φ.

En prenant la rotation d'angle π autour de l'axe qui passe par les milieux des arêtes qui joignent les sommets des grandes diagonales que l'on veut échanger, on va bien échanger les deux grandes diagonales que l'on veut échanger en laissant les deux autres fixes. Exemple en faisant la rotation de π autour de (IJ), on va échanger (A_1B_1) et (A_2B_2) en laissant fixe (A_3B_3) et (A_4B_4).

Donc φ est surjective.

Étape 3 : *Étude de $Isom^+(C)$*

Si on restreint φ aux $\mathrm{Isom}^+(C)$, on a un isomorphisme car $-Id$ est une isométrie indirecte donc $\ker(\varphi_{|\mathrm{Isom}^+(C)}) = \{Id\}$ et elle reste surjective car les rotations sont des isométries positives. Ainsi

$$\mathrm{Isom}^+(C) \simeq \mathfrak{S}_4$$

Étape 4 : *Étude de $Isom(C)$*

On va utiliser le lemme suivant :

Lemme 1. Soit $N, H \lhd G$ tels que $|N||H| = |G|$ et $N \cap H = \{e\}$ où e est le neutre de G. Alors

$$G \simeq N \times H$$

Ici on prend $G = \mathrm{Isom}(C)$, $N = \mathrm{Isom}^+(C)$ distingué dans G car d'indice 2 et $H = \{Id, -Id\}$ distingué dans G car $\{Id, -Id\} \subset Z(G)$ le centre de G. On a bien $2|\mathrm{Isom}^+(C)| = |\mathrm{Isom}(C)|$ et $\mathrm{Isom}^+(C) \cap \{Id, -Id\} = \{Id\}$ car $-Id$ est une isométrie indirecte. Ainsi on a

$$\mathrm{Isom}(C) \simeq \mathrm{Isom}^+(C) \times \{Id, -Id\}$$

De plus, on a $\mathrm{Isom}^+(C) \simeq \mathfrak{S}_4$ et $\{Id, -Id\} \simeq \mathbb{Z}/2\mathbb{Z}$, d'où le résultat voulu

$$\mathrm{Isom}(C) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$$

□

Remarques :

On pourra, grâce à cette étude, donner le nombre de coloriages différents d'un cube par exemple (57 pour 3 couleurs)

Astuces de l'agrégatif :

Attention, il faut bien maitriser la géométrie affine, notamment les histoires d'isométries affines et repère affine.

Démonstration du lemme. On pose l'application

$$\varphi : \begin{cases} N \times H & \to & G \\ (n,h) & \mapsto & nh \end{cases}$$

Étape 1 : *Injectivité de φ*

Soient $n_1, n_2 \in N$, $h_1, h_2 \in H$ tels que $n_1h_1 = n_2h_2$. On veut prouver que $n_1 = n_2$ et $h_1 = h_2$.

$$n_1h_1 = n_2h_2 \iff \underbrace{n_2^{-1}n_1}_{\in N} = \underbrace{h_2h_1^{-1}}_{\in H} \in N \cap H = \{e\}$$

D'où $n_2^{-1}n_1 = e \iff n_1 = n_2$ et $h_2h_1^{-1} = e \iff h_1 = h_2$. Donc φ est bien injective.

Étape 2 : *Bijectivité de φ*

On utilise l'égalité des cardinaux entre $|N \times H| = |N||H| = |G|$ et l'injectivité de φ pour prouver que φ est bijective.

Étape 3 : *Montrons que φ est un morphisme*

On veut prouver que $n_1h_1n_2h_2 = n_1n_2h_1h_2$ pour avoir $\varphi(n_1,h_1)\varphi(n_2,h_2) = \varphi((n_1,h_1)(n_2,h_2))$. Ce qui est équivalent que de prouver que $h_1n_2 = n_2h_1$ et donc de prouver que $n_2^{-1}h_1n_2h_1^{-1} = e$. Or comme H est distingué dans G on a

$$\underbrace{n_2^{-1}h_1n_2}_{\in H}h_1^{-1} \in H$$

et comme N est distingué dans G, on a

$$n_2^{-1}\underbrace{h_1n_2h_1^{-1}}_{\in N} \in N$$

Donc $n_2^{-1}h_1n_2h_1^{-1} = e$ puisque $N \cap H = \{e\}$.

Ainsi φ est bien un isomorphisme.

□

Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

Leçons : 101 ; 104 ; 106 ; 190

Références : CALDERO–GERMONI, *Nouvelles Histoires Hédonistes de Groupes et Géométries Tome 2* (p.66) [CG18]

Prérequis :

- les orbites d'une action sont disjointes [1]
- la relation orbite/stabilisateur
- même polynôme caractéristique pour des matrices semblables [2]

On notera $\mathcal{D}_n(q)$ l'ensemble des matrices diagonalisables dans $\mathcal{M}_n(\mathbb{F}_q)$ où q est une puissance d'un nombre premier.

Introduction :

L'avantage des corps finis et notamment des espaces vectoriels de dimension finie sur les corps finis, c'est qu'ils sont justement finis. On peut alors se demander la proportion de matrices inversibles parmi toutes les matrices, ou la proportion de matrices diagonalisables parmi toutes les matrices. Pour cela, on va dénombrer $\mathrm{GL}_n(\mathbb{F}_q)$ et $\mathcal{D}_n(q)$.

Théorème 1. Soient q une puissance d'un nombre premier et $n \in \mathbb{N}$. On a alors

$$|\mathcal{D}_n(q)| = \sum_{\substack{m_1+\cdots+m_q=n \\ m_i \geqslant 0}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathrm{GL}_{m_i}(\mathbb{F}_q)|}$$

où, par convention, $|\mathrm{GL}_0(\mathbb{F}_q)| = 1$.

Démonstration. On va étudier l'action par conjugaison de $\mathrm{GL}_n(\mathbb{F}_q)$ sur $\mathcal{D}_n(q)$.

$$\varphi : \left\{ \begin{array}{ccc} \mathrm{GL}_n(\mathbb{F}_q) \times \mathcal{D}_n(q) & \to & \mathcal{D}_n(q) \\ (P, A) & \mapsto & PAP^{-1} \end{array} \right.$$

Étape 1 : *Etudions les orbites de cette action*

Soit $A \in \mathcal{D}_n(q)$, il existe donc une matrice $P \in \mathrm{GL}_n(\mathbb{F}_q)$ telle que

$$P^{-1}AP = \begin{pmatrix} \alpha_1 I_{m_1} & 0 & \dots & 0 \\ 0 & \alpha_2 I_{m_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & \alpha_q I_{m_q} \end{pmatrix}$$

où $m = (m_1, \dots, m_q) \in \mathbb{N}^q$ tel que $m_1 + \cdots + m_q = n$ et où l'on écrit $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_q\}$.

1. cela s'écrit bien
2. cela vient de $\det(AB) = \det A \det B$

Pour chaque $m = (m_1, \dots, m_q) \in \mathbb{N}^q$ tel que $m_1 + \cdots + m_q = n$, on notera D_m cette matrice. Ainsi $D_m \in \mathcal{O}rb(A)$.

Soit m' tel que $D_{m'}$ est dans $\mathcal{O}rb(A)$. Regardons le polynôme caractéristique de $D_{m'}$.

$$\prod_{i=1}^{q}(X-\alpha_i)^{m'_i} = \chi_{D_{m'}} = \chi_A = \chi_{D_m} = \prod_{i=1}^{q}(X-\alpha_i)^{m_i}$$

D'où $m_i = m'_i$ pour tout $i \in \{1, \dots, q\}$, ce qui donne $D_m = D_{m'}$.

On vient de démontrer que, pour D_m et $D_{m'}$ différents, on a $\mathcal{O}rb(D_m) \cap \mathcal{O}rb(D_{m'}) = \emptyset$, autrement dit

$$\mathcal{D}_n(q) = \bigsqcup_{\substack{m_1+\cdots+m_q=n \\ m_i \geqslant 0}} \mathcal{O}rb(D_m)$$

puisque dans chaque orbite, il y a au moins une matrice de la forme D_m.

Ainsi

$$|\mathcal{D}_n(q)| = \sum_{\substack{m_1+\cdots+m_q=n \\ m_i \geqslant 0}} |\mathcal{O}rb(D_m)|$$

On utilise la relation orbite/stabilisateur [3]

$$|\mathrm{GL}_n(\mathbb{F}_q)| = |\mathcal{O}rb(D_m)||\mathcal{S}tab(D_m)|$$

Étape 2 : *Etudions le stabilisateur de D_m*

Soit $P \in \mathcal{S}tab(D_m)$, on a donc $PD_m = D_mP$. Ainsi, pour toute valeur propre λ de D_m, pour tout $X \in E_\lambda$ [4],

$$D_mPX = PD_mX = \lambda PX$$

Donc $PX \in E_\lambda$, P stabilise donc tous les sous espaces propres, donc P est de la forme

$$P = \begin{pmatrix} P_1 & 0 & \dots & 0 \\ 0 & P_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & P_q \end{pmatrix}$$

où $P_i \in \mathrm{GL}_{m_i}(\mathbb{F}_q)$. Inversement, toute matrice de cette forme est dans le stabilisateur de D_m. De ce fait,

$$|\mathcal{S}tab(D_m)| = \prod_{i=1}^{q} |\mathrm{GL}_{m_i}(\mathbb{F}_q)|$$

On peut donc conclure

$$\begin{aligned} |\mathcal{D}_n(q)| &= \sum_{\substack{m_1+\cdots+m_q=n \\ m_i \geqslant 0}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathcal{S}tab(D_m)|} \\ &= \sum_{\substack{m_1+\cdots+m_q=n \\ m_i \geqslant 0}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathrm{GL}_{m_i}(\mathbb{F}_q)|} \end{aligned}$$

□

3. car l'application $\begin{cases} G/\mathcal{S}tab(x) & \to & \mathcal{O}rb(x) \\ g & \mapsto & g.x \end{cases}$ est une bijection

4. E_λ est l'espace propre de D_m associé à la valeur propre λ

Pour compléter le résultat, il faut connaître le cardinal des matrices inversibles de taille n dans F_q.

Théorème 2. Soient q une puissance d'un nombre premier et $n \in \mathbb{N}$. On a alors

$$|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$$

Démonstration. On a une bijection entre les bases de $\mathbb{F}_q^n$ et les matrices de $\mathrm{GL}_n(\mathbb{F}_q)$.

$$\varphi : \begin{cases} \{\text{bases de } \mathbb{F}_q^n\} & \to & \mathrm{GL}_n(\mathbb{F}_q) \\ (x_1, \dots, x_n) & \mapsto & \begin{pmatrix} & & \\ x_1 & \dots & x_n \\ & & \end{pmatrix} \end{cases}$$

Il suffit donc de compter les bases de $\mathbb{F}_q^n$. On a $(q^n - 1)$ choix pour le premier vecteur car il ne faut pas prendre le vecteur nul, ensuite pour le deuxième vecteur on a $(q^n - q)$ choix car il ne faut pas prendre un vecteur colinéaire au premier. Puis on a $(q^n - q^2)$ choix pour le troisième car il faut prendre un vecteur de $\mathbb{F}_q^n \backslash \mathrm{Vect}(x_1, x_2)$. etc... jusqu'au $n^{\text{ième}}$ vecteur où l'on a $(q^n - q^{n-1})$ choix. Ce qui fait que l'on trouve

$$|\{\text{bases de } \mathbb{F}_q^n\}| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$$

Ce qui conclut la preuve. □

Remarques :

Grâce au deuxième théorème, on peut aussi étudier les isomorphismes exceptionnels [CG18, p.49]

Astuces de l'agrégatif :

Le développement est assez court, il permet de bien prendre son temps pour expliquer tout ce qu'il faut comprendre, notamment la structure de la preuve dans l'étude de l'action.

Loi de réciprocité quadratique

(inspiré de la version de Maxence Brévard)

Leçons : 121 ; 123 ; 126 ; 170 ; 190

Références : CALDERO–GERMONI, *Nouvelles Histoires Hédonistes de Groupes et Géométrie Tome 1* (p.304)[CG17]

Prérequis :

- la classification des formes quadratiques sur un corps fini
- le symbole de Legendre et la propriété $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$
- définition d'un hyperplan affine
- les orbites d'une action sont disjointes
- la relation orbite/stabilisateur

Introduction :

La loi de réciprocité quadratique est un outil très puissant dans la théorie des corps finis car elle permet d'étudier le résidu quadratique d'un nombre premier q sur $\mathbb{F}_p$ en connaissant le résidu quadratique p sur $\mathbb{F}_q$.

Théorème 1 (Loi de réciprocité quadratique)**.** Soient p, q deux entiers premiers impairs distincts. Alors :

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

Idée de la preuve : On construit une forme quadratique φ' sur $\mathbb{F}_q^p$ équivalente à la forme quadratique de matrice l'identité φ. On montre alors que leurs boules unités

$$X' = \{x \in \mathbb{F}_q^p, \varphi'(x) = 1\} \quad \text{et} \quad X = \{x \in \mathbb{F}_q^p, \varphi(x) = x_1^2 + \cdots + x_p^2 = 1\}$$

sont équipotentes. On dénombre X en faisant agir $\mathbb{F}_p$ sur X et X' en faisant apparaître un hyperplan affine de $\mathbb{F}_q^p$.

Nous aurons besoin du lemme combinatoire suivant :

Lemme 1. Soit p impair premier et $a \in \mathbb{F}_p^*$. Alors

$$|\{x \in F_p, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$$

Démonstration du lemme. Le polynôme $ax^2 - 1$ admet au plus deux racines dans le corps $\mathbb{F}_p$. Comme $a \in \mathbb{F}_p$ et $\mathbb{F}_p$ est un corps, on réécrit l'équation souhaitée : $x^2 = a^{-1}$. Distinguons deux cas :

— Si a n'est pas un carré, a^{-1} ne l'est pas non plus, il n'y a donc aucune solution. L'égalité est immédiate.

— Sinon a est un carré donc a^{-1} l'est aussi, on écrit $a^{-1} = \varepsilon^2$. On a donc deux solutions distinctes : ε et $-\varepsilon$. On vérifie alors l'égalité souhaitée

D'où le résultat. □

Démonstration de la loi de réciprocité quadratique. Considérons la forme quadratique définie pour tout $x = (x_1, \cdots, x_p) \in \mathbb{F}_q^p$ par $\varphi(x) = x_1^2 + \cdots + x_p^2$. Notons $X = \{x \in \mathbb{F}_q^p, \varphi(x) = 1\}$ la boule unité de $\mathbb{F}_q^p$.

Étape 1 : *Dénombrons X modulo p*

On fait agir le groupe $\mathbb{F}_p$ sur X par permutations circulaires des coordonnées.

$$\phi : \begin{cases} \mathbb{F}_p \times X & \to X \\ (\alpha, (x_1, x_2, \ldots, x_p)) & \mapsto (x_{1+\alpha[p]}, x_{2+\alpha[p]}, \ldots, x_{p+\alpha[p]}) \end{cases}$$

La relation orbite-stabilisateur assure alors l'égalité :

$$\forall x \in \mathbb{F}_q^p,\ |Stab_x|.|Orb_x| = |\mathbb{F}_p| = p$$

Comme p est premier, il y a deux types d'orbites :

— des orbites de taille p, de stabilisateur $\{e\}$. On notera k le nombre d'orbites de taille p.

— des orbites de taille 1, de stabilisateur $\mathbb{F}_p$, qui sont de la forme : $\{(x, \cdots, x)\}, x \in \mathbb{F}_q$ avec $px^2 = 1$.[1] D'après le lemme, il y en a donc $1 + \left(\frac{p}{q}\right)$.

Comme les orbites sont disjointes, on a

$$|X| = \sum |\Omega_p| + \sum |\Omega_1| = \left(1 + \left(\frac{p}{q}\right)\right) \times 1 + k \times p \equiv 1 + \left(\frac{p}{q}\right)\ [p]$$

$$\boxed{|X| = 1 + \left(\frac{p}{q}\right)\ [p]}$$

Étape 2 : *Étudions un autre ensemble : X'*

On définit la forme quadratique φ' pour $x \in \mathbb{F}_q^p$ par

$$\varphi'(x_1, x_2, \ldots, x_{p-2}, x_{p-1}, x_p) = 2(x_1x_2 + \cdots + x_{p-2}x_{p-1}) + (-1)^{\frac{p-1}{2}} x_p^2$$

On notera X' l'ensemble $\{x \in \mathbb{F}_q^p, \varphi'(x) = 1\}$, la boule unité de $\mathbb{F}_q^p$ pour φ'. On pose $d = \frac{p-1}{2}$ et $a = (-1)^d$. La matrice de φ' dans la base canonique est :

$$A = \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & \ddots & \\ & & & & & & \ddots \\ & & & & & & & a \end{pmatrix}$$

Comme $det(\varphi') = det(A) = (-1)^d a = 1 = det(\varphi)$, d'après le théorème de **classification des formes quadratiques** sur les corps finis, φ et φ' sont équivalentes. Il existe un isomorphisme linéaire $u \in \mathcal{L}(\mathbb{F}_q)$ tq $\varphi' = \varphi \circ u$. Cet isomorphisme fournit une bijection entre les deux sphères X' et X. Ainsi

$$\boxed{|X| = |X'|}$$

1. car il faut que $\phi(\alpha, x) = x$ pour tout $\alpha \in \mathbb{F}_p$ et que $\varphi(x) = 1$

Étape 3 : *Dénombrons X' modulo p*

— Si $(x_1, x_3, \dots, x_{p-2}) = (0, \dots, 0)$, on choisit indifféremment le vecteur $(x_2, x_4, \dots, x_{p-1})$ dans $\mathbb{F}_q^d$ (q^d choix possibles). On choisit ensuite $x_p \in \mathbb{F}_q$ vérifiant $ax_p^2 = 1$. D'après le lemme, il y a $1 + \left(\frac{a}{q}\right)$ possibilités.

— Sinon, on choisit les $x_1, x_3, \dots, x_{p-2}$ ($q^d - 1$ choix). On choisit $x_p \in \mathbb{F}_q$ (q possibilités). Enfin, le vecteur $(x_2, x_4, \dots, x_{p-1})$ est alors un élément quelconque de l'hyperplan affine

$$H = \left\{2(x_1x_2 + \cdots + x_{p-2}x_{p-1}) + ax_p^2 - 1 = 0\right\}$$

de cardinal $|H| = q^{d-1}$.

Donc

$$|X'| = q^d\left(1 + \left(\frac{a}{q}\right)\right) + (q^d - 1)qq^{d-1}$$

$$\boxed{|X'| = q^d\left(\frac{a}{q}\right) + q^{2d}}$$

Comme $|X| = |X'|$ et en faisant le calcul dans $\mathbb{F}_p$, on obtient finalement :

$$1 + \left(\frac{p}{q}\right) = q^d\left(\frac{a}{q}\right) + q^{2d}$$

Or $q^d = q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$ et par petit théorème de Fermat, $q^{2d} = q^{p-1} = 1[p]$.

D'autre part, $\left(\frac{a}{q}\right) = a^{\frac{q-1}{2}}$. Ainsi on obtient l'égalité suivante :

$$1 + \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)a^{\frac{q-1}{2}} + 1$$

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

On a cette égalité dans $\mathbb{F}_p$, or le symbole de Legendre est un élément de $\{-1, +1\}$ et $p \neq 2$, donc les deux membres sont des éléments de $\{-1, +1\}$. Ains l'égalité est vraie dans $\mathbb{Z}$. □

Remarques :

Il y a beaucoup de preuves différentes de ce résultat.

Astuces de l'agrégatif :

En fonction du temps, je ne démontre pas le lemme qui est une simple étude de cas, parfois je fais une application pour trouver une condition nécessaire sur p pour que 3 soit un carré modulo p (utile dans le critère de primalité des nombres de Mersenne)

Condition nécessaire pour que 3 soit un carré modulo p avec p premier.
On utilise la loi de réciprocité quadratique avec 3 et p.

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$$

On suppose que 3 est un carré modulo p. Donc $\left(\frac{3}{p}\right) = 1$.

Ainsi si $p \equiv 1$ [3], on a $\left(\frac{p}{3}\right) = 1$ donc nécessairement, on a $\frac{p-1}{2}$ qui doit être pair, d'où $p \equiv 1$ [4]. Par le lemme chinois, on a $p \equiv 1$ [12].

Et si $p \equiv 2$ [3], on a $\left(\frac{p}{3}\right) = -1$ donc nécessairement, on a $\frac{p-1}{2}$ qui doit être impair, d'où $p \equiv 3$ [4]. Par le lemme chinois, on a $p \equiv -1$ [12].

Donc si 3 est un carré modulo p, on a nécessairement $p \equiv \pm 1$ [12].

Décomposition de Dunford

Leçons : 153 ; 157

Références : GOURDON, *Algèbre* (p.194) [GOU08a]

Prérequis :

- le lemme des noyaux
- la définition d'un projecteur [1]
- le théorème de Bézout avec plusieurs polynômes
- le théorème de codiagonalisabilité
- la diagonalisabilité d'un projecteur [2]

Introduction :

La décomposition de Dunford permet de mieux comprendre l'endomorphisme que l'on étudie et est plus poussée qu'une simple trigonalisation. Elle permet de calculer l'exponentielle facilement grâce au binome de Newton et la commutativité des endomorphismes d et n.

Théorème 1. Soit $u \in \mathcal{L}(E)$ tel que χ_u est scindé. Alors il existe un unique couple $(d,n) \in \mathcal{L}(E)^2$ tel que

- d est diagonalisable
- n est nilpotent
- $u = d + n$
- d et n commutent

De plus, d et n sont des polynômes en u.

Lemme 1. Soit $u \in \mathcal{L}(E)$ et P annulateur de u :

$$P = \alpha \prod_{i=1}^{r} M_i^{\alpha_i} \text{ (décomposition en irréductibles) } [3]$$

Notons pour tout $i \in [\![1;r]\!]$, $N_i = \ker M_i^{\alpha_i}(u)$.

Alors $E = \bigoplus_{i=1}^{r} N_i$ et pour tout $i \in [\![1;r]\!]$, la projection sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$ est un polynôme en u.

Démonstration du lemme. Par le lemme des noyaux, on a

$$E = \bigoplus_{i=1}^{r} N_i$$

1. endomorphisme p tel que $p \circ p = p$
2. car $X(X-1)$ est scindé à racines simples et annule p le projecteur
3. α est un inversible

Notons $Q_i = \prod_{j \neq i} M_j^{\alpha_j}$, on remarque que les (Q_i) sont premiers entre eux dans leur ensemble. Donc le théorème de Bézout nous donne des polynômes $(U_i) \in \mathbb{K}[X]$ tels que

$$\sum_{i=1}^{r} Q_i U_i = 1$$

Notons $P_i = Q_i U_i$ et $p_i = P_i(u)$.

Étape 1 : *Montrons que p_i est un projecteur.*

On a, par la relation de Bézout que l'on a ci-dessus,

$$\sum_{j=1}^{r} p_j = Id.$$

Donc, pour tout $i \in [\![1; r]\!]$,

$$\sum_{j=1}^{r} p_j \circ p_i = p_i$$

Or pour tout $j \neq i$, on a $p_j \circ p_i = U_i U_j(u) \circ \underbrace{Q_i Q_j(u)}_{=0} = 0$ car $P \mid Q_i Q_j$ et $P(u) = 0$.

On trouve donc

$$p_i^2 = p_i$$

Étape 2 : *Montrons que $Im(p_i) = N_i$.*

Par double inclusion,

$\boxed{\subset}$ Soit $x \in \mathrm{Im}(p_i)$. Alors il existe y tel que $x = p_i(y)$. On veut montrer que $x \in N_i$, *i.e.* $M_i^{\alpha_i}(u)(x) = 0$.

$$\begin{aligned} M_i^{\alpha_i}(u)(x) &= M_i^{\alpha_i}(u)(p_i(y)) \\ &= M_i^{\alpha_i} Q_i U_i(u)(y) \\ &= 0 \end{aligned}$$

car $P \mid M_i^{\alpha_i} Q_i$. Donc $x \in N_i$.

$\boxed{\supset}$ Soit $x \in N_i$. On a alors $M_i^{\alpha_i}(u)(x) = 0$. Or, par la relation de Bézout, on a

$$x = \sum_{j=1}^{r} p_j(x) = p_i(x)$$

car pour tout $j \neq i$, on a $p_j = Q_j U_j(u)$ et $Q_j = \prod_{k \neq j} M_k^{\alpha_k}$.

D'où $x \in \mathrm{Im}(p_i)$.

Étape 3 : *Montrons que* $\ker(p_i) = \bigoplus_{j \neq i} N_j$

Par double inclusion,

$\boxed{\subset}$ Soit $x \in \ker(p_i)$. On a

$$x = \sum_{j=1}^{r} p_j(x) = \sum_{j \neq i} p_j(x) \in \bigoplus_{j \neq i} \mathrm{Im}(p_j) = \bigoplus_{j \neq i} N_j$$

$\boxed{\supset}$ Pour tout $j \neq i$, $N_j \subset \ker(p_i)$ car

$$M_j^{\alpha_j} \mid Q_j \mid P_i$$

Ainsi, on a

$$\bigoplus_{j\neq i} N_j \subset \ker(p_i)$$

Donc p_i est le projecteur sur N_i parallèlement à $\bigoplus_{j\neq i} N_j$. De plus, $p_i = P_i(u)$ qui est donc bien un polynôme en u. □

Démonstration du théorème.
Existence : Le polynôme $\chi_u = \prod_{i=1}^{r}(X-\lambda_i)^{\alpha_i}$ est scindé. On peut donc appliquer le lemme à χ_u. Avec les mêmes notations que dans le lemme, on pose

$$d = \sum_{i=1}^{r} \lambda_i p_i \in \mathbb{K}[u]$$

qui est diagonalisable [4].

On pose maintenant $n = u - d \in \mathbb{K}[u]$.

Il suffit de montrer maintenant que n est nilpotent. On a

$$n = u - d = \sum_{i=1}^{r} (u - \lambda_i Id_E) \circ p_i$$

car $\sum p_i = Id_E$. On a alors, pour tout $k \geqslant 1$,

$$n^k = \sum_{i=1}^{r} (u - \lambda_i Id_E)^k \circ p_i$$

car tout commute et $p_i \circ p_j = \delta_{i,j} p_i$.

Ainsi, pour $k = \max_{i=1}^{r} \alpha_i$, on a pour tout $i \in [\![1; r]\!]$,

$$(u - \lambda_i Id_E)^k \circ p_i = 0$$

car $P \mid (X-\lambda_i)^k P_i$

De ce fait, on a $n^k = 0$. Donc n est nilpotent.

Ce qui conclut l'existence car on a d diagonalisable, n nilpotent, $d + n = u$ et $d \circ n = n \circ d$ puisque ce sont des polynômes en u.

Unicité : Soit d' et n' qui vérifient les conclusions de la décomposition de Dunford. On veut montrer que $d = d'$ et $n = n'$.

Comme d' et d sont des polynômes en u, ils commutent, ils sont donc codiagonalisables. Ainsi $d - d'$ est diagonalisable.

De même, n' et n sont des polynômes en u, donc ils commutent. Ainsi par le binôme de Newton, on a $n' - n$ qui est nilpotent.

Or

$$u = d + n = d' + n'$$

Donc

$$d - d' = n' - n$$

C'est donc un endomorphisme diagonalisable et nilpotent, autrement dit nul. Ainsi $d = d'$ et $n' = n$. Ce qui conclut l'unicité de la décomposition de Dunford. □

4. car les p_i sont diagonalisables (projecteurs donc $X(X-1)$ est annulateur et scindé à racines simples) et ils commutent (car polynômes en u) donc il existe une base de codiagonalisation

Remarques :

— Cette décomposition est lourde à trouver donc peu utilisé en pratique. Pour calculer l'exponentielle d'une matrice, on ne calcule pas en pratique la décomposition de Dunford.

— La décomposition de Jordan est plus poussée

— Attention, il faut que le polynôme caractéristique soit scindé (pas toujours vrai sur $\mathbb{R}$)

— Il existe d'autres preuves de la décomposition de Dunford, notamment avec la méthode de Newton.

Astuces de l'agrégatif :

On pourrait tenter de mettre ce développement dans le leçon 156 en justifiant le fait que connaître la décomposition de Dunford permet de calculer très rapidement l'exponentielle. En effet, $A = D + N$ donne $\exp(A) = \exp(D)\exp(N)$ car D et N commutent. Puis $\exp(N)$ est en fait une somme finie car N est nilpotente et $\exp(D)$ est facile à calculer puisque l'exponentielle d'une matrice diagonale est la diagonale des exponentielles des coefficients diagonaux et que la conjugaison par P peut sortir de la somme de l'exponentielle. Cependant, dans ce développement, on ne parle jamais d'exponentielle, je trouve donc que c'est un recasage un peu trop abusif dans une leçon dédiée à l'exponentielle matricielle.

Questions possibles :

- Pourquoi il y a unicité du projecteur qui projette sur un espace F parallèlement à un espace G ?

  Réponse : il suffit d'écrire la matrice du projecteur dans une base adaptée à $F \oplus G$

- Pourquoi un endomorphisme diagonalisable et nilpotent est nul ?

  Réponse : car X^k est annulateur, donc la seule valeur propre possible est 0, donc quand on diagonalise, on trouve l'endomorphisme nul

Image de l'exponentielle

Leçons : 153 ; 156 ; 214

Références : ZAVIDOVIQUE, *Un max de Math* (p.48) [ZAV13] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 178) [LMLBP20]

Ce développement est un résultat sur l'exponentielle matricielle, qui se place donc naturellement dans la leçon 156. L'essentiel du développement repose sur l'étude de l'image des polynômes de matrices par l'application exponentielle, ce qui justifie le placement de ce développement dans la leçon 153 par l'utilisation des propriétés topologiques liées à $\mathbb{C}[A]$. Le principal outil de la preuve est la connexité de $\mathbb{C}[A]^\times$, qui permet de déduire l'égalité $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$. Cette preuve constitue donc une belle illustration de la leçon 204. Enfin, du fait de l'utilisation du théorème d'inversion locale pour montrer que $\exp(\mathbb{C}[A])$ est ouvert dans $\mathbb{C}[A]^\times$, ce développement trouve tout à fait sa place dans la leçon 214.

Prérequis :

- le théorème d'inversion locale
- pour tout $A \in \mathcal{M}_n(\mathbb{C})$, $\exp(A) \in \mathrm{GL}_n(\mathbb{C})$.[1]
- un sous espace vectoriel de dimension finie est fermé
- $\mathbb{C}$ privé d'un nombre fini de points est connexe par arcs
- connexe par arcs implique connexe

Introduction :

On voudrait étudier l'application exponentielle sur les matrices et notamment son image par les matrices réelles et complexes. Pour faire cela, on va donner un résultat plus général : on va caractériser l'image des polynômes en A par l'exponentielle.

Théorème 1. Soit $A \in \mathcal{M}_n(\mathbb{C})$, on a

$$\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$$

où $\mathbb{C}[A]^\times$ désigne les inversibles de l'anneau $\mathbb{C}[A]$.

Démonstration. Soit $A \in \mathrm{GL}_n(\mathbb{C})$

Étape 1 : *Montrons que* $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap GL_n(\mathbb{C})$

$\boxed{\subset}$ On a $\mathbb{C}[A]^\times \subset \mathbb{C}[A]$ et pour tout $M \in \mathbb{C}[A]^\times$, il existe $N \in \mathbb{C}[A]$ telle que $MN = I_n$, donc M est inversible, i.e. $M \in \mathrm{GL}_n(\mathbb{C})$. D'où

$$\mathbb{C}[A]^\times \subset \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$$

$\boxed{\supset}$ Soit $M \in \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$, on considère le polynôme caractéristique

$$\chi_M = \sum_{i=0}^{n} a_i X^i$$

1. il suffit de voir que $I_n = \exp(0) = \exp(A - A) = \exp(A)\exp(-A)$, donc $\exp(A)$ est inversible.

Comme $M \in \mathrm{GL}_n(\mathbb{C})$, on a $a_0 = \det(M) \neq 0$ et, par le théorème de Cayley-Hamilton, on a

$$M\Big(\sum_{i=1}^{n} a_i M^{i-1}\Big) = -a_0 I_n$$

Donc $M \in \mathbb{C}[A]^\times$ car $\dfrac{-1}{a_0}\Big(\sum_{i=1}^{n} a_i M^{i-1}\Big) \in \mathbb{C}[A]$ puisque $M \in \mathbb{C}[A]$.

Étape 2 : *Montrons que* $\exp(\mathbb{C}[A]) \subset \mathbb{C}[A]^\times$

Soit $M \in \exp(\mathbb{C}[A])$, on a donc $M \in \mathrm{GL}_n(\mathbb{C})$ et il existe $N \in \mathbb{C}[A]$ tel que $M = \exp(N)$. Il faut donc prouver que $\exp(N)$ est un polynôme en A. L'ensemble $\mathbb{C}[A]$ est un sous espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ qui est de dimension finie, donc $\mathbb{C}[A]$ est fermé. Or

$$\forall n \in \mathbb{N},\ \sum_{i=0}^{n} \frac{N^i}{i!} \in \mathbb{C}[A]\ [2]$$

Donc $\exp(N) \in \mathbb{C}[A]$.

Étape 3 : *Montrons que* $\mathbb{C}[A]^\times$ *est connexe*

On veut montrer que $\mathbb{C}[A]^\times$ est connexe par arcs. Soient M_1 et M_2 dans $\mathbb{C}[A]^\times$. Pour tout $z \in \mathbb{C}$, on pose

$$P(z) = \det(zM_1 + (1-z)M_2) \in \mathbb{C}$$

Il faut trouver un chemin $\gamma : [0,1] \to \mathbb{C}$ (avec $\gamma(0) = 0$ et $\gamma(1) = 1$) continu tel que $P \circ \gamma$ reste dans $\mathbb{C}^*$. Or le polynôme P n'est pas nul ($P(0) \neq 0$) donc ne s'annule qu'un nombre fini de fois, notons Z cet ensemble. De plus $\mathbb{C}\backslash Z$ est connexe par arcs car on a enlevé qu'un nombre fini de points à $\mathbb{C}$. Donc il existe un chemin γ qui évite les points de Z. Ainsi il existe un chemin continu qui relie M_1 et M_2 dans $\mathrm{GL}_n(\mathbb{C})$. Donc $\mathbb{C}[A]^\times$ est connexe par arcs et par conséquent connexe.

Étape 4 : *Montrons que* $\exp(\mathbb{C}[A])$ *est ouvert dans* $\mathbb{C}[A]^\times$

On va appliquer le Théorème d'Inversion Locale [3] à

$$\exp : \mathbb{C}[A] \to \mathbb{C}[A]$$

On a $\mathrm{d}_0 \exp = Id$ bijectif, donc il existe un voisinage $\mathcal{U}$ ouvert de 0 dans $\mathbb{C}[A]$ et un voisinage $\mathcal{V}$ ouvert de I_n dans $\mathbb{C}[A]$ (qui est en fait aussi dans $\mathrm{GL}_n(\mathbb{C})$ [4] donc dans $\mathbb{C}[A]^\times$) tels que exp soit un $\mathcal{C}^1-$difféomorphisme entre $\mathcal{U}$ et $\mathcal{V}$.

Soit $\exp(M) \in \exp(\mathbb{C}[A])$. On pose

$$\mathcal{V}_M = \{V \exp(M), V \in \mathcal{V}\}$$

On a $\exp(M) \in \mathcal{V}_M$ et on veut prouver que $\mathcal{V}_M$ est un ouvert contenu dans $\exp(\mathbb{C}[A])$. $\mathcal{V}_M$ est bien ouvert car $\mathcal{V}$ l'est et $\exp(M)$ est inversible. De plus, pour tout $V \in \mathcal{V}$, il existe $U \in \mathcal{U}$ tel que $V = \exp(U)$. D'où

$$V \exp(M) = \exp(U)\exp(M) = \exp(U+M) \in \exp(\mathbb{C}[A])\ [5]$$

Donc $\exp(\mathbb{C}[A])$ est un ouvert de $\mathbb{C}[A]^\times$.

2. car $\mathbb{C}[A]$ est stable par produit et somme finie
3. Remarquons que $\mathbb{C}[A]$ est fermé et donc cela pourrait poser problème mais, en fait, on regarde $\mathbb{C}[A]$ muni de la topologie de $\mathcal{M}_n(\mathbb{C})$ et $\mathbb{C}[A]$ est ouvert relativement à $\mathbb{C}[A]$
4. car l'exponentielle va dans $\mathrm{GL}_n(\mathbb{C})$
5. U et M commutent car ce sont tous les deux des polynômes en A

Étape 5 : *Montrons que* $\exp(\mathbb{C}[A])$ *est fermé dans* $\mathbb{C}[A]^\times$

On veut montrer que $E = \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}(A))$ est un ouvert de $\mathbb{C}[A]^\times$. Montrons que :

$$E = \bigcup_{M\in E} M\exp(\mathbb{C}[A])$$

$\boxed{\subset}$ Soit $M \in E$, on a $M = M\exp(0) \in \bigcup_{M\in E} M\exp(\mathbb{C}[A])$.

$\boxed{\supset}$ Soit $M \in E$, $P \in \mathbb{C}[X]$. On pose

$$N = M\exp(P(A))$$

Donc

$$M = N\exp(-P(A))$$

Ainsi si $N \in \exp(\mathbb{C}[A])$, on aura aussi $M \in \exp(\mathbb{C}[A])$ ce qui est exclu car $M \in E$. Ce qui entraine que $N \notin \exp(\mathbb{C}[A])$ donc $N \in E$.

Or, pour tout $M \in E$, on a $M\exp(\mathbb{C}[A])$ qui est un ouvert de $\mathbb{C}[A]^\times$ car M est inversible et $\exp(\mathbb{C}[A])$ est ouvert (étape 4). Ainsi E est ouvert dans $\mathbb{C}[A]^\times$ car c'est une réunion quelconque d'ensembles ouverts. Donc $\exp(\mathbb{C}[A])$ est fermé dans $\mathbb{C}[A]^\times$.

Étape 6 : *Conclusion*

L'ensemble $\exp(\mathbb{C}[A])$ est ouvert et fermé dans $\mathbb{C}[A]^\times$ qui est connexe. Or $I_n = \exp(0) \in \exp(\mathbb{C}[A])$ donc $\exp(\mathbb{C}[A]) \neq \varnothing$. De ce fait

$$\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$$

Ce qui conclut la preuve.

□

Corollaire 1. On a :

$$\exp(\mathcal{M}_n(\mathbb{C})) = \mathrm{GL}_n(\mathbb{C})$$

Démonstration. Soit $A \in \mathrm{GL}_n(\mathbb{C})$, on a donc $A \in \mathbb{C}[A]^\times$, donc par le théorème précédent, il existe $P \in \mathbb{C}[X]$ tel que $A = \exp(P(A))$. On a donc bien un antécédent dans $\mathcal{M}_n(\mathbb{C})$. □

Corollaire 2. On a :

$$\exp(\mathcal{M}_n(\mathbb{R})) = \{A^2, A \in \mathrm{GL}_n(\mathbb{R})\}$$

Démonstration. Si $A \in \exp(\mathcal{M}_n(\mathbb{R}))$, on a $B \in \mathcal{M}_n(\mathbb{R})$ telle que $A = \exp(B)$. On a alors

$$A = \exp\left(\frac{B}{2}\right)^2$$

avec $\exp\left(\frac{B}{2}\right) \in \mathrm{GL}_n(\mathbb{R})$. Réciproquement, soit $A \in \mathrm{GL}_n(\mathbb{R})$, on a donc $A \in \mathbb{C}[A]^\times$, donc par le théorème précédent, il existe $P \in \mathbb{C}[X]$ tel que

$$A = \exp(P(A))$$

P est complexe mais A est réelle, donc, en passant au conjugué, on a

$$A = \exp(\overline{P(A)}).$$

Ce qui nous donne

$$A^2 = \exp(P(A))\exp(\overline{P(A)}) = \exp(P(A) + \overline{P(A)})$$

Or $P + \overline{P}$ est à coefficients réels donc $(P + \overline{P})(A)$ est dans $\mathcal{M}_n(\mathbb{R})$. Donc $(P + \overline{P})(A)$ est un antécédent de A pour l'exponentielle. □

Astuces de l'agrégatif :

— Les deux corollaires peuvent être regroupés en un seul.

— Il faut faire attention aux ensembles que l'on utilise pour appliquer le théorème d'inversion locale. Ce théorème s'applique pour une application d'un ouvert d'un Banach vers un espace de Banach. Ici, on utilise que $\mathbb{C}[A]$ est un ouvert de l'espace de Banach $\mathbb{C}[A]$.

— Quand on utilise le théorème d'inversion locale, il faut bien comprendre que $\mathrm{d}_0 \exp$ est l'identité des fonctions de $\mathcal{M}_n(\mathbb{C})$ dans $\mathcal{M}_n(\mathbb{C})$, et non la matrice identité I_n.

Remarques :

— Plus généralement, le même théorème d'inversion locale permet de donner un difféomorphisme local entre un voisinage de l'identité dans un groupe $G \leqslant \mathcal{G}_n(\mathbb{C})$ et un voisinage de zéro dans l'algèbre de Lie associée, $\mathfrak{g} = \mathrm{Lie}(G)$. Un argument de connexité similaire permet alors de déduire que l'algèbre de Lie $\mathfrak{g}$ détermine la composante connexe de l'identité de G.

— Par les mêmes arguments qu'à la question **a)**, on a aussi

$$\mathbb{R}[A]^\times = \mathbb{R}[A] \cap \mathcal{G}_n(\mathbb{R}).$$

Par contre, l'égalité $\exp(\mathbb{R}[A]) = \mathbb{R}[A]^\times$ est fausse. Par exemple, $-I_n \notin \exp(\mathcal{M}_n(\mathbb{R}))$ puisque $\mathrm{Sp}(\exp(\mathcal{M}_n(\mathbb{R}))) \subset]0, +\infty[$ alors que $-I_n \in \mathbb{R}[A]^\times$. On voit bien la particularité topologique de $\mathbb{C}$ dans la preuve : retirer un nombre fini de points de $\mathbb{C}$ conserve la connexité, ce qui n'est pas vrai dans $\mathbb{R}$. En effet, on peut relier deux déterminants dans $\mathbb{C}^*$, mais pas dans $\mathbb{R}^*$ qui n'est pas connexe.

— On peut voir que $\exp(\mathcal{M}_n(\mathbb{R})) \neq \mathcal{G}_n(\mathbb{R})$, en utilisant le fait que $\exp(\mathcal{M}_n(\mathbb{R})) \subset \mathcal{G}_n^+(\mathbb{R})$. Cependant $\exp(\mathcal{M}_n(\mathbb{R})) \neq \mathcal{G}_n^+(\mathbb{R})$ car, par exemple, la matrice $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ est dans $\mathcal{G}_n^+(\mathbb{R})$ mais pas dans $\exp(\mathcal{M}_n(\mathbb{R}))$.

— On a montré que l'application $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathcal{G}_n(\mathbb{C})$ est surjective, mais elle n'est pas injective pour $n \geqslant 1$ et $\exp : \mathcal{M}_n(\mathbb{R}) \to \mathcal{G}_n(\mathbb{R})$ n'est pas injective pour $n \geqslant 2$. Par exemple, $\exp \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \exp \begin{pmatrix} 0 & -2\pi \\ 2\pi & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Cependant $\exp : \mathcal{D}_n(\mathbb{C}) \to \mathcal{G}_n(\mathbb{C})$ est injective, où $\mathcal{D}_n(\mathbb{C})$ désigne l'ensemble des matrices diagonalisables de $\mathcal{M}_n(\mathbb{C})$.

— Si on restreint l'exponentielle à $\mathcal{A}_n(\mathbb{R})$, l'ensemble des matrices antisymétriques, on a alors la surjectivité dans $SO_n(\mathbb{R})$.

— Si on restreint l'exponentielle à $\mathcal{S}_n(\mathbb{R})$, l'ensemble des matrices symétriques, on a alors la surjectivité dans $\mathcal{S}_n^{++}(\mathbb{R})$ l'ensemble des matrices réelles symétriques définies positives. Il y a même un homéomorphisme.

Questions possibles :

- Calculer la différentielle de exp en 0.
- Montrer que $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathcal{G}_n(\mathbb{C})$ n'est pas injective.
- Pourquoi un sous-espace vectoriel de dimension finie est-il fermé ?
- Si Z est fini, montrer que $\mathbb{C} \backslash Z$ est connexe par arcs.
- Si $\mathcal{U}$ est un ouvert de $\mathcal{G}_n(\mathbb{C})$ et $M \in \mathcal{G}_n(\mathbb{C})$, montrer que $M\mathcal{U}$ est ouvert.
- Rappeler pourquoi, si $A, B \in \mathcal{M}_n(\mathbb{C})$ commutent, $\exp(A+B) = \exp(A)\exp(B)$.
- Pourquoi $\overline{\exp(A)} = \exp(\overline{A})$?

Convergence de polygones vers l'isobarycentre

Leçons : 152 ; 182 ; 226

Références : GOURDON, *Algèbre* (p.146)

Prérequis :

- calcul du déterminant de Van Der Monde
- propriété d'associativité des barycentres

Introduction :

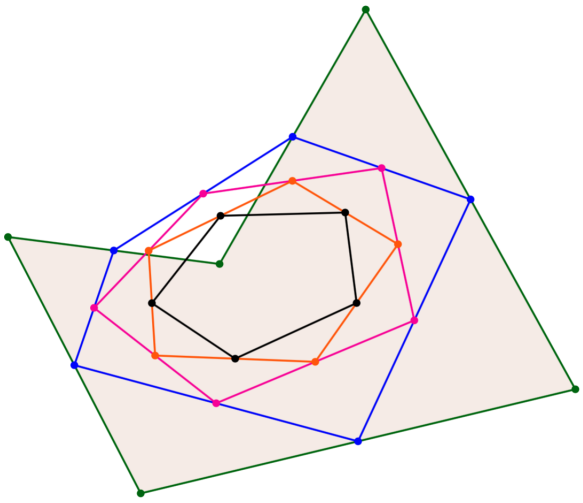
On souhaite observer vers quelle limite tend une suite de polygones définie en prenant le polygone qui relie les milieux de chaque coté du polygone précédent. On tend en fait vers un point qui est l'isobarycentre du premier polygone.

Théorème 1. Soit $z^{(0)} = (z_1, \dots, z_n) \in \mathbb{C}^n$. On considère la suite $(z^{(k)})_{k\in\mathbb{N}}$ définie par :

$$z^{(k+1)} = \left(\frac{z_1^{(k)} + z_2^{(k)}}{2}, \frac{z_2^{(k)} + z_3^{(k)}}{2}, \dots, \frac{z_{n-1}^{(k)} + z_n^{(k)}}{2}, \frac{z_n^{(k)} + z_1^{(k)}}{2}\right)$$

Alors la suite $(z^{(k)})_{k\in\mathbb{N}}$ converge vers l'isobarycentre de $z^{(0)}$, i.e. $(z^{(k)})_{k\in\mathbb{N}}$ tend vers $(g, g, \dots, g)$ quand k tend vers l'infini où g est l'isobarycentre de $z^{(0)}$.

Illustration 1.



Convergence des polygones ($z^{(0)}$: vert, $z^{(1)}$: bleu, $z^{(2)}$: rose, $z^{(3)}$: orange, $z^{(4)}$: noir)

Lemme 1.
Soit $A = \begin{pmatrix} a_0 & a_1 & & & a_{n-1} \\ a_{n-1} & \ddots & \ddots & & \\ & \ddots & \ddots & \ddots & \\ a_2 & & \ddots & \ddots & a_1 \\ a_1 & a_2 & & a_n & a_0 \end{pmatrix}$ une matrice circulante. On note $P = \sum_{j=0}^{n-1} a_j X^j$ le polynôme associé à A et $\omega = e^{i2\pi/n}$ une racine primitive $n^{\text{ième}}$ de l'unité. Alors

$$\det(A) = \prod_{j=0}^{n-1} P(\omega^j)$$

Démonstration du lemme.
On pose la matrice suivante

$$\Omega = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & (\omega^2)^2 & \dots & (\omega^{n-1})^2 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{n-1} & (\omega^2)^{n-1} & \dots & (\omega^{n-1})^{n-1} \end{pmatrix}$$

Comme tous les $(\omega^j)_{j=1}^{n-1}$ sont distincts, on a $\det \Omega \neq 0$.
En calculant $A\Omega$, on obtient

$$A\Omega = \begin{pmatrix} P(1) & P(\omega) & P(\omega^2) & \dots & P(\omega^{n-1}) \\ P(1) & \omega P(\omega) & \omega^2 P(\omega^2) & \dots & \omega^{n-1} P(\omega^{n-1}) \\ P(1) & \omega^2 P(\omega) & (\omega^2)^2 P(\omega^2) & \dots & (\omega^{n-1})^2 P(\omega^{n-1}) \\ \vdots & \vdots & \vdots & & \vdots \\ P(1) & \omega^{n-1} P(\omega) & (\omega^2)^{n-1} P(\omega^2) & \dots & (\omega^{n-1})^{n-1} P(\omega^{n-1}) \end{pmatrix}$$

En calculant le déterminant et en factorisant chaque colonne par les $P(\omega^j)$, on obtient donc

$$\det A\Omega = \det A \det \Omega = \prod_{j=0}^{n-1} P(\omega^j) \det \Omega$$

Ainsi

$$\det A = \prod_{j=0}^{n-1} P(\omega^j)$$

□

Démonstration du théorème. On a $z^{(k+1)} = Az^{(k)}$ où

$$A = \begin{pmatrix} 1/2 & 1/2 & 0 & \dots & 0 \\ 0 & 1/2 & 1/2 & 0 & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ 0 & & 0 & 1/2 & 1/2 \\ 1/2 & 0 & \dots & 0 & 1/2 \end{pmatrix}$$

Par récurrence, on a $z^{(k)} = A^k z^{(0)}$. On veut donc étudier la limite de A^k. Pour cela, on va essayer de diagonaliser A.

$$\chi_A(X) = \det(XI_d - A) = \begin{vmatrix} X-\frac{1}{2} & -\frac{1}{2} & 0 & \dots & 0 \\ 0 & X-\frac{1}{2} & -\frac{1}{2} & 0 & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ 0 & & 0 & X-\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & 0 & \dots & 0 & X-\frac{1}{2} \end{vmatrix}$$

Par le lemme précédent, avec le polynome $P(t) = X - \frac{1}{2} - \frac{1}{2}t$, on a

$$\chi_A(X) = \prod_{j=0}^{n-1} \left(X - \left(\frac{1+\omega^j}{2} \right) \right)$$

Donc A est diagonalisable, puisque χ_A est scindé à racines simples.

$$A = Q^{-1} \begin{pmatrix} 1 & & & \\ & \frac{1+\omega}{2} & & \\ & & \ddots & \\ & & & \frac{1+\omega^{n-1}}{2} \end{pmatrix} Q$$

Or $\left| \frac{1+\omega^j}{2} \right| < 1$ pour tout $j \in [\![1, n-1]\!]$. [1]

Ainsi $A^k = Q^{-1} \begin{pmatrix} 1 & & & \\ & \left(\frac{1+\omega}{2}\right)^k & & \\ & & \ddots & \\ & & & \left(\frac{1+\omega^{n-1}}{2}\right)^k \end{pmatrix} Q \xrightarrow[k\to+\infty]{} Q^{-1} \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} Q$

On pose $A^{(\infty)} = Q^{-1} \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} Q$

Ainsi on obtient l'existence de la limite des $(z^{(k)})_k$, on a $\lim\limits_{k\to\infty} z^{(k)} = A^{(\infty)} z^{(0)}$. On note cette limite $z^{(\infty)}$.

Or, comme on a $z^{(k+1)} = Az^{(k)}$, en passant à la limite, on trouve $z^{(\infty)} = Az^{(\infty)}$.

Donc $z^{(\infty)} \in \operatorname{Ker}(A - I_n)$ qui est de dimension 1 [2]. Or $(1, \dots, 1) \in \operatorname{Ker}(A - I_n)$ donc $z^{(\infty)} = \lambda(1, \dots, 1)$.

De plus, pour tout $k \in \mathbb{N}$, les $z^{(k)}$ ont même barycentre (on utilise la propriété d'associativité des barycentres). En passant à la limite, $z^{(\infty)}$ a le même barycentre que tous les $z^{(k)}$ que l'on notera g.

$$g = \frac{1}{n} \sum_{j=1}^{n} z_j^{(\infty)} = \frac{n\lambda}{n} = \lambda$$

Ainsi $z^{(\infty)} = (g, \dots, g)$. □

1. On peut le voir sur un dessin pour se convaincre, on peut faire un calcul avec l'angle moitié pour être rigoureux et le prouver par un calcul

$$\left| \frac{1 + e^{\frac{i2\pi j}{n}}}{2} \right| = \left| e^{\frac{i\pi j}{n}} \frac{e^{-\frac{i\pi j}{n}} + e^{\frac{i\pi j}{n}}}{2} \right| = \left| e^{\frac{i\pi j}{n}} \cos\left(\frac{\pi j}{n}\right) \right| < 1$$

grâce au cosinus

2. puisque $\chi_A = \prod_{j=0}^{n-1} \left(X - \left(\frac{1+\omega^j}{2} \right) \right)$

Remarques :
Le résultat reste vrai si on ne prend pas le milieu mais un autre rapport sur le segment.

Astuces de l'agrégatif :
Attention aux indices, on a n pour la dimension des vecteurs, k pour l'indice de suite, j pour les différentes sommations, le i complexe[3], etc.

Banach–Steinhaus

Leçons : 208 ; 246

Références : GOURDON, *Analyse* (p.398)

Prérequis :

- théorème de Baire
- calcul du noyau de Dirichlet
- un Banach est d'intérieur non vide
- $(\mathcal{C}_b^0(\mathbb{R},\mathbb{C}), \|.\|_\infty)$ est complet

Introduction :

Le théorème de Banach–Steinhaus est un théorème essentiel qui permet de déduire des informations globales (normes d'opérateurs) à partir d'informations ponctuelles (normes à x fixé). C'est une application directe du théorème de Baire.

Théorème 1 (Banach–Steinhaus)**.** Soit E un espace de Banach, F un espace vectoriel normé. Soit $(T_i)_{i\in I}$ une famille quelconque d'applications linéaires continues de E vers F. Alors on a deux cas disjoints possibles :

(i) $\sup\{\|T_i\|_{\mathcal{L}(E,F)}, i \in I\} < \infty$

(ii) il existe $x \in E$ tel que $\sup\{\|T_i(x)\|_F, i \in I\} = \infty$

Démonstration. S'il existe $x \in E$ tel que $\sup\{\|T_i(x)\|_F, i \in I\} = \infty$, alors il existe une suite $(i_n) \in I^{\mathbb{N}}$ tel que $\|T_{i_n}(x)\|_F$ tend vers $+\infty$ quand n tend vers l'infini.
Or $\|T_{i_n}\|_{\mathcal{L}(E,F)} = \sup\left\{\dfrac{\|T_{i_n}(y)\|_F}{\|y\|_E}, y \in E\backslash\{0\}\right\} \geqslant \dfrac{\|T_{i_n}(x)\|_F}{\|x\|_E}$ qui tend vers $+\infty$ donc on a bien

$$\sup\{\|T_i\|_{\mathcal{L}(E,F)}, i \in I\} = \infty.$$

Ainsi si on est dans le cas (ii), on n'est pas dans le cas (i).

Montrons maintenant que si on n'est pas dans le cas (ii), on est dans le cas (i).
On considère maintenant que, pour tout $x \in E$, $\sup\{\|T_i(x)\|_F, i \in I\} < \infty$.
Pour chaque $n \in \mathbb{N}^*$ et $i \in I$, on pose l'ensemble

$$F_{n,i} = \{x \in E, \|T_i(x)\|_F \leqslant n\}.$$

$F_{n,i}$ est fermé car $F_{n,i} = T_i^{-1}([0;n])$ avec $[0;n]$ fermé et T_i continue pour tout $i \in I$. On considère

$$F_n = \bigcap_{i\in I} F_{n,i}$$

qui est fermé pour tout $n \in \mathbb{N}^*$ car l'intersection quelconque de fermés est fermée. De plus, pour tout $x \in E$, il existe $n \in \mathbb{N}^*$ tel que $\sup\{\|T_i(x)\|_F, i \in I\} \leqslant n$, d'où

$$E = \bigcup_{n\in\mathbb{N}^*} F_n.$$

On utilise le théorème de Baire, E est d'intérieur non vide[1], donc il existe n_0 tel que F_{n_0} soit aussi d'intérieur non vide.

Ainsi il existe un $y \in E$ et $r > 0$ tel que $B(y,r) \subset F_{n_0}$, ce qui se traduit par :

$$\forall z \in B(y,r),\ \|T_i(z)\|_F \leqslant n_0 \text{ pour tout } i \in I.$$

Soit $x \in B(0,1)$, on veut prouver que $\|T_i(x)\|_F$ est borné pour tout $i \in I$. Or on a

$$T_i(x) = \frac{1}{r}(T_i(y+rx) - T(y))$$

car T est linéaire et avec y et $y+rx$ dans $B(y,r)$, donc

$$\|T_i(x)\|_F = \|\frac{1}{r}(T_i(y+rx) - T(y))\| \leqslant \frac{2n_0}{r} \quad \text{pour tout } i \in I.$$

Donc, en passant au sup sur i, on a $\sup\{\|T_i\|_{\mathcal{L}(E,F)}, i \in I\} \leqslant \frac{2n_0}{r}$. Ainsi

$$\sup\{\|T_i\|_{\mathcal{L}(E,F)}, i \in I\} < \infty.$$

□

Application 1. Il existe des fonctions continues dont la série de Fourier diverge et donc ne coïncide pas avec leur série de Fourier.

Démonstration. On pose $\mathcal{C}_{2\pi} := \{f \in \mathcal{C}^0(\mathbb{R},\mathbb{R}) \text{ avec } f\ 2\pi-\text{périodique }\}$ muni de la norme uniforme $\|.\|$. Pour $f \in \mathcal{C}_{2\pi}$ et $n \in \mathbb{N}$, on note

$$c_n(f) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)e^{-int}dt \quad \text{et} \quad S_n(f) : x \mapsto \sum_{k=-n}^{n} c_k(f)e^{-ikx}.$$

Pour tout $n \in N$, on pose l'application

$$\ell_n : \left\{ \begin{array}{ccc} \mathcal{C}_{2\pi} & \to & \mathbb{C} \\ f & \mapsto & S_n(f)(0) \end{array} \right.$$

Étape 1 : *L'application ℓ_n est linéaire et continue pour tout $n \in \mathbb{N}$.*

Soit $n \in \mathbb{N}$, l'application ℓ_n est linéaire par linéarité de la somme et de l'intégrale.

Soit $f \in \mathcal{C}_{2\pi}$,

$$\begin{aligned} |\ell_n(f)| &= \Big| \sum_{k=-n}^{n} c_k(f) \Big| \\ &= \Big| \sum_{k=-n}^{n} \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)e^{-ikt}dt \Big| \\ &= \frac{1}{2\pi}\Big| \int_{-\pi}^{\pi} f(t) \sum_{k=-n}^{n} e^{-ikt}dt \Big| \\ &\leqslant \frac{1}{2\pi}\int_{-\pi}^{\pi} |f(t)||Dn(t)|dt \\ &\leqslant \|f\|\|D_n\|_1 \end{aligned}$$

1. car E est un espace topologique, il est donc ouvert pour sa topologie et donc égal à son intérieur, de plus, comme c'est un espace vectoriel, il est non vide (il y a 0 dedans). Donc E est bien d'intérieur non vide

On a bien D_n intégrable puisque $D_n(t) = \dfrac{\sin\left((2n+1)\frac{t}{2}\right)}{\sin\left(\frac{t}{2}\right)}$ continue sur $[-\pi;\pi]$ puisque $D_n(0) = 2n+1$ comme vu dans la note [2].

Ainsi on a pour tout $f \in \mathcal{C}_{2\pi}$, $|\ell_n(f)| \leqslant \|D_n\|_1 \|f\|$. Donc ℓ_n est continue.

Étape 2 : *Prouvons que* $\|\ell_n\|_{\mathcal{L}(\mathcal{C}_{2\pi},\mathbb{C})} = \|D_n\|_1$

Par le calcul précédent, on sait que $\|\ell_n\|_{\mathcal{L}(\mathcal{C}_{2\pi},\mathbb{C})} \leqslant \|D_n\|_1$. On va approcher $\|\ell_n\|_{\mathcal{L}(\mathcal{C}_{2\pi},\mathbb{C})}$. Pour tout $\varepsilon > 0$, on définit $f_\varepsilon = \dfrac{D_n(t)}{|D_n(t)| + \varepsilon}$ qui appartient à la boule unité (i.e $f_\varepsilon \in B_\infty(0,1)$).

Pour tout $n \in \mathbb{N}$,

$$\begin{aligned} |\ell_n(f_\varepsilon)| &\leqslant \frac{1}{2\pi}\int_{-\pi}^{\pi} |f(t)||Dn(t)|dt \\ &\leqslant \frac{1}{2\pi}\int_{-\pi}^{\pi} \frac{|Dn(t)|^2}{|Dn(t)|+\varepsilon}dt \end{aligned}$$

Lorsque l'on fait tendre ε vers 0, avec ε positif, cela converge vers $\|D_n\|_1$ par convergence dominée [3]. Ainsi $\|\ell_n\|_{\mathcal{L}(\mathcal{C}_{2\pi},\mathbb{C})} = \|D_n\|_1$.

Étape 3 : $(\|D_n\|_1)_{n\in\mathbb{N}}$ *diverge quand* n *tend vers l'infini.*

Pour tout $n \in \mathbb{N}$,

$$\|D_n\|_1 = \frac{1}{2\pi}\int_{-\pi}^{\pi} \frac{\left|\sin\left((2n+1)\frac{t}{2}\right)\right|}{\left|\sin\left(\frac{t}{2}\right)\right|}dt = \frac{1}{\pi}\int_0^{\pi} \frac{\left|\sin\left((2n+1)\frac{t}{2}\right)\right|}{\left|\sin\left(\frac{t}{2}\right)\right|}dt \geqslant \frac{1}{\pi}\int_0^{\pi} \frac{\left|\sin\left((2n+1)\frac{t}{2}\right)\right|}{\left|\frac{t}{2}\right|}dt$$

puisque $\sin(x) \leqslant x$ sur $\left[0, \frac{\pi}{2}\right]$. En posant le changement de variable $u = \frac{(2n+1)t}{2}$, on a

$$\|D_n\|_1 \geqslant \frac{2}{\pi}\int_0^{\frac{(2n+1)\pi}{2}} \frac{|\sin u|}{u}du$$

Or $\displaystyle\int_0^{+\infty} \frac{|\sin u|}{u}du$ diverge [4], donc $\|D_n\|_1$ diverge aussi.

Étape 4 : *Utilisation du théorème de Banach–Steinhaus*

On veut appliquer le théorème de Banach–Steinhaus avec :

- $E = \mathcal{C}_{2\pi}$ qui est bien un Banach puisque c'est un fermé de $(\mathcal{C}_b^0(\mathbb{R},\mathbb{C}), \|.\|)$ qui est un Banach.
- $F = \mathbb{C}$ qui est bien un espace vectoriel normé
- $I = \mathbb{N}$
- $T_n = \ell_n$ applications linéaires continues grâce à l'étape 1.

Ainsi on peut appliquer le théorème de Banach–Steinhaus.
Or, par l'étape 3, $\sup_{n\in\mathbb{N}} \|\ell_n\|_{\mathcal{L}(\mathcal{C}_{2\pi},\mathbb{C})} = +\infty$, donc on est dans le deuxième cas, il existe $f \in \mathcal{C}_{2\pi}$ telle que $\sup_{n\in\mathbb{N}} |\ell_n(f)| = \infty$, i.e. il existe $f \in \mathbb{C}_{2\pi}$ telle que $|S_n(f)(0)|$ diverge.

□

2. Utiliser l'équivalent en 0 de sinus : $\dfrac{\sin\left((2n+1)\frac{t}{2}\right)}{\sin\left(\frac{t}{2}\right)} \underset{x\to 0}{\sim} \dfrac{(2n+1)\frac{t}{2}}{\frac{t}{2}} \underset{x\to 0}{\sim} 2n+1$

3. on a la majoration $\left|\dfrac{|D_n(t)|^2}{|D_n(t)|+\varepsilon}\right| \leqslant |D_n(t)|$ qui est intégrable sur $[-\pi,\pi]$ comme vu précédemment

4. $\displaystyle\int_0^{n\pi} \frac{|\sin u|}{u} \geqslant \sum_{k=1}^{n}\int_{(k-1)\pi}^{k\pi} \frac{|\sin u|}{k\pi}du = \frac{2}{\pi}\sum_{k=1}^{n}\frac{1}{k} \xrightarrow[n\to\infty]{} +\infty$

Remarques :

Ce n'est pas évident de trouver dans la pratique un tel f. La série de Fourier de la fonction suivante f diverge (exemple du Gourdon Analyse)

$$\forall x \in [-\pi, \pi] \quad f(x) = \sum_{p=1}^{+\infty} \frac{1}{p^2} \sin\left((2^{p^3}+1)\frac{|x|}{2}\right)$$

Astuces de l'agrégatif :

On n'est pas obligé de découper les étapes de l'application, car cela prend du temps mais cela structure la preuve au moins dans la tête. Pendant le développement, je ne fais pas la divergence de $\|D_n\|_1$, faute de temps. Je dis juste à l'oral que c'est dû à la non intégrabilité du sinus cardinal.

Voici une autre application du théorème de Banach–Steinhaus :

Application 2. Soit E un Banach, F un espace vectoriel normé et une suite $(T_n)_{n\in\mathbb{N}}$ d'applications linéaires continues de E et F qui converge simplement vers une application T. Alors $\sup\{\|T_n\|_{\mathcal{L}(E,F)}, n \in \mathbb{N}\} < \infty$ et T est linéaire continue.

Méthode de Newton

Leçons : 219 ; 223 ; 226 ; 228 ; 229

Références : ROUVIÈRE, *Petit Guide de Calcul Différentiel* (p.152) [ROU09]

Prérequis :

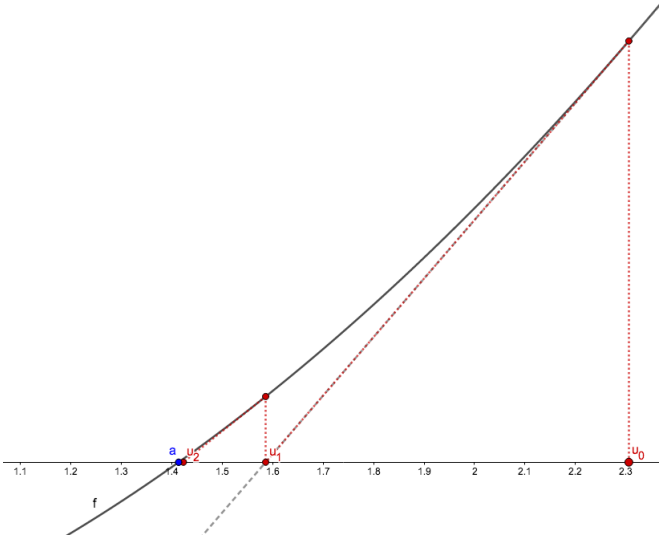
- la formule de Taylor–Lagrange
- une fonction f est convexe si et seulement si $f'' \geqslant 0$

Introduction :

Lorsque l'on étudie une fonction f, il est naturel de se demander quand est ce que cette fonction s'annule. Parfois, trouver les zéros explicites d'une fonction est extrêmement difficile voire impossible, on peut alors vouloir approcher des zéros de f. La méthode de Newton est pour cela un bon outil pour avoir une convergence relativement rapide vers un zéro de notre fonction, il faut évidemment se placer dans un bon cadre d'hypothèses pour assurer cette convergence. Dans ce développement, nous nous placerons dans deux cadres différents, un premier qui nécessite d'être assez proche du zéro à approcher et un deuxième qui nous permet de nous affranchir de cette contrainte mais en imposant des hypothèses plus fortes sur la fonction à étudier.

Théorème 1 (Méthode de Newton)**.** Soit $f \in \mathcal{C}^2(I, \mathbb{R})$, on suppose qu'il existe $a \in \overset{\circ}{I}$ tel que $f(a) = 0$ et $f'(a) \neq 0$.
Alors il existe $\alpha > 0$ tel que pour tout $u_0 \in]a - \alpha, a + \alpha[$, la suite définie par $u_{n+1} = g(u_n) = u_n - \dfrac{f(u_n)}{f'(u_n)}$ converge vers a de manière quadratique.

Commençons par illustrer le théorème :



Approximation de $\sqrt{2}$ par la méthode de Newton sur $f(x) = x^2 - 2$ avec $u_0 = 2.3$.

Démonstration. Quitte à multiplier f par -1, on peut supposer que $f'(a) > 0$.

Ainsi comme f' est continue, il existe un $\alpha > 0$ tel que f' soit strictement positive sur $J :=]a-\alpha; a+\alpha[\subset I$.

Soit $x \in J$, $|g(x) - a| = \left| x - \dfrac{f(x)}{f'(x)} - a \right| = \left| \dfrac{f(a) - f(x) - (a-x)f'(x)}{f'(x)} \right|$ car $f(a) = 0$.

On utilise Taylor–Lagrange pour avoir un élément $e \in]a, x[$ tel que

$$f(a) - f(x) - (a-x)f'(x) = \frac{1}{2} f''(e)(a-x)^2.$$

Ainsi on a $|g(x) - a| = \dfrac{|f''(e)|(a-x)^2}{2f'(x)} \leqslant C(x-a)^2$ où on définit C par $C := \dfrac{\sup_J |f''|}{2\inf_J |f'|}$, elle est bien définie car f' et f'' sont continues sur J et sur $\bar{J}$, $f' > 0$.

Quitte à réduire α, on peut supposer que $\alpha < \frac{1}{C}$.

Ainsi pour $x \in J$, $|g(x) - a| \leqslant C\alpha^2 < C\,\frac{1}{C}\alpha \leqslant \alpha$.

Donc pour $u_0 \in J$, la suite récurrente (u_n) est bien définie. Il faut prouver que (u_n) converge vers a de façon quadratique : pour tout $n \in \mathbb{N}$,

$$C|u_{n+1} - a| \leqslant C^2 |u_n - a|^2 \leqslant C^4 |u_{n-1} - a|^4 \leqslant \cdots \leqslant (C|u_0 - a|)^{(2^n)} \leqslant (C\alpha)^{(2^n)}.$$

Or $C\alpha < 1$ donc (u_n) converge vers a car $(C\alpha)^{2^n}$ tend vers 0 quand n tend vers $+\infty$ et de manière quadratique car $|u_{n+1} - a| \leqslant C|u_n - a|^2$ pour tout $n \in \mathbb{N}^*$. □

Théorème 2. Sous les hypothèses du théorème précédent, si on suppose, de plus, que f est convexe sur I et que $f'(a) > 0$, alors le résultat précédent est vrai pour tout $u_0 \in I \cap [a, +\infty[$.

Démonstration. Comme f est convexe, f' est croissante, donc puisque $f'(a) > 0$, on a f' positive à droite de a qui implique que f est positive à droite de a.

Soit d la borne supérieure de l'intervalle I. On veut prouver que :

$$a \leqslant g(x) \leqslant x \leqslant d \text{ pour tout } x \in [a, d].$$

Soit $x \in [a, d]$, on a

$$x - g(x) = x - x + \frac{f(x)}{f'(x)} = \frac{f(x)}{f'(x)} \geqslant 0$$

car f et f' sont positives à droite de a. D'où $g(x) \leqslant x$.

Soit $x \in [a, d]$,on a

$$g(x) - a = x - a - \frac{f(x)}{f'(x)} = \frac{f''(e)}{2f'(x)}(x-a)^2 \geqslant 0$$

par Taylor–Lagrange sur l'intervalle $]a, x[$ et par convexité de f, on a f'' positive (et f' positive à droite de a). Donc $a \leqslant g(x)$.

Ainsi la suite (u_n), définie par récurrence pour $u_0 \in [a, d]$, est décroissante et minorée par a, donc converge vers un point fixe de g. Or les points fixes de g sont les zéros de f et le seul zéro de f sur $[a, d]$ est a. Donc (u_n) converge vers a.

Pour le caractère quadratique, on utilise la même preuve que dans le théorème précédent, car comme (u_n) converge vers a, il existe un rang n_0 tel que pour tout $n \geqslant n_0$, $|u_n - a| < \alpha$ (α définie dans la preuve précédente). □

Remarques :

— La méthode de Newton marche en dimension supérieure, on pose alors $g(x) = x - Df(x)^{-1} \circ f(x)$.

— Il existe d'autres méthode pour trouver des zéros d'une fonction, comme la méthode de la sécante (mais qui ne marche pas en dimension supérieure) et la méthode de la dichotomie.

— On pose cette fonction g car c'est le point d'abscisse par lequel passe la tangente à la courbe de la fonction f au point x. En effet, la tangente au point x_0 a pour équation $y = f'(x_0)(x - x_0) + f(x_0)$.

Astuces de l'agrégatif :

Le théorème de Newton possède de nombreux énoncés. Pour éviter de faire des hypothèses sur a, on pourrait juste dire que la fonction f' est strictement positive sur un intervalle $[c, d]$ avec $f(c) < 0$ et $f(d) > 0$. Ainsi par le théorème des valeurs intermédiaires, il y a existence de a tel que $f(a) = 0$ et unicité par le caractère strictement croissant de f sur $[c, d]$.

Le fait de faire des hypothèses sur a n'est pas non plus aberrant. Par exemple, si on veut approcher un nombre algébrique avec la méthode de Newton (car elle converge vite), on connait les propriétés des zéros, donc on peut vérifier les hypothèses sur a et appliquer le théorème ci-dessous pour trouver les décimales de notre zéro.

Dans le livre de Dieudonné, *Calcul Infinitésimal*, il a un énoncé plus général de la méthode de Newton.

Questions possibles :

- Donner un équivalent de $x_{n+1} - a$.

  Réponse : $x_{n+1} - a \underset{n\to+\infty}{\sim} \dfrac{f''(a)}{2f'(a)}(x_n - a)^2$

- Donner un cas où la méthode de Newton ne converge pas.

Réciproques partielles du théorème de Césaro

Leçons : 223 ; 230

Références : FRANCINOU–GIANELLA–NICOLAS, *Oraux X-ENS Analyse 1* (p.68)

Prérequis :

- le théorème de Césaro
- la comparaison série/intégrale

Astuces de l'agrégatif :
J'ai fait deux versions de ce développement que je mets à la suite, une première qui est orientée "suites" et une deuxième orientée "séries".

Introduction :
Le théorème de Césaro est un théorème nous donnant la convergence de la suite des moyennes pour une suite convergente. La réciproque est fausse : si la suite des moyennes converge, la suite initiale ne converge pas forcément (par exemple, $u_n = (-1)^n$ est un terme de suite qui ne converge pas alors que la suite des moyennes converge vers 0). Ainsi on voudrait renforcer les hypothèses que l'on fait sur la suite u_n pour avoir une réciproque au théorème de Césaro.

Théorème 1 (Réciproque partielle de Césaro)**.** Soit $(u_n)_{n\in\mathbb{N}^*}$ une suite dans $\mathbb{K}$ telle que la suite $\left(\sigma_n = \frac{1}{n}\sum_{k=1}^{n} u_k\right)_{n\in\mathbb{N}^*}$ converge vers $\ell \in \mathbb{K}$.

(i) Si (u_n) est réelle monotone, alors (u_n) converge vers ℓ.

(ii) Si $u_n - u_{n-1} = O\left(\frac{1}{n}\right)$ (*i.e.* il existe $C \geqslant 0$ telle que $|u_n - u_{n-1}| \leqslant \frac{C}{n}$ pour tout $n \in \mathbb{N}^*$ [1]), alors (u_n) converge vers ℓ.

Démonstration.
(i) Pour (u_n) réelle monotone, on veut prouver l'équivalence :

$$(u_n) \text{ converge vers } \ell \iff (\sigma_n) \text{ converge vers } \ell$$

$\boxed{\Longrightarrow}$ Cela vient du théorème de Césaro.
$\boxed{\Longleftarrow}$ Réciproquement, on raisonne par contraposée. Si (u_n) ne converge pas, alors (u_n) tend vers l'infini car (u_n) est supposée monotone. Quitte à prendre $(-u_n)$, on considère que (u_n) est croissante vers $+\infty$.

On va prouver que le théorème de Césaro peut être appliqué pour une limite infinie.
Pour tout $A \geqslant 0$, il existe un rang n_0 telle que pour tout $n \geqslant n_0$, $u_n \geqslant A$. On pose la suite (v_n) définie par $v_n = \min(u_n, A)$. On a l'inégalité $v_n \leqslant u_n$ pour tout $n \in \mathbb{N}^*$. De ce fait, on a aussi

$$\frac{1}{n}\sum_{k=1}^{n} v_k \leqslant \frac{1}{n}\sum_{k=1}^{n} u_k$$

1. Dans la définition classique, c'est qu'il existe une constante à partir d'un certain rang n_0, donc quitte à augmenter cette constante, on peut avoir l'inégalité pour les n_0 termes et donc on a une constante pour tout $n \in \mathbb{N}$

pour tout $n \in \mathbb{N}^*$.

Or la suite (v_n) converge vers A, donc $\left(\frac{1}{n}\sum_{k=1}^{n} v_k\right)$ converge aussi vers A (par le théorème de Césaro).

Donc on a

$$A = \liminf \left(\frac{1}{n}\sum_{k=1}^{n} v_k\right) \leqslant \liminf \left(\frac{1}{n}\sum_{k=1}^{n} u_k\right) = \liminf \sigma_n$$

Ainsi la suite (σ_n) diverge aussi vers $+\infty$.

Donc (u_n) et (σ_n) convergent. Par le théorème de Césaro, (u_n) et (σ_n) possèdent la même limite.

(ii) On suppose que (σ_n) converge vers une limite ℓ. L'idée va être de prouver que la moyenne des termes entre n et nx avec $x > 1$ converge aussi vers ℓ et ensuite de rapprocher x de 1 pour n'avoir que le terme u_n dans la moyenne, ce qui prouvera que la suite (u_n) converge aussi vers ℓ.

On pose, pour tout $t \geqslant 1$,

$$\sigma_t := \frac{1}{t}\sum_{1\leqslant k\leqslant t} u_k = \frac{E(t)}{t}\sigma_{E(t)}$$

où $E(t)$ est la partie entière de t. De plus, $\sigma_{E(t)}$ tend vers ℓ quand t tend vers $+\infty$, et $\frac{E(t)}{t}$ tend vers 1 quand t tend vers $+\infty$. Donc σ_t tend vers ℓ quand t tend vers $+\infty$.

Pour $x > 1$, on pose

$$M_n(x) = \frac{1}{E(nx-n)}\sum_{n<k\leqslant nx} u_k = \frac{nx\sigma_{nx} - n\sigma_n}{E(n(x-1))} = \frac{n(x-1)}{E(n(x-1))}\frac{(x\sigma_{nx} - \sigma_n)}{(x-1)}.$$

Or $\frac{n(x-1)}{E(n(x-1))}$ tend vers 1 quand n tend vers $+\infty$ et σ_{nx} et σ_n tendent vers ℓ quand n tend vers $+\infty$ par ce qui précède. Donc $M_n(x)$ tend vers $\frac{x\ell - \ell}{x-1} = \ell$ quand n tend vers $+\infty$.

On veut maintenant comparer le terme u_n avec $M_n(x)$.
Or on peut écrire

$$u_n = \frac{1}{E(nx-n)}\sum_{n<k\leqslant nx} u_n.$$

Ainsi pour tout $n \in \mathbb{N}^*$,

$$|M_n(x) - u_n| = \left|\frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}(u_k - u_n)\right| \leqslant \frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}|u_k - u_n|$$

On va vouloir majorer $u_k - u_n$, on va utiliser l'hypothèse qui nous donne un $C \geqslant 0$ tel que pour tout $j \in \mathbb{N}^*$ on ait $|u_j - u_{j-1}| \leqslant \frac{C}{j}$.
Pour tout $k > n$, on a

$$\begin{aligned}|u_k - u_n| = \left|\sum_{j=n+1}^{k}(u_j - u_{j-1})\right| &\leqslant \sum_{j=n+1}^{k}|u_j - u_{j-1}| \leqslant \sum_{j=n+1}^{k}\frac{C}{j} \\ &\leqslant \sum_{j=n+1}^{k}\int_{j-1}^{j}\frac{C}{t}dt \leqslant C\int_{n}^{k}\frac{1}{t}dt = C\ln\left(\frac{k}{n}\right)\end{aligned}$$

(par comparaison avec l'intégrale de $\frac{1}{t}$).

On reprend la majoration précédente,

$$\begin{aligned}
|M_n(x) - u_n| &\leqslant \frac{1}{E(n(x-1))} \sum_{n<k\leqslant nx} |u_k - u_n| \\
&\leqslant \frac{1}{E(n(x-1))} \sum_{n<k\leqslant nx} C \ln\left(\frac{k}{n}\right) \\
&\leqslant \frac{1}{E(n(x-1))} \sum_{n<k\leqslant nx} C \ln\left(\frac{nx}{n}\right) \\
&\leqslant \frac{1}{E(n(x-1))} \sum_{n<k\leqslant nx} C \ln(x) \\
&\leqslant C \ln(x).
\end{aligned}$$

On obtient une majoration indépendante de n.

Soit $\varepsilon > 0$, on choisit $x_0 > 1$ tel que $C\ln(x_0) < \varepsilon$. De plus, on a montré que $M_n(x)$ converge vers ℓ pour tout $x > 1$, donc il existe un rang $n_0 \in \mathbb{N}^*$ tel que pour tout $n \geqslant n_0$, on ait

$$|M_n(x_0) - \ell| < \varepsilon.$$

Ainsi pour tout $n \geqslant n_0$,

$$|u_n - l| \leqslant |u_n - M_n(x_0)| + |M_n(x_0) - \ell| \leqslant C\ln(x_0) + \varepsilon < 2\varepsilon.$$

Donc la suite (u_n) converge vers ℓ. □

Astuces de l'agrégatif :

Pour le (i), je ne fais pas les deux implications, j'explique juste l'implication qui nous intéresse.

Pour la leçon 230, je fais apparaître des séries pour étudier une vraie somme (c'est la version qui colle le plus à la référence d'ailleurs)

Introduction :

Le théorème de Césaro est un théorème nous donnant la convergence de la suite des moyennes pour une suite convergente. La réciproque est fausse : si la suite des moyennes converge, la suite initiale ne converge pas forcément (par exemple, $u_n = (-1)^n$ est un terme de suite qui ne converge pas alors que la suite des moyennes converge vers 0). Ainsi on voudrait renforcer les hypothèses que l'on fait sur la suite u_n pour avoir une réciproque au théorème de Césaro.

Théorème 1 (Réciproque partielle de Césaro)**.** Soit $(u_n)_{n\in\mathbb{N}^*}$ une suite dans $\mathbb{K}$. Pour tout $n \in \mathbb{N}^*$, on pose $S_n = \sum_{i=1}^{n} u_i$ et $\sigma_n = \frac{1}{n}\sum_{k=1}^{n} S_k$.

(i) Si (u_n) est réelle et positive, alors

$$(S_n) \text{ converge vers } \ell \iff (\sigma_n) \text{ converge vers } \ell.$$

(ii) Si $u_n = O\left(\frac{1}{n}\right)$ (*i.e.* il existe $C \geqslant 0$ telle que $|u_n| \leqslant \frac{C}{n}$ pour tout $n \in \mathbb{N}^*$ [1]), alors

$$(S_n) \text{ converge vers } \ell \iff (\sigma_n) \text{ converge vers } \ell.$$

Démonstration.

(i) Pour (u_n) réelle positive, on veut prouver l'équivalence :

$$(S_n) \text{ converge vers } \ell \quad \Longleftrightarrow \quad (\sigma_n) \text{ converge vers } \ell$$

$\boxed{\Longrightarrow}$ Cela vient du théorème de Césaro.

$\boxed{\Longleftarrow}$ On raisonne par contraposée. Comme (u_n) est positive, alors (S_n) est croissante. Ainsi si (S_n) ne converge pas, alors (S_n) tend vers l'infini. On suppose que donc que (S_n) diverge vers $+\infty$.

On va prouver que le théorème de Césaro peut être appliqué pour une limite infinie.
Pour tout $A \geqslant 0$, il existe un rang n_0 telle que pour tout $n \geqslant n_0$, $S_n \geqslant A$. On pose la suite (T_n) définie par $T_n = \min(S_n, A)$. On a l'inégalité $T_n \leqslant S_n$ pour tout $n \in \mathbb{N}^*$. De ce fait, on a aussi

$$\frac{1}{n}\sum_{k=1}^{n} T_k \leqslant \frac{1}{n}\sum_{k=1}^{n} S_k$$

pour tout $n \in \mathbb{N}^*$.

Or la suite (T_n) converge vers A, donc $\left(\frac{1}{n}\sum_{k=1}^{n} T_k\right)$ converge aussi vers A (par le théorème de Césaro).

Donc on a

$$A = \liminf\left(\frac{1}{n}\sum_{k=1}^{n} T_k\right) \leqslant \liminf\left(\frac{1}{n}\sum_{k=1}^{n} S_k\right) = \liminf \sigma_n$$

Ainsi la suite (σ_n) diverge aussi vers $+\infty$.

Donc (S_n) et (σ_n) convergent. Par le théorème de Césaro, (S_n) et (σ_n) possèdent la même limite.

(ii) On va montrer l'équivalence voulue

$$(S_n) \text{ converge vers } \ell \quad \Longleftrightarrow \quad (\sigma_n) \text{ converge vers } \ell$$

$\boxed{\Longrightarrow}$ Cela vient du théorème de Césaro.

$\boxed{\Longleftarrow}$ Réciproquement, on suppose que (σ_n) converge vers une limite ℓ. L'idée va être de prouver que la moyenne des termes S_k entre n et nx avec $x > 1$ converge aussi vers ℓ et ensuite de rapprocher x de 1 pour n'avoir que le terme S_n dans la moyenne, ce qui va nous prouver que la suite (S_n) converge aussi vers ℓ.

On pose, pour tout $t \geqslant 1$,

$$\sigma_t =: \frac{1}{t}\sum_{1\leqslant k\leqslant t} S_k = \frac{E(t)}{t}\sigma_{E(t)}$$

où $E(t)$ est la partie entière de t. De plus, $\sigma_{E(t)}$ tend vers ℓ quand t tend vers $+\infty$, et $\frac{E(t)}{t}$ tend vers 1 quand t tend vers $+\infty$. Donc σ_t tend vers ℓ quand t tend vers $+\infty$.

Pour $x > 1$, on pose

$$M_n(x) = \frac{1}{E(nx-n)}\sum_{n<k\leqslant nx} u_k = \frac{nx\sigma_{nx} - n\sigma_n}{E(n(x-1))} = \frac{n(x-1)}{E(n(x-1))}\frac{(x\sigma_{nx} - \sigma_n)}{(x-1)}.$$

1. Dans la définition classique, c'est qu'il existe une constante à partir d'un certain rang n_0, donc quitte à augmenter cette constante, on peut avoir l'inégalité pour les n_0 termes et donc on a une constante pour tout $n \in \mathbb{N}$

Or $\dfrac{n(x-1)}{E(n(x-1))}$ tend vers 1 quand n tend vers $+\infty$ et σ_{nx} et σ_n tendent vers l quand n tend vers $+\infty$ par ce qui précède. Donc $M_n(x)$ tend vers $\dfrac{x\ell-\ell}{x-1}=\ell$ quand n tend vers $+\infty$.

On veut maintenant comparer le terme S_n avec $M_n(x)$.
Or on peut écrire

$$S_n=\frac{1}{E(nx-n)}\sum_{n<k\leqslant nx}S_n.$$

Ainsi pour tout $n\in\mathbb{N}^*$,

$$|M_n(x)-S_n|=|\frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}(S_k-S_n)|\leqslant\frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}|S_k-S_n|$$

On va vouloir majorer S_k-S_n, on va utiliser l'hypothèse qui nous donne un $C\geqslant 0$ tel que pour tout $j\in\mathbb{N}^*$ on ait $|u_j|\leqslant\frac{C}{j}$.
Pour tout $k>n$, on a

$$\begin{aligned}|S_k-S_n|=\left|\sum_{j=n+1}^{k}u_j\right|&\leqslant\sum_{j=n+1}^{k}|u_j|\leqslant\sum_{j=n+1}^{k}\frac{C}{j}\\&\leqslant\sum_{j=n+1}^{k}\int_{j-1}^{j}\frac{C}{t}dt\leqslant C\int_n^k\frac{1}{t}dt=C\ln\left(\frac{k}{n}\right)\end{aligned}$$

(par comparaison avec l'intégrale de $\frac{1}{t}$).

On reprend la majoration précédente,

$$\begin{aligned}|M_n(x)-S_n|&\leqslant\frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}|S_k-S_n|\\&\leqslant\frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}C\ln\left(\frac{k}{n}\right)\\&\leqslant\frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}C\ln\left(\frac{nx}{n}\right)\\&\leqslant\frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}C\ln(x)\\&\leqslant C\ln(x).\end{aligned}$$

On obtient une majoration indépendante de n.

Soit $\varepsilon>0$, on choisit $x_0>1$ tel que $C\ln(x_0)<\varepsilon$. De plus, on a montré que $M_n(x)$ converge vers ℓ pour tout $x>1$, donc il existe un rang $n_0\in\mathbb{N}^*$ tel que pour tout $n\geqslant n_0$, on ait

$$|M_n(x_0)-\ell|<\varepsilon.$$

Ainsi pour tout $n\geqslant n_0$,

$$|S_n-l|\leqslant|S_n-M_n(x_0)|+|M_n(x_0)-\ell|\leqslant C\ln(x_0)+\varepsilon<2\varepsilon.$$

Donc la suite (S_n) converge vers ℓ. □

Astuces de l'agrégatif :
Pour le (i), je ne fais pas les deux implications, j'explique juste l'implication qui nous intéresse.

Formule des compléments

(rédigé par Emilie Tezenas)

Leçons : 236 ; 239 ; 265

Références : BERNIS–BERNIS, *Analyse pour l'agrégation de mathématiques, 40 développements* (p.74)

Prérequis :

- Théorème des Résidus
- Convergence dominée
- Fubini-Tonelli
- Changement de variable sur $\mathbb{R}^d$
- le prolongement analytique
- les déterminations du logarithme complexe

Introduction :

La formule des compléments est une équation fonctionnelle qui permet de faire le lien entre la fonction Γ et le sinus complexe. On montre l'égalité sur un intervalle ouvert de $\mathbb{R}$, et l'on peut ensuite prolonger le résultat à la bande ouverte de $\mathbb{C}$ correspondante en utilisant l'holomorphie des fonctions en jeu sur cet ensemble et leur égalité sur un domaine contenant un point d'accumulation.

Théorème 1. Pour tout $z \in \mathbb{C}$ tel que $\Re(z) \in]0;1[$,

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

Démonstration. **Étape 1 :** *Calcul sous forme d'intégrale de $\Gamma(x)\Gamma(1-x)$ pour $x \in]0,1[$*
Soit donc $x \in]0;1[$. On a :

$$\Gamma(x)\Gamma(1-x) = \int_0^\infty t^{x-1}e^{-t}\mathrm{d}t \int_0^\infty s^{-x}e^{-s}\mathrm{d}s$$

Les intégrandes étant toutes positives, on applique Fubini-Tonelli pour poursuivre le calcul en interversant les intégrales.

$$\Gamma(x)\Gamma(1-x) = \int_0^\infty \int_0^\infty \left(\frac{t}{s}\right)^x \frac{1}{t} e^{-(t+s)}\mathrm{d}s\mathrm{d}t$$

On réalise maintenant le changement de variable suivant :

$$\varphi : \left\{ \begin{array}{ccc} \left(\mathbb{R}_+^*\right)^2 & \to & \left(\mathbb{R}_+^*\right)^2 \\ (s,t) & \mapsto & \left(s+t, \frac{t}{s}\right) \end{array} \right.$$

φ est bien un $\mathcal{C}^1$-difféomorphisme. On calcule le Jacobien de son inverse, en notant $u = s + t$ et $v = \frac{t}{s}$:

$$|J_\varphi| = \begin{vmatrix} 1 & 1 \\ -\frac{t}{s^2} & \frac{1}{s} \end{vmatrix} = \frac{s+t}{s^2}$$

D'où

$$|J_{\varphi^{-1}}| = \frac{s^2}{s+t} = \frac{u}{(1+v)^2}$$

.

D'autre part, on a $\frac{1}{t} = \frac{1+v}{uv}$. Revenons maintenant au calcul, où on effectue le changement de variable, puis on utilise encore Fubini-Tonelli plusieurs fois :

$$\begin{aligned}
\Gamma(x)\Gamma(1-x) &= \int_0^\infty \int_0^\infty v^x e^{-u} \frac{1+v}{uv} \frac{u}{(1+v)^2} \mathrm{d}u\mathrm{d}v \\
&\overset{F.T}{=} \int_0^\infty \frac{v^{x-1}}{1+v} \left(\int_0^\infty e^{-u} \mathrm{d}u \right) \mathrm{d}v \\
&= \int_0^\infty \frac{v^{x-1}}{1+v} \mathrm{d}v \\
&= \int_0^\infty \frac{\mathrm{d}v}{v^{1-x}(1+v)}
\end{aligned}$$

On utilise l'invariance de $\Gamma(x)\Gamma(1-x)$ par changement de variable $x \mapsto 1-x$, pour finalement obtenir

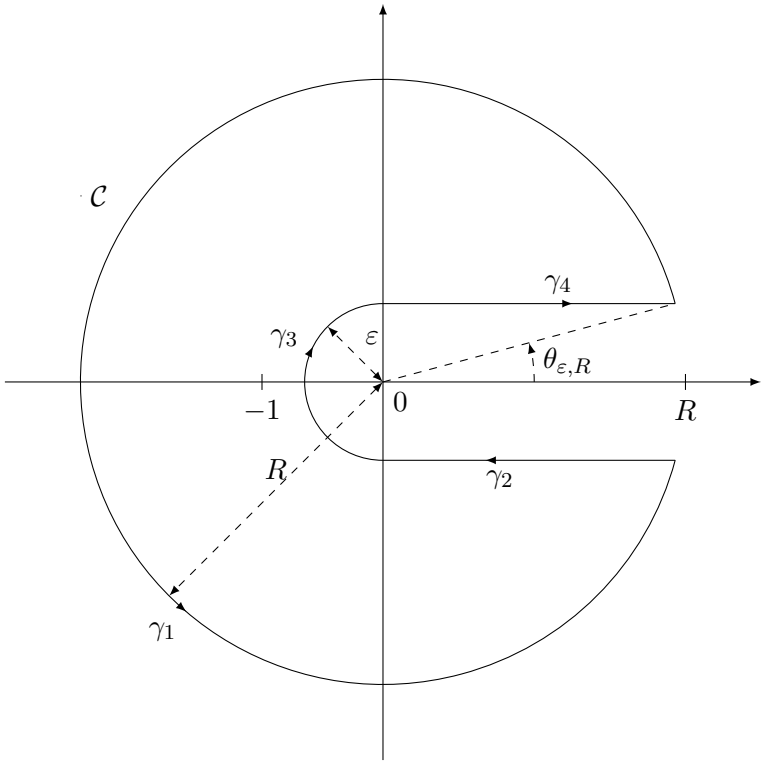
$$\Gamma(x)\Gamma(1-x) = \int_0^\infty \frac{\mathrm{d}v}{v^x(1+v)}$$

Γ est bien définie pour $\{\Re > 0\}$, donc comme $x \in [0,1]$, $\Gamma(x)\Gamma(1-x) < \infty$. La fonction $x \mapsto \frac{1}{t^x(1+t)}$ est donc intégrable sur $[0; +\infty]$.

On a donc obtenu une expression de $\Gamma(x)\Gamma(1-x)$ sous forme intégrale.

Étape 2 : *Calcul de* $\displaystyle\int_0^{+\infty} \frac{dv}{v^x(1+v)}$ *à l'aide du théorème des résidus.*

On va utiliser le Théorème des Résidus appliqué à la fonction $f : \begin{cases} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \frac{1}{z^x(1+z)} \end{cases}$ sur le contour suivant :



f est méromorphe sur $\mathbb{C} \setminus \mathbb{R}^+$ et possède un pôle simple en -1. On intègre f sur le contour $\mathcal{C}$ présenté sur la figure ci-dessus. On décompose ce contour en quatre parties, les deux segments et les deux arcs de cercle, que l'on paramètrera séparément. On fait ensuite tendre ε vers 0 et R vers $+\infty$.
Munis de ce contour, on peut maintenant choisir une détermination du logarithme complexe qui nous permet de bien définir le z^x dans l'expression de f. On choisit la détermination de droite $\mathbb{R}^+$, i.e. pour $z \in \mathbb{C}, \quad z^x = e^{x(\ln(|z|)+\theta)}$, avec $\theta \in]0; 2\pi[$. Il faudra dans la suite du calcul faire attention à l'argument des complexes lorsque ε tend vers 0 : sur le segment γ_2, l'argument de $z^x = e^{x\log(z)}$ tend vers 2π, alors qu'il tend vers 0 sur le segment γ_4.

Théorème des Résidus
Le théorème des Résidus appliqué à f donne

$$\int_{\mathcal{C}} f(z)\mathrm{d}z = 2i\pi \mathrm{Res}_{-1}(f) = 2i\pi(-1)^{-x} = 2i\pi e^{-i\pi x}$$

Il est important de remarquer que le fait que $(-1)^{-x} = e^{-i\pi x}$ provient de la détermination du logarithme choisie.

Intégrale sur γ_1
On utilise la paramétrisation suivante :

$$\gamma_1 : \left\{ \begin{array}{ccc} [\theta_{\varepsilon,R}; 2\pi - \theta_{\varepsilon,R}] & \longrightarrow & \mathbb{C} \\ t & \longmapsto & Re^{it} \end{array} \right.$$

Où $\theta_{\varepsilon,R} = \arctan\frac{\varepsilon}{\sqrt{\varepsilon^2+R^2}} \underset{\varepsilon\to 0}{\longrightarrow} 0$

L'intégrale de f sur cet arc de cercle devient alors :

$$\int_{\gamma_1} f(z)\mathrm{d}z = \int_{\theta_{\varepsilon,R}}^{2\pi-\theta_{\varepsilon,R}} \frac{iRe^{it}}{(Re^{it})^x(1+Re^{it})}\mathrm{d}t$$

$$\xrightarrow[\varepsilon\to 0]{} \int_0^{2\pi} \frac{iRe^{it}}{(Re^{it})^x(1+Re^{it})}\mathrm{d}t$$

où la limite en $\varepsilon \to 0$ est obtenue par un rapide Théorème de Convergence Dominée applicable grâce à l'intégrabilité sur le segment $[0;2\pi]$ de l'intégrande.
On cherche maintenant à passer à la limite en $R \to +\infty$. On remarque que pour $t \in [0;2\pi]$, on a :

$$\left|\frac{iRe^{it}}{(Re^{it})^x(1+Re^{it})}\right| \leq \frac{R}{R^x(R-1)} \underset{R\to+\infty}{\sim} R^{-x} \xrightarrow[R\to+\infty]{} 0 \quad \text{car } x>0$$

Une majoration par inégalité triangulaire donne alors :

$$\int_{\gamma_1} f(z)\mathrm{d}z \xrightarrow[R\to+\infty]{\varepsilon\to 0} 0$$

Intégrale sur γ_3 On utilise le même genre de paramétrisation :

$$\gamma_3 : \left\{ \begin{array}{ccc} [\frac{\pi}{2};\frac{3\pi}{2}] & \longrightarrow & \mathbb{C} \\ t & \longmapsto & \varepsilon e^{i(2\pi-t)} \end{array} \right.$$

L'intégrale de f sur cet arc de cercle devient alors :

$$\int_{\gamma_3} f(z)\mathrm{d}z = \int_{\frac{\pi}{2}}^{\frac{3\pi}{2}} \frac{-i\varepsilon e^{-it}}{(\varepsilon e^{-it})^x(1+\varepsilon e^{-it})}\mathrm{d}t$$

Ici encore une majoration par inégalité triangulaire suffit à conclure sur la limite de cette intégrale quand $\varepsilon \to 0$. En effet,

$$\left|\frac{-i\varepsilon e^{-it}}{(\varepsilon e^{-it})^x(1+\varepsilon e^{-it})}\right| \leq \frac{\varepsilon}{\varepsilon^x(1-\varepsilon)} \underset{\varepsilon\to 0}{\sim} \varepsilon^{1-x} \xrightarrow[\varepsilon\to 0]{} 0 \quad \text{car } 1-x>0$$

Intégrale sur γ_2 :
On paramétrise le segment comme suit :

$$\gamma_2 : \left\{ \begin{array}{ccc} [-\sqrt{R^2-\varepsilon^2};0] & \longrightarrow & \mathbb{C} \\ t & \longmapsto & -i\varepsilon - t \end{array} \right.$$

L'intégrale de f sur ce segment devient alors :

$$\begin{aligned} \int_{\gamma_2} f(z)\mathrm{d}z &= \int_{-\sqrt{R^2-\varepsilon^2}}^{0} \frac{-\mathrm{d}t}{(-i\varepsilon-t)^x(1-t-i\varepsilon)} \\ &= -\int_0^{\sqrt{R^2-\varepsilon^2}} \frac{\mathrm{d}t}{(-i\varepsilon+t)^x(1+t-i\varepsilon)} \\ &= -\int_0^{+\infty} \mathbb{1}_{[0;\sqrt{R^2-\varepsilon^2}]}(t) \frac{\mathrm{d}t}{(-i\varepsilon+t)^x(1+t-i\varepsilon)} \end{aligned}$$

Où la deuxième égalité est obtenue en effectuant le changement de variable $t \mapsto -t$.
On applique le Théorème de Convergence Dominée pour calculer la limite en $\varepsilon \to 0$.

— Pour tout $t \in \mathbb{R}_+$, $\mathbb{1}_{[0;\sqrt{R^2-\varepsilon^2}]}(t)\frac{-1}{(-i\varepsilon+t)^x(1+t-i\varepsilon)} \xrightarrow[\varepsilon\to 0]{} \mathbb{1}_{[0;R]}\frac{-1}{(te^{2i\pi})^x(1+t)}$ en tenant compte de la détermination du logarithme choisie, l'argument de $-i\varepsilon+t$ tend vers 2π.

— Pour $t \in \mathbb{R}_+$, $\left|\mathbb{1}_{[0;\sqrt{R^2-\varepsilon^2}]}(t)\frac{1}{(-i\varepsilon+t)^x(1+t-i\varepsilon)}\right| \leq \frac{1}{t^x(1+t)}$. En effet, pour $t \in \mathbb{R}_+$,

$$|t - i\varepsilon| = \sqrt{t^2+\varepsilon^2} \geq \sqrt{t^2} = t$$

et de même, $|1+t-i\varepsilon| = \sqrt{(1+t)^2+\varepsilon^2} \geq 1+t$.
De plus, on a vu à la fin de la première étape que $\frac{1}{t^x(1+t)}$ est intégrable (le fait que $x \in [0,1]$ est crucial). On a donc dominé l'intégrande par une fonction intégrable sur $[0;+\infty]$.

Le Théorème de Convergence Dominée donne alors

$$\int_{\gamma_2} f(z)\mathrm{d}z \underset{\varepsilon\to 0}{\longrightarrow} -\int_0^{+\infty} \mathbb{1}_{[0;R]}(t)\frac{\mathrm{d}t}{t^x e^{2i\pi x}(1+t)}$$

Un deuxième TCD, avec la même domination donne également, pour la limite en $R \to +\infty$

$$\int_{\gamma_2} f(z)\mathrm{d}z \underset{\substack{\varepsilon\to 0\\ R\to+\infty}}{\longrightarrow} -\int_0^{+\infty} \frac{\mathrm{d}t}{t^x e^{2i\pi x}(1+t)}$$

Intégrale sur γ_4 :

On paramétrise le segment de manière similaire à γ_2 :

$$\gamma_4 : \left\{ \begin{array}{ccc} [0;\sqrt{R^2-\varepsilon^2}] & \longrightarrow & \mathbb{C} \\ t & \longmapsto & i\varepsilon + t \end{array} \right.$$

L'intégrale de f sur ce segment devient alors :

$$\begin{aligned}\int_{\gamma_4} f(z)\mathrm{d}z &= \int_0^{\sqrt{R^2-\varepsilon^2}} \frac{\mathrm{d}t}{(i\varepsilon+t)^x(1+t+i\varepsilon)} \\ &= \int_0^{+\infty} \mathbb{1}_{[0;\sqrt{R^2-\varepsilon^2}]}(t)\frac{\mathrm{d}t}{(i\varepsilon+t)^x(1+t+i\varepsilon)}\end{aligned}$$

On applique encore le Théorème de Convergence Dominée pour passer à la limite en $\varepsilon \to 0$:

— Pour tout $t \in \mathbb{R}_+$, $\mathbb{1}_{[0;\sqrt{R^2-\varepsilon^2}]}(t)\frac{1}{(i\varepsilon+t)^x(1+t+i\varepsilon)} \underset{\varepsilon\to 0}{\longrightarrow} \mathbb{1}_{[0;R]}\frac{1}{t^x(1+t)}$ en tenant compte de la détermination du logarithme choisie, l'argument de $i\varepsilon + t$ tend vers 0.

— On domine de la même façon que précédemment : pour $t \in \mathbb{R}_+$, $\left|\mathbb{1}_{[0;\sqrt{R^2-\varepsilon^2}]}(t)\frac{1}{(i\varepsilon+t)^x(1+t+i\varepsilon)}\right| \leq \frac{1}{t^x(1+t)}$, intégrable sur $[0;+\infty]$.

On obtient donc, après avoir appliqué une nouvelle fois le TCD pour passer à la limite en $R \to +\infty$,

$$\int_{\gamma_4} f(z)\mathrm{d}z \underset{\substack{\varepsilon\to 0\\ R\to+\infty}}{\longrightarrow} \int_0^{+\infty} \frac{\mathrm{d}t}{t^x(1+t)}$$

Retour au Théorème des Résidus

En passant à la limite en $\varepsilon \to 0$, puis en $R \to +\infty$ dans l'égalité donnée par le Théorème des Résidus, on obtient :

$$\begin{aligned}2i\pi e^{-i\pi x} &= \lim_{\substack{\varepsilon\to 0\\ R\to+\infty}} \left(\int_{\gamma_1} f(z)\mathrm{d}z + \int_{\gamma_2} f(z)\mathrm{d}z + \int_{\gamma_3} f(z)\mathrm{d}z + \int_{\gamma_4} f(z)\mathrm{d}z\right) \\ &= 0 - e^{-2i\pi x}\int_0^{+\infty} \frac{\mathrm{d}t}{t^x(1+t)} + 0 + \int_0^{+\infty} \frac{\mathrm{d}t}{t^x(1+t)}\end{aligned}$$

$$= (1 - e^{-2i\pi x}) \int_0^{+\infty} \frac{dt}{t^x(1+t)}$$

On en déduit que pour tout $x \in]0,1[$, on a

$$\int_0^{+\infty} \frac{dt}{t^x(1+t)} = 2i\pi \frac{e^{-i\pi x}}{1 - e^{-2i\pi x}} = \frac{\pi}{\sin(\pi x)}$$

On a donc finalement bien montré que pour tout $x \in]0;1[$,

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

On étend la validité de cette formule à tout $z \in \Re \in]0;1[$ par prolongement analytique des fonctions holomorphes $\Gamma(z)\Gamma(1-z)$ et $\frac{\pi}{\sin(\pi z)}$ sur cette bande. □

Astuces de l'agrégatif :

Le développement est long, il faut passer plus rapidement sur certaines intégrales mais sans oublier les arguments essentiels qui permettent de justifier ce que l'on fait. Personnellement, je fais celle sur γ_2 en priorité puis celle sur γ_1 si j'ai le temps.

Cauchy–Lipschitz et lemme de Gronwall

Leçons : 203 ; 208 ; 220

Références : ROUVIÈRE, *Petit Guide du Calcul Différentiel* (p.170)

Prérequis :

- le théorème de point fixe de Picard
- $(\mathcal{C}(I,\mathbb{R}),\|.\|_\infty)$ est complet
- le théorème fondamental de l'analyse

Introduction :

Le théorème de Cauchy–Lipschitz est un incontournable des équations différentielles ordinaires. En effet, ce théorème assure, sous de bonnes hypothèses, l'existence et l'unicité des solutions d'un problème de Cauchy. C'est un théorème extrêmement général, on n'a pas de tel théorème pour les équations aux dérivées partielles pour lesquelles on est obligé de faire du cas par cas. On montrera ensuite un lemme de Gronwall qui est un outil essentiel en théorie des équations ordinaires comme on le verra par la suite.

Théorème 1. Soient I un intervalle de $\mathbb{R}$ et $f : I \times \mathbb{R}^n \to \mathbb{R}^n$ une fonction globalement lipschitzienne par rapport à la deuxième composante x (de constante L). Alors, pour tout $(t_0, x_0) \in I \times \mathbb{R}^n$, il existe une unique solution sur I au problème :

$$\begin{cases} x' = f(t,x) \text{ sur } I \\ x(t_0) = x_0 \end{cases}$$

Démonstration. Soit $(t_0, x_0) \in I \times \mathbb{R}^n$. On notera $\|.\|$ une norme sur $\mathbb{R}^n$.

Étape 1 : *Montrons le théorème dans le cas I compact*

On pose $\mathcal{E} = \mathcal{C}(I,\mathbb{R}^n)$ muni de la norme

$$\forall x \in \mathcal{E}, \quad \|x\|_{\mathcal{E}} = \sup_{t\in I} e^{-2L|t-t_0|}\|x(t)\|$$

Le but est d'utiliser le théorème de point fixe de Picard sur la fonction

$$\varphi : \begin{cases} (\mathcal{E},\|.\|_{\mathcal{E}}) & \to & (\mathcal{E},\|.\|_{\mathcal{E}}) \\ x & \mapsto & x_0 + \displaystyle\int_{t_0}^{t} f(s,x(s))ds \end{cases}$$

Il faut donc vérifier que $(\mathcal{E},\|.\|_{\mathcal{E}})$ est un espace de Banach. On a $(\mathcal{C}(I;\mathbb{R}^n),\|.\|_\infty)$ qui est complet et $\|.\|_\infty$ et $\|.\|_{\mathcal{E}}$ qui sont équivalentes [1] donc $(\mathcal{E},\|.\|_{\mathcal{E}})$ est bien complet.

Montrons que φ est contractante. Soit $x, y \in \mathcal{E}$, soit $t \geqslant t_0$,

1. On utilise le caractère compact de I. Pour tout $x \in \mathcal{E}$, pour tout $t \in I$,

$$e^{-2L|I|}\|x(t)\| \leqslant e^{-2L|t-t_0|}\|x(t)\| \leqslant \|x(t)\|$$

d'où

$$e^{-2L|I|}\|x\|_\infty \leqslant \|x\|_{\mathcal{E}} \leqslant \|x\|_\infty$$

en passant au sup

$$\begin{aligned}
\|\varphi(x)(t)-\varphi(y)(t)\| &\leqslant \left\| \int_{t_0}^{t} f(s,x(s))-f(s,y(s))ds \right\| \\
&\leqslant \int_{t_0}^{t} \|f(s,x(s))-f(s,y(s))\|ds \\
&\leqslant \int_{t_0}^{t} L\|x(s)-y(s)\|ds \\
&\leqslant \int_{t_0}^{t} Le^{2L(s-t_0)}e^{-2L(s-t_0)}\|x(s)-y(s)\|ds \\
&\leqslant \int_{t_0}^{t} Le^{2L(s-t_0)}\|x-y\|_{\mathcal{E}}ds \\
&\leqslant \|x-y\|_{\mathcal{E}} L\left[\frac{e^{2L(s-t_0)}}{2L}\right]_{t_0}^{t} \\
&\leqslant \frac{1}{2}\|x-y\|_{\mathcal{E}}(e^{2L(t-t_0)}-1) \\
&\leqslant \frac{1}{2}\|x-y\|_{\mathcal{E}}e^{2L(t-t_0)}
\end{aligned}$$

Ainsi

$$e^{-2L(t-t_0)}\|\varphi(x)(t)-\varphi(y)(t)\| \leqslant \frac{1}{2}\|x-y\|_{\mathcal{E}}$$

On peut faire de même pour $t \leqslant t_0$.

$$\begin{aligned}
\|\varphi(x)(t)-\varphi(y)(t)\| &\leqslant \left\| \int_{t_0}^{t} f(s,x(s))-f(s,y(s))ds \right\| \\
&\leqslant \int_{t}^{t_0} \|f(s,x(s))-f(s,y(s))\|ds \\
&\leqslant \int_{t}^{t_0} L\|x(s)-y(s)\|ds \\
&\leqslant \int_{t}^{t_0} Le^{2L(t_0-s)}e^{-2L(t_0-s)}\|x(s)-y(s)\|ds \\
&\leqslant \int_{t}^{t_0} Le^{2L(t_0-s)}\|x-y\|_{\mathcal{E}}ds \\
&\leqslant \|x-y\|_{\mathcal{E}} L\left[\frac{e^{2L(t_0-s)}}{2L}\right]_{t}^{t_0} \\
&\leqslant \frac{1}{2}\|x-y\|_{\mathcal{E}}(e^{2L(t_0-t)}-1) \\
&\leqslant \frac{1}{2}\|x-y\|_{\mathcal{E}}e^{2L(t_0-t)}
\end{aligned}$$

Ainsi

$$e^{-2L(t_0-t)}\|\varphi(x)(t)-\varphi(y)(t)\| \leqslant \frac{1}{2}\|x-y\|_{\mathcal{E}}$$

En passant au sup sur $t \in I$, on obtient

$$\|\varphi(x)-\varphi(y)\|_{\mathcal{E}} \leqslant \frac{1}{2}\|x-y\|_{\mathcal{E}}$$

Donc φ est contractante, on peut appliquer le théorème de point fixe de Picard.

Il existe donc un unique point fixe $\tilde{x}$ de φ. On a donc

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

Autrement dit,

$$\begin{cases} \tilde{x}' = f(t, \tilde{x}) \text{ sur } I \\ \tilde{x}(t_0) = x_0 \end{cases}$$

Étape 2 : *Montrons le théorème dans le cas général*

On peut écrire

$$I = \bigcup_{k \in \mathbb{N}} I_k$$

où $I_k = I \cap [-k; k]$.

Tous les I_k, sont compacts, donc on peut appliquer l'étape 1, on obtient des solutions x_k définies sur I_k. Or, pour tout $k \in \mathbb{N}$, $x_{k+1|_{I_k}} = x_k$ par unicité. Donc l'application

$$x : \begin{cases} I & \to & \mathbb{R}^n \\ t & \mapsto & x_k(t) \quad \text{si } t \text{ est dans } I_k \end{cases}$$

est bien définie, de manière unique et est solution du problème.

Cela conclut donc la preuve du théorème. □

Théorème 2. Dans le même cadre, soient x et y deux solutions, on a alors :

$$\forall t \in I, \quad \|x(t) - y(t)\| \leqslant \|x(t_0) - y(t_0)\| e^{L|t-t_0|}$$

Démonstration. On pose $\psi(t) = \|x(t) - y(t)\|$. Pour tout $t \geqslant t_0$, on a

$$\psi(t) \leqslant \psi(t_0) + \int_{t_0}^{t} L\psi(s)ds$$

par la formule de φ dans la preuve précédente.

La fonction ψ n'est pas dérivable, donc on va poser $\phi(t) = \displaystyle\int_{t_0}^{t} \psi(s)ds$ et utiliser la dérivée de ϕ. On a

$$\phi'(t) \leqslant \psi(t_0) + L\phi(t)$$

On observe que

$$\frac{d}{dt}[\phi(t)e^{-L(t-t_0)}] = (\phi'(t) - L\phi(t))e^{-L(t-t_0)} \leqslant \psi(t_0)e^{-L(t-t_0)}$$

On intègre (bornes croissantes) entre t_0 et t pour trouver

$$\begin{aligned} \phi(t)e^{-L(t-t_0)} &\leqslant \psi(t_0) \int_{t_0}^{t} e^{-L(s-t_0)}ds \\ &\leqslant \psi(t_0) \left[\frac{e^{-L(s-t_0)}}{-L}\right]_{t_0}^{t} \\ &\leqslant \psi(t_0) \frac{(1 - e^{-L(t-t_0)})}{L} \end{aligned}$$

D'où

$$\phi(t) \leqslant \psi(t_0) \frac{e^{L(t-t_0)} - 1}{L}$$

Ainsi en réinjectant dans $\phi'(t) \leqslant \psi(t_0) + L\phi(t)$, on trouve

$$\psi(t) \leqslant \psi(t_0) + L\psi(t_0) \frac{e^{L(t-t_0)} - 1}{L} = \psi(t_0)e^{L(t-t_0)}$$

On peut faire de même pour $t \leqslant t_0$, ce qui permet de conclure la preuve du théorème.
Pour tout $t \leqslant t_0$, on a

$$\psi(t) \leqslant \psi(t_0) + \int_t^{t_0} L\psi(s)ds$$

par la formule de φ dans la preuve précédente.

La fonction ψ n'est pas dérivable, donc on va poser $\phi(t) = \int_t^{t_0} \psi(s)ds$ et utiliser la dérivée de ϕ. On a

$$\phi'(t) = -\psi(t) \geqslant -\psi(t_0) - L\phi(t)$$

En dérivant, on a

$$\frac{d}{dt}[\phi(t)e^{Lt}] = (\phi'(t) + L\phi(t))e^{Lt} \geqslant -\psi(t_0)e^{Lt}$$

On intègre (bornes croissantes) entre t et t_0 pour trouver

$$\begin{aligned} -\phi(t)e^{Lt} &\geqslant -\psi(t_0) \textstyle\int_t^{t_0} e^{Ls}ds \\ \phi(t)e^{Lt} &\leqslant \psi(t_0) \left[\frac{e^{Ls}}{L}\right]_t^{t_0} \\ &\leqslant \psi(t_0)\frac{(e^{Lt_0} - e^{Lt})}{L} \end{aligned}$$

D'où

$$\phi(t) \leqslant \psi(t_0)\frac{e^{L(t_0-t)} - 1}{L}$$

Ainsi en réinjectant dans $\psi(t) \leqslant \psi(t_0) + L\phi(t)$, on trouve

$$\psi(t) \leqslant \psi(t_0) + L\psi(t_0)\frac{e^{L(t_0-t)} - 1}{L} = \psi(t_0)e^{L(t_0-t)}$$

□

Remarques :

Il faut bien faire attention aux cas $t \leqslant t_0$. Ne pas oublier de préciser que les cas $t \leqslant t_0$ se traitent de manière similaire pendant le développement.

Selon le temps, on n'est pas obligé de faire le lemme de Gronwall

Translatés d'une fonction $\mathcal{C}^1$

Leçons : 151 ; 159 ; 221 ; 228

Références : FRANCINOU–GIANELLA–NICOLAS, *Oraux X-ENS Algèbre 1* (p.300)

Prérequis :

- les solution d'une équation différentielle linéaire d'ordre p forment un espace vectoriel de dimension p.
- $(E^*)^\circ = \{0\}$

Introduction :

On sait que les solutions d'une équation différentielle linéaire forment un espace vectoriel de dimension finie. On va montrer une sorte de réciproque : si les translatés de f engendrent un espace de dimension finie, alors f est solution d'une équation différentielle linéaire.

Notations :

- on note $f_a : \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & f(x+a) \end{cases}$ les translatés de f (pour $a \in \mathbb{R}$).

Théorème 1. Soit $f \in \mathcal{C}^1(\mathbb{R}, \mathbb{R})$. La fonction f est solution d'une équation différentielle linéaire homogène à coefficients constants si et seulement si les translatés de f engendrent un espace vectoriel de dimension finie.

Lemme 1. Soient $f_1, \dots, f_n$ des applications de $\mathbb{R}$ dans $\mathbb{R}$. On a alors

$$(f_1, \dots, f_n) \text{ libre dans } \mathcal{F}(\mathbb{R}, \mathbb{R}) \iff \text{il existe } (x_1, \dots, x_n) \in \mathbb{R}^n \text{ tels que la matrice } (f_i(x_j))_{1 \leqslant i,j \leqslant n} \text{ soit inversible}$$

Démonstration du lemme. $\boxed{\Longleftarrow}$ Par contraposée, si $f_1, \dots, f_n$ sont liées, alors, pour tous les $(x_1, \dots, x_n) \in \mathbb{R}^n$, les colonnes de la matrice $(f_i(x_j))_{1 \leqslant i,j \leqslant n}$ sont liées. Ainsi la matrice ne sera pas inversible.

$\boxed{\Longrightarrow}$ Si $\mathcal{B} = (f_1, \dots, f_n)$ libre dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$, alors $F = \text{Vect}(f_1, \dots, f_n)$ de dimension n. Pour tout $a \in \mathbb{R}$, on pose la forme linéaire sur F suivante

$$e_a : \begin{cases} F & \to & \mathbb{R} \\ f & \mapsto & f(a) \end{cases}$$

L'ensemble $A = \{e_a, a \in \mathbb{R}\}$ est une partie génératrice de F^*.

En effet, si $f \in A^\circ$, on a $f(a) = e_a(f) = 0$ pour tout $a \in \mathbb{R}$, donc f est la fonction nulle, ainsi $A^\circ = \{0\}$. On peut alors écrire

$$\text{Vect}(A) = (\text{Vect}(A)^\circ)^\perp = (A^\circ)^\perp = \{0\}^\perp = F^*$$

On peut donc choisir $x_1, \dots, x_n$ tels que $(e_{x_1}, \dots, e_{x_n})$ base de F^*. On pose ensuite la matrice $M = (f_i(x_j))_{1 \leqslant i,j \leqslant n}$.

Montrons que les lignes $L_1, \dots, L_n$ de M forment une famille libre.

Soit $(\lambda_1, \dots, \lambda_n) \in \mathbb{R}^n$ tels que $\sum_{i=1}^{n} \lambda_i L_i = 0$. On a alors

$$\forall j \in [\![1; n]\!], \quad \sum_{i=1}^{n} \lambda_i f_i(x_j) = 0$$

Autrement dit, $e_{x_j}\left(\sum_{i=1}^{n} \lambda_i f_i\right) = 0$. Comme $(e_{x_j})_{1 \leqslant j \leqslant n}$ est une base de F^*, on a

$$\sum_{i=1}^{n} \lambda_i f_i \in (F^*)^\circ = \{0\},$$

ainsi

$$\sum_{i=1}^{n} \lambda_i f_i = 0$$

Or $(f_1, \dots, f_n)$ forment une base de F, donc $\lambda_1 = \dots = \lambda_n = 0$.

La matrice M est donc inversible. □

Démonstration du théorème. $\boxed{\implies}$ Soit (E) l'équation différentielle linéaire homogène à coefficients constants dont f est solution. On note p l'ordre de (E). Tous les translatés de f sont des solutions de (E) (car (E) est homogène). Or l'ensemble des solutions d'une équation différentielle linéaire d'ordre p forme un espace vectoriel de dimension p. Ainsi l'ensemble des translatés de f engendre un espace vectoriel de dimension inférieure à p, donc de dimension finie.

$\boxed{\impliedby}$ On note F l'ensemble engendré par les translatés de f. Par hypothèse, F est de dimension finie, on note n sa dimension.

On considère $a_1, \dots, a_n$ tels que $(f_{a_1}, \dots, f_{a_n})$ soit une base de F. Par le lemme, il existe $x_1, \dots, x_n$ tels que $M = (f_{a_i}(x_j))_{1 \leqslant i,j \leqslant n}$ soit inversible.

La fonction f étant $\mathcal{C}^1$, les fonctions f_{a_i} le sont aussi. Donc tout élément de F est de classe $\mathcal{C}^1$.

Soit $g \in F$. Montrons que $g' \in F$.

On a, pour tout $a \in \mathbb{R}$, $g_a \in F$ car $g_a \in \mathrm{Vect}(f_{a_1+a}, \dots, f_{a_n+a}) \subset F$.
Il existe donc $\lambda_1(a), \dots, \lambda_n(a)$ tels que

$$g_a = \sum_{i=1}^{n} \lambda_i(a) f_{a_i}$$

On veut maintenant montrer que les λ_i sont dérivables.
On a, pour tout $1 \leqslant j \leqslant n$,

$$g(a + x_j) = g_a(x_j) = \sum_{i=1}^{n} \lambda_i(a) f_{a_i}(x_j)$$

Autrement dit,

$${}^tM \begin{pmatrix} \lambda_1(a) \\ \vdots \\ \lambda_n(a) \end{pmatrix} = \begin{pmatrix} g(a + x_1) \\ \vdots \\ g(a + x_n) \end{pmatrix}$$

D'où

$$\begin{pmatrix}\lambda_1(a)\\ \vdots \\ \lambda_n(a)\end{pmatrix} = {}^tM^{-1}\begin{pmatrix}g(a+x_1)\\ \vdots \\ g(a+x_n)\end{pmatrix} \text{ car } M \text{ est inversible donc } {}^tM \text{ aussi}$$

Comme ${}^tM^{-1}$ est indépendante de a, pour tout $j \in [\![1;n]\!]$, λ_j est combinaison des $g_{x_1}, \dots, g_{x_n}$. Les λ_i sont donc des fonctions $\mathcal{C}^1$ comme les g_{x_i}. On a

$$\forall x \in \mathbb{R}, \quad g(x+a) = \sum_{i=1}^{n} \lambda_i(a) f_{a_i}(x)$$

En dérivant par rapport à a, on a :

$$g'(x+a) = \sum_{i=1}^{n} \lambda_i'(a) f_{a_i}(x)$$

On applique en $a = 0$,

$$g'(x) = \sum_{i=1}^{n} \lambda_i'(0) f_{a_i}(x)$$

Ainsi

$$g' = \sum_{i=1}^{n} \lambda_i'(0) f_{a_i} \in F$$

Donc tout élément de F est $\mathcal{C}^\infty$ et pour tout $k \in \mathbb{N}$, on a $g^{(k)} \in F$.

Ainsi, on peut appliquer ce résultat pour notre fonction f. Or l'espace vectoriel F étant de dimension finie n, il existe $p \in [\![1;n]\!]$ tel que

$$f^{(p)} \in \text{Vect}(f, f', \dots, f^{(p-1)})$$

La fonction f est donc solution d'une équation différentielle linéaire homogène à coefficient constant d'ordre p. □

Remarques :

En fait, on peut prendre une fonction f seulement continue et dérivable, car on montre que f' est dans l'espace F des translatés de f, donc $f \in \mathcal{C}^1$ gratuitement.

Astuces de l'agrégatif :

J'écris *EDO* pour équation différentielle ordinaire dans le développement.

Questions possibles :

- Pourquoi $(F^*)^\circ = \{0\}$?
- Pourquoi $\text{Vect}A = \text{Vect}(A^\circ)^\perp$ en dimension finie ?

Méthode de Gradient à pas optimal

(rédigé par Rémi Moreau et Vincent Béhani)

Leçons : 162 ; 219 ; 226 ; 229 ; 233

Références : RAMIS–WARUSFEL, *Cours de Mathématiques pures et appliquées* (p.412) ou HERON, *Analyse numérique* (p.15 et 263)

Prérequis :

- le théorème spectral
- $\text{Cond}_2(A) = \dfrac{\mu_n}{\mu_1}$ où μ_1 et μ_n sont respectivement les valeurs propres minimales et maximales de A.

Introduction :

Comme on va le voir dans le théorème suivant et l'algorithme du gradient à pas optimal, on cherche à trouver une solution de $AX = B$ en l'approchant par une suite. Ainsi on veut trouver le minimum de la fonctionnelle convexe f présentée ci dessous. Le théorème 1 et l'algorithme sont des éléments à mettre dans le plan de la leçon et le développement consiste en la démonstration du théorème 2 avec l'inégalité de Kantorovich.

Théorème 1. Si $A \in \mathcal{S}_n^{++}(\mathbb{R})$ alors :

$$AX_0 = B \iff X_0 \text{ minimise l'application } f : \left\{ \begin{array}{ccc} \mathbb{R}^n & \to & \mathbb{R} \\ X & \mapsto & \frac{1}{2}\langle AX, X\rangle - \langle B, X\rangle \end{array} \right.$$

Démonstration. Soit $X_0 \in \mathbb{R}^n$ solution du système $AX = B$. Remarquons que pour tout $H \in \mathbb{R}^n$, puisque $A \in \mathcal{S}_n^{++}(\mathbb{R})$ on a :

$$\begin{array}{rcl} f(X_0 + H) & = & \frac{1}{2}\langle AX_0, X_0\rangle + \frac{1}{2}\langle AH, X_0\rangle + \frac{1}{2}\langle AX_0, H\rangle + \frac{1}{2}\langle AH, H\rangle - \langle B, X_0\rangle - \langle B, H\rangle \\ & = & f(X_0) + \frac{1}{2}\langle AX_0, H\rangle + \frac{1}{2}\langle AX_0, H\rangle + \frac{1}{2}\langle AH, H\rangle - \langle B, H\rangle \\ & = & f(X_0) + \langle B, H\rangle + \frac{1}{2}\langle AH, H\rangle - \langle B, H\rangle \\ & = & f(X_0) + \frac{1}{2}\langle AH, H\rangle \\ & \geq & f(X_0) \end{array}$$

avec $\frac{1}{2}\langle AH, H\rangle > 0$ si et seulement si $H \neq 0$. Alors X_0 est l'unique minimum global de f.

Réciproquement, supposons que $X_0 \in \mathbb{R}^n$ minimise f. Alors $\nabla f(X_0) = 0$. Or le calcul précédent indique que pour tout $H \in \mathbb{R}^n$ et tout $X \in \mathbb{R}^n$:

$$f(X + H) \underset{\|H\| \to 0}{=} f(X) + \langle AX - B, H\rangle + \mathcal{O}(\|H\|^2)$$

Ainsi $\nabla f(X_0) = AX_0 - B = 0$ implique que X_0 est solution du système $AX = B$. □

Algorithme du gradient à pas optimal :

Soit $X_0 \in \mathbb{R}^n$ et $R_0 = AX_0 - B$. Soit $\varepsilon > 0$:
tant que $\frac{\|R_n\|}{\|R_0\|} \geq \varepsilon$:

- $\alpha_{n+1} = \frac{\|R_n\|^2}{\langle AR_n, R_n\rangle}$;
- $X_{n+1} = X_n - \alpha_{n+1} R_n$;

- $R_{n+1} = AX_{n+1} - B$;

Résultat : $\frac{\|R_n\|}{\|R_0\|} = \frac{\|AX_n - B\|}{\|AX_0 - B\|} < \varepsilon$.

Cherchant la solution du système $AX = B$, on cherche à minimiser la fonction :

$$f : \left\{ \begin{array}{ccc} \mathbb{R}^n & \to & \mathbb{R} \\ X & \mapsto & \frac{1}{2}\langle AX, X\rangle - \langle B, X\rangle \end{array} \right.$$

Partant d'un vecteur $X_0 \in \mathbb{R}^n$, on construit une suite $(X_k)_{k\in\mathbb{N}}$ convergeant vers son unique minimum global. Or puisque $\nabla f(X_k)$ est la direction selon laquelle f croît le plus à partir de X_k, cherchons X_{k+1} de la forme $X_{k+1} = X_k - \alpha_{k+1}\nabla f(X_k)$ tel que $f(X_k - \alpha_{k+1}\nabla f(X_k))$ soit minimal. Considérons l'application :

$$\phi_k : \left\{ \begin{array}{ccc}]0, +\infty[& \to & \mathbb{R} \\ t & \mapsto & f(X_k - t\nabla f(X_k)) \end{array} \right.$$

Pour tout $t > 0$, on a :

$$\begin{array}{rcl} \phi_k(t) & = & f(X_k) + \langle AX_k, -t\nabla f(X_k)\rangle + \frac{1}{2}\langle A(-t\nabla f(X_k)), -t\nabla f(X_k)\rangle - \langle B, -t\nabla f(X_k)\rangle \\ & = & f(X_k) - t\langle AX_k - B, \nabla f(X_k)\rangle + \frac{t^2}{2}\langle A\nabla f(X_k), \nabla f(X_k)\rangle \end{array}$$

Or $R_k = AX_k - B = \nabla f(X_k)$ donc :

$$\phi_k(t) = f(X_k) - t\|R_k\|^2 + \frac{t^2}{2}\langle AR_k, R_k\rangle$$

Ainsi pour tout $t > 0$ on a :

$$\phi_k'(t) = -\|R_k\|^2 + t\langle AR_k, R_k\rangle \geq 0 \quad \Longleftrightarrow \quad t \geq \frac{\|R_k\|^2}{\langle AR_k, R_k\rangle} = \alpha_{k+1}$$

Donc ϕ_k est décroissante sur $]0, \alpha_{k+1}]$ et croissante sur $[\alpha_{k+1}, +\infty[$, elle atteint alors son minimum en $\alpha_{k+1} = \frac{\|R_k\|^2}{\langle AR_k, R_k\rangle}$.

Théorème 2 (Méthode du gradient à pas optimal)**.** L'algorithme du gradient converge vers la solution $\overline{X}$ du système $AX = B$ et pour tout $k \in \mathbb{N}$:

$$\|X_k - \overline{X}\| \leq \sqrt{\mathrm{Cond}(A)}\left(\frac{\mathrm{Cond}(A) - 1}{\mathrm{Cond}(A) + 1}\right)^k \|X_0 - \overline{X}\|$$

Lemme 1 (Inégalité de Kantorovich)**.** Toute matrice $A \in \mathcal{S}_n^{++}(\mathbb{R})$, de valeurs propres minimale et maximale respectivement μ_1 et μ_n, vérifie pour tout $X \in \mathbb{R}^n\backslash\{0\}$:

$$\frac{\|X\|^4}{\|X\|_{A^{-1}}^2\|X\|_A^2} \geq 4\frac{\mu_1\mu_n}{(\mu_1 + \mu_n)^2}$$

où $\|X\|_A^2 = \langle AX, X\rangle$.

Démonstration du lemme. Puisque $A \in \mathcal{S}_n^{++}(\mathbb{R})$, il existe une base $(e_i)_{i\in\{1,\dots,n\}}$ orthonormale de $\mathbb{R}^n$ constituée de vecteurs propres de A associés aux valeurs propres $(\mu_i)_{i\in\{1,\dots,n\}}$. Soit un vecteur

non nul $X = \sum_{i=1}^{n} x_i e_i \in \mathbb{R}^n$ exprimé dans la base tel que $AX = A\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{n} \mu_i x_i e_i$. Alors puisque $\sqrt{ab} \leq \frac{1}{2}(a+b)$ pour tout a et b positifs, on a :

$$\begin{aligned}\sqrt{\|X\|_{A^{-1}}^2 \|X\|_A^2} &= \sqrt{\left(\sum_{i=1}^{n} \tfrac{1}{\mu_i} x_i^2\right)\left(\sum_{j=1}^{n} \mu_j x_j^2\right)} = \sqrt{\tfrac{\mu_1}{\mu_n}\left(\sum_{i=1}^{n} \tfrac{\mu_n}{\mu_i} x_i^2\right)\left(\sum_{j=1}^{n} \tfrac{\mu_j}{\mu_1} x_j^2\right)} \\ &\leq \tfrac{1}{2}\sqrt{\tfrac{\mu_1}{\mu_n}}\left(\sum_{i=1}^{n} \tfrac{\mu_n}{\mu_i} x_i^2 + \sum_{j=1}^{n} \tfrac{\mu_j}{\mu_1} x_j^2\right) \leq \tfrac{1}{2}\sqrt{\tfrac{\mu_1}{\mu_n}} \sum_{i=1}^{n} \left(\tfrac{\mu_n}{\mu_i} + \tfrac{\mu_i}{\mu_1}\right) x_i^2\end{aligned}$$

Or l'application $\psi : \left\{ \begin{array}{ccc} [\mu_1, \mu_n] & \to & \mathbb{R} \\ x & \mapsto & \frac{\mu_n}{x} + \frac{x}{\mu_1} \end{array} \right.$ est dérivable et de dérivée $\psi'(x) = \frac{1}{\mu_1} - \frac{\mu_n}{x^2}$ pour tout $x \in [\mu_1, \mu_n]$. Ainsi pour tout $x \in [\mu_1, \mu_n]$:

$$\psi'(x) \geq 0 \iff \tfrac{1}{\mu_1} \geq \tfrac{\mu_n}{x^2} \iff x \geq \sqrt{\mu_1 \mu_n}$$

Donc ψ est décroissante sur $[\mu_1, \sqrt{\mu_1\mu_n}]$ et croissante sur $[\sqrt{\mu_1\mu_n}, \mu_n]$. L'application ψ atteint dès lors son maximum en μ_1 et μ_n car $\psi(\mu_1) = 1 + \frac{\mu_n}{\mu_1} = \psi(\mu_n)$. D'où :

$$\begin{aligned}\sqrt{\|X\|_{A^{-1}}^2 \|X\|_A^2} &\leq \tfrac{1}{2}\sqrt{\tfrac{\mu_1}{\mu_n}} \sum_{i=1}^{n} \left(1 + \tfrac{\mu_n}{\mu_1}\right) x_i^2 \leq \tfrac{1}{2}\left(\sqrt{\tfrac{\mu_1}{\mu_n}} + \sqrt{\tfrac{\mu_n}{\mu_1}}\right) \sum_{i=0}^{n} x_i^2 \\ &\leq \tfrac{1}{2}\left(\sqrt{\tfrac{\mu_1}{\mu_n}} + \sqrt{\tfrac{\mu_n}{\mu_1}}\right) \|X\|^2\end{aligned}$$

Or remarquons que :

$$\sqrt{\frac{\mu_1}{\mu_n}} + \sqrt{\frac{\mu_n}{\mu_1}} = \frac{\mu_1 + \mu_n}{\sqrt{\mu_1\mu_n}}$$

ce qui donne :

$$\|X\|_{A^{-1}}^2 \|X\|_A^2 \leq \frac{1}{4}\frac{(\mu_1+\mu_n)^2}{\mu_1\mu_n}\|X\|^4 \implies \frac{\|X\|^4}{\|X\|_{A^{-1}}^2 \|X\|_A^2} \geq 4\frac{\mu_1\mu_n}{(\mu_1+\mu_n)^2}$$

□

Démonstration du théorème. Montrons que la suite $(X_k)_{k\in\mathbb{N}}$ converge vers la solution $\overline{X}$ du système $AX = B$. Remarquons tout d'abord que pour tout $k \in \mathbb{N}$:

$$\begin{aligned}\langle R_{k+1}, R_k\rangle &= \langle AX_{k+1} - B, R_k\rangle = \langle AX_k - B - \alpha_{k+1}AR_k, R_k\rangle = \langle R_k, R_k\rangle - \alpha_{k+1}\langle AR_k, R_k\rangle \\ &= \|R_k\|^2 - \tfrac{\|R_k\|^2}{\|R_k\|_A^2}\|R_k\|_A^2 = 0\end{aligned}$$

Ainsi on calcule :

$$\begin{aligned}\|X_{k+1} - \overline{X}\|_A^2 &= \langle A(X_{k+1} - \overline{X}), X_{k+1} - \overline{X}\rangle \\ &= \langle AX_{k+1} - B, X_{k+1} - X_k\rangle + \langle A(X_{k+1} - \overline{X}), X_k - \overline{X}\rangle \\ &= \langle R_{k+1}, -\alpha_{k+1}R_k\rangle + \langle A(X_{k+1} - X_k), X_k - \overline{X}\rangle + \langle A(X_k - \overline{X}), X_k - \overline{X}\rangle \\ &= \langle X_{k+1} - X_k, A(X_k - \overline{X})\rangle + \|X_k - \overline{X}\|_A^2 \\ &= -\alpha_{k+1}\langle R_k, AX_k - B\rangle + \|X_k - \overline{X}\|_A^2 \\ &= -\alpha_{k+1}\langle R_k, R_k\rangle + \|X_k - \overline{X}\|_A^2 \\ &= -\tfrac{\|R_k\|^4}{\|R_k\|_A^2} + \|X_k - \overline{X}\|_A^2\end{aligned}$$

Remarquons que :

$$\|X_k - \overline{X}\|_A^2 = \langle A(X_k - \overline{X}), X_k - \overline{X}\rangle = \langle AX_k - B, A^{-1}(AX_k - B)\rangle = \langle R_k, A^{-1}R_k\rangle = \|R_k\|_{A^{-1}}^2$$

Ainsi :

$$\begin{aligned}\|X_{k+1}-\overline{X}\|_A^2 &= \left(1-\frac{\|R_k\|^4}{\|R_k\|_A^2\|R_k\|_{A^{-1}}^2}\right)\|X_k-\overline{X}\|_A^2 \leq \left(1-\frac{4\mu_1\mu_n}{(\mu_1+\mu_n)^2}\right)\|X_k-\overline{X}\|_A^2 \\ &\leq \frac{(\mu_n-\mu_1)^2}{(\mu_n+\mu_1)^2}\|X_k-\overline{X}\|_A^2\end{aligned}$$

En itérant cette inégalité, on a pour tout $k \in \mathbb{N}$:

$$\|X_k-\overline{X}\|_A \leq \left(\frac{\mu_n-\mu_1}{\mu_n+\mu_1}\right)^k \|X_0-\overline{X}\|_A$$

En remarquant que $0 < \frac{\mu_n-\mu_1}{\mu_n+\mu_1} < 1$, on a convergence de la suite $(X_k)_{k\in\mathbb{N}}$ vers $\overline{X}$. De plus pour tout $X = \sum_{i=1}^n x_i e_i \in \mathbb{R}^n$ exprimé dans une base orthonormale de vecteurs propres de A :

$$\mu_1\|X\|^2 = \sum_{i=1}^n \mu_1 x_i^2 \leq \sum_{i=1}^n \mu_i x_i^2 = \|X\|_A^2 \leq \sum_{i=1}^n \mu_n x_i^2 = \mu_n\|X\|^2$$

Alors :

$$\|X_k-\overline{X}\| \leq \frac{1}{\sqrt{\mu_1}}\|X_k-\overline{X}\|_A \leq \frac{1}{\sqrt{\mu_1}}\left(\frac{\mu_n-\mu_1}{\mu_n+\mu_1}\right)^k \|X_0-\overline{X}\|_A \leq \sqrt{\frac{\mu_n}{\mu_1}}\left(\frac{\mu_n-\mu_1}{\mu_n+\mu_1}\right)^k \|X_0-\overline{X}\|$$

Or on sait que $\mathrm{Cond}_2(A) = \frac{\mu_n}{\mu_1}$, d'où :

$$\sqrt{\frac{\mu_n}{\mu_1}}\frac{\mu_n-\mu_1}{\mu_n+\mu_1} = \sqrt{\frac{\mu_n}{\mu_1}}\frac{\frac{\mu_n}{\mu_1}-1}{\frac{\mu_n}{\mu_1}+1} = \sqrt{\mathrm{Cond}_2(A)}\frac{\mathrm{Cond}_2(A)-1}{\mathrm{Cond}_2(A)+1}$$

D'où l'inégalité :

$$\|X_k-\overline{X}\| \leq \sqrt{\mathrm{Cond}_2(A)}\left(\frac{\mathrm{Cond}_2(A)-1}{\mathrm{Cond}_2(A)+1}\right)^k \|X_0-\overline{X}\|$$

□

Astuces de l'agrégatif :

Comme je l'ai dit plus haut, le développement se concentre sur le theorème 2 et le lemme 1. S'il reste du temps, il est bien d'expliquer pourquoi on fait tout cela avec notamment le théorème 1 et la raison pour laquelle α_{k+1} est défini comme ça.

Questions possibles :

- Est-ce qu'on peut changer le rôle de μ_1 et μ_n ?
- Vaut-il mieux que les valeurs propres soient rapprochées ou éloignées pour améliorer la vitesse de convergence ?
- Quel est le lien entre l'algorithme et le théorème qui dit que $\bar{X}$ est solution de $AX = b$ SSI $\bar{X}$ minimise la fonctionnelle convexe

$$f : \begin{cases} \mathbb{R}^n & \to & \mathbb{R} \\ X & \mapsto & \frac{1}{2}\langle AX, X\rangle - \langle b, X\rangle \end{cases}$$

Nombres de Bell

Leçons : 190 ; 230 ; 243

Références : FRANCINOU–GIANELLA–NICOLAS, *Oraux X-ENS Algèbre 1* (p.12)

Prérequis :

- notion de famille sommable [1]
- notion de série entière
- définition de l'exponentielle

Introduction :

On veut étudier le nombre de partitions différentes de $[\![1;n]\!]$ que l'on appellera B_n. Ce sont les nombres de Bell. On va étudier une série entière liée à ses nombres pour en déduire une expression explicite des B_n.

Théorème 1. Soit $n \geqslant 0$, on note B_n le nombre de partitions différentes de $[\![1;n]\!]$ (On prend $B_0 = 1$ par convention).

Alors on a :

— la relation de récurrence $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$,

— le rayon de convergence R de $f(z) = \sum_{n\geqslant 0} \frac{B_n}{n!} z^n$ est supérieur à 1,

— pour tout $z \in B(0,R)$, l'égalité $f(z) = \exp(e^z - 1)$

— pour tout $k \in \mathbb{N}$, $B_k = \frac{1}{e}\left(\sum_{n=0}^{+\infty} \frac{n^k}{n!}\right)$

Démonstration. **Étape 1 :** *Montrons la relation de récurrence* $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$

Soit $n \geqslant 0$. On veut dénombrer le nombre de partitions différentes de $[\![1;n+1]\!]$, pour cela on regarde la partie qui contient l'élément $n+1$. On note k le nombre d'éléments qui sont dans la même partie que $n+1$ ($n+1$ exclu), on a alors k entre 0 et n. Pour choisir ces k éléments, on a $\binom{n}{k}$ choix puisqu'il faut choisir k éléments parmi n. Il reste $n-k$ éléments qu'il faut partitionner. Par définition de B_n, on a donc B_{n-k} partitions différentes pour les $n-k$ éléments restants. On obtient donc la relation suivante :

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} = \sum_{k=0}^{n} \binom{n}{n-k} B_k = \sum_{k=0}^{n} \binom{n}{k} B_k$$

par changement d'indice et puisque $\binom{n}{n-k} = \binom{n}{k}$.

1. Une famille de complexe $(u_{n,k})$ indicée sur $\mathbb{N}^2$ est dite sommable si et seulement si
— pour tout $n \in \mathbb{N}$, $\sigma_n = \sum_k |u_{n,k}|$ converge
— la série de terme σ_n converge

Étape 2 : *Montrons que le rayon de convergence R est supérieur à 1*

On veut montrer que $B_n \leqslant n!$ pour avoir $\dfrac{B_n}{n!} \leqslant 1$ afin d'avoir un rayon de convergence R plus grand que 1 [2]. On va raisonner par récurrence.
Initialisation : pour $n = 0$, on a $B_0 = 1 = 0!$. Donc la propriété est vraie au rang 0.
Hérédité : on suppose que l'on a $B_k \leqslant k!$ pour tout $k \leqslant n$.

$$\begin{aligned}
B_{n+1} &= \sum_{k=0}^{n} \binom{n}{k} B_k \\
&\leqslant \sum_{k=0}^{n} \binom{n}{k} k! \text{ par hypothèse de récurrence} \\
&\leqslant \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} k! \\
&\leqslant n! \sum_{k=0}^{n} \frac{1}{(n-k)!} \\
&\leqslant n! \sum_{k=0}^{n} 1 \text{ car } \frac{1}{(n-k)!} \leqslant 1 \\
&\leqslant (n+1)!
\end{aligned}$$

Conclusion : Donc la propriété est vraie pour tout $n \in \mathbb{N}$.

Ainsi, le rayon de convergence R de la série entière $f(z) = \sum_{n\geqslant 0} \dfrac{B_n}{n!} z^n$ est supérieur à 1. [3]

Étape 3 : *Trouvons une expression pour f*

On peut donc écrire $f(z) = \sum_{n\geqslant 0} \dfrac{B_n}{n!} z^n$ pour tout $z \in B(0, R)$.

On veut trouver une équation différentielle avec pour inconnue f. Pour tout $z \in B(0, R)$,

$$\begin{aligned}
f'(z) &= \sum_{n=1}^{\infty} n \frac{B_n}{n!} z^{n-1} \\
&= \sum_{n=1}^{\infty} \frac{B_n}{(n-1)!} z^{n-1} \\
&= \sum_{n=0}^{\infty} \frac{B_{n+1}}{n!} z^n \\
&= \sum_{n=0}^{\infty} \frac{1}{n!} \left(\sum_{k=0}^{n} \binom{n}{k} B_k \right) z^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \frac{B_k}{k!} \frac{1}{(n-k)!} \right) z^n \\
&= \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n \right) \left(\sum_{n=0}^{\infty} \frac{1}{n!} z^n \right)
\end{aligned}$$

2. car le rayon de la série entière $\sum_{n\geqslant 0} z^n$ vaut 1

3. car $\forall n \in \mathbb{N}$, $\left| \dfrac{B_n}{n!} z^n \right| \leqslant |z|^n$

$$= e^z f(z)$$

On a donc l'équation différentielle

$$f' = e^z f$$

ce qui donne que $f(z) = C\exp(e^z)$ où C est une constante.
Or $f(0) = 1$, d'où $C = e^{-1}$. Autrement dit, $f(z) = \exp(e^z - 1)$ pour tout $z \in B(0, R)$.

Étape 4 : *Trouvons une expression explicite pour les coefficients B_n*

On veut exprimer f sous forme de série entière pour pouvoir identifier les coefficients. Pour faciliter les calculs on va regarder $\exp(e^z)$. On fixe $z \in B(0, R)$.

$$\begin{aligned}\exp(e^z) &= \sum_{n=0}^{\infty} \frac{e^{nz}}{n!} \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{\infty} \frac{(nz)^k}{k!} \right) \frac{1}{n!} \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \frac{(nz)^k}{k!n!}\end{aligned}$$

On voudrait intervertir les deux signes $\sum$. Pour cela, on va montrer que la famille $u_{n,k} = \dfrac{(nz)^k}{k!n!}$ est sommable pour pouvoir utiliser Fubini. [4]

$$\forall n \geqslant 0, \quad \sum_{k=0}^{\infty} |u_{n,k}| = \sum_{k=0}^{\infty} \frac{(n|z|)^k}{n!k!} = \frac{e^{n|z|}}{n!}$$

or $\dfrac{e^{n|z|}}{n!}$ est un terme de série convergente qui converge vers $\exp(e^{|z|})$.
Ainsi on peut intervertir les signes $\sum$. On a alors, pour tout $z \in B(0, R)$,

$$\begin{aligned}f(z) &= \frac{1}{e}\exp(e^z) \\ &= \frac{1}{e} \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} \frac{(nz)^k}{k!n!} \\ &= \frac{1}{e} \sum_{k=0}^{\infty} \frac{z^k}{k!} \sum_{n=0}^{\infty} \frac{n^k}{n!} \\ &= \sum_{k=0}^{\infty} \left(\frac{1}{e} \sum_{n=0}^{\infty} \frac{n^k}{n!} \right) \frac{z^k}{k!}\end{aligned}$$

Par unicité du développement en série entière sur $B(0, R)$, on a donc

$$\boxed{B_k = \frac{1}{e} \sum_{n=0}^{\infty} \frac{n^k}{n!}}$$

□

Remarques :

À la fin du développement, comme $\exp(e^z)$ est une somme de termes qui converge sur $\mathbb{C}$, on trouve que le rayon de convergence R de la série entière $\displaystyle\sum_{n\geqslant 0} \frac{B_n}{n!} z^n$ est en fait infini.

4. sachant qu'on travaille ici à z fixé

Astuces de l'agrégatif :

C'est facile de s'emmêler sur les indices n et k, un moyen pour se souvenir lequel utiliser c'est de se dire qu'au début, on étudie B_{n+1} donc on indice sur k puis ensuite on met tout le temps n pour la première somme. La seule exception est à la dernière étape, mais c'est normal de commencer par k puisque tout le but est d'inverser les deux sommations.

Formule d'inversion de la fonction caractéristique

Leçons : 236 ; 239 ; 250 ; 260 ; 264

Références : OUVRARD, *Probabilités 2* (p.233)

Prérequis :

- la fonction de répartition F_X caractérise la loi de X (voir appendice)
- théorème de convergence dominée
- théorème de Fubini
- l'intégrale de Dirichlet $\displaystyle\int_0^{+\infty} \frac{\sin(u)}{u} du = \frac{\pi}{2}$ [1]
- le nombre de discontinuité d'une fonction croissante est dénombrable

Introduction :

En sachant que la fonction caractéristique n'est autre qu'une transformée de Fourier, on se demande qu'elle est la fonction caractéristique inverse. De plus, est ce que cette fonction inverse pourrait nous donner la loi suivie par notre variable aléatoire. On va voir qu'en effet, la fonction caractéristique caractérise la loi (on le montrera en montrant qu'elle caractérise la fonction de répartition qui caractérise la loi), on donnera l'expression explicite de la loi de probabilité pour le cas discret et le cas à densité.

Théorème 1. La fonction caractéristique d'une loi de probabilité détermine cette loi, ainsi deux variables ont même loi si et seulement si elles ont les mêmes fonctions caractéristiques.

De plus, si X est une variable aléatoire discrète, on a

$$\mathbb{P}(X = n) = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} e^{-inT} \varphi_X(t) dt.$$

Et si X est une variable aléatoire réelle et que $\varphi_X \in L^1$, alors X admet une densité donnée par

$$f_X(x) = \frac{1}{2\pi} \int_{\mathbb{R}} e^{-ixt} \varphi_X(t) dt$$

Remarques :

On va se servir du fait que la fonction de répartition $F_X(t) = \mathbb{P}(X \leqslant t)$ caractérise la loi. Donc il faut bien connaître ce résultat.

Démonstration. Soient $T > 0$ et deux réels a et b tels que $a < b$. On pose la fonction K_T définie sur $\mathbb{R}$ par

$$\boxed{K_T(x) = \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} e^{ixt} dt}$$

1. on peut le prouver en appliquant le théorème des résidus sur un contour bien choisi

On va vouloir utiliser le théorème de convergence dominée pour avoir

$$\lim_{T\to\infty}\int_{\mathbb{R}} K_T d\mathbb{P}_X = \int_{\mathbb{R}} \lim_{T\to\infty} K_T d\mathbb{P}_X$$

Étape 1 : *Calculons* $\lim_{T\to\infty} K_T$

$$\begin{aligned}
K_T(x) &= \frac{1}{2\pi}\left(\int_0^T \frac{e^{-iat}-e^{-ibt}}{it}e^{ixt}dt + \int_T^0 \frac{e^{iau}-e^{ibu}}{iu}e^{-ixu}du\right) \text{ [2]}\\
&= \frac{1}{2\pi}\left(\int_0^T \frac{e^{i(x-a)t}-e^{i(x-b)t}}{it}dt - \int_0^T \frac{e^{-i(x-a)t}-e^{-i(x-b)t}}{it}dt\right)\\
&= \frac{1}{2\pi}\left(\int_0^T \frac{e^{i(x-a)t}-e^{-i(x-a)t}}{it}dt - \int_0^T \frac{e^{i(x-b)t}-e^{-i(x-b)t}}{it}dt\right)\\
&= \frac{1}{2\pi}\left(\int_0^T \frac{e^{i(x-a)t}-e^{-i(x-a)t}}{it}dt - \int_0^T \frac{e^{i(x-b)t}-e^{-i(x-b)t}}{it}dt\right)\\
&= \frac{1}{\pi}\left(\int_0^T \frac{\sin((x-a)t)}{t}dt - \int_0^T \frac{\sin((x-b)t)}{t}dt\right)\\
&= \frac{1}{\pi}\left(\int_0^{(x-a)T} \frac{\sin u}{u}du - \int_0^{(x-b)T} \frac{\sin u}{u}du\right) \text{ [3]}
\end{aligned}$$

En posant la fonction $\phi(y) = \int_0^y \frac{\sin u}{u}du, \quad \forall y \in \mathbb{R}$ [4], on a donc

$$K_T(x) = \frac{1}{\pi}\left(\phi(T(x-a)) - \phi(T(x-b))\right)$$

Or on sait que $\int_0^{+\infty} \frac{\sin(u)}{u}du = \frac{\pi}{2}$, donc en faisant une distinction de cas $x < a$, $x = a$, $a < x < b$, $x = b$ et $b < x$, on donne la limite de $K_T(x)$.

- Si $x < a$, on a $\lim_{T\to\infty} T(x-a) = -\infty$ et $\lim_{T\to\infty} T(x-b) = -\infty$, d'où

$$\lim_{T\to\infty} K_T(x) = \frac{1}{\pi}(-\frac{\pi}{2} + \frac{\pi}{2}) = 0$$

- Si $x = a$, on a $\lim_{T\to\infty} T(x-a) = 0$ et $\lim_{T\to\infty} T(x-b) = -\infty$, d'où

$$\lim_{T\to\infty} K_T(x) = \frac{1}{\pi}(0 + \frac{\pi}{2}) = \frac{1}{2}$$

- Si $a < x < b$, on a $\lim_{T\to\infty} T(x-a) = +\infty$ et $\lim_{T\to\infty} T(x-b) = -\infty$, d'où

$$\lim_{T\to\infty} K_T(x) = \frac{1}{\pi}(\frac{\pi}{2} + \frac{\pi}{2}) = 1$$

- Si $x = b$, on a $\lim_{T\to\infty} T(x-a) = +\infty$ et $\lim_{T\to\infty} T(x-b) = 0$, d'où

$$\lim_{T\to\infty} K_T(x) = \frac{1}{\pi}(\frac{\pi}{2} - 0) = \frac{1}{2}$$

2. par le changement de variable $u = -t$
3. par le changement de variable $u = (x-a)t$ et $u = (x-b)t$
4. on peut remarquer que ϕ est impaire, cela nous servira pour la limite en $-\infty$

- Si $b < x$, on a $\lim_{T\to\infty} T(x-a) = +\infty$ et $\lim_{T\to\infty} T(x-b) = +\infty$, d'où

$$\lim_{T\to\infty} K_T(x) = \frac{1}{\pi}(\frac{\pi}{2} - \frac{\pi}{2}) = 0$$

Ainsi on peut écrire

$$\lim_{T\to\infty} K_T(x) = \mathbb{1}_{]a,b[}(x) + \frac{\delta_a(x) + \delta_b(x)}{2}$$

Ainsi

$$\begin{aligned}\int_{\mathbb{R}} \lim_{T\to\infty} K_T d\mathbb{P}_X &= \int_{\mathbb{R}} \mathbb{1}_{]a,b[}(x) + \frac{\delta_a(x) + \delta_b(x)}{2} d\mathbb{P}_X \\ &= \mathbb{P}(X \in]a,b[) + \frac{\mathbb{P}(X=a) + \mathbb{P}(X=b)}{2}\end{aligned}$$

Étape 2 : *Calculons* $\lim_{T\to\infty} \int_{\mathbb{R}} K_T d\mathbb{P}_X$

$$\begin{aligned}\int_{\mathbb{R}} K_T(x) d\mathbb{P}_X &= \int_{\mathbb{R}} \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} e^{ixt} dt d\mathbb{P}_X \\ \text{par Fubini}^{5} &= \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} \int_{\mathbb{R}} e^{ixt} d\mathbb{P}_X dt \\ &= \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} \varphi_X(t) dt\end{aligned}$$

On utilise maintenant le théorème de convergence dominée, puisque $|K_T| \leqslant \frac{2\|\phi\|_\infty}{\pi}$, d'où

$$\lim_{T\to\infty} \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} \varphi_X(t) dt = \mathbb{P}(X \in]a,b[) + \frac{\mathbb{P}(X=a) + \mathbb{P}(X=b)}{2}$$

Étape 3 : *Lien avec la fonction de répartition*

On sait que $F_X(b) - F_X(a) = \mathbb{P}(X \in]a,b[) + \mathbb{P}(X=b)$, donc on a

$$F_X(b) - F_X(a) = \lim_{T\to\infty} \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} \varphi_X(t) dt - \frac{\mathbb{P}(X=a) - \mathbb{P}(X=b)}{2}$$

Soit $\mathcal{D}$ les points où F_X est discontinue. L'ensemble $\mathcal{D}$ est dénombrable car F_X est croissante. Ainsi, pour tout $b \notin \mathcal{D}$, on a

$$F_X(b) = \lim_{\substack{a\to-\infty \\ a\notin\mathcal{D}}} \lim_{T\to\infty} \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-iat} - e^{-ibt}}{it} \varphi_X(t) dt$$

Or $\mathbb{R}\backslash\mathcal{D}$ est dense dans $\mathbb{R}$[6] et F_X est continue à droite. Ainsi, F_X est caractérisée par φ_X, donc comme F_X caractérise la loi de X, alors φ_X caractérise la loi de X.

5. puisque $\left|\frac{1}{2\pi}\frac{e^{-iat} - e^{-ibt}}{it} e^{ixt}\right| = \left|\frac{1}{2\pi} e^{-i(a+b)t/2} \frac{e^{i(b-a)t} - e^{-i(b-a)t}}{it} e^{ixt}\right| = \frac{1}{\pi}\left|\frac{e^{i(b-a)t} - e^{-i(b-a)t}}{2i(b-a)t/2} \frac{b-a}{2}\right| = \frac{1}{\pi}\left|\sin\left(\frac{(b-a)t}{2}\right)\frac{b-a}{2}\right| \leqslant \frac{1}{\pi}\frac{b-a}{2}$ donc l'intégrale sur $[-T,T]$ est majorée par $\frac{T(b-a)}{\pi}$ qui est intégrable sous la mesure $d\mathbb{P}_X$ puisque c'est une mesure de proba donc toutes les constantes sont intégrables.

6. puisque $\mathcal{D}$ est dénombrable

Étape 4 : *Résultat pour X une variable discrète*

Soit b un atome de la variable aléatoire X. On considère maintenant

$$\boxed{J_T(x) = \frac{1}{2T}\int_{-T}^{T} e^{-ibt}e^{ixt}dt}$$

On va utiliser la même technique pour J_T qu'avec K_T en utilisant le théorème de convergence dominée.

Pour $x = b$, on a $J_T(x) = 1$. Pour $x \neq b$, on a

$$J_T(x) = \frac{1}{2T}\left[\frac{e^{-i(b-x)t}}{-i(b-x)}\right]_{-T}^{T} = \operatorname{sinc}(T(x-b))$$

Ainsi $\lim\limits_{T\to+\infty} J_T(x) = \delta_b(x)$.

On utilise Fubini [7] pour intervertir de nouveaux les intégrales :

$$\begin{aligned}\int_R J_T(x)d\mathbb{P}_X(x) &= \int_R \frac{1}{2T}\int_{-T}^{T} e^{-ibt}e^{ixt}dtd\mathbb{P}_X(x)\\ &= \frac{1}{2T}\int_{-T}^{T} e^{-ibt}\int_R e^{ixt}d\mathbb{P}_X(x)dt\\ &= \frac{1}{2T}\int_{-T}^{T} e^{-ibt}\varphi_X(t)dt\end{aligned}$$

On utilise maintenant le théorème de convergence dominée puisque $|J_T(x)| = |\operatorname{sinc}(T(x-b))| \leqslant 1$ intégrable pour la mesure $d\mathbb{P}_X$, ainsi

$$\begin{aligned}\lim_{T\to\infty}\int_{\mathbb{R}} J_T d\mathbb{P}_X &= \int_{\mathbb{R}}\lim_{T\to\infty} J_T d\mathbb{P}_X\\ \lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T} e^{-ibt}\varphi_X(t)dt &= \int_{\mathbb{R}}\delta_b(x)d\mathbb{P}_X = \mathbb{P}(X=b)\end{aligned}$$

On a donc le résultat souhaité pour une variable aléatoire discrète.

Étape 5 : *Résultat pour X une variable réelle telle que $\varphi_X \in L^1$*

Comme $\varphi_X \in L^1$, la loi de X n'admet pas d'atome puisque

$$\left|\frac{1}{2T}\int_{-T}^{T}\varphi_X(t)e^{-ibt}dt\right| \leqslant \frac{1}{2T}\|\varphi_X\|_{L^1} \xrightarrow[T\to\infty]{} 0$$

et on vient de prouver que si y'a un atome $\mathbb{P}(X=b) = \lim\limits_{T\to\infty}\frac{1}{2T}\int_{-T}^{T} e^{-ibt}\varphi_X(t)dt$.

Par la première partie, on a donc

$$\mathbb{P}_X(]a,b[) = \lim_{T\to\infty}\frac{1}{2\pi}\int_{-T}^{T}\frac{e^{-iat}-e^{-ibt}}{it}\varphi_X(t)dt$$

On applique de nouveau le théorème de Fubini [8] afin d'obtenir

$$\frac{1}{2\pi}\int_{-T}^{T}\frac{e^{-iat}-e^{-ibt}}{it}\varphi_X(t)dt = \frac{1}{2\pi}\int_{-T}^{T}\left(\int_a^b e^{-ixt}dx\right)\varphi_X(t)dt$$

7. puisque $\left|\frac{1}{2T}e^{-ibt}e^{ixt}\right| \leqslant \frac{1}{2T}$, ainsi l'intégrale sur $[-T,T]$ est majorée par 1 qui est intégrable pour la mesure de proba $d\mathbb{P}_X$

8. puisque les segments d'intégration sont finis et que $\varphi_X \in L^1$

$$= \int_a^b \frac{1}{2\pi} \int_{-T}^{T} e^{-ixt} \varphi_X(t) dt dx$$

En introduisant naturellement $\boxed{g_T(x) = \frac{1}{2\pi} \int_{-T}^{T} e^{-ixt} \varphi_X(t) dt}$, on a donc

$$\mathbb{P}_X(]a,b[) = \lim_{T\to\infty} \int_a^b g_T(x) dx$$

Pour conclure, il faut donc intervertir l'intégration et la limite, on utilise de nouveau le théorème de convergence dominée puisque $|g_T(x)| \leqslant \frac{1}{2\pi} \|\varphi_X\|_{L^1}$ est intégrable sur $[a,b]$, ainsi

$$\begin{aligned} \mathbb{P}_X(]a,b[) &= \int_a^b \lim_{T\to\infty} g_T(x) dx \\ &= \int_a^b \left(\frac{1}{2\pi} \int_{\mathbb{R}} e^{-ixt} \varphi_X(t) dt \right) dx \end{aligned}$$

Ainsi on trouve bien $f_X(t) = \frac{1}{2\pi} \int_{\mathbb{R}} e^{-ixt} \varphi_X(t) dt$. □

Remarques :

On a montré que $\varphi_X \in L^1$ implique X est à densité, cependant la réciproque est fausse. Par exemple, une variable suivant une loi exponentielle, possède par définition une densité, or sa fonction caractéristique n'est pas intégrable sur $\mathbb{R}$

$$\varphi_X(t) = \int_0^{+\infty} e^{itx} e^{-x} dx = \frac{1}{t^2+1} + \frac{it}{t^2+1}$$

Et $|\varphi_X(t)| \underset{+\infty}{\sim} \frac{1}{|t|}$ non intégrable en $+\infty$.

Il faut savoir montrer que la fonction de répartition caractérise la loi en utilisant le lemme des classes monotones. (voir appendice)

Astuces de l'agrégatif :

Ce développement est très long, je m'arrête souvent après l'étape 4, je vais plus vite sur certains points en fonction de la leçon dans laquelle on est.

Durant le développement, j'explique juste à l'oral la limite de K_T, je n'écris pas la distinction de cas proprement, je donne juste l'expression de la limite.

J'écris les fonctions K_T et J_T sous ses formes là au début car je me souviens que quand on va intégrer sous $d\mathbb{P}_X$, il faut faire apparaitre la fonction caractéristique d'où le $+$ devant ixt dans l'exponentielle, et ensuite le reste est avec un $-$ dans l'argument des exponentielles.

Théorème des extrema liés

Leçons : 152 ; 159 ; 214 ; 219

Références : ROUVIÈRE, *Petit Guide du Calcul Différentiel* (p.372) et BECK–MALICK–PEYRÉ, *Objectif Agrégation* (p.20)

Prérequis :

- Théorème des sous-variétés
- Caractérisation du plan tangent [1]
- $(F^\perp)^\circ = F$ en dimension finie
- $A \subset B \implies B^\perp \subset A^\perp$

Introduction :

L'étude des extrema est très utile dans l'optimisation : chercher le maximum ou le minimum d'une quantité. Pour trouver ces extrema, on a des outils classiques comme l'étude des dérivées (en une ou plusieurs dimensions) première ou seconde. On va utiliser le théorème des extrema liés pour trouver des extrema sous contrainte. Par exemple, on pourra trouver la plus petite surface d'un parallélépipède rectangle à volume fixé [2].

Lemme 1. Soit $\varphi, \varphi_1, \dots, \varphi_k$ des formes linéaires sur $\mathbb{R}^n$, on a

$$\varphi \in \mathrm{Vect}(\varphi_1, \dots, \varphi_k) \iff \bigcap_{i=1}^{k} \ker \varphi_i \subset \ker \varphi$$

Démonstration du lemme. $\boxed{\implies}$ Soit $x \in \bigcap_{i=1}^{k} \ker \varphi_i$,

$$\forall i \in \{1, \dots, k\} \quad \varphi_i(x) = 0$$

1. Pour ce dont on a besoin ici, il suffit d'avoir $T_a\Gamma \subset \ker dF(a)$ et l'égalité des dimensions
égalité des dimensions : Le plan tangent est de dimension k (dimension de la sous-variété). Comme $dF(a)$ est linéaire de $\mathbb{R}^n$ dans $\mathbb{R}^{n-k}$, par le théorème du rang, on a

$$n = \dim \ker dF(a) + \ \mathrm{rg}\ dF(a)$$

Par surjectivité de $dF(a)$, puisque F est une submersion, on a

$$\mathrm{rg}\ dF(a) = \dim \mathbb{R}^{n-k} = n - k$$

inclusion : Soit $v = \gamma'(0)$, avec $\gamma :]-1, 1[\to \Gamma \in \mathcal{C}^1$ et $a = \gamma(0)$, on a pour tout $t \in]-1, 1[$,

$$F \circ \gamma(t) = 0$$

Donc on a $(F \circ \gamma)'(0) = 0$, ce qui est équivalent à avoir

$$dF(\gamma(0)).(\gamma'(0)) = 0$$

c'est à dire $dF(a).v = 0$, d'où $v \in \ker dF(a)$

2. ce qui peut servir pour optimiser le format des briques de lait par exemple

On a $\varphi \in \text{Vect}(\varphi_1, \dots, \varphi_k)$, donc

$$\varphi = \sum_{i=1}^{k} \lambda_i \varphi_i$$

Ainsi $\varphi(x) = 0$, donc $x \in \ker \varphi$. Ce qui prouve que

$$\bigcap_{i=1}^{k} \ker \varphi_i \subset \ker \varphi$$

$\boxed{\Longleftarrow}$ On suppose que $\bigcap_{i=1}^{k} \ker \varphi_i \subset \ker \varphi$, donc

$$\text{Vect}(\varphi_1, \dots, \varphi_k)^\circ \subset \text{Vect}(\varphi)^\circ \,[3]$$

Par dualité, on a

$$\text{Vect}(\varphi) = (\text{Vect}(\varphi)^\circ)^\perp \subset \text{Vect}(\varphi_1, \dots, \varphi_k)$$

car on est en dimension finie [4] et que le passage à l'orthogonal inverse le sens de l'inclusion.

Ainsi, comme $\varphi \in \text{Vect}(\varphi)$, on trouve le résultat souhaité

$$\varphi \in \text{Vect}(\varphi_1, \dots, \varphi_k)$$

□

Théorème 1 (Extrema liés)**.** Soit U un ouvert de $\mathbb{R}^n$, soient $f, g_1, \dots, g_{n-k} \in \mathcal{C}^1(U, \mathbb{R})$. On pose

$$\Gamma = \{x \in U, g_1(x) = g_2(x) = \cdots = g_{n-k}(x) = 0\}$$

Si $f_{|\Gamma}$ admet un minimum en a et la famille $\{dg_i(a)\}_{i=1}^{n-k}$ est libre, alors il existe des réels $\lambda_1, \dots, \lambda_{n-k} \in \mathbb{R}$ tels que

$$df(a) = \sum_{i=1}^{n-k} \lambda_i dg_i(a)$$

Démonstration du théorème. On remarque que Γ est une sous variété en a de dimension k comme zéro de la submersion

$$F : \begin{cases} U & \to & R^{n-k} \\ x & \mapsto & (g_1(x), \dots, g_{n-k}(x)) \end{cases}$$

On a bien $\Gamma = F^{-1}(\{0\})$ et $dF(a)$ est surjective [5]. Le plan tangent de Γ en a est

$$T_a\Gamma = \ker dF(a) = \bigcap_{i=1}^{n-k} \ker dg_i(a)$$

Soit $v \in T_a\Gamma$, il existe donc $\gamma :]-1; 1[\to \Gamma$ telle que $\gamma(0) = a$ et $\gamma'(0) = v$. Or a est un extremum de $f_{|\Gamma}$, donc 0 est un extremum de $f \circ \gamma$.

$$0 = (f \circ \gamma)'(0) = df(\gamma(0)).\gamma'(0) = df(a).v$$

3. Soit $x \in \text{Vect}(\varphi_1, \dots, \varphi_k)^\circ$, comme $\varphi_i \in \text{Vect}(\varphi_1, \dots, \varphi_k)$ pour tout i, on a donc $\varphi_i(x) = 0$, ainsi $\varphi(x) = 0$ (par hypothèse) et $\lambda\varphi(x) = 0$ donc pour tout $\psi \in \text{Vect}(\varphi)$, $\psi(x) = 0$, donc $x \in \text{Vect}(\varphi)^\circ$

4. ce qui nous donne bien $(F^\circ)^\perp = F$, on a l'inclusion $F \subset F^\circ)^\perp$ et l'égalité des dimensions

5. En effet, la matrice de $dF(a)$ est la matrice de taille $n \times (n-k)$ contenant les $dg_i(a)$ sur chaque ligne. Cette matrice est de rang $n-k$ car la famille $dg_i(a)$ est libre, donc comme $dF(a)$ va dans $\mathbb{R}^{n-k}$, on a la surjectivité de $dF(a)$ (car $\text{rg } dF(a) = n - k = \dim \mathbb{R}^{n-k}$)

Ainsi $v \in \ker df(a)$, on a donc

$$\bigcap_{i=1}^{n-k} \ker dg_i(a) \subset \ker df(a)$$

Par le lemme précédent, on a donc

$$df(a) \in \mathrm{Vect}(dg_1(a), \dots, dg_{n-k}(a))$$

Ce qui permet de conclure la preuve du théorème. □

Application 1 (Inégalité d'Hadamard)**.** Pour tout $x_1, x_2, \dots, x_n \in \mathbb{R}^n$,

$$\det(x_1, x_2, \dots, x_n) \leqslant \prod_{i=1}^{n} \|x_i\|_2$$

Démonstration de l'inégalité. On va utiliser le théorème des extrema liés [6] à la fonction det sur la sous variété

$$\Gamma = \{x_1, x_2, \dots, x_n \in \mathbb{R}^n, \forall i \in \{1, \dots, n\} g_i(x_1, \dots, x_n) = \|x_i\|_2^2 - 1 = 0\}$$

Il existe un maximum de det sur Γ, car Γ est compact [7] et det est continu.

On note $v = (v_1, \dots, v_n)$ un élement de Γ tel que $\det(v) = \det(v_1, \dots, v_n)$ soit maximal.

On a $\det(v) \neq 0$ car, pour une base orthonormale, on a un déterminant valant 1, donc v ne serait pas un maximum.

Ainsi la famille $v_1, \dots, v_n$ est libre, ce qui nous dit que la famille des formes linéaires $\langle v_i, . \rangle$ est libre, or $dg_i(v) = 2\langle v_i, . \rangle$ donc la famille $dg_1(v), \dots, dg_n(v)$ est libre.

On peut donc bien appliquer le théorème des extrema liés, il existe $(\lambda_i)_1^n$ tels que
Pour tout $h = (h_1, \dots, h_n) \in (\mathbb{R}^n)^n$

$$d\det(v).h = \sum_{i=1}^{n} \det(v_1, \dots, v_{i-1}, h_i, v_{i+1}, \dots, v_n) = \sum_{j=1}^{n} 2\lambda_j \langle v_j, h_j \rangle$$

Ainsi pour tout $j \in \{1, \dots, n\}$, $h = (h_1, \dots, h_n) = (0, \dots, 0, v_j, 0 \dots, 0)$ (où v_j est en place j) on trouve

$$\det(v) = 2\lambda_j \|v_j\|_2^2 = 2\lambda_j$$

car $v \in \Gamma$, d'où $\lambda_j \neq 0$ pour tout $j \in \{1, \dots, n\}$.

Puis pour tout $j \in \{1, \dots, n\}$, $k \in \{1, \dots, n\}$, $h = (h_1, \dots, h_n) = (0, \dots, 0, v_j, 0 \dots, 0)$ (où v_j est en place k) on trouve

$$0 = 2\lambda_k \langle v_k, v_j \rangle$$

Comme tous les λ_i sont non nuls, on a $\langle v_i, v_j \rangle = 0$ pour tout $i \neq j$.

Donc comme $v \in \Gamma$, $v_1, \dots, v_n$ est une famille orthonormale, donc de déterminant ± 1. Ainsi

$$|\det(v)| = 1$$

Pour tout $x_1, \dots, x_n \in \mathbb{R}^n$,

$$|\det(x_1, \dots, x_n)| = |\det(\frac{x_1}{\|x_1\|_2}, \dots, \frac{x_n}{\|x_n\|_2})| \prod_{i=1}^{n} \|x_i\|_2 \leqslant \prod_{i=1}^{n} \|x_i\|_2$$

car $\dfrac{x_1}{\|x_1\|_2}, \dots, \dfrac{x_n}{\|x_n\|_2} \in \Gamma$ et que le maximum de $|\det(\Gamma)|$ est 1.

□

6. ici on travaille dans $\mathbb{R}^{n^2}$, avec une sous variété de dimension $n^2 - n$ en utilisant $g_i(x_1, \dots, x_n) = \|x_i\|_2^2 - 1$
7. c'est la sphère unité donc un fermé borné en dimension finie

Remarques :

On peut prouver l'inégalité d'Hadamard sans avoir recours aux extrema liés (c'est fait dans le GOURDON *Algèbre* [GOU08a])

Astuces de l'agrégatif :

On utilise qu'un sens du lemme, donc on pourrait ne prouver qu'un sens mais bon c'est joli d'avoir une équivalence.

On peut montrer l'inégalité arithmético géométrique et l'inégalité d'Hölder avec le théorème des extrema liés.

Attention, pour la preuve du théorèmes des extrema liés, on utilise une sous-variété locale en a, donc il faudrait dire rigoureusement qu'il existe un petit voisinage de a sur lequel toutes les $dg_i(a)$ sont linéairement indépendantes (condition ouverte donc cela ne pose pas de problèmes) si on veut vraiment une sous variété, mais on n'en a pas besoin, on a seulement besoin d'un point lisse (voir Rouvière [ROU09]) mais je préfère parler de sous-variétés. Pour ne pas avoir de problème de sous-variété, on peut supposer que la famille $dg_i(x)$ est libre pour tout $x \in U$. Cependant, il faudrait trouver l'ouvert U pour l'application au déterminant. On peut en trouver un car la liberté est une condition ouverte (si $\det x \neq 0$, il existe un petit voisinage autour de x tel que $\det \neq 0$ sur le voisinage) mais cela revient à considérer une sous variété sur un petit ouvert (d'où ma volonté de parler de sous-variété car on s'y ramène facilement).

Nombres de zéros des solutions d'une équation différentielle

Leçons : 220 ; 221 ; 224

Références : QUÉFFELEC–ZUILY, *Analyse pour l'agrégation* (p.404)

Prérequis :

- le lemme de relèvement [ROU09, p.305]

Introduction :

On veut étudier l'équation différentielle

$$y'' + qy = 0 \tag{E}$$

On suppose que

- $q \in \mathcal{C}^1([a;+\infty[, \mathbb{R}_+^*)$
- $\displaystyle\int_a^{+\infty} \sqrt{q(u)}du = +\infty$
- $q'(x) = o\left(q^{3/2}(x)\right)$

Soit y une solution non nulle de (E), on cherche à obtenir un équivalent à l'infini de

$$N : x \mapsto \text{Card}(\{u \in [a,x], y(u) = 0\})$$

Théorème 1.

$$N(x) \underset{x\to+\infty}{\sim} \frac{1}{\pi}\int_a^x \sqrt{q(u)}du$$

Lemme 1. Soit y_1, y_2 deux fonctions $\mathcal{C}^1([a,+\infty[, \mathbb{R}_+)$ sans zéro commun.

Alors il existe $r, \theta : [a,+\infty[\to \mathbb{R}$ de classes $\mathcal{C}^1$ tels que $y_1(t) + iy_2(t) = r(t)e^{i\theta(t)}$ pour tout $t \in [a,+\infty[$ avec $r(t) > 0$.

Démonstration du théorème. **Étape 1 :** *Changement de variable*

On pose $\tau(x) = \displaystyle\int_a^x \sqrt{q(u)}du$.

La fonction τ est de classe $\mathcal{C}^1$ sur $[a,+\infty[$[1]. La fonction τ est même une bijection de $[a,+\infty[$ vers $[0,+\infty[$. En effet,

$$\forall x \geqslant a, \quad \tau'(x) = \sqrt{q(x)} > 0, \quad \tau(a) = 0 \text{ et } \tau(x) \xrightarrow[x\to+\infty]{} +\infty$$

On pose alors $Y = y \circ \tau^{-1}$. On a alors $\forall x > 0$,

$$y'(x) = Y'(\tau(x))\sqrt{q(x)} \text{ et } y''(x) = Y''(\tau(x))q(x) + Y'(\tau(x))\frac{q'(x)}{2\sqrt{q(x)}}$$

1. car $u \mapsto \sqrt{u}$ est continue

En injectant ces expressions dans l'équation (E), on a

$$0 = y'' + qy = q(x)Y''(\tau(x)) + Y'(\tau(x))\frac{q'(x)}{2\sqrt{q(x)}} + q(x)Y(\tau(x))$$

On pose maintenant $t = \tau(x)$ et $\varphi(t) = \dfrac{q'(x)}{2q^{3/2}(x)}$ [2] qui tend vers 0 quand t tend vers l'infini par hypothèse.

En divisant par $q(x)$, on a donc Y solution de

$$Y'' + \varphi Y' + Y = 0 \tag{E'}$$

Étape 2 : *Utilisation du lemme*

On veut montrer que Y et Y' n'ont pas de zero commun pour utiliser le lemme.

Par l'absurde, soit $t_0 \in [0, +\infty[$, telle que $Y(t_0) = Y'(t_0) = 0$. Alors le problème

$$\begin{cases} Y''(t) + \varphi(t)Y'(t) + Y(t) = 0 \\ Y'(t_0) = Y(t_0) = 0 \end{cases}$$

est un problème de Cauchy et par le théorème de Cauchy-Lipschitz, on a $Y(t) = 0$ pour tout $t \in [0, +\infty[$. Ainsi on aurait $y(u) = 0$ pour tout $u \in [a, +\infty[$, ce qui est absurde par hypothèse sur y.

Ainsi Y et Y' n'ont pas de zero commun. Donc par le lemme, il existe deux fonctions r et θ telles que

$$Y = r\sin(\theta) \text{ et } Y' = r\cos(\theta)$$

Étape 3 : *Équivalent de $\theta(t)$*

On a le système [3]

$$Y' = r'\sin\theta + r\theta'\cos\theta = r\cos\theta \tag{i}$$
$$Y'' = r'\cos\theta - r\theta'\sin\theta = -\varphi r\cos\theta - r\sin\theta \tag{ii}$$

On veut éliminer les r', donc on multiplie (i) par $\cos\theta$ et (ii) par $\sin\theta$, puis on fait la soustraction des deux expressions. On obtient alors

$$\cancel{r'\sin\theta\cos\theta} + r\theta'\cos^2\theta - \cancel{r'\sin\theta\cos\theta} + r\theta'\sin^2\theta = r\cos^2\theta + \varphi r\cos\theta\sin\theta + r\sin^2\theta$$

Ainsi, on trouve

$$r\theta' = r + \varphi r\sin\theta\cos\theta$$ [4]

Puis comme $r > 0$ pour tout t, on a

$$\theta' = 1 + \varphi\sin\theta\cos\theta$$

Donc

$$|\theta'(t) - 1| \leqslant |\varphi(t)| \xrightarrow[t\to+\infty]{} 0 \text{ par hypothèse sur } \varphi$$

D'où $\theta'(t) \underset{\infty}{\sim} 1$ puis $\theta(t) \underset{\infty}{\sim} t$ en intégrant.

Comme $\theta'(t)$ tend vers 1 quand t tend vers $+\infty$, il existe t_0 telle que $\theta' > 0$ sur $[t_0, +\infty[$, ainsi θ est une bijection sur $[t_0, +\infty[$.

2. où $x = \tau^{-1}(t)$

3. pour trouver (i), on dérive l'expression Y du lemme pour avoir Y' qui est égale à l'expression Y' du lemme, puis pour (ii), on dérive l'expression Y' du lemme pour avoir Y'' qui est égale à $-\varphi Y' - Y$ car Y vérifie l'équation (E')

4. car $\cos^2\theta + \sin^2\theta = 1$

Étape 4 : *Étude asymptotique*

On pose l'ensemble

$$M(t) = \#\{u \in [0,t], \quad Y(u) = 0\}$$

Par l'absurde, on va montrer que $M(t_0) < +\infty$. Sinon l'ensemble des zéros de Y dans $[0,t_0]$ aurait un point d'accumulation u. Soit (u_n) une suite de zéros de Y qui tend vers u. Alors $\dfrac{Y(u_n)-Y(u)}{u_n-u} \xrightarrow[n\to\infty]{} Y'(u)$. Or $Y(u_n)-Y(u)=0$ pour tout n, donc $Y'(u)=0$. Ainsi $Y(u)=Y'(u)=0$ or c'est impossible comme on l'a prouvé au début de l'étape 2.

Ainsi $M(t) \underset{t\to\infty}{\sim} \#\{u \in [t_0,t], \quad Y(u)=0\}$ car $M(t_0) < +\infty$.

$$\begin{aligned}
M(t) &\underset{t\to\infty}{\sim} \#\{u \in [t_0,t], \quad Y(u)=0\} \\
&\underset{t\to\infty}{\sim} \#\{u \in [t_0,t], \quad r(u)\sin(\theta(u))=0\} \\
&\underset{t\to\infty}{\sim} \#\{u \in [t_0,t], \quad \sin(\theta(u))=0\} \\
&\underset{t\to\infty}{\sim} \#\{v \in [\theta(t_0),\theta(t)], \quad \sin(v)=0\} \\
&\underset{t\to\infty}{\sim} \#\{k \in \mathbb{Z}, \quad \theta(t_0) \leqslant k\pi \leqslant \theta(t)\} \\
&\underset{t\to\infty}{\sim} \frac{\theta(t)-\theta(t_0)}{\pi} \\
&\underset{t\to\infty}{\sim} \frac{\theta(t)}{\pi} \text{ car } \frac{\theta(t_0)}{\pi} \text{ est fini} \\
&\underset{t\to\infty}{\sim} \frac{t}{\pi} \text{ car } \theta(t) \sim t
\end{aligned}$$

Or on remarque que $N(x) = M(\tau(x))$[5]. Donc

$$\begin{aligned}
N(x) &= M(\tau(x)) \\
&\underset{t\to\infty}{\sim} \frac{\tau(x)}{\pi} \\
&\underset{t\to\infty}{\sim} \frac{1}{\pi}\int_a^x \sqrt{q(u)}du
\end{aligned}$$

Ce qui conclut la preuve du théorème. □

Remarques :

Le changement de variable est là pour se rapprocher de l'équation différentielle $y''+y=0$ que l'on sait bien résoudre. C'est pourquoi on demande à ce que la fonction φ tende vers 0.

Astuces de l'agrégatif :

Je ne mettais pas tout le temps les variables mais il faut bien comprendre que $y, Y, q, \tau, \varphi, \theta, r$ sont des fonctions et t, x, u sont des variables.

Je mettais le lemme dans le plan sans le réécrire au tableau. Je ne faisais pas la preuve du lemme pendant le développement par manque de temps. La preuve du théorème est suffisamment longue comme ça. Je mets ci-dessous la preuve du lemme de relèvement.

Démonstration du lemme. Comme y_1 et y_2 ne s'annulent pas en même temps, on peut écrire

$$r(t) = \sqrt{y_1(t)^2+y_2(t)^2} > 0 \quad \text{et} \quad u(t) = \frac{y_1(t)+iy_2(t)}{r(t)}.$$

5. il suffit de se souvenir que $y(x) = Y(\tau(x))$

On a donc

$$r \in \mathcal{C}^1([a,+\infty[,\mathbb{R}_+) \quad \text{et} \quad u \in \mathcal{C}^1([a,+\infty[,\mathbb{S}^1)$$

où $\mathbb{S}^1$ est le cercle unité de $\mathbb{C}$.

On veut maintenant trouver $\theta : [a,+\infty[\to \mathbb{R}$ telle que $u(t) = e^{i\theta(t)}$ pour tout $t \in [a,+\infty[$.

Analyse : On a $u'(t) = i\theta'(t)e^{i\theta(t)}$, d'où $\theta'(t) = -i\dfrac{u'(t)}{u(t)}$ existe bien car $u(t) \neq 0$ pour tout $t \in [a,+\infty[$.

Soit $\theta_0 \in \mathbb{R}$ tel que $u(a) = e^{i\theta_0}$. On pose

$$\theta(t) = \theta_0 - i\int_a^t \frac{u'(\sigma)}{u(\sigma)}d\sigma.$$

Synthèse : $u \in \mathbb{S}^1$ donc $u\bar{u} = 1$. On dérive $u'(t)\bar{u}(t) + u(t)\bar{u}'(t) = 0$. D'où

$$\frac{u'(t)}{u(t)} = -\frac{\bar{u}'(t)}{\bar{u}(t)}$$

Donc $\dfrac{u'(t)}{u(t)}$ est imaginaire pur.

Ainsi $\theta(t) \in \mathbb{R}$, pour tout $t \in [0,+\infty[$.

De plus,

$$\begin{aligned}(ue^{-i\theta})' &= u'(t)e^{-i\theta(t)} - i\theta'(t)u(t)e^{-i\theta(t)} \\ &= \left(u'(t) - i \times -i\frac{u'(t)}{u(t)}u(t)\right)e^{-i\theta(t)} = 0\end{aligned}$$

Donc $ue^{-i\theta}$ est constante et $u(a) = e^{i\theta_0} = e^{i\theta(a)}$. D'où $u(t) = e^{i\theta(t)}$ pour tout $t \in [a,+\infty[$ avec θ de classe $\mathcal{C}^1$.

Ainsi $y_1(t) + iy_2(t) = r(t)e^{i\theta(t)}$ pour tout $t \in [a,+\infty[$.

□

Morphismes d'algèbre de $\mathcal{C}(K, \mathbb{R})$ sur $\mathbb{R}$

Leçons : 159 ; 203

Références : FRANCINOU–GIANELLA–NICOLAS, *Oraux X-ENS* (je n'ai pas trouvé dans lequel c'était fait, si tu trouves, dis le moi s'il te plait)

Prérequis :

- la définition d'un morphisme d'algèbre [1]
- la propriété de Borel-Lebesgue
- la définition d'un idéal propre [2]

Théorème 1. Soit K un espace métrique compact. Les morphismes d'algèbre de $\mathcal{C}(K, \mathbb{R})$ dans $\mathbb{R}$ sont exactement les morphismes d'algèbre de la forme $f \mapsto f(s)$ pour $s \in K$ et l'application nulle.

Démonstration. Soit φ un morphisme d'algèbre de $\mathcal{C}(K, \mathbb{R})$ dans R non nul. On sait que $\ker(\varphi)$ est un idéal propre de $\mathcal{C}(K, \mathbb{R})$ par le morphisme d'anneau φ et un hyperplan de $\mathcal{C}(K, \mathbb{R})$ en utilisant l'aspect linéaire du morphisme d'algèbre.

Lemme 1. L'ensemble des formes linéaires sur $\mathcal{C}(K, \mathbb{R})$ nulles sur un hyperplan H forme une droite vectorielle du dual $\mathcal{C}(K, \mathbb{R})^*$.

Démonstration du lemme. Soit S un supplémentaire de H et f_0 un élément non nul de S. On a alors

$$\mathcal{C}(K, \mathbb{R}) = H \oplus \mathbb{R} f_0$$

Soit ψ_0 une forme linéaire de $\mathcal{C}(K, \mathbb{R})$ nulle sur H telle que $\psi_0(f_0) \neq 0$. Pour tout ψ forme linéaire de $\mathcal{C}(K, \mathbb{R})$ nulle sur H, on pose

$$\lambda = \frac{\psi(f_0)}{\psi_0(f_0)}.$$

On considère la forme linéaire

$$\phi = \psi - \lambda \psi_0$$

Or ϕ est nulle sur H puisque ψ et ψ_0 le sont. De plus $\phi(f_0) = \psi(f_0) - \frac{\psi(f_0)}{\psi_0(f_0)} \psi_0(f_0) = 0$. Ainsi ϕ est nulle partout, ce qui implique $\psi = \lambda \psi_0$. Ainsi ψ appartient à la droite vectorielle portée par ψ_0.

Réciproquement, les éléments de $\mathbb{R}\psi_0$ sont des formes linéaires de $\mathcal{C}(K, \mathbb{R})$ nulles sur l'hyperplan H. □

Ainsi l'ensemble des formes linéaires nulles sur $\ker(\varphi)$ est $\mathbb{R}\varphi$ car φ est non nul.

Soit $s \in K$, on pose

$$I_s := \{f \in \mathcal{C}(K, \mathbb{R}), f(s) = 0\}$$

On remarque que I_s est un idéal propre de $C(K, \mathbb{R})$.

(Pour tout $g \in \mathcal{C}(K, \mathbb{R})$ et tout $f \in I_s$, $fg(s) = f(s)g(s) = 0$ car $f(s) = 0$, d'où $fg \in I_s$, et la fonction identiquement égale à 1 qui est bien continue n'est pas dans I_s donc I_s est propre.)

1. morphisme d'anneau et application linéaire d'une algèbre vers une autre algèbre
2. idéal d'un anneau A qui n'est pas A tout entier

On veut prouver que tout idéal propre J de $C(K,\mathbb{R})$ est inclus dans I_s pour un certain $s \in K$. Par l'absurde, on suppose que J n'est dans aucun I_s, il existe donc pour tout $s \in K$, un $f_s \in J$ tel que $f_s(s) \neq 0$.

Or les f_s sont continues donc il existe $r_s > 0$ tel que f_s soit non nulle sur $B(s, r_s)$. On utilise maintenant le caractère compact de K par la propriété de Borel Lebesgue.

$$K \subset \bigcup_{s \in K} B(s, r_s)$$

Donc il existe $s_1, \dots, s_n$ tels que

$$K \subset \bigcup_{i=1}^{n} B(s_i, r_{s_i})$$

On a $f_{s_i} \in J$, donc $f_{s_i}^2 \in J$ et $f_{s_i}^2 > 0$ sur $B(s_i, r_{s_i})$ pour tout $i \in \{1, \dots, n\}$. On considère la fonction

$$f = \sum_{i=1}^{n} f_{s_i}^2 \in J$$

On a donc $f > 0$ sur K, ainsi $1 = \frac{1}{f}.f \in J$ par structure d'idéal. Donc $J = \mathcal{C}(K,\mathbb{R})$, ce qui est absurde puisque J est supposé propre.

Or $\ker(\varphi)$ est un idéal propre, donc il existe un $s \in K$ tel que $\ker(\varphi) \subset I_s$. Or la forme linéaire $\alpha_s : f \mapsto f(s)$ est nulle sur $\ker(\varphi)$, donc il existe λ tel que

$$\alpha_s = \lambda\varphi$$

Autrement dit,

$$\forall f \in \mathcal{C}(K,\mathbb{R}) \quad f(s) = \lambda\varphi(f)$$

Soit $f \in \mathcal{C}(K,\mathbb{R})$ telle que $f(s) \neq 0$. On a

$$f(s)^2 = \alpha_s(f)^2 = \alpha_s(f^2) = \lambda\varphi(f^2) = \lambda(\varphi(f))^2$$

et

$$\lambda f(s)^2 = \lambda^2(\varphi(f))^2 = (\lambda\varphi(f))^2 = f(s)^2$$

Donc $\lambda = 1$, ainsi $\varphi = \alpha_s$, c'est-à-dire φ est de la forme $f \mapsto f(s)$.

Réciproquement, $f \mapsto f(s)$ et l'application nulle sont des morphismes d'algèbre de $\mathcal{C}(K,\mathbb{R})$ vers $\mathbb{R}$. □

Remarques :

Il faut bien faire attention aux objets que l'on manipule, il ne faut pas confondre les objets $f(s)$ et α_s.

Il faut savoir ce qu'est un morphisme d'algèbre (morphisme d'anneau et application linéaire d'une algèbre vers une autre algèbre), ici on a $(\mathcal{C}(K,\mathbb{R}), +, \times, .)$ et $(\mathbb{R}, +, \times, .)$ deux $\mathbb{R}$-algèbres. On a $(f \times g)(s) = f(s) \times g(s)$.

Théorème Central Limite

Leçons : 260 ; 264

Références : QUEFFÉLEC–ZUILY, *Analyse pour l'agrégation* (p.540)

Prérequis :

- la convergence en loi
- le DL de φ_X pour X variable centrée réduite

Introduction :

Le Théorème Central Limite est un théorème de convergence en loi très important en probabilité et en statistique, il permet notamment de montrer des intervalles de confiance. Son plus gros point fort est que ses hypothèses sont très générales, il est valable pour n'importe quelle distribution (discrète ou continue) de variables aléatoires identiquement distribuées indépendantes L^2.

Théorème 1. Soit X_i des variables aléatoires réelles indépendantes identiquement distribuées (v.a.r.i.i.d.) dans L^2 avec $\mathbb{E}(X_1) = m$ et $\mathrm{Var}(X_1) = \sigma^2$. Alors on a

$$\frac{\sum_{i=1}^{n} X_i - m}{\sqrt{n}\sigma} \overset{\mathcal{L}oi}{\Longrightarrow} Z$$

où Z est une v.a.r. qui suit une loi normale centrée réduite ($\mathcal{N}(0,1)$)

On va utiliser les deux lemmes suivants :

Lemme 1. Soit $Z \sim \mathcal{N}(0,1)$. Alors on a

$$\varphi_Z(t) = e^{-\frac{t^2}{2}}$$

Lemme 2. Si la suite $(z_n) \in \mathbb{C}^{\mathbb{N}}$ converge vers un complexe z, alors

$$\left(1 + \frac{z_n}{n}\right)^n \xrightarrow[n\to\infty]{} e^z$$

Démonstration du théorème. On peut supposer que les variables X_i sont centrées réduites (quitte à prendre $\dfrac{X_i - m}{\sigma}$)

On veut donc prouver que

$$\frac{\sum_i X_i}{\sqrt{n}} \overset{\mathcal{L}oi}{\Longrightarrow} Z \sim \mathcal{N}(0,1)$$

On note $S_n = \sum_{i=1}^{n} X_i$.

Pour prouver la convergence en loi, il suffit de prouver la convergence simple de la fonction caractéristique. On veut donc prouver que

$$\varphi_{\frac{S_n}{\sqrt{n}}}(t) \xrightarrow[n\to+\infty]{} f(t) \quad \forall t \in \mathbb{R}$$

où f est la fonction caractéristique d'une loi $\mathcal{N}(0,1)$.

Dans un premier temps, étudions $\varphi_{\frac{S_n}{\sqrt{n}}}$.

On a

$$\varphi_{\frac{S_n}{\sqrt{n}}}(t) = \varphi_{S_n}\left(\frac{t}{\sqrt{n}}\right) = \left(\varphi_{X_1}\left(\frac{t}{\sqrt{n}}\right)\right)^n \text{ [1]}$$

Or, comme $\varphi_{X_1} \in \mathcal{C}^2(\mathbb{R})$ [2], par la formule de Taylor Young, il existe ε_n qui tend vers 0 quand n tend vers 0 tel que

$$\varphi_{X_1}\left(\frac{t}{\sqrt{n}}\right) = \varphi_{X_1}(0) + \frac{t}{\sqrt{n}}\varphi'_{X_1}(0) + \frac{t^2}{2n}\varphi''_{X_1}(0) + \frac{\varepsilon_n}{n}$$

On remarque que

$$\begin{aligned}
&\varphi_{X_1}(0) = \mathbb{E}(e^{i\times 0\times X_1}) = 1\\
&\varphi'_{X_1}(0) = \mathbb{E}(iX_1) = i\mathbb{E}(X_1) = 0 \text{ car la variable est centrée}\\
&\varphi''_{X_1}(0) = \mathbb{E}(-X_1^2) = -\mathrm{Var}(X_1) + \underbrace{\mathbb{E}(X_1)^2}_{=0} = -1 \text{ car la variable est réduite}
\end{aligned}$$

On a donc

$$\varphi_{\frac{S_n}{\sqrt{n}}}(t) = \left(1 - \frac{t^2}{2n} + \frac{\varepsilon_n}{n}\right)^n \xrightarrow[n\to+\infty]{} e^{-\frac{t^2}{2}}$$

On a utilisé le lemme 2 avec $z_n = -\dfrac{t^2}{2} + \varepsilon_n$ qui tend vers $z = -\dfrac{t^2}{2}$.

Enfin, par le lemme 1, on a $\varphi_Z(t) = e^{-\frac{t^2}{2}}$.

Donc

$$\frac{S_n}{\sqrt{n}} \overset{\mathcal{L}oi}{\Longrightarrow} Z \sim \mathcal{N}(0,1)$$

Ce qui conclut la preuve du théorème. □

Lemme 1. Soit $Z \sim \mathcal{N}(0,1)$. Alors on a

$$\varphi_Z(t) = e^{-\frac{t^2}{2}}$$

Démonstration du lemme 1. Pour tout $t \in \mathbb{R}$,

$$\varphi_Z(t) = \mathbb{E}(e^{itZ}) = \frac{1}{\sqrt{2\pi}}\int_{\mathbb{R}} e^{itx}e^{-\frac{x^2}{2}}dx$$

On pose la fonction

$$G(z) = \frac{1}{\sqrt{2\pi}}\int_{\mathbb{R}} \underbrace{e^{zx}e^{-\frac{x^2}{2}}}_{f(z,x)}dx$$

On va montrer que G est holomorphe sur $\mathbb{C}$ en utilisant le théorème d'holomorphie sous l'intégrale sur le disque $D(0,R)$ pour tout $R > 0$.

1. puisque $\varphi_{\frac{S_n}{\sqrt{n}}}(t) = \mathbb{E}\left(e^{it\frac{S_n}{\sqrt{n}}}\right) = \mathbb{E}\left(e^{i\frac{t}{\sqrt{n}}S_n}\right) = \mathbb{E}\left(e^{i\frac{t}{\sqrt{n}}\sum_k X_k}\right) = \mathbb{E}\left(\prod_{k=1}^n e^{i\frac{t}{\sqrt{n}}X_k}\right) = \prod_k \mathbb{E}\left(e^{i\frac{t}{\sqrt{n}}X_k}\right) = \prod_k \mathbb{E}\left(e^{i\frac{t}{\sqrt{n}}X_1}\right) = \prod_{k=1}^n \varphi_{X_1}\left(\frac{t}{\sqrt{n}}\right) = \left(\varphi_{X_1}\left(\frac{t}{\sqrt{n}}\right)\right)^n$

2. puisque X_1 est dans L^2, on peut appliquer le théorème de dérivation sous le signe intégral

- $\forall z \in D(0,R), \quad x \mapsto f(z,x)$ est intégrable sur $\mathbb{R}$.
- $\forall x \in \mathbb{R}, \quad z \mapsto f(z,x)$ est holomorphe sur $D(0,R)$.
- $\forall x \in \mathbb{R}, \forall z \in D(0,R), \quad |f(z,x)| \leqslant e^{Rx}e^{-\frac{x^2}{2}}$ intégrable sur $\mathbb{R}$.

Donc $G(z) = \dfrac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} e^{zx}e^{-\frac{x^2}{2}}dx$ est holomorphe sur $\mathbb{C}$.
Or, pour tout $u \in \mathbb{R}$,

$$\begin{aligned} G(u) &= \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} e^{ux}e^{-\frac{x^2}{2}}dx \\ &= \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} e^{-\frac{(x-u)^2}{2}}e^{\frac{u^2}{2}}dx \\ &= e^{\frac{u^2}{2}} \end{aligned}$$

En utilisant le fait que $\dfrac{1}{\sqrt{2\pi}} \displaystyle\int_{\mathbb{R}} e^{-\frac{(x-u)^2}{2}}dx = 1$ car c'est l'intégrale de la densité d'une loi normale réduite d'espérance u.

On a alors que $z \mapsto e^{\frac{z^2}{2}}$ et G sont holomorphes et coïncident sur $\mathbb{R}$. Ainsi elles coïncident sur $\mathbb{C}$ par le théorème de prolongement analytique.

On peut alors écrire

$$\varphi_Z(t) = G(it) = e^{\frac{(it)^2}{2}} = e^{-\frac{t^2}{2}}$$

Ce qui achève la preuve du lemme 1. □

Lemme 2. Si la suite $(z_n) \in \mathbb{C}^{\mathbb{N}}$ converge vers un complexe z, alors

$$\left(1 + \frac{z_n}{n}\right)^n \xrightarrow[n\to\infty]{} e^z$$

Démonstration du lemme 2.

$$e^{z_n} - \left(1 + \frac{z_n}{n}\right)^n = \sum_{k=0}^{+\infty} a_{k,n} z_n^k$$

où $a_{k,n} = \begin{cases} \dfrac{1}{k!}\left(1 - \dfrac{n(n-1)\dots(n-k+1)}{n^k}\right) & \text{si } k \leqslant n \\ \dfrac{1}{k!} & \text{sinon} \end{cases}$

On a donc $a_{k,n} \geqslant 0$ pour tout $k, n \in \mathbb{N}$.
D'où

$$\begin{aligned} \left|e^{z_n} - \left(1 + \frac{z_n}{n}\right)^n\right| &\leqslant \sum_{k=0}^{+\infty} a_{k,n}|z_n|^k \text{ car } a_{k,n} \geqslant 0 \\ &\leqslant e^{|z_n|} - \left(1 + \frac{|z_n|}{n}\right)^n \\ &\leqslant e^{|z_n|} - \exp\left(n \ln\left(1 + \frac{|z_n|}{n}\right)\right) \\ &\leqslant e^{|z_n|} - \exp\left(n\left(\frac{|z_n|}{n} - \frac{|z_n|^2}{2n^2}\right)\right) \text{ car } \ln(1+x) \geqslant x - \frac{x^2}{2} \text{ pour } x > 0 \\ &\leqslant e^{|z_n|} - \exp\left(|z_n| - \frac{|z_n|^2}{2n}\right) \end{aligned}$$

$$\leqslant e^{|z_n|}\left(1-\exp\left(-\frac{|z_n|^2}{2n}\right)\right)$$
$$\leqslant e^{|z_n|}\frac{|z_n|^2}{2n} \text{ en utilisant l'inégalité } 1-e^{-x}\leqslant x \quad \forall x\in\mathbb{R}$$

D'où

$$\left|e^z-\left(1+\frac{z_n}{n}\right)^n\right| \leqslant \underbrace{|e^z-e^{z_n}|}_{\xrightarrow[n\to\infty]{}0} + \underbrace{e^{|z_n|}}_{\xrightarrow[n\to\infty]{}e^z}\ \underbrace{\frac{|z_n|^2}{2n}}_{\xrightarrow[n\to\infty]{}0}$$

Ce qui conclut la preuve du lemme 2. □

Remarques :

Historiquement, on a prouvé le théorème de Moivre-Laplace, qui est le théorème central limite pour des variables suivant des lois de Bernoulli.

Astuces de l'agrégatif :

Il faut faire attention à son insertion dans la leçon 264, puisque c'est un théorème qui sort du cadre des seules variables discrètes. Cependant, c'est une généralisation du théorème de Moivre-Laplace, et c'est tellement utilisé même avec des variables aléatoires discrètes que personnellement je trouve qu'il a toute sa place dans cette leçon.

Générateurs de $\mathrm{SL}_2(\mathbb{Z})$

Leçons : 108 ; 182 ; 183

Références : FRANCINOU–GIANELLA–NICOLAS, *Oraux X-ENS Algèbre 1* (p.55)

Prérequis :

- Action de groupe
- Groupe engendré par des éléments
- Compréhension du repère complexe et des transformations comme la rotation et la translation

Notations :

- $\mathrm{SL}_2(\mathbb{Z})$ désigne l'ensemble des matrices 2×2 à coefficients entiers de déterminant égal à 1.
- $\Re(z)$ désigne la partie réelle de z où $z \in \mathbb{C}$.
- $\Im(z)$ désigne la partie imaginaire de z où $z \in \mathbb{C}$.

Introduction :

On va montrer que le groupe $\mathrm{SL}_2(\mathbb{Z})$ est engendré par seulement deux matrices. Ces deux matrices correspondent à des transformations du plan complexe quand on fait agir $\mathrm{SL}_2(\mathbb{Z})$ sur une partie du plan complexe.

Théorème 1. Le groupe $\mathrm{SL}_2(\mathbb{Z})$ est engendré par $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Démonstration. On note $\mathbb{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$ le demi plan de Poincaré.

On fait agir $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$.

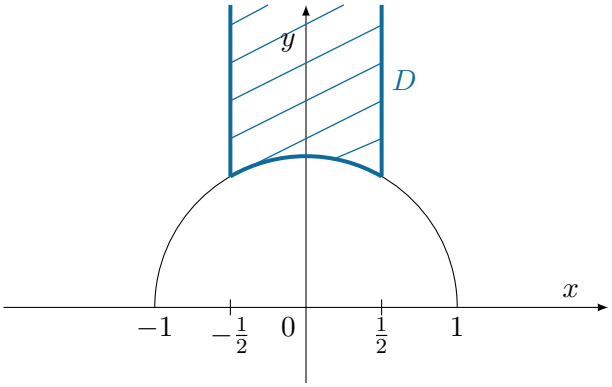
$$\forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \forall z \in \mathbb{H}, A \cdot z = \frac{az+b}{cz+d}$$

Il faut prouver que $\Im(A \cdot z) > 0$.

$$\begin{aligned} \Im(A \cdot z) &= \Im\left(\frac{az+b}{cz+d}\right) \\ &= \Im\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) \\ &= \Im\left(\frac{acz\bar{z}+bd+bc\bar{z}+adz}{|cz+d|^2}\right) \\ &= \underbrace{(ad-bc)}_{=1\,[1]} \frac{\Im(z)}{|cz+d|^2} > 0 \end{aligned}$$

On note $G = \langle S, T\rangle$ le sous groupe de $\mathrm{SL}_2(\mathbb{Z})$ engendré par les matrices S et T et

$$D = \left\{ z \in \mathbb{H},\ |z| \geqslant 1,\ |\Re(z)| \leqslant \frac{1}{2} \right\}$$



On veut montrer que $\mathrm{SL}_2(\mathbb{Z}) = G$.

Lemme 1. Toute orbite de l'action restreinte à G rencontre l'ensemble D.

Démonstration. Autrement dit, on veut prouver que pour tout $z \in \mathbb{H}$, il existe une matrice $A \in G$ telle que $A \cdot z \in D$.

Soit $z \in \mathbb{H}$. On va montrer que le nombre de couple $(c, d) \in \mathbb{Z}^2$ tel que $|cz + d| \leqslant 1$ est fini.

$$|c|\Im(z) \leqslant |\Im(cz + d)| \leqslant |cz + d| \leqslant 1$$

Ainsi

$$|c| \leqslant \frac{1}{\Im(z)} \text{ et } |d| \leqslant 1 - |z||c|$$

Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, on a vu que $\Im(A \cdot z) = \dfrac{\Im(z)}{|cz + d|^2}$, il y a donc un nombre fini de couples (c, d) tels que

$$\Im(A \cdot z) \geqslant \Im(z)$$

II existe donc une matrice $A_1 \in G$ telle que $\Im(A_1 \cdot z)$ soit maximal.

On note $z_1 = A_1 \cdot z$.

Le but maintenant est de translater le point z_1 pour arriver dans la bande de l'ensemble D.

On sait que

$$\forall u \in \mathbb{C}, \quad T \cdot u = u + 1$$

On pose $n = \lfloor \Re(z_1) + \frac{1}{2} \rfloor$ afin d'avoir

$$-\frac{1}{2} \leqslant \Re(z_1) - n = \Re(z_1 - n) = \Re(T^{-n} \cdot z_1) \leqslant \frac{1}{2}$$

et on a $\Im(T^{-n} \cdot z_1 = \Im(z_1)$.

On pose donc $z_2 = T^{-n} \cdot z_1$.

On veut montrer que $|z_2| \geqslant 1$. Supposons que l'on ait $|z_2| < 1$, on aurait alors

$$\begin{aligned} \Im(S \cdot z_2) &= \Im\left(-\frac{1}{z_2}\right) \\ &= \Im\left(-\frac{\bar{z_2}}{|z_2|^2}\right) \end{aligned}$$

1. car $A \in \mathrm{SL}_2(\mathbb{Z})$ donc $\det A = ad - bc = 1$

$$= \frac{\Im(z_2)}{|z_2|^2}$$
$$> \Im(z_2)$$

Ce qui est absurde par maximalité de $\Im(z_1) = \Im(z_2)$.

Ainsi $z_2 \in D$ et on a obtenu z_2 à partir de z qu'en faisant agir des matrices de G. Ce qui conclut la preuve du lemme. □

Pour $z \in D$ fixé, on cherche à caractériser les matrices $A \in \mathrm{SL}_2(\mathbb{Z})$ telles que $A \cdot z \in D$.

Lemme 2. Soient $z \in D$ et $A \in \mathrm{SL}_2(\mathbb{Z})$ telle que $A \cdot z \in D$. Alors la matrice A est dans G.

Démonstration. On écrit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On peut se restreindre à $|cz + d| \leqslant 1$, autrement dit $\Im(A \cdot z) \geqslant \Im(z)$. En effet, supposons que $\Im(A \cdot z) < \Im(z) = \Im(A^{-1} \cdot (A \cdot z))$, on pourrait faire l'étude sur A^{-1}, et si A^{-1} est dans G alors A le sera aussi car G est un groupe.

Dans le lemme précédent, on a vu que si $|cz + d| \leqslant 1$, on avait alors

$$|c| \leqslant \frac{1}{\Im(z)} \leqslant \frac{2}{\sqrt{3}} < 2$$

car $z \in D$ donc sa partie imaginaire est supérieure à $\frac{\sqrt{3}}{2}$.

Comme $c \in \mathbb{Z}$, on peut faire une distinction de cas sur $c \in \{-1, 0, 1\}$.

☞ Si $\underline{c = 0}$, on a alors que $\det(A) = ad = 1$. Quitte à changer A en $-A$ (ce qui ne change pas la valeur de $A \cdot z$), on peut supposer $a = d = 1$. On a donc

$$A \cdot z = z + b$$

On sait que $z \in D$ et $A \cdot z \in D$, donc

— Si $\underline{|\Re(z)| < \frac{1}{2}}$, on a forcément $b = 0$. Donc $A = \pm I_2 \in G$.

— Si $\underline{\Re(z) = \frac{1}{2}}$, on a $b = 0$ ou $b = -1$. Donc $A = \pm I_2 \in G$ ou $A = \pm T^{-1} \in G$.

— Si $\underline{\Re(z) = -\frac{1}{2}}$, on a $b = 0$ ou $b = 1$. Donc $A = \pm I_2 \in G$ ou $A = \pm T \in G$.

☞ Si $\underline{c = 1}$, on a alors $|z + d| \leqslant 1$. Comme $z \in D$ et $A \cdot z \in D$, il n'y a que 3 choix possibles pour d.

(i) $d = 0$

(ii) $d = 1$ et $z = j$

(iii) $d = -1$ et $z = j + 1$

(i) Si $d = 0$, on a alors $\det(A) = -b = 1$ et $A \cdot z = a - \dfrac{1}{z}$. L'hypothèse $|cz + d| \leqslant 1$ se traduit par $|z| \leqslant 1$ et puisque $z \in D$, on a $|z| = z\bar{z} = 1$. On a donc

$$A \cdot z = a - \bar{z}$$

Comme il faut que $A \cdot z$ soit dans D et que $z \in D$, on a trois cas possibles pour a [2] :

— Si $a = 0$, on a $A = S \in G$.

— Si $a = 1$ (et $z = j$), on a $A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = TS \in G$.

2. en effet, comme a est réel (même entier), on ne peut pas avoir $a > 1$

— Si $a = -1$ (et $z = 1 + j$), on a $A = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = (ST)^2 \in G$.

(ii) Si $d = 1$ et $z = j$, on a alors $\det(A) = a - b = 1$, d'où $b = a - 1$. Ainsi

$$A \cdot z = \frac{aj + a - 1}{j + 1} = a + j$$

qui n'appartient à D seulement si $a = 0$ ou $a = 1$ ce qui donne les matrices

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = ST \in G \quad \text{ou} \quad A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = TST \in G$$

(iii) Si $d = -1$, même genre de considérations qui amènent à

$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = (TS)^2 \in G \quad \text{ou} \quad A = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} = (TS)^2 S \in G$$

☞ Si $c = -1$, on se ramène à $c = 1$ en changeant A en $-A$.

□

On sait déjà que

$$G \subset \mathrm{SL}_2(\mathbb{Z})$$

Réciproquement, prenons une matrice $A \in \mathrm{SL}_2(\mathbb{Z})$. Soit $z \in D$. On a alors $A \cdot z \in \mathbb{C}$. Par le lemme 1, on peut trouver $B \in G$ telle que $B \cdot (A \cdot z) \in D$.

Comme $z \in D$ et $BA \cdot z \in D$, par le lemme 2, on sait que $BA \in G$. En multipliant par $B^{-1} \in G$ à gauche, on trouve que la matrice A est dans G.

On peut donc conclure que

$$G = \mathrm{SL}_2(\mathbb{Z})$$

□

Astuces de l'agrégatif :

Pour le premier lemme finalement ce que l'on fait c'est que l'on remonte le point z avec des transformations dans G puis on translate ce point jusqu'à arriver dans D avec la matrice T qui translate de 1.

Peut-être qu'il peut être judicieux de mettre les produits matriciels des matrices S et T en annexe, et pendant le développement pour la distinction de cas, on dit « comme on le voit dans l'annexe, notre matrice appartient bien à G en tant que produit de S et T et de leur inverse ».

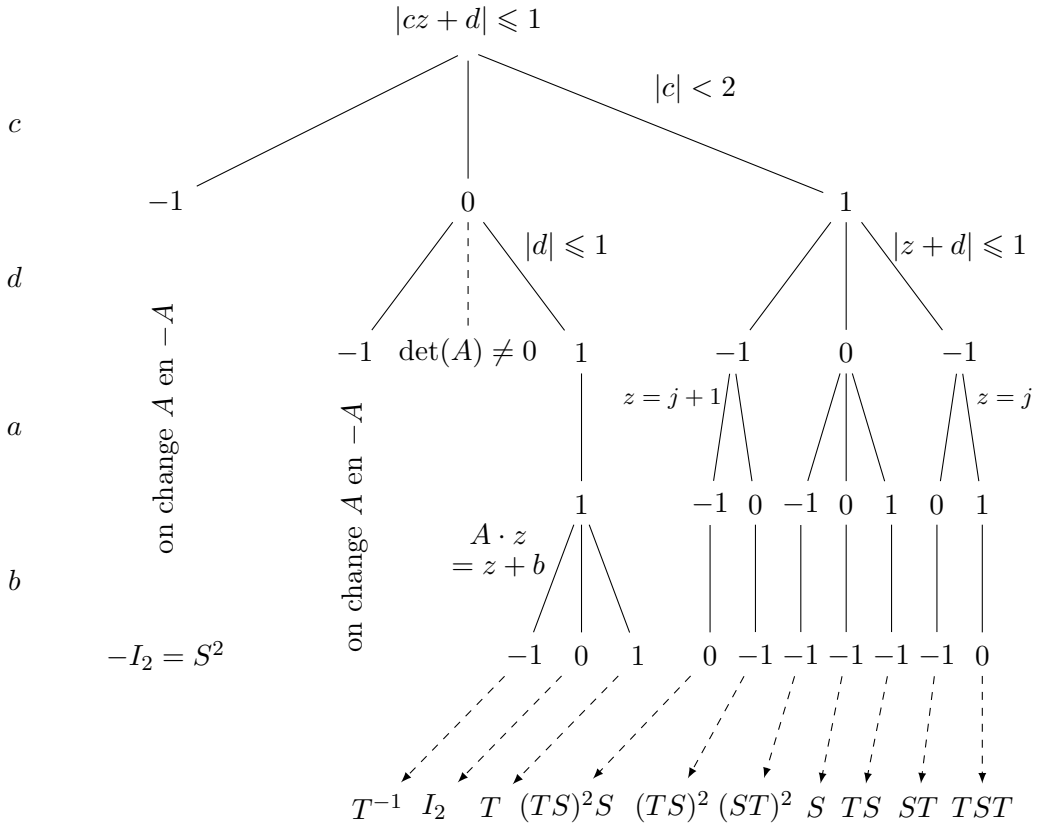
Je fais plein de dessins, notamment dans la disjonction de cas du lemme 2, pour montrer ce que fait l'action de A sur z dans chaque cas. Il peut être intéressant d'écrire la matrice A en faisant changer les coefficients au fur et à mesure de la disjonction de cas.

Questions possibles :

- Expliciter les cas non traités de la disjonction de cas.

Voir page suivant pour un schéma récapitulatif sur le lemme 2.

Schéma du lemme 2 : Dans ce schéma on représente les différents choix que l'on fait dans l'ordre c, d, a puis b.



Automorphismes de $\mathfrak{S}_n$

Leçons : 104 ; 105 ; 108

Références : PERRIN, *Cours d'algèbre* (p.30)

"*Ce développement permet de donner une caractérisation du nombre* 6. "David Xu [1]

Prérequis :

- la famille des $(1i)$ engendre $\mathfrak{S}_n$
- un morphisme conserve l'ordre
- existence et unicité de la décomposition en cycle à support disjoint

On rappelle la définition d'un automorphisme intérieur.

Définition 1. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. On dit que φ est intérieur s'il existe $g \in \mathfrak{S}_n$ tel que pour tout $\sigma \in \mathfrak{S}_n$, on ait $\varphi(\sigma) = g\sigma g^{-1}$.

Introduction :

Pour des groupes relativement simples comme $\mathbb{Z}/n\mathbb{Z}$, on connait le groupe des automorphismes : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. On va étudier ici les automorphismes de $\mathfrak{S}_n$ et notamment on va voir que pour tout $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont exactement les automorphismes intérieurs de $\mathfrak{S}_n$ que l'on sait très bien décrire par un élément de $\mathfrak{S}_n$ (c.f. la définition ci-desus).

Théorème 1. Si $n \neq 6$, alors les automorphismes de $\mathfrak{S}_n$ sont les automorphismes intérieurs, i.e. $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

Lemme 1. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Si φ envoie les transpositions sur les transpositions alors φ est intérieur.

Démonstration du lemme. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ qui envoie les transpositions sur les transpositions. On sait que l'ensemble $\{\tau_i := (1, i), \forall i \in \{2, \dots, n\}\}$ engendre $\mathfrak{S}_n$. On va donc étudier l'image des transpositions par φ.

Comme φ envoie transposition sur transposition, $\varphi(\tau_2)$ et $\varphi(\tau_3)$ sont des transpositions, mais

$$\tau_2 \circ \tau_3 = (132)$$

qui est d'ordre 3, donc $\varphi(\tau_2) \circ \varphi(\tau_3)$ est aussi d'ordre 3, donc $\varphi(\tau_2)$ et $\varphi(\tau_3)$ ont un élément en commun, on le note α_1. On écrit donc

$$\varphi(\tau_2) = (\alpha_1\alpha_2) \quad \text{et} \quad \varphi(\tau_3) = (\alpha_1\alpha_3)$$

De plus, $\alpha_2 \neq \alpha_3$ car φ est injectif [2].

Soit $i \in \{4, \dots, n\}$, on va regarder $\varphi(\tau_i)$, par le même argument que ci-dessus, il a élément commun avec $(\alpha_1\alpha_2)$ et $(\alpha_1\alpha_3)$

1. à ne pas dire le jour de l'oral
2. car φ est un automorphisme, donc il est bijectif par définition

Par l'absurde, considérons que $\varphi(\tau_i) = (\alpha_2\alpha_3)$, on aurait alors

$$\varphi(\tau_2 \circ \tau_3 \circ \tau_i) = (\alpha_1\alpha_2)(\alpha_1\alpha_3)(\alpha_2\alpha_3) = (\alpha_1\alpha 3) = \varphi(\tau_3)$$

Par injectivité de φ, on a donc

$$\tau_i = \tau_3 \circ \tau_2 \circ \tau_3 = (13)(12)(13) = (23)$$

ce qui est impossible par définition des τ_i. Ainsi l'élément en commun est forcément α_1. On peut donc écrire

$$\forall i \in \{2, \dots, n\} \quad \varphi(\tau_i) = (\alpha_1\alpha_i)$$

où tous les α_i sont distincts par injectivité de φ.

On pose alors la permutation

$$\alpha : \begin{cases} \{1, \dots, n\} & \to & \{1, \dots, n\} \\ i & \mapsto & \alpha_i \end{cases}$$

bien défini car tous les α_i sont distincts, sont dans $\{1, \dots, n\}$ et car il y en a n.

Ainsi on a

$$\varphi(\tau_i) = \alpha^{-1} \circ \tau_i \circ \alpha$$

Ce qui conclut la preuve car φ est donc intérieur. □

Proposition 1. Soit $\sigma \in \mathfrak{S}_n$, on écrit σ comme produit de cycles à supports disjoints et on note $n = k_1 + 2k_2 + 3k_3 + \cdots + nk_n$ où k_i est le nombre de i-cycle dans la permutation σ. Alors le centralisateur [a] de σ a pour cardinal

$$|c(\sigma)| = \prod_{i=1}^{n} i^{k_i} k_i!$$

a. le centralisateur de σ est $c(\sigma) = \{g \in \mathfrak{S}_n, g\sigma g^{-1} = \sigma\}$

Démonstration de la proposition.

Étape 1 : *Commençons par le cas où σ est un cycle*

Soit $\sigma = (x_1 \dots x_r)$ un cycle. Soit g un élément de $c(\sigma)$, on a donc

$$g\sigma g^{-1} = (g(x_1) \dots g(x_r))$$

Il faut donc que g envoie les éléments du cycle sur les éléments du cycle. Pour les $(n-r)$ autres éléments, il n'y a pas de containtes, donc on a $(n-r)!$ choix possibles. De plus, g a r choix pour l'image de x_1, mais une fois cette image fixée les autres sont elles-aussi fixées. Donc il a $(n-r)!r$ choix pour g, ainsi

$$|c(\sigma)| = (n-r)!r$$

Étape 2 : *Cas général*

Soit σ une permutation. Soit g un élément de $c(\sigma)$, on a $g\sigma g^{-1}$ qui envoie les $i-$cycles sur les $i-$cycles.

Pour chaque i, il y a k_i $i-$cyles, par définition. Pour chaque $i-$cycle $c_{j,i}$, on va fixer sur quel $i-$cycle, g enverra $c_{j,i}$. On a k_i choix pour $c_{1,i}$, puis $k_i - 1$ choix pour $c_{2,i}$, jusqu'à un seul choix pour $c_{k_i,i}$. Ainsi il y a $k_i!$ pour savoir sur quel $i-$cycle, g enverra chaque $i-$cycle.

Ensuite, pour chaque $i-$cycle, il faut choisir l'image du premier élément du cycle (comme à l'étape 1). Donc, comme on a k_i $i-$cycles, on a i^{k_i} choix possibles.

On a donc $i^{k_i}k_i!$ choix pour les $i-$cycles. Il faut faire cela pour chaque i, d'où

$$|c(\sigma)| = \prod_{i=1}^{n} i^{k_i}k_i!$$

□

Démonstration du théorème. Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. On veut utiliser le lemme, donc on regarde si les transpositions s'envoient sur les transpositions. Soit τ une transposition. On sait que $\varphi(\tau)$ est d'ordre 2 car τ est d'ordre 2 et qu'un automorphisme conserve l'ordre. Donc $\varphi(\tau)$ est un produit de k transpositions à supports disjoints.

On va maintenant regarder le centralisateur pour utiliser la proposition. On a $c(\varphi(\tau)) = \varphi(c(\tau))$ (preuve par double inclusion). Donc $|c(\tau)| = |\varphi(c(\tau))| = |c(\varphi(\tau))|$.

Par la proposition

$$|c(\tau)| = 1^{n-2}(n-2)! \times 2^1 1! = 2(n-2)!$$

car il y a qu'un cycle de taille 2 et $n-2$ cycles de taille 1 et

$$|c(\varphi(\tau))| = 1^{n-2k}(n-2k)! \times 2^k k! = 2^k(n-2k)!k!$$

car il y a k cycles de taille 2 et $n-2k$ cycles de taille 1.

On veut que ces deux quantités soient égales.

$$\begin{aligned}
2(n-2)! = 2^k(n-2k)!k! &\iff \frac{(n-2)!}{(n-2k)!}\frac{1}{2^{k-1}k!} = 1 \\
&\iff \binom{n-2}{2k-2}\frac{(2k-2)!}{2^{k-1}k!} = 1 \\
&\iff \binom{n-2}{2k-2}\frac{(2k-2)(2k-4)\dots 4\times 2\times (2k-3)(2k-5)\dots 3\times 1}{2^{k-1}(k-1)!k} = 1 \\
&\iff \binom{n-2}{2k-2}\frac{(2k-3)(2k-5)\dots 3\times 1}{k} = 1
\end{aligned}$$

C'est impossible si $k \geqslant 4$ car $\dfrac{(2k-3)(2k-5)\dots 3\times 1}{k} > 1$ et le coefficient binomiale est supérieur à 1, donc on regarde les cas $k=1$, $k=2$ et $k=3$.

— Si $k=1$, alors l'image de τ est une transposition.

— Si $k=2$, on a $\binom{n-2}{2}\frac{1}{2} = 1 \iff (n-2)(n-3) = 4 \iff n^2-5n+2 = 0$. Or $\Delta = 5^2 - 4\times 2 = 17$ donc les solutions ne sont pas entières. Donc le cas $k=2$ est impossible.

— Si $k=3$, on a $\binom{n-2}{4} = 1 \iff (n-2)(n-3)(n-4)(n-5) = 4! \iff n = 6$.

Ainsi si $n \neq 6$, on est forcément dans le cas $k=1$ et donc toute transposition s'envoie sur une transposition, donc, par le lemme, φ est intérieur. Ainsi

$$\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$$

□

Remarques :

Il existe bien des automorphismes de $\mathfrak{S}_6$ qui ne sont pas intérieurs.

Donc pour $n=6$ on a $\mathrm{Aut}(\mathfrak{S}_n) \neq \mathrm{Int}(\mathfrak{S}_n)$. $\mathrm{Int}(\mathfrak{S}_n)$ est d'indice 2 dans $\mathrm{Aut}(\mathfrak{S}_n)$. C'est donc bien une caractérisation. (dans le développement, on ne prouve qu'un sens)

Etude du groupe $O(p,s)$

Leçons : 106 ; 156 ; 170

Références : CALDERO–GERMONI, *Nouvelles histoires hédonistes de groupes et de géométries Tome 1* (p.359)

Prérequis :

- $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme
- décomposition polaire sur $\mathbb{R}$
- l'unicité de la racine carrée pour une matrice symétrique

Définition 1. On s'intéresse aux formes quadratiques q qui sont représentées par la matrice $I_{ps} = \begin{pmatrix} I_p & 0 \\ 0 & -I_s \end{pmatrix}$ et on pose $O(p,s)$ le groupe orthogonal de la forme quadratique q non dégénérée de signature (p,s). D'un point de vue matriciel, ce sont les matrices $A \in \mathrm{GL}_n(\mathbb{R})$ telle que ${}^tAI_{ps}A = I_{ps}$.

Introduction :

On veut obtenir une écriture plus simple de $O(p,s)$, notamment pour étudier ces propriétés topologiques (compacité, connexité). C'est une bonne application de l'homéomorphisme exponentielle de $\mathcal{S}_n(\mathbb{R})$ vers $\mathcal{S}_n^{++}(\mathbb{R})$.

Théorème 1. Il existe un homéomorphisme

$$O(p,s) \simeq O_p(\mathbb{R}) \times O_s(\mathbb{R}) \times \mathbb{R}^{ps}$$

Démonstration.

Étape 1 : *Montrons que* $O(p,s) \simeq (O(p,s) \cap O_n(\mathbb{R})) \times (O(p,s) \cap \mathcal{S}_n^{++}(\mathbb{R}))$

Soit $M \in O(p,s) \subset GL_n(\mathbb{R})$, donc il existe un unique couple $(O,S) \in O_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R})$ tel que $M = OS$ (décomposition polaire). On a alors ${}^tMM = S^2$. De plus, ${}^tM \in O(p,s)$ car

$${}^tMI_{ps}M = I_{ps} \iff ({}^tM)^{-1} = I_{ps}MI_{ps} \iff M^{-1} = I_{ps}{}^tMI_{ps} \iff MI_{ps}{}^tM = I_{ps}$$

De plus, $O(p,s)$ est un groupe donc ${}^tMM \in O(p,s)$, c'est-à-dire $S^2 \in O(p,s)$. On note $T = S^2 \in \mathcal{S}_n^{++}(\mathbb{R})$ (car $T = {}^tMM$) et U l'unique matrice de $\mathcal{S}_n(\mathbb{R})$ telle que $T = \exp(U)$. On a alors $S = \exp(\frac{U}{2})$ par unicité de la racine carrée [1]. On veut prouver que $S \in O(p,s)$ sachant que l'on a déjà $T \in O(p,s)$.

$$\begin{aligned} T \in O(p,s) &\iff {}^tTI_{ps}T = I_{ps} \\ &\iff {}^t\exp(U) = I_{ps}exp(-U)I_{ps} \\ &\iff \exp({}^tU) = \exp(U) = \exp(-I_{ps}UI_{ps}) \\ &\iff U = -I_{ps}UI_{ps} \\ &\iff UI_{ps} + I_{ps}U = 0 \\ &\iff \frac{U}{2}I_{ps} + I_{ps}\frac{U}{2} = 0 \end{aligned}$$

1. à savoir prouver

$$\iff S \in O(p,s)$$

par l'homéomorphisme $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$.

Ainsi $S \in O(p,s)$ et donc $O = MS^{-1} \in O(p,s)$. Ainsi la restriction de l'homéomorphisme de la décomposition polaire au groupe $O(p,s)$ donne l'homéomorphisme suivant

$$\varphi : O(p,s) \xrightarrow{\sim} (O(p,s) \cap O_n(\mathbb{R})) \times (O(p,s) \cap \mathcal{S}_n^{++}(\mathbb{R}))$$

Étape 2 : *Montrons que* $O(p,s) \cap O_n(\mathbb{R}) \simeq O_p(\mathbb{R}) \times O_s(\mathbb{R})$

Soit une matrice $M \in O(p,s) \cap O_n(\mathbb{R})$, on écrit $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ où $A \in \mathcal{M}_p(\mathbb{R})$ et $D \in \mathcal{M}_s(\mathbb{R})$.

On a

$$ {}^tMI_{ps}M = I_{ps} \iff \begin{pmatrix} {}^tAA - {}^tCC & {}^tAB - {}^tCD \\ {}^tBA - {}^tDC & {}^tBB - {}^tDD \end{pmatrix} = \begin{pmatrix} I_p & 0 \\ 0 & -I_s \end{pmatrix}$$

Donc en particulier

$$(1) \begin{cases} {}^tAA - {}^tCC = I_p \\ {}^tDD - {}^tBB = I_q \end{cases}$$

Et aussi

$$ {}^tMM = I_n \iff \begin{pmatrix} {}^tAA + {}^tCC & {}^tAB + {}^tCD \\ {}^tBA + {}^tDC & {}^tBB + {}^tDD \end{pmatrix} = \begin{pmatrix} I_p & 0 \\ 0 & I_s \end{pmatrix}$$

Donc en particulier

$$(2) \begin{cases} {}^tAA + {}^tCC = I_p \\ {}^tDD + {}^tBB = I_s \end{cases}$$

En combinant les lignes (1) et (2), on a ${}^tAA = I_p$, ${}^tDD = I_s$, ${}^tBB = 0$ et ${}^tCC = 0$ ce qui donne $A \in O_p(\mathbb{R})$, $D \in O_s(\mathbb{R})$, $B = 0$ et $C = 0$ (en utilisant le produit scalaire $\langle R, S \rangle = \sqrt{\mathrm{Tr}({}^tRS)}$ puisque $\langle B, B \rangle = 0$ implique $B = 0$). Ainsi l'application

$$\psi : \begin{cases} O(p,s) \cap O_n(\mathbb{R}) & \xrightarrow{\sim} & O_p(\mathbb{R}) \times O_s(\mathbb{R}) \\ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} & \mapsto & (A, D) \end{cases}$$

est un homéomorphisme (car continue, bijective et d'inverse continue).

Étape 3 : *Montrons que* $O(p,s) \cap \mathcal{S}_n^{++}(\mathbb{R}) \simeq \mathbb{R}^{ps}$

On pose l'ensemble $L = \{U \in \mathcal{S}_n(\mathbb{R}) / UI_{ps} + I_{ps}U = 0\}$. On a vu à l'étape 1 que l'exponentielle est un homéomorphisme de $\mathcal{S}_n(\mathbb{R}) \cap L$ dans $\mathcal{S}_n^{++}(\mathbb{R}) \cap O(p,s)$.

Soit $U \in \mathcal{S}_n(\mathbb{R}) \cap L$, on écrit $U = \begin{pmatrix} A & B \\ {}^tB & D \end{pmatrix}$ où A et D sont symétriques et respectivement de taille p et s. On a

$$UI_{ps} + I_{ps}U = \begin{pmatrix} 2A & 0 \\ 0 & -2D \end{pmatrix} = 0$$

Par conséquent, on a $A = 0$ et $D = 0$. Donc $U = \begin{pmatrix} 0 & B \\ {}^tB & 0 \end{pmatrix}$, or $B \in \mathcal{M}_{p,s}(\mathbb{R})$, on note $B = (b_{i,j})$ (avec $1 \leqslant i \leqslant p$ et $1 \leqslant j \leqslant s$) et on pose l'homéomorphisme

$$\phi : \begin{cases} \mathcal{S}_n(\mathbb{R}) \cap L & \xrightarrow{\sim} & \mathbb{R}^{ps} \\ \begin{pmatrix} 0 & B \\ {}^tB & 0 \end{pmatrix} & \mapsto & (b_{1,1} \dots b_{1,s} b_{2,1} \dots b_{2,s} \dots b_{p,1} \dots b_{p,s}) \end{cases}$$

Ainsi on a bien un homéomorphisme $\boxed{O(p,s) \simeq O_p(\mathbb{R}) \times O_s(\mathbb{R}) \times \mathbb{R}^{ps}}$

□

Remarques :

— Si $p \neq 0$, $s \neq 0$, le groupe $O(p,s)$ admet quatre composantes connexes.

— Le groupe $O(p,s)$ est compacte si et seulement si $p = 0$ ou $s = 0$.

Astuces de l'agrégatif :

Il faut bien maitriser l'homéomorphisme exp : $\mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ et la décomposition polaire car c'est cela qui justifie les homéomorphismes que l'on manipule. De plus, il faut savoir prouver que la racine carrée (symétrique) d'une matrice symétrique est unique.

Les calculs sont assez longs notamment à l'étape 2, j'ai mis en gris les calculs que je ne faisais pas pendant le développement, d'autant plus qu'ils ne sont pas utiles à la résolution.

Questions possibles :

- Que se passe-t-il si la forme quadratique n'est pas dégénérée ?

Réponse : On veut caractériser les matrices M telles que ${}^tM\tilde{I}_{ps}M = \tilde{I}_{ps}$ avec $p+s<n$ et

$$\tilde{I}_{ps} = \begin{pmatrix} I_{ps} & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R})$$

D'où en écrivant $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ puis en faisant le calcul, on a

$$\begin{pmatrix} {}^tAI_{ps}A & {}^tAI_{ps}B \\ {}^tBI_{ps}A & {}^tBI_{ps}B \end{pmatrix} = \begin{pmatrix} I_{ps} & 0 \\ 0 & 0 \end{pmatrix}$$

Ainsi, on a $B = 0$ et ${}^tAI_{ps}A = I_{ps}$, donc on peut choisir indifféremment C et D qui ont en tout $n \times (n-p-s)$ coefficients. D'où pour une forme quadratique de signature (p,s) d'un espace de dimension n avec $p+s \leqslant n$, on a

$$O(p,s) \simeq O_p(\mathbb{R}) \times O_s(\mathbb{R}) \times \mathbb{R}^{ps} \times \mathbb{R}^{n(n-p-s)}$$

$$O(p,s) \simeq O_p(\mathbb{R}) \times O_s(\mathbb{R}) \times \mathbb{R}^{(n-p)(n-s)}$$

Théorème de Carathéodory

Leçons : 126 ; 151

Références : GOURDON, *Analyse* (p.54)

Prérequis :

- définition de Conv(A)
- le rang sur $\mathbb{Q}$ est le même que le rang sur $\mathbb{R}$
- théorème du rang

Introduction :

On va montrer un théorème qui nous permet de majorer le nombre de points utiles pour exprimer n'importe quel point d'un espace de dimension finie. Par exemple, dans $\mathbb{R}^n$, on pourra exprimer tous les points par seulement n+1 points. Ensuite, on utilisera ce théorème pour montrer l'existence de solutions d'un système diophantien.

Théorème 1. Soit A une partie de $\mathbb{R}^n$, on a

$$\text{Conv}(A) = \left\{ \sum_{i=0}^{n+1} \lambda_i a_i, \text{ avec } a_i \in A, \lambda_i \geqslant 0, \sum_i \lambda_i = 1 \right\}$$

Démonstration.
L'inclusion $\boxed{\supset}$ est claire par définition de Conv(A).

Pour l'inclusion $\boxed{\subset}$, on prend $x \in \text{Conv}(A)$, donc on peut écrire x sous la forme

$$x = \sum_{i=0}^{p} \lambda_i a_i \text{ avec } a_i \in A, \lambda_i \geqslant 0, \sum_i \lambda_i = 1$$

où p est l'entier minimal tel que l'on puisse écrire x sous cette forme.

Raisonnons par l'absurde, supposons que $p \geqslant n+2$. On pose

$$\phi : \left\{ \begin{array}{ccc} \mathbb{R}^p & \to & \mathbb{R}^n \times \mathbb{R} \\ (\nu_i)_1^p & \mapsto & \left(\sum_i \nu_i a_i, \sum_i \nu_i \right) \end{array} \right.$$

L'application ϕ est linéaire, donc on peut appliquer le théorème du rang :

$$p = \dim \mathbb{R}^p = \dim \ker \phi + \text{ rg } \phi$$

Or

$$\text{rg } \phi \leqslant n+1$$

Donc on a

$$\dim \ker \phi \geqslant p - n - 1 \geqslant 1$$

Ainsi on peut choisir $(\alpha_i)_1^p \in \ker \phi \setminus \{0\}$.

On pose

$$\mu_i(t) = \lambda_i + t\alpha_i \text{ pour tout } i \in \{1, \dots, p\} \text{ et pour tout } t \in \mathbb{R}$$

Ainsi on a

$$\sum_{i=1}^{p} \mu_i(t) = \underbrace{\sum_{i=1}^{p} \lambda_i}_{=1} + t \underbrace{\sum_{i=1}^{p} \alpha_i}_{=0} = 1$$

et

$$\sum_{i=1}^{p} \mu_i(t) a_i = \underbrace{\sum_{i=1}^{p} \lambda_i a_i}_{=x} + t \underbrace{\sum_{i=1}^{p} \alpha_i a_i}_{=0} = x$$

Donc maintenant il faut trouver $\tau \in \mathbb{R}$ tel que

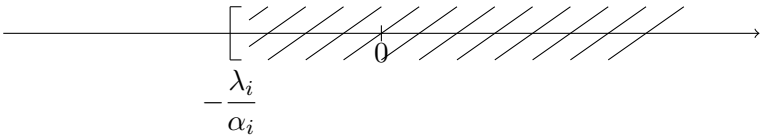
(i) $\mu_i(\tau) \geqslant 0$ pour tout $i \in \{1, \dots, p\}$ (pour coller à la définition des éléments de l'enveloppe convexe)

(ii) il existe i_0 tel que $\mu_{i_0}(\tau) = 0$ (pour donner une contradiction avec l'aspect p minimal)

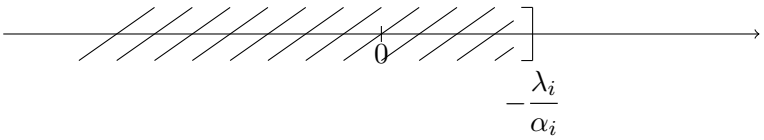
Pour avoir $\mu_i(t) \geqslant 0$

— Si $\alpha_i = 0$, $\mu_i(t) = \lambda_i \geqslant 0$.

— Si $\alpha_i > 0$, il faut que $t \geqslant -\frac{\lambda_i}{\alpha_i}$ [1] avec $-\frac{\lambda_i}{\alpha_i} \leqslant 0$



— Si $\alpha_i < 0$, il faut que $t \leqslant -\frac{\lambda_i}{\alpha_i}$ [2] avec $-\frac{\lambda_i}{\alpha_i} \geqslant 0$



Comme les α_i sont non tous nuls [3], il existe au moins un α_i non nul et comme $\sum_i \alpha_i = 0$, il existe k et j tels que $\alpha_k > 0$ et $\alpha_j < 0$.

Ainsi on peut poser

$$\tau = \max\{-\frac{\lambda_i}{\alpha_i}, i \in \{1, \dots, p\}, \alpha_i > 0\}$$

On a donc pour tout $i \in \{1, \dots, p\}$, $\mu_i(\tau) \geqslant 0$ [4]. On a donc le point (i).

La valeur τ est atteinte en un certain i_0. Or, comme $\tau = -\frac{\lambda_{i_0}}{\alpha_{i_0}}$, on a $\mu_{i_0}(\tau) = \lambda_{i_0} + \tau\alpha_{i_0} = 0$. Cela montre le point (ii).

Donc

$$\sum_{i=1}^{p} \mu_i(\tau)\alpha_i = \sum_{i \neq i_0} \mu_i(\tau)\alpha_i = x$$

Ainsi, on a exprimé x avec $p-1$ points, cela contredit donc la minimalité de p.

On a donc prouvé que $p \leqslant n+1$. Ce qui conclut la preuve du théorème. □

1. $\lambda_i + t\alpha_i \geqslant 0 \iff t\alpha_i \geqslant -\lambda_i \iff t \geqslant -\frac{\lambda_i}{\alpha_i}$
2. $\lambda_i + t\alpha_i \geqslant 0 \iff t\alpha_i \geqslant -\lambda_i \iff t \leqslant -\frac{\lambda_i}{\alpha_i}$
3. car les α_i sont dans $\ker \phi$ privé de $\{0\}$
4. car par définition de τ on a le résultat pour les $\alpha_i > 0$, on a $\tau \leqslant 0$ et si $\alpha_i < 0$, on a $-\frac{\lambda_i}{\alpha_i} \geqslant 0 \geqslant \tau$

Application 1. Soit $A \in \mathcal{M}_{m,n}(\mathbb{Z})$.
Il y a équivalence entre les deux assertions suivantes :

(i) le système diophantien $Ax = 0$ admet une solution non nulle $x \in \mathbb{N}^n$

(ii) $0_{\mathbb{R}^m} \in \mathrm{Conv}(A_1, \dots, A_n)$ où $A_1, \dots, A_n$ sont les colonnes de la matrice A.

Démonstration. $\boxed{(i) \Longrightarrow (ii)}$ Soit $x \in \mathbb{N}^n$ une solution de $Ax = 0$, d'où

$$0_{\mathbb{R}^m} = \sum_{i=1}^{n} A_i x_i$$

Comme, pour tout $i \in \{1, \dots, n\}$, on a $x_i \geqslant 0$ et x est non nul, on peut prendre

$$\lambda_i = \frac{x_i}{\sum_j x_j}$$

On a donc

$$0_{\mathbb{R}^m} = \sum_{i=1}^{n} \lambda_i A_i$$

avec $\lambda_i \geqslant 0$ et $\sum_i \lambda_i = 1$, donc $0_{\mathbb{R}^m} \in \mathrm{Conv}(A)$.

$\boxed{(ii) \Longrightarrow (i)}$ Soit l minimal tel que $0_{\mathbb{R}^m}$ soit dans l'enveloppe convexe de l colonnes de A. On a alors

$$0_{\mathbb{R}^m} = \sum_{j=1}^{l} \lambda_j A_{i_j} \tag{3.1}$$

avec $\lambda_j \geqslant 0$ et $i_j \in \{1, \dots, n\}$ distincts.

On note $r = \mathrm{rg}_{\mathbb{R}}(A_{i_1}, \dots, A_{i_l})$.

Alors, comme $A_{i_1}, \dots, A_{i_l}$ sont liées par (3.1), on a $\boxed{r < l}$.

De plus, $0_{\mathbb{R}^m} \in \mathrm{Vect}(A_{i_1}, \dots, A_{i_l})$ qui est un espace vectoriel de dimension r sur $\mathbb{R}$, donc on a besoin d'au plus $r+1$ éléments de $\{A_{i_1}, \dots, A_{i_l}\}$ pour exprimer $0_{\mathbb{R}^m}$ par le théorème de Carathéodory. Ainsi, par minimalité de l, on a $\boxed{l \leqslant r+1}$. On peut donc en conclure que

$$l = r + 1.$$

On pose

$$\widetilde{A} = \begin{pmatrix} A_{i_1} & \dots & A_{i_l} \end{pmatrix} \in \mathcal{M}_{n,r+1}(\mathbb{Q})$$

qui est une matrice de rang r sur $\mathbb{Q}$. Ainsi, elle est de noyau non réduit à $\{0\}$ puisque le théorème du rang nous donne

$$r + 1 = \dim \ker \widetilde{A} + r$$

Soit $\tilde{y} \in \mathbb{Q}^{r+1}$ non nul tel que $\widetilde{A}\tilde{y} = 0$. On pose $y \in \mathbb{Q}^n$ non nul tel que

$$\begin{cases} y_i = \tilde{y}_i & \text{si } i \text{ est un des } i_j \\ y_i = 0 & \text{sinon} \end{cases}$$

Ainsi

$$Ay = \sum_{i=1}^{n} y_i A_i = \sum_{i \in (i_j)_{j=1}^{l}} \widetilde{y_i} \widetilde{A_i} = \widetilde{A}\tilde{y} = 0_{\mathbb{R}^m}$$

Comme $y \in \mathbb{Q}^n$, quitte à multiplier y par un entier suffisamment grand, on peut prendre un $y \in \mathbb{Z}^n$ (toujours non nul).

On veut maintenant montrer que l'on peut trouver $y \in \mathbb{N}^n$. On sait que

$$(\lambda_1, \dots, \lambda_{r+1}) \in \mathbb{R}_+^{r+1} \cap \ker_{\mathbb{R}} \widetilde{A}$$

Comme le rang ne dépend pas du corps de base, c'est aussi un élément de $\ker_{\mathbb{Q}} \widetilde{A}$. Or on sait que $\dim \ker_{\mathbb{Q}} \widetilde{A} = 1$, donc y et λ sont liés. Il existe donc $\alpha \in \mathbb{R}$ tel que $\alpha y = \lambda$ et on sait que tous les λ_i sont positifs (par définition des λ_i dans (3.1)). Donc tous les y_i sont de même signe, ainsi, quitte à multiplier par -1, on les prend positifs. On vient donc de montrer qu'il existe $y \in \mathbb{N}^n$ non nul tel que $Ay = 0$. □

Remarques :

Je ne vois aucun exemple où on aurait besoin de cette application pour gagner du temps par rapport au temps qu'on prendrait à le faire à la main. Si tu en vois, n'hésite pas à m'envoyer un mail [5].

Astuces de l'agrégatif :

Il faut bien comprendre pourquoi

$$\mathrm{Conv}(A) = \left\{ \sum_{i=0}^{N} \lambda_i a_i, \text{ avec } N \in \mathbb{N}, a_i \in A, \lambda_i \geqslant 0, \sum_i \lambda_i = 1 \right\}$$

et ensuite ce qui est fort dans ce théorème c'est qu'on borne ce N par $n+1$ où n est la dimension de l'espace vectoriel dans lequel on est.

Questions possibles :

- Trouver un convexe de $\mathbb{R}^n$, qui n'est pas engendré par $n+1$ points.

  Réponse : le cercle

5. pierre.le-barbenchon@ens-rennes.fr

Théorème de Fermat modulaire

Leçons : 120 ; 121 ; 126 ; 190

Références : LANDMAN–ROBERTSON, *Ramsey Theory on the Integers*(p.222) [LR03]

Prérequis :

- le lemme des tiroirs
- l'ordre de $A = \{a^r, a \in (\mathbb{Z}/p\mathbb{Z})^\times\}$

Introduction :

L'équation de Fermat-Wiles $x^n + y^n = z^n$ n'admet pas de solution non triviale pour $n \geqslant 3$ dans $\mathbb{Z}$. Cependant si on ne se place plus sur $\mathbb{Z}$ mais sur $\mathbb{Z}/p\mathbb{Z}$ pour un p bien choisi, l'équation admet au moins une solution non triviale. C'est ce résultat là que l'on va prouver maintenant en utilisant des lemmes de dénombrement.

Théorème 1. Soit $r \in \mathbb{N}^*$, il existe un entier q tel que pour tout entier premier $p > q$, l'équation $x^r + y^r = z^r$ admet une solution dans $\mathbb{Z}/p\mathbb{Z}$ avec x, y, z tous non nuls.

Lemme 1. Soient $r \in \mathbb{N}^*$ et $a_1, \dots, a_r \in \mathbb{C}^r$ deux à deux distincts, il existe un entier $N(r)$ tel que pour tout ensemble fini E de cardinal $n \geqslant N(r)$ et pour toute application $\chi : \mathcal{P}_2(E) \to \{a_1, \dots, a_r\}$, il existe trois éléments distincts $x, y, z \in E$ tels que $\chi(\{x, y\}) = \chi(\{x, z\}) = \chi(\{y, z\})$, où $\mathcal{P}_2(E)$ est l'ensemble des sous ensembles de cardinal 2 de E.

Remarques :

L'ensemble $\{a_1, \dots, a_r\}$ peut être vu comme un ensemble de couleurs, ce qui fait de χ un coloriage par r couleurs des sous ensembles de cardinal 2 de E.

Démonstration du Lemme 1. On va procéder par récurrence sur r.
Initialisation : Pour $r = 1$, toute application χ sera constante égale à la couleur c_1. Donc dès que l'ensemble E sera de cardinal supérieur à 3, on pourra trouver trois éléments distincts qui ont la même couleur. Ainsi on peut prendre $N(r) = 3$.

Hérédité : On suppose que l'on a le résultat au rang $r-1$, on veut le prouver au rang r.

Soit un ensemble E de cardinal n et soit une application $\chi : \mathcal{P}_2(E) \to \{c_1, \dots, c_r\}$. On pose l'application

$$\chi_x : \left\{ \begin{array}{ccc} E\backslash\{x\} & \to & \{c_1, \dots, c_r\} \\ y & \mapsto & \chi(\{x, y\}) \end{array} \right. .$$

On a $E\backslash\{x\} = \bigsqcup_{i=1}^{r} \chi_x^{-1}(\{c_i\})$, or $E\backslash\{x\}$ est de cardinal $n-1$, donc il existe un $i_0 \in [\![1; r]\!]$ tel que

$$|\chi_x^{-1}(\{c_{i_0}\})| \geqslant \lceil \frac{n-1}{r} \rceil,$$

par le lemme des tiroirs. On pose

$$X := \chi_x^{-1}(\{c_{i_0}\}).$$

S'il existe $y, z \in X$ distincts tels que $\chi(\{y,z\}) = c_{i_0}$, on aura x, y, z distincts tels que $\chi(\{x,y\}) = \chi(\{x,z\}) = \chi(\{y,z\}) = c_{i_0}$.

Sinon on prend l'application

$$\tilde{\chi} : \begin{cases} \mathcal{P}_2(X) & \to & \{c_1, \dots, c_{i_0-1}, c_{i_0+1}, \dots, c_r\} \\ \{y,z\} & \mapsto & \chi(\{y,z\}) \end{cases},$$

on veut appliquer l'hypothèse de récurrence sur $\tilde{\chi}$ car il y a $r-1$ couleurs. Il faut que $|X| \geqslant N(r-1)$ pour pouvoir appliquer l'hypothèse.
Prenons $N(r) = rN(r-1)+1$ ainsi

$$|X| \geqslant \lceil \frac{n-1}{r} \rceil \geqslant \lceil \frac{N(r)-1}{r} \rceil \geqslant N(r-1)$$

donc on peut appliquer l'hypothèse de récurrence ainsi il existe $t, y, z \in X$ distincts tels que

$$\chi(\{t,y\}) = \chi(\{y,z\}) = \chi(\{t,z\})$$

puisque $\tilde{\chi} = \chi_{|\mathcal{P}_2(X)}$. Donc comme $X \subset E$, on a le résultat pour $N(r) = rN(r-1)+1$. □

Lemme 2 (de Schur)**.** Soient $r \in \mathbb{N}*$ et $a_1, \dots, a_r \in \mathbb{C}^r$ deux à deux distincts, il existe un entier $s(r)$ tel que pour tout $n \geqslant s(r)$ et pour toute application $\sigma : [\![1;n]\!] \to \{c_1, \dots, c_r\}$, il existe trois éléments x, y, z de $[\![1;n]\!]$ tels que $x+y=z$ et $\sigma(x) = \sigma(y) = \sigma(z)$.

Démonstration du lemme 2. Soit $r \in \mathbb{N}^*$ et $n \in \mathbb{N}$, soit une application $\sigma : [\![1;n]\!] \to \{c_1, \dots, c_r\}$, On veut se ramener au cas du lemme 1. On prend $E = [\![1;n+1]\!]$ et on pose l'application

$$\chi : \begin{cases} \mathcal{P}_2(E) & \to & \{c_1, \dots, c_r\} \\ \{x,y\} & \mapsto & \sigma(|x-y|) \end{cases}.$$

Pour $n+1 \geqslant N(r)$, on a x, y, z distincts dans $[\![1;n+1]\!]$ tel que

$$\chi(\{x,y\}) = \chi(\{x,z\}) = \chi(\{y,z\}).$$

On suppose $x < y < z$, et on pose

$$X := y - x, \quad Y := z - y \quad \text{et} \quad Z := z - x,$$

on a bien $X, Y, Z \in [\![1;n]\!]$. Ainsi, on a

$$X + Y = Z \quad \text{et} \quad \sigma(X) = \sigma(Y) = \sigma(Z).$$

Donc on peut prendre $s(r) = N(r) - 1$ pour bien vérifier $n+1 \geqslant N(r)$. □

Démonstration du théorème. Soit $r \in \mathbb{N}^*$, on prend un nombre premier $p > s(r)$. On pose l'ensemble

$$A = \{a^r, a \in (\mathbb{Z}/p\mathbb{Z})^\times\}$$

qui est un sous groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$. On partitionne $(\mathbb{Z}/p\mathbb{Z})^\times$ par les classes à gauche de A :

$$(\mathbb{Z}/p\mathbb{Z})^\times = \bigsqcup_{i=1}^{k} a_i A \quad \text{où } a_i \in (\mathbb{Z}/p\mathbb{Z})^\times \text{ et } k = |(\mathbb{Z}/p\mathbb{Z})^\times / A|.$$

On veut prouver que A est de cardinal $\dfrac{p-1}{\text{pgcd}(p-1,r)}$. On sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, donc il existe $\xi \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre $p-1$ tel que ξ engendre $(\mathbb{Z}/p\mathbb{Z})^\times$. Donc ξ^r engendre A[1], or ξ^r est d'ordre $\dfrac{p-1}{\text{pgcd}(p-1,r)}$. Ainsi A est de cardinal $\dfrac{p-1}{\text{pgcd}(p-1,r)}$.

Donc $k = \text{pgcd}(p-1,r) \leqslant r$.

On prend l'application

$$\sigma : \left\{ \begin{array}{ccc} [\![1, p-1]\!] & \to & \{a_1, \ldots, a_k\} \\ x & \mapsto & a_i \text{ SSI } \bar{x} \in a_i A \end{array} \right. .$$

On a $p-1 \geqslant s(r)$ et $k \leqslant r$, donc il existe $X, Y, Z \in (\mathbb{Z}/p\mathbb{Z})^\times$ tels que $X + Y = Z$ et X, Y, Z appartiennent à la même classe $a_i A$, d'où on peut écrire

$$a_i x^r + a_i y^r = a_i z^r$$

avec a_i inversible, par conséquent, on a

$$x^r + y^r = z^r$$

dans $\mathbb{Z}/p\mathbb{Z}$ et x, y, z tous non nuls dans $\mathbb{Z}/p\mathbb{Z}$ car ils sont dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

□

Astuces de l'agrégatif :

Le développement est relativement long, en fonction de la leçon dans laquelle je mets ce développement je choisissais ce que je démontrais

- pour la 120, je passe forcément plus de temps sur la dernière démonstration, j'enlève la preuve du lemme 1, en disant que la preuve était une récurrence non triviale utilisant le lemme des tiroirs
- pour la 126, je fais à peu près comme pour la 120
- pour la 190, je passe vite sur la preuve du théorème en temps que tel car l'outil de dénombrement que l'on utilise est le lemme des tiroirs dans la preuve du lemme 1.

1. il suffit d'écrire ... en disant que chaque élément α de $(\mathbb{Z}/p\mathbb{Z})^\times$ s'écrit $\alpha = \xi^k$ avec $k \in \mathbb{Z}$

Méthode QR

Leçons : 157 ; 162 ; 233

Références : CIARLET, *Introduction à l'analyse numérique matricielle et à l'optimisation* (p.124)

Prérequis :

- La décomposition QR est un produit d'une matrice unitaire (i.e $Q^*Q = I_n$) et d'une matrice triangulaire supérieure dont les coefficients diagonaux sont réels et strictement positifs
- La décomposition LU est un produit d'une matrice inférieure avec des 1 sur la diagonale et d'une matrice triangulaire supérieure.
- L'application
$$\begin{cases} U_n(\mathbb{C}) \times T_n^+(\mathbb{C}) & \to & GL_n(\mathbb{C}) \\ (Q,R) & \mapsto & QR \end{cases}$$
est un homéomorphisme. [1]

Introduction :

La méthode QR que nous présenterons ci-dessous est l'outil le plus utilisé pour calculer les valeurs propres d'une matrice quelconque (pas forcément symétrique). Pour les matrices symétriques, cette méthode est aussi efficace que la méthode de Jacobi. Pour tout $A \in \mathcal{G}L_n(\mathbb{C})$, on va faire converger une suite de matrices vers une matrice triangulaire ayant sur sa diagonale les valeurs propres de A.

Théorème 1. Soient $A \in GL_n(\mathbb{C})$ et $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ vérifiant

$$|\lambda_1| > |\lambda_2| > \cdots > |\lambda_n| > 0$$

tels qu'il existe une matrice inversible P d'inverse admettant une décomposition LU et que l'on ait

$$P^{-1}AP = D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

Alors la suite définie par

$$\begin{cases} A_1 = A \\ A_{k+1} = R_k Q_k \text{ où } Q_k R_k \text{ est la décomposition } QR \text{ de } A_k \end{cases}$$

converge vers une matrice triangulaire supérieure dont la diagonale est $\mathrm{diag}(\lambda_1, \dots, \lambda_n)$.

Démonstration. On notera $Q^{(k)} = Q_1 \dots Q_k$ et $R^{(k)} = R_k \dots R_1$. On a alors

$$A^k = Q^{(k)} R^{(k)}$$

1. $T_n^+(\mathbb{C})$ est l'ensemble des matrices triangulaires supérieures de $\mathcal{M}_n(\mathbb{C})$ à coefficients diagonaux réels strictement positifs.

que l'on peut prouver par un calcul [2]. On a aussi

$$A_{k+1} = Q^{(k)*} A Q^{(k)}$$

que l'on peut prouver par récurrence [3].

L'idée est de trouver l'expression de $Q^{(k)}$ pour avoir le comportement de A_k et pour trouver $Q^{(k)}$ on va trouver la décomposition QR de A^k d'une autre manière.

Étape 1 : *Trouver la décomposition QR de A^k d'une autre manière*

On a $A^k = PD^kP^{-1}$, donc en notant QR la décomposition QR de P [4], on a

$$A^k = QRD^kLU = QR(D^kLD^{-k})D^kU$$

On veut étudier le comportement de D^kLD^{-k}. Grâce à la décroissance des modules des λ_i et du fait qu'il y a des coefficients 1 sur la diagonale de L, on a D^kLD^{-k} converge vers I_n [5]

Ainsi on a aussi $RD^kLD^{-k}R^{-1}$ qui converge vers I_n quand k tend vers l'infini. On note maintenant O_kT_k la décomposition QR de $RD^kLD^{-k}R^{-1}$. De ce fait, par l'homéomorphisme de la décomposition QR et comme O_kT_k converge vers I_n alors on a aussi O_k et T_k qui convergent vers I_n.

Pour l'instant, on a

$$A^k = (QO_k)(T_kRD^kU)$$

QO_k est bien unitaire car Q et O_k le sont. De plus, T_kRD^kU est triangulaire supérieure mais elle n'est pas à diagonale réelle strictement positive à cause de D^k et U. On factorise D (resp. U) par une matrice diagonale Δ_1 (resp. Δ_2) qui contient les $e^{i\theta}$ où θ est un argument de chaque coefficient de la diagonale de D (resp. U) [6]. Donc $D = \Delta_1|D|$ où $|D|$ est la matrice $\mathrm{diag}(|\lambda_1|, \dots, |\lambda_n|)$ et $U = \Delta_2 U'$.

Si $U = \begin{pmatrix} \rho_1 e^{i\theta_1} & & (*) \\ & \ddots & \\ 0 & & \rho_n e^{i\theta_n} \end{pmatrix}$, alors on a $\Delta_2 = \begin{pmatrix} e^{i\theta_1} & & 0 \\ & \ddots & \\ 0 & & e^{i\theta_n} \end{pmatrix}$ et $U' = \begin{pmatrix} \rho_1 & & (*) \\ & \ddots & \\ 0 & & \rho_n \end{pmatrix}$

Ainsi $|D|$ et U' sont bien triangulaires supérieures de diagonale réelle strictement positive.

On a alors

$$A^k = (QO_k\Delta_1^k\Delta_2)(\Delta_2^{-1}\Delta_1^{-k}T_kR\Delta_1^k|D|^k\Delta_2U')$$

Maintenant on a bien $\Delta_2^{-1}\Delta_1^{-k}T_kR\Delta_1^k|D|^k\Delta_2U') \in T_n^+(\mathbb{C})$ et on a $QO_k\Delta_1^k\Delta_2$ unitaire. Donc on a bien une décomposition QR de A^k.

Comme $A^k = Q^{(k)}R^{(k)}$ est aussi une décomposition QR de A^k, on a, par unicité de la décomposition QR,

$$Q^{(k)} = QO_k\Delta_1^k\Delta_2$$

Étape 2 : *Convergence de A_k*

On a alors

$$A_{k+1} = (QO_k\Delta_1^k\Delta_2)^*A(QO_k\Delta_1^k\Delta_2) = (\Delta_1^k\Delta_2)^*O_k^*Q^*AQO_k(\Delta_1^k\Delta_2)$$

2. $A^k = (Q_1R_1)^k = Q_1(R_1Q_1)^{k-1}R_1 = Q_1A_2^{k-1}R_1 = Q_1(Q_2R_2)^{k-1}R_1 = Q_1Q_2(R_2Q_2)^{k-2}R_2R_1 = \dots = Q_1\dots Q_{k-1}R_{k-1}Q_{k-1}R_{k-1}\dots R_1 = Q_1\dots Q_{k-1}A_kR_{k-1}\dots R_1 = Q_1\dots Q_{k-1}Q_kR_kR_{k-1}\dots R_1 = Q^{(k)}R^{(k)}$

3. $A_{k+1} = R_kQ_k = Q_k^*Q_kR_kQ_k = Q_k^*A_kQ_k = Q_k^*Q^{(k-1)*}AQ^{(k-1)}Q_k = Q^{(k)*}AQ^{(k)}$

4. puisque P est inversible (par l'homéomorphisme de la proposition 1)

5. Le calcul des coefficients de D^kLD^{-k} donne

$$(D^kLD^{-k})_{ij} = \begin{cases} 0 \text{ si } i < j \\ 1 \text{ si } i = j \\ \left(\frac{\lambda_i}{\lambda_j}\right)^k \text{ si } i > j \end{cases}$$

6. c'est possible car U est inversible puisque P^{-1} l'est donc aucun des coefficients diagonaux de U est nul et les λ_i sont supposés de module strictement positifs

Or

$$Q^*AQ = Q^*QRDR^{-1}Q^{-1}Q = RDR^{-1}$$

en se rappelant que $P = QR$ et $A = PDP^{-1}$. De plus comme R est triangulaire supérieure on a

$$RDR^{-1} = \begin{pmatrix} \lambda_1 & & (*) \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

Nous avons vu que O_k tend vers I_n donc on a

$$O_k^*Q^*AQO_k \text{ qui converge vers } \begin{pmatrix} \lambda_1 & & (*') \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

De plus, la conjugaison par $\Delta_1^k\Delta_2$ ne changera ni les coefficients nuls sous la diagonale ni la diagonale. Donc (A_k) converge bien vers une matrice triangulaire supérieure dont la diagonale est $\text{diag}(\lambda_1, \dots, \lambda_n)$. □

Remarques :

- Si A est réelle et satisfait les hypothèses, alors les valeurs propres sont réelles et toutes les matrices que l'on considère sont réelles.
- Attention, si l'on deux valeurs propres de même module, le théorème est faux, par exemple, si A est orthogonale, alors $A_k = A$ pour tout k et donc elle ne converge pas vers une matrice triangulaire supérieure a priori. Cependant, si plusieurs valeurs propres ont même module, on va avoir une convergence vers une matrice triangulaire par blocs et chaque bloc concerne les valeurs propres d'un même module.
- En pratique, on met la matrice A sous forme de Hessenberg (extension au cas non symétrique de Householder) car la suite des (A_k) restera sous forme de Hessenberg, ce qui simplifiera les calculs.
- Pour trouver les vecteurs propres de A, on met A sous forme de Hessenberg : $A = PHP^{-1}$, on aura alors

  $$A_{k+1} = (Q_1Q_2 \dots Q_k)^{-1}H(Q_1Q_2 \dots Q_k)$$

  On aura alors $Q_1Q_2 \dots Q_k$ qui convergera vers une matrice contenant les vecteurs propres en colonne

Irréductibilité des polynômes cyclotomiques

Leçons : 141

Références : PERRIN, *Cours d'algèbre* (p.82) et DEMAZURE, *Cours d'algèbre* (p.206)

Prérequis :

- la division euclidienne dans $\mathbb{Z}[X]$
- $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$
- les polynômes cyclotomiques sont dans $\mathbb{Z}[X]$
- lien entre l'irréductibilité sur $\mathbb{Z}$ et sur $\mathbb{Q}$ (voir Appendice)

Notations :

- $\mu_n^\times(\mathbb{C})$ désignent les racines $n^{\text{ième}}$ primitives de l'unité sur $\mathbb{C}$, autrement dit, les générateurs du groupe $\mathbb{U}_n$ des racines $n^{\text{ième}}$ de l'unité.
- $\mu_n(\mathbb{C})$ désignent l'ensemble de toutes les racines $n^{\text{ième}}$ de l'unité sur $\mathbb{C}$.

Introduction :

On va montrer que les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$ et unitaires donc irréductibles aussi sur $\mathbb{Z}$.

Pour $n \in \mathbb{N}$, on définit le polynôme cyclotomique par

$$\phi_n(X) = \prod_{\zeta \in \mu_n^\times(\mathbb{C})} (X - \zeta)$$

Ainsi ϕ_n est de degré $\varphi(n)$ où $\varphi(n)$ est l'indicatrice d'Euler.

Théorème 1. Soit $n \in \mathbb{N}^*$. Le polynôme cyclotomique ϕ_n est dans $\mathbb{Z}[X]$ et est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$.

Idée de la preuve : On commencera par montrer que ϕ_n est dans $\mathbb{Z}[X]$ et unitaire. Ainsi il suffit de montrer qu'il est irréductible sur $\mathbb{Q}$ pour avoir le résultat du théorème (voir Appendice). Pour montrer que ϕ_n est irréductible sur $\mathbb{Q}$, on va montrer qu'il est égal au polynôme minimal d'une racine $n^{\text{ième}}$ primitive de l'unité. Pour cela, on montrera qu'il divise ϕ_n, qu'il est unitaire et qu'il est de degré égal au degré de ϕ_n.

Démonstration.
Étape 1 : *Montrons que tous les $\phi_n \in \mathbb{Z}[X]$ et sont unitaires.*

On procède par récurrence forte sur $n \in \mathbb{N}^*$.
Initialisation : Pour $n = 1$, on a

$$\phi_1(X) = X - 1 \in \mathbb{Z}[X] \text{ unitaire}$$

car 1 est la seule racine unième de l'unité.

Hérédité : Soit $n > 1$. On suppose que pour tout $k \in [\![1; n-1]\!]$, on a $\phi_k \in \mathbb{Z}[X]$ et unitaire.

Or on sait que dans $\mathbb{C}[X]$, on a

$$\phi_n = \frac{X^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \phi_d}$$ [1]

On note $F = \prod_{\substack{d|n \\ d \neq n}} \phi_d$ qui est, par hypothèse de récurrence, dans $\mathbb{Z}[X]$ et unitaire [2].

On a donc

$$X^n - 1 = F\phi_n \text{ dans } \mathbb{C}[X]$$

Comme F est unitaire, on peut faire la division euclidienne dans $\mathbb{Z}[X]$, on a donc

$$X^n - 1 = FP + R \text{ avec } \deg R < \deg F$$

Or c'est la même division que dans $\mathbb{C}[X]$, donc $P = \phi_n$ et $R = 0$. Ainsi, comme P est dans $\mathbb{Z}[X]$ et unitaire (car on divise un polynôme unitaire par un polynôme unitaire), on a $\phi_n \in \mathbb{Z}[X]$ et unitaire.

Conclusion : Ainsi pour tout $n \in \mathbb{N}^*$, le polynôme ϕ_n est dans $\mathbb{Z}[X]$ et est unitaire.

Étape 2 : *Définition des polynômes minimaux de racines $n^{ième}$ primitives de l'unité.*

Soit ζ une racine $n^{\text{ième}}$ primitive de l'unité. Soit p un nombre premier qui est premier avec n, *i.e.* $p \wedge n = 1$. On note $\omega = \zeta^p$, qui est donc aussi une racine $n^{\text{ième}}$ primitive de l'unité.

On note Π_ζ (respectivement Π_ω) le polynôme minimal de ζ (resp. ω) sur $\mathbb{Q}$.

Étape 3 : *Montrons que Π_ζ et Π_ω sont dans $\mathbb{Z}[X]$ et divisent ϕ_n.*

On utilise le caractère factoriel de $\mathbb{Z}[X]$ [3]. On peut donc écrire

$$\phi_n = \prod_i F_i^{\alpha_i}$$

où les (F_i) sont irréductibles sur $\mathbb{Z}$ et on peut les supposer unitaires car ϕ_n est unitaire.

On a $\phi_n(\zeta) = \phi_n(\omega) = 0$ car ce sont des racines $n^{\text{ième}}$ de l'unité. Il existe donc deux indices i_0 et i_1 dans $[\![1; r]\!]$ tels que

$$F_{i_0}(\zeta) = 0 \quad \text{et} \quad F_{i_1}(\omega) = 0$$

Or comme les polynômes F_{i_0} et F_{i_1} sont irréductibles, unitaires dans $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, on a

$$\Pi_\zeta = F_{i_0} \in \mathbb{Z}[X] \quad \text{et} \quad \Pi_\omega = F_{i_1} \in \mathbb{Z}[X]$$ [4]

Par définition des (F_i), on a donc

$$\Pi_\zeta \mid \phi_n \quad \text{et} \quad \Pi_\omega \mid \phi_n \text{ dans } \mathbb{Z}[X].$$

1. car $X^n - 1$ a pour racine toutes les racines $n^{\text{ième}}$ de l'unité et donc en partitionnant $\mu_n(\mathbb{C})$ par les $\mu_d^\times(\mathbb{C})$ avec $d \mid n$, on trouve $X^n - 1 = \prod_{d \mid n} \phi_d$
2. comme produit de polynômes unitaires
3. car $\mathbb{Z}$ l'est et on a un théorème qui dit que A est factoriel si et seulement si $A[X]$ est factoriel
4. car les polynômes minimaux sont irréductibles (voir Appendice)

Étape 4 : *Montrons que* $\Pi_\zeta = \Pi_\omega$.

Raisonnons par l'absurde, on suppose que $\Pi_\zeta \neq \Pi_\omega$. On sait qu'ils sont irréductibles dans $\mathbb{Z}[X]$ (par l'étape 3). On a donc

$$\Pi_\zeta \Pi_\omega \mid \phi_n \text{ dans } \mathbb{Z}[X]$$ [5]

Or par définition de ω et de Π_ω, on a

$$\Pi_\omega(\zeta^p) = 0$$

Donc

$$\Pi_\zeta \mid \Pi_\omega(X^p) \text{ dans } \mathbb{Z}[X]$$

A première vue, on a pour l'instant que

$$\Pi_\zeta \mid \Pi_\omega(X^p) \text{ dans } \mathbb{Q}[X]$$

C'est-à-dire

$$\Pi_\omega(X^p) = \Pi_\zeta(X)Q(X)$$

avec $Q \in \mathbb{Q}[X]$. Mais par la même technique qu'à l'étape 1, on peut effectuer la division euclidienne de $\Pi_\omega(X^p)$ par $\Pi_\zeta(X)$ dans $\mathbb{Z}[X]$

$$\Pi_\omega(X^p) = \Pi_\zeta(X)S(X) + R(X)$$

d'où $S = Q$ et $R = 0$. Donc $Q \in \mathbb{Z}[X]$. Ainsi

$$\Pi_\zeta \mid \Pi_\omega(X^p) \text{ dans } \mathbb{Z}[X]$$

On va noter $\overline{P} \in \mathbb{F}_p[X]$ la réduction du polynôme $P \in \mathbb{Z}[X]$ modulo p. Notre but est de prendre un facteur irréductible A de $\overline{\Pi_\zeta(X)}$, de montrer qu'il est forcément de degré 0 et inversible, donc il y aura contradiction car un facteur irréductible ne peut pas être inversible par définition.

On a par ce qui précède que

$$\overline{\Pi_\zeta(X)} \mid \overline{\Pi_\omega(X^p)} = \overline{\Pi_\omega(X)}^p \text{ dans } \mathbb{Z}[X]$$

Soit A un facteur irréductible de $\overline{\Pi_\zeta(X)}$ dans $\mathbb{F}_p[X]$. D'où

$$A \mid \overline{\Pi_\omega(X)}^p$$

Mais, par le caractère irréductible de A, on a

$$A \mid \overline{\Pi_\omega(X)} \text{ dans } \mathbb{F}_p[X]$$

Comme on a $\Pi_\zeta\Pi_\omega \mid \phi_n$ dans $\mathbb{Z}[X]$, on a

$$\overline{\Pi_\zeta\Pi_\omega} \mid \overline{\phi_n} \text{ dans } \mathbb{F}_p[X]$$

Donc

$$A^2 \mid \overline{\phi_n} \text{ dans } \mathbb{F}_p[X]$$

Puis

$$A^2 \mid \overline{X^n - 1} \text{ dans } \mathbb{F}_p[X] \tag{3.2}$$

5. puisque les indices i_0 et i_1 sont différents.

Il existe donc $B \in \mathbb{F}_p[X]$ tel que $\overline{X^n - 1} = A^2 B$. En dérivant, on trouve

$$\overline{nX^{n-1}} = A(2A'B + AB')$$

Ainsi, on a

$$A \mid \overline{nX^{n-1}} \tag{3.3}$$

On peut alors trouver à partir de (3.3) et (3.2) [6] que

$$A \mid \overline{nX^n} \quad \text{et} \quad A \mid \overline{nX^n - n}\,[7]$$

En utilisant la propriété $a \mid b$ et $a \mid c$ implique $a \mid b + c$, on a

$$A \mid \overline{n} \neq 0, \quad \overline{n} \neq 0 \text{ car } n \wedge p = 1$$

Ainsi A est de degré 0, et non nul, ce qui contredit l'irréductibilité de A (puisque $\mathfrak{p}$ est un corps).

On peut donc en conclure que

$$\Pi_\zeta = \Pi_\omega$$

Étape 5 : *Montrons que toute racine $n^{ième}$ primitive de l'unité est racine de Π_ζ.*

Toutes les racines $n^{\text{ième}}$ primitive de l'unité peuvent s'écrire ζ^m où $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ et $m \wedge n = 1$. Il faut remarquer qu'on a donc $p_i \wedge n = 1$ pour tout $i \in [\![1; s]\!]$.

Par l'étape 4, on sait que

$$\Pi_\zeta(\zeta) = 0 \implies \Pi_\zeta(\zeta^p) = 0$$

On peut donc prouver par récurrence sur le nombre de facteurs premiers de m que $\Pi_\zeta(\zeta^m) = 0$.

En effet, on va commencer par montrer que $\Pi_\zeta(\zeta) = 0 \implies \Pi_\zeta(\zeta^{p_1}) = 0$ car $\Pi_\zeta = \Pi_{\zeta^{p_1}}$. Puis on va montrer que $\Pi_\zeta(\zeta^{p_1}) = 0 \implies \Pi_\zeta(\zeta^{p_1^2}) = 0$ [8], etc jusqu'à $\Pi_\zeta(\zeta^{p_1^{\alpha_1}}) = 0$. Ensuite, on continue en montrant que $\Pi_\zeta(\zeta^{p_1^{\alpha_1}}) = 0 \implies \Pi_\zeta(\zeta^{p_1^{\alpha_1} p_2}) = 0$ [9], etc jusqu'à montrer que $\Pi_\zeta(\zeta^m) = 0$.

Étape 6 : *Conclusion.*

On sait que par l'étape 5, toute racine primitive est racine de Π_ζ donc $\deg \Pi_\zeta \geqslant \varphi(n)$. De plus, on a

$$\Pi_\zeta \mid \phi_n$$

Ainsi $\deg \Pi_\zeta = \varphi(n)$. Comme Π_ζ et ϕ_n sont unitaires, de même degré et que l'un divise l'autre, on a

$$\phi_n = \Pi_\zeta$$

On peut conclure que ϕ_n est irréductible sur $\mathbb{Q}$ car par définition des polynômes minimaux Π_ζ est irréductible sur $\mathbb{Q}$.

Enfin, comme ϕ_n est unitaire, à coefficients entiers et irréductible sur $\mathbb{Q}$, il est irréductible sur $\mathbb{Z}$ (voir Appendice). □

6. on a simplement multiplier la partie de droite par quelque chose, ça ne change donc pas le fait que A divise quelque chose de plus gros

7. car pour la deuxième divisibilité, on a $A \mid \overline{n(X^n - 1)}$

8. ici le ζ^{p_1} joue le rôle de ζ de l'étape 4 et $\zeta^{p_1^2} = (\zeta^{p_1})^{p_1}$ joue le rôle de ω

9. ici le $\zeta^{p_1^{\alpha_1}}$ joue le rôle de ζ de l'étape 4 et $(\zeta^{p_1^{\alpha_1}})^{p_2}$ joue le rôle de ω

Remarques :

Les premiers polynômes cyclotomiques sont

$$\begin{aligned}\phi_1(X) &= X-1\\ \phi_2(X) &= X+1\\ \phi_3(X) &= X^2+X+1\\ \phi_4(X) &= X^2+1\\ \phi_5(X) &= X^4+X^3+X^2+X+1\\ \phi_6(X) &= X^2-X+1\end{aligned}$$

Pour p premier,

$$\phi_p(X) = X^{p-1}+X^{p-2}+\cdots+X+1$$

On peut définir les polynômes cyclotomiques sur d'autres corps que sur $\mathbb{C}$. En effet, on pose alors la définition

$$\phi_{n,k}(X) = \prod_{\zeta\in\mu_n^\times(\mathbb{K}_n)} (X-\zeta)$$

où $\mathbb{K}_n$ est le corps de décomposition de X^n-1 sur le corps k.

Astuces de l'agrégatif :

Il faut faire attention aux espaces dans lesquels on vit [10], notamment lorsque l'on écrit $\Pi_\zeta \mid \Pi_\omega(X^p)$, est ce que l'on est dans $\mathbb{Z}[X]$ ou dans $\mathbb{Q}[X]$? La division euclidienne vit dans $\mathbb{C}[X]$, $\mathbb{Q}[X]$ ou $\mathbb{Z}[X]$, etc. La division euclidienne n'est licite que dans un anneau euclidien et $K[X]$ est euclidien si et seulement si K est un corps. Cependant, on peut effectuer la division euclidienne dans $A[X]$ où A est un anneau si on divise par un polynôme unitaire (c'est ce qu'on fait ici dans l'étape 1).

Le polynôme minimal d'un élément n'a de sens que dans un anneau principal puisqu'il est élément générateur de l'idéal annulant. Donc on ne peut pas définir le polynôme minimal sur $\mathbb{Z}[X]$. Le polynôme minimal est irréductible (voir Appendice).

L'étape 4 peut paraître longue et pas très intuitive, mais si on a dans la tête que si $a \mid b$ alors $a \mid bc$, on comprend bien comment cela s'enchaîne.

10. comme dans la vraie vie finalement

Formule de Poisson et Shannon

Leçons : 239 ; 246 ; 250

Références : BERNIS–BERNIS, *Analyse pour l'agrégation de mathématiques, 40 développements* (p.253)

Prérequis :

- le Théorème de Dirichlet
- l'espace de Schwartz $\mathcal{S}(\mathbb{R}) = \{f \in \mathcal{C}^\infty(\mathbb{R}, \mathbb{C}), \quad \forall \alpha, \beta \in \mathbb{N}, \|x^\alpha f^{(\beta)}\|_\infty < +\infty\}$
- la formule d'inversion de la transformée de Fourier dans la classe de Schwartz

$$2\pi f(x) = \hat{\hat{f}}(-x), \quad \forall x \in \mathbb{R}$$

Introduction :

La formule sommatoire de Poisson est une égalité entre des valeurs de la fonction f et ces coefficients de Fourier, elle permet notamment d'étudier le problème de l'échantillonnage de Shannon (repliements de spectre que l'on voit en physique quand les fréquences d'échantillonage sont trop grandes).

Théorème 1 (Formule Sommatoire de Poisson)**.** Soit $f \in \mathcal{S}(\mathbb{R})$.
Alors la série $\sum_{n\in\mathbb{Z}} f(.+2\pi n)$ converge normalement sur tout compact et

$$\forall x \in \mathbb{R}, \ \sum_{n\in\mathbb{Z}} f(x+2\pi n) = \frac{1}{2\pi} \sum_{n\in\mathbb{Z}} \hat{f}(n) e^{inx}$$

où $\hat{f}(\xi) = \int_{-\infty}^{+\infty} f(x) e^{-i\xi x} dx$.

Démonstration. **Étape 1 :** *Convergence normale de la somme.*

Puisque $f \in \mathcal{S}(\mathbb{R})$, il existe $M > 0$ telle que

$$\forall x \in \mathbb{R}, \ (1+x^2)|f(x)| \leqslant M.$$

Soit $[-K, K]$ un compact de $\mathbb{R}$, pour tout $x \in [-K, K]$ et $|n| > K$, on a

$$|f(x+2\pi n)| \leqslant \frac{M}{1+(x+2\pi n)^2} \leqslant \frac{M}{1+(2\pi|n|-K)^2}$$

qui est un terme positif de série convergente. Donc

$$\sum_{n\in\mathbb{Z}} \|f(.+2\pi n)\|_{\infty,K} \text{ converge}$$

Ainsi $\sum_{n\in\mathbb{Z}} f(.+2\pi n)$ converge normalement sur tout compact. Donc

$$\text{pour tout } x \in \mathbb{R}, \ \sum_{n\in\mathbb{Z}} f(x+2\pi n) \text{ converge}$$

On notera cette somme $F(x)$.

Étape 2 : *F est de classe $\mathcal{C}^1$.*

On peut faire la même chose avec f' car on a les mêmes hypothèses sur f et sur f' (on n'a pas utilisé le caractère $\mathcal{C}^1$ de f). Puisque $f \in \mathcal{C}^1$, $\sum f(.+2\pi n)$ converge simplement et $\sum f'(.+2\pi n)$ converge uniformément sur tout compact. On a $F \in \mathcal{C}^1$.

Étape 3 : *F est 2π-périodique.*

$$\text{Pour tout } x \in \mathbb{R},\ \sum_{n=-N}^{N} f(x+2\pi+2\pi n) = \sum_{n=-N-1}^{N+1} f(x+2\pi n) - f(x-2\pi N) - f(x-(N+1)2\pi)$$

Le membre de gauche tend vers $F(x+2\pi)$ et le membre de droit tend vers $F(x)$ quand N tend vers l'infini. Donc $F(x) = F(x+2\pi)$ pour tout $x \in \mathbb{R}$. Ainsi F est 2π-périodique.

Étape 4 : *Utilisation du théorème de Dirichlet sur F.*

On a $F \in \mathcal{C}^1$ et 2π-périodique, donc on peut appliquer le théorème de Dirichlet.
Ainsi $F(x) = \sum_{n\in\mathbb{Z}} c_n(F) e^{inx}$.
On calcule donc les coefficients de Fourier de F. Pour tout $n \in \mathbb{Z}$,

$$\begin{aligned}
c_n(F) &= \frac{1}{2\pi}\int_{-\pi}^{\pi} F(x)e^{-inx}dx \\
&= \frac{1}{2\pi}\int_{-\pi}^{\pi} \sum_{k=-\infty}^{+\infty} f(x+2\pi k)e^{-inx}dx \\
&= \frac{1}{2\pi}\sum_{k=-\infty}^{+\infty}\int_{-\pi}^{\pi} f(x+2\pi k)e^{-inx}dx \\
&= \frac{1}{2\pi}\sum_{k=-\infty}^{+\infty}\int_{(2k-1)\pi}^{(2k+1)\pi} f(u)e^{-inu}du \\
&= \frac{1}{2\pi}\int_{-\infty}^{+\infty} f(u)e^{-inu}du \\
&= \frac{1}{2\pi}\hat{f}(n)
\end{aligned}$$

D'où l'égalité pour tout $x \in \mathbb{R}$,

$$\sum_{n\in\mathbb{Z}} f(x+2\pi n) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} \hat{f}(n)e^{inx}$$

□

Proposition 1. Si de plus $\hat{f}$ est à support inclus dans $[-F, F]$ où $F \in \mathbb{R}_+^*$ [1]et si $2F \leqslant 2\pi$, alors, pour tout $x \in \mathbb{R}$, on a

$$f(x) = \sum_{k=-\infty}^{+\infty} f(k)\ \mathrm{sinc}(\pi(x-k))$$

Démonstration. On a $\hat{f} \in \mathcal{S}(\mathbb{R})$ car l'espace de Schwartz est stable par transformée de Fourier. Ainsi en appliquant la formule sommatoire de Poisson à $\hat{f}$, on trouve

$$\forall \xi \in \mathbb{R}, \quad \sum_{k=-\infty}^{+\infty} \hat{f}(\xi + 2\pi k) = \frac{1}{2\pi} \sum_{k=-\infty}^{+\infty} \hat{\hat{f}}(k) e^{ik\xi}$$

Par la formule d'inversion de Fourier dans $\mathcal{S}(\mathbb{R})$, on a

$$\hat{\hat{f}}(k) = 2\pi f(-k)$$

Donc

$$\sum_{k=-\infty}^{+\infty} \hat{f}(\xi + 2\pi k) = \sum_{k=-\infty}^{+\infty} f(-k) e^{ik\xi}.$$

On a $2F \leqslant 2\pi$, donc $\hat{f}(\xi + 2\pi k) = 0$ si $|\xi + 2\pi k| > \pi$. [2]
Donc si $\xi \in [-\pi, \pi]$, $\quad \forall k \in \mathbb{Z}\backslash\{0\}, \quad |\xi + 2\pi k| > \pi$.
Or on sait que le support de $\hat{f}$ est inclus dans $[-\pi, \pi]$, donc on a, pour tout $\xi \in \mathbb{R}$,

$$\begin{aligned}
\hat{f}(\xi) &= \mathbb{1}_{[-\pi,\pi]}(\xi) \hat{f}(\xi + 0) \\
&= \mathbb{1}_{[-\pi,\pi]}(\xi) \sum_{k=-\infty}^{+\infty} \hat{f}(\xi + 2\pi k) \\
&= \mathbb{1}_{[-\pi,\pi]}(\xi) \sum_{k=-\infty}^{+\infty} f(-k) e^{ik\xi}
\end{aligned}$$

On utilise de nouveau l'inversion de Fourier, afin d'avoir pour tout $x \in \mathbb{R}$,

$$\begin{aligned}
f(x) &= \frac{1}{2\pi} \int_{-\infty}^{+\infty} \hat{f}(\xi) e^{i\xi x} d\xi \\
&= \frac{1}{2\pi} \int_{-\pi}^{\pi} \sum_{k=-\infty}^{+\infty} f(-k) e^{ik\xi} e^{i\xi x} d\xi \\
&= \frac{1}{2\pi} \int_{-\pi}^{\pi} \sum_{k=-\infty}^{+\infty} f(-k) e^{i(k+x)\xi} d\xi \\
&= \frac{1}{2\pi} \int_{-\pi}^{\pi} \sum_{k=-\infty}^{+\infty} f(k) e^{i(x-k)\xi} d\xi
\end{aligned}$$

Or $\sum_{k=-\infty}^{+\infty} f(k) e^{i(x-k)\xi}$ converge normalement sur $[-\pi, \pi]$ donc uniformément sur $[-\pi, \pi]$, puisque

$$\begin{aligned}
|f(k) e^{i(x-k)\xi}| &\leqslant |f(k)| \\
&\leqslant \frac{M}{1 + k^2}
\end{aligned}$$

Ainsi l'interversion du signe intégral et du signe somme est licite, puisqu'on intègre sur le compact $[-\pi, \pi]$.

$$f(x) = \frac{1}{2\pi} \sum_{k=-\infty}^{+\infty} f(k) \int_{-\pi}^{\pi} e^{i(x-k)\xi} d\xi$$

1. On note F car cela représente la fréquence en physique.
2. par définition du support de $\hat{f}$

$$
\begin{aligned}
&= \begin{cases} \dfrac{1}{2\pi} \displaystyle\sum_{k=-\infty}^{+\infty} f(k) \left[\frac{e^{i(x-k)\xi}}{i(x-k)} \right]_{-\pi}^{\pi} & \text{si } x \notin \mathbb{Z} \\ \dfrac{1}{2\pi} \displaystyle\sum_{k \neq x} f(k) \left[\frac{e^{i(x-k)\xi}}{i(x-k)} \right]_{-\pi}^{\pi} + f(k) & \text{sinon} \end{cases} \\
&= \begin{cases} \dfrac{1}{2\pi} \displaystyle\sum_{k=-\infty}^{+\infty} f(k) \frac{e^{i(x-k)\pi} - e^{-i(x-k)\pi}}{i(x-k)} & \text{si } x \notin \mathbb{Z} \\ \dfrac{1}{2\pi} \displaystyle\sum_{k \neq x} f(k) \frac{e^{i(x-k)\pi} - e^{-i(x-k)\pi}}{i(x-k)} + f(k) & \text{sinon} \end{cases} \\
&= \frac{1}{2\pi} \sum_{k=-\infty}^{+\infty} f(k)\ 2\pi\ \mathrm{sinc}(\pi(x-k)) \\
&= \sum_{k=-\infty}^{+\infty} f(k)\ \mathrm{sinc}(\pi(x-k))
\end{aligned}
$$

Ce qui conclut la preuve du théorème. □

Astuces de l'agrégatif :

Il faut faire attention au sens que l'on donne aux séries que l'on manipule (famille sommable ? limite d'une somme partielle ?)

La définition de la transformée de Fourier n'est pas unique, j'ai choisi de prendre celle-ci car elle coïncide avec la définition que je me donne dans mon plan. J'ai donc changé la formule sommatoire de Poisson par rapport à celle qu'on a l'habitude de voir (voir l'appendice sur les conventions de Fourier)

Il faut savoir prouver la formule d'inversion de Fourier. Une technique est de poser la fonction

$$f_\varepsilon : t \mapsto e^{-\varepsilon t^2} e^{itx} \hat{f}(t)$$

et de faire tendre ε vers 0.

Remarques :

Si on considère les coefficients de Fourier pour des pulsations quelconques on aurait : $\forall T > 0, \omega = \dfrac{2\pi}{T}, \forall f \in \mathcal{C}^1, f(x) = O\left(\frac{1}{x^2}\right), f'(x) = O\left(\frac{1}{x^2}\right)$

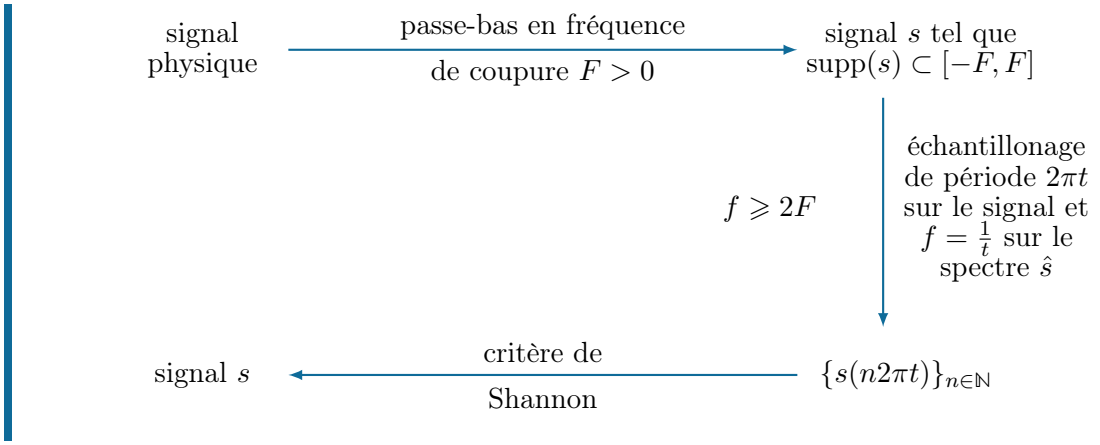
$$\forall x \in \mathbb{R}, \sum_{-\infty}^{+\infty} f(x+nT) = \frac{1}{T} \sum_{n=-\infty}^{+\infty} \hat{f}(n\omega) e^{in\omega x}$$

et $\forall s \in \mathcal{S}(\mathbb{R})$, si $\mathrm{supp}\hat{s} \subset [-F, F]$ où $0 < F \leqslant \dfrac{f}{2}$, on pose $t = \dfrac{1}{f}$

$$\forall \xi \in \mathbb{R}, \sum_{-\infty}^{+\infty} \hat{s}(\xi + nf) = t \sum_{n=-\infty}^{+\infty} \hat{\hat{s}}(2\pi nt) e^{2\pi int\xi}$$

$$\forall x \in \mathbb{R}, s(x) = \sum_{-\infty}^{+\infty} s(n2\pi t) \mathrm{sinc}(\frac{f}{2}x - \pi n)$$

On a noté f la fréquence d'échantillonage, t la période d'échantillonage et F la plus grande fréquence présente dans le spectre en fréquence du signal.


signal physique
passe-bas en fréquence de coupure $F > 0$
signal s tel que $\text{supp}(s) \subset [-F, F]$
$f \geqslant 2F$
échantillonage de période $2\pi t$ sur le signal et $f = \frac{1}{t}$ sur le spectre $\hat{s}$
signal s
critère de Shannon
$\{s(n2\pi t)\}_{n\in\mathbb{N}}$

Formule de Poisson et équivalent de Θ

Leçons : 224 ; 243 ; 246

Références : GOURDON, *Analyse* (p.269)

Prérequis :

- théorème de Dirichlet
- la convergence normale implique la convergence uniforme qui implique la convergence simple
- notions de série entière
- la formule de Cauchy
- $\int_{\mathbb{R}} e^{-\omega x^2} dx = \sqrt{\frac{\pi}{\omega}}$

Introduction :

La formule sommatoire est une identité classique et est un moyen très efficace pour prouver l'équation que vérifie la fonction Θ de Jacobi. En effet, on obtient des informations au voisinage de 1 en connaissant des informations en 0. La fonction Θ de Jacobi est une fonction spéciale, donc l'écriture usuelle est une fonction à deux variables.

Théorème 1 (Formule Sommatoire de Poisson)**.** Soit $f \in \mathcal{C}^1(\mathbb{R}, \mathbb{C})$ telle que $f(x) \underset{x\to\pm\infty}{=} O\Big(\frac{1}{x^2}\Big)$ et $f'(x) \underset{x\to\pm\infty}{=} O\Big(\frac{1}{x^2}\Big)$.
Alors la série $\sum_{n\in\mathbb{Z}} f(.+2\pi n)$ converge normalement sur tout compact et

$$\forall x \in \mathbb{R},\ \sum_{n\in\mathbb{Z}} f(x+2\pi n) = \frac{1}{2\pi} \sum_{n\in\mathbb{Z}} \hat{f}(n) e^{inx}$$

où $\hat{f}(\xi) = \int_{-\infty}^{+\infty} f(x) e^{-i\xi x} dx$.

Démonstration. **Étape 1 :** *Convergence normale de la somme.*

Par hypothèse, il existe $M > 0$ telle que

$$\forall x \in \mathbb{R},\ |f(x)| \leqslant \frac{M}{1+x^2}.$$

Soit $[-K, K]$ un compact de $\mathbb{R}$, pour tout $x \in [-K, K]$ et $|n| > K$, on a

$$|f(x+2\pi n)| \leqslant \frac{M}{1+(x+2\pi n)^2} \leqslant \frac{M}{1+(2\pi|n|-K)^2}$$

qui est un terme positif de série convergente. Donc

$$\sum_{n\in\mathbb{Z}} \|f(.+2\pi n)\|_{\infty,K} \text{ converge}$$

Ainsi $\sum_{n\in\mathbb{Z}} f(.+2\pi n)$ converge normalement sur tout compact. Donc

$$\text{pour tout } x\in\mathbb{R},\quad \sum_{n\in\mathbb{Z}} f(x+2\pi n) \text{ converge}$$

On notera cette somme $F(x)$.

Étape 2 : *F est de classe $\mathcal{C}^1$.*

On peut faire la même chose avec f' car on a les mêmes hypothèses sur f et sur f' (on n'a pas utilisé le caractère $\mathcal{C}^1$ de f). Puisque $f\in\mathcal{C}^1$, $\sum f(.+2\pi n)$ converge simplement et $\sum f'(.+2\pi n)$ converge uniformément sur tout compact. On a $F\in\mathcal{C}^1$.

Étape 3 : *F est 2π-périodique.*

$$\text{Pour tout } x\in\mathbb{R},\quad \sum_{n=-N}^{N} f(x+2\pi+2\pi n) = \sum_{n=-N-1}^{N+1} f(x+2\pi n) - f(x-2\pi N) - f(x-(N+1)2\pi)$$

Le membre de gauche tend vers $F(x+2\pi)$ et le membre de droit tend vers $F(x)$ quand N tend vers l'infini. Donc $F(x)=F(x+2\pi)$ pour tout $x\in\mathbb{R}$. Ainsi F est 2π-périodique.

Étape 4 : *Utilisation du théorème de Dirichlet sur F.* [1]

On a $F\in\mathcal{C}^1$ et 2π-périodique, donc on peut appliquer le théorème de Dirichlet.
Ainsi $F(x)=\sum_{n\in\mathbb{Z}} c_n(F)e^{inx}$.

On calcule donc les coefficients de Fourier de F. Pour tout $n\in\mathbb{Z}$,

$$\begin{aligned}
c_n(F) &= \frac{1}{2\pi}\int_{-\pi}^{\pi} F(x)e^{-inx}dx \\
&= \frac{1}{2\pi}\int_{-\pi}^{\pi} \sum_{k=-\infty}^{+\infty} f(x+2\pi k)e^{-inx}dx \\
&= \frac{1}{2\pi}\sum_{k=-\infty}^{+\infty}\int_{-\pi}^{\pi} f(x+2\pi k)e^{-inx}dx \\
&= \frac{1}{2\pi}\sum_{k=-\infty}^{+\infty}\int_{(2k-1)\pi}^{(2k+1)\pi} f(u)e^{-inu}du \\
&= \frac{1}{2\pi}\int_{-\infty}^{+\infty} f(u)e^{-inu}du \\
&= \frac{1}{2\pi}\hat{f}(n)
\end{aligned}$$

D'où l'égalité pour tout $x\in\mathbb{R}$,

$$\sum_{n\in\mathbb{Z}} f(x+2\pi n) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} \hat{f}(n)e^{inx}$$

□

1. On n'est pas obligé d'utiliser le théorème de Dirichlet. Comme $F\in\mathcal{C}^0_{2\pi}\cap\mathcal{C}^1$, la série de Fourier converge et comme $F\in\mathcal{C}^0$, par le théorème de Fejer, F est égale à sa série de Fourier si celle-ci converge et c'est le cas.

Définition 1. On définit $\Theta(z) = \sum_{n\in\mathbb{Z}} z^{n^2}$

Proposition 1. Θ est une série entière de rayon de convergence égal à 1.

Démonstration. On peut écrire

$$\Theta(z) = \sum_{n\in\mathbb{N}} a_n z^n \text{ où } a_n = \begin{cases} 2 & \text{si } n \text{ est un carré non nul} \\ 1 & \text{si } n = 0 \\ 0 & \text{sinon} \end{cases}$$

On voit alors que R le rayon de convergence vaut 1, puisque si $|z| > 1$, la série diverge grossièrement et pour $r \leqslant 1$, on a $|a_n|r^n$ borné. Donc $R = 1$. □

Théorème 2. On a $\Theta(x) \underset{x\to 1^-}{\sim} \sqrt{\frac{\pi}{1-x}}$.

Démonstration. On pose la fonction $f : x \mapsto e^{-\omega x^2}$ pour $\omega > 0$. La fonction f vérifie les hypothèses du théorème précédent, donc on peut appliquer la formule sommatoire de Poisson au point $x = 0$. On a

$$\sum_{n\in\mathbb{Z}} f(2\pi n) = \frac{1}{2\pi} \sum_{n\in\mathbb{Z}} \hat{f}(n)$$

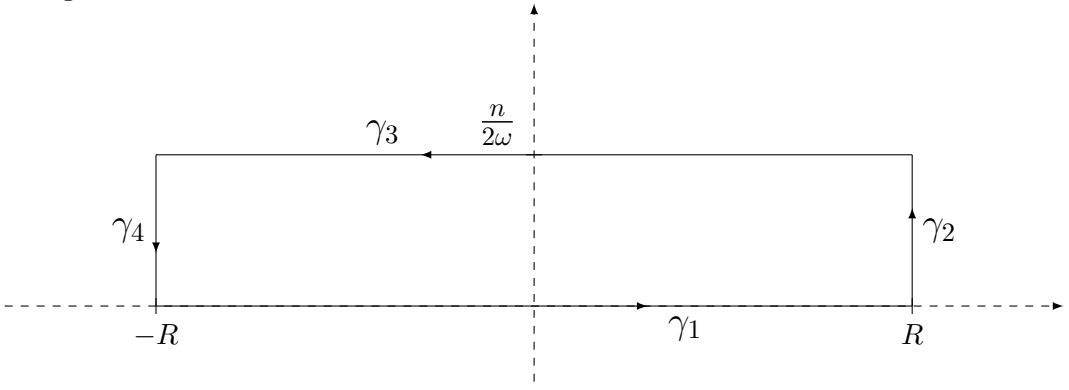
Or on a

$$\sum_{n\in\mathbb{Z}} f(2\pi n) = \sum_{n\in\mathbb{Z}} e^{-\omega 4\pi^2 n^2} = \Theta(e^{-\omega 4\pi^2})$$

On veut donc calculer $\hat{f}(n)$

$$\begin{aligned} \hat{f}(n) &= \int_{-\infty}^{+\infty} f(x)e^{-inx}dx \\ &= \int_{-\infty}^{+\infty} e^{-\omega x^2}e^{-inx}dx \\ &= \int_{-\infty}^{+\infty} e^{-\omega(x+\frac{in}{2\omega})^2}e^{-\frac{n^2}{4\omega}}dx \\ &= e^{-\frac{n^2}{4\omega}} \int_{-\infty}^{+\infty} e^{-\omega(x+\frac{in}{2\omega})^2}dx \end{aligned}$$

On veut calculer donc $\int_{-\infty}^{+\infty} e^{-\omega(x+\frac{in}{2\omega})^2}dx$ en posant la fonction holomorphe $g : z \mapsto e^{-\omega z^2}$ et en l'intégrant sur le contour suivant



On trouve donc $\int_{-\infty}^{+\infty} e^{-\omega(x+\frac{in}{2\omega})^2}dx = \int_{-\infty}^{+\infty} e^{-\omega x^2}dx = \sqrt{\frac{\pi}{\omega}}$.

Ainsi

$$\Theta(e^{-\omega 4\pi^2}) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} e^{-\frac{n^2}{4\omega}}\sqrt{\frac{\pi}{\omega}} = \frac{1}{2\pi}\sqrt{\frac{\pi}{\omega}}\Theta(e^{-\frac{1}{4\omega}})$$

On fait le changement de variable $x = e^{-\omega 4\pi^2}$, on a $x \to 1^-$ quand $\omega \to 0^+$. $\Theta(e^{-\frac{1}{4\omega}})$ tend vers 1 quand ω tend vers 0^+ car $e^{-\frac{1}{4\omega}}$ tend vers 0. Donc

$$\Theta(x) \underset{x\to 1^-}{\sim} \frac{1}{2\pi}\sqrt{\frac{\pi}{\omega}} \underset{x\to 1^-}{\sim} \frac{1}{2\pi}\sqrt{\frac{4\pi^2\pi}{-\ln(x)}} \underset{x\to 1^-}{\sim} \sqrt{\frac{\pi}{1-x}}$$

car[2] $-\ln(x) \underset{x\to 1^-}{\sim} 1-x$. On a donc bien

$$\Theta(x) \underset{x\to 1^-}{\sim} \sqrt{\frac{\pi}{1-x}}$$

□

Astuces de l'agrégatif :

Il faut faire attention à la définition de la convergence de la somme $\sum_{n\in\mathbb{Z}} f(.+2\pi n)$.

J'ai changé la formule sommatoire de Poisson par rapport à celle qu'on a l'habitude de voir car je voulais que la convention que j'ai prise pour la transformée de Fourier soit la même que celle de mon plan. (voir l'appendice sur les conventions de Fourier)

Dans un soucis de temps, je ne détaille pas l'intégration sur le contour dans le développement.

On revient sur le calcul de l'intégrale sur le contour : g est holomorphe sur $\mathbb{C}$, donc

$$\underbrace{\int_{\gamma_1} g(z)dz}_{I_1} + \underbrace{\int_{\gamma_2} g(z)dz}_{I_2} + \underbrace{\int_{\gamma_3} g(z)dz}_{I_3} + \underbrace{\int_{\gamma_4} g(z)dz}_{I_4} = 0$$

On pose :

$$\gamma_1 : \begin{cases} [-R;R] & \to & \mathbb{C} \\ t & \mapsto & t \end{cases} \qquad \gamma_2 : \begin{cases} [0;\frac{n}{2\omega}] & \to & \mathbb{C} \\ t & \mapsto & R+it \end{cases}$$

$$\gamma_3 : \begin{cases} [-R;R] & \to & \mathbb{C} \\ t & \mapsto & -t+\frac{in}{2\omega} \end{cases} \qquad \gamma_4 : \begin{cases} [0;\frac{n}{2\omega}] & \to & \mathbb{C} \\ t & \mapsto & -R+i(\frac{n}{2\omega}-t) \end{cases}$$

$$I_1 = \int_{\gamma_1} g(z)dz = \int_{-R}^{R} e^{-\omega t^2}dt \qquad I_2 = \int_{\gamma_2} g(z)dz = \int_0^{\frac{n}{2\omega}} e^{-\omega(R+it)^2}idt$$

$$I_3 = \int_{\gamma_3} g(z)dz = -\int_{-R}^{R} e^{-\omega(t-\frac{in}{2\omega})^2}dt \qquad I_4 = \int_{\gamma_4} g(z)dz = -\int_0^{\frac{n}{2\omega}} e^{-\omega(R-i(\frac{n}{2\omega}-t))^2}idt$$

Or I_2 et I_4 convergent vers 0 quand R tend vers $+\infty$ par convergence dominée car $e^{-\omega(R-i(\frac{n}{2\omega}-t))^2}i$ tend vers 0 et on a $|e^{-\omega(R-i(\frac{n}{2\omega}-t))^2}i| \leqslant e^{-\omega R}$ intégrable sur $[0;\frac{n}{2\omega}]$.

De plus, I_1 tend vers $\int_{-\infty}^{+\infty} e^{-\omega t^2}dt$ par convergence dominée avec $|\mathbb{1}_{-R;R}e^{-\omega t^2}| \leqslant e^{-\omega t^2}$ intégrable.

2. ici, on ne compose pas des équivalents, on prend juste une puissance et ça on a le droit

De même, I_3 tend vers $\int_{-\infty}^{+\infty} e^{-\omega(t-\frac{in}{2\omega})^2}dt$ par convergence dominée par une majoration similaire.

En conclusion, $\int_{-\infty}^{+\infty} e^{-\omega t^2}dt - \int_{-\infty}^{+\infty} e^{-\omega(t-\frac{in}{2\omega})^2}dt = 0$.

D'où,

$$\int_{-\infty}^{+\infty} e^{-\omega t^2}dt = \int_{-\infty}^{+\infty} e^{-\omega(t-\frac{in}{2\omega})^2}dt$$

Formule de Poisson et fonction Θ

Leçons : 246 ; 265

Références : GOURDON, *Analyse* (p.269)

Prérequis :

- théorème de Dirichlet
- la convergence normale implique la convergence uniforme qui implique la convergence simple
- la formule de Cauchy
- $\displaystyle\int_{\mathbb{R}} e^{-\omega x^2} dx = \sqrt{\frac{\pi}{\omega}}$

Introduction :

La formule sommatoire est une identité classique et est un moyen très efficace pour prouver l'équation que vérifie la fonction Θ de Jacobi. En effet, on obtient des informations au voisinage de 1 en connaissant des informations en 0. La fonction Θ de Jacobi est une fonction spéciale, donc l'écriture usuelle est une fonction à deux variables. [1]

Théorème 1 (Formule Sommatoire de Poisson)**.** Soit $f \in \mathcal{C}^1(\mathbb{R}, \mathbb{C})$ telle que $f(x) \underset{x\to\pm\infty}{=} O\Big(\frac{1}{x^2}\Big)$ et $f'(x) \underset{x\to\pm\infty}{=} O\Big(\frac{1}{x^2}\Big)$.
Alors la série $\displaystyle\sum_{n\in\mathbb{Z}} f(.+2\pi n)$ converge normalement sur tout compact et

$$\forall x \in \mathbb{R},\ \sum_{n\in\mathbb{Z}} f(x+2\pi n) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} \hat{f}(n) e^{inx}$$

où $\hat{f}(\xi) = \displaystyle\int_{-\infty}^{+\infty} f(x) e^{-i\xi x} dx$.

Démonstration. **Étape 1 :** *Convergence normale de la somme.*

Par hypothèse, il existe $M > 0$ telle que

$$\forall x \in \mathbb{R},\ |f(x)| \leqslant \frac{M}{1+x^2}.$$

Soit $[-K, K]$ un compact de $\mathbb{R}$, pour tout $x \in [-K, K]$ et $|n| > K$, on a

$$|f(x+2\pi n)| \leqslant \frac{M}{1+(x+2\pi n)^2} \leqslant \frac{M}{1+(2\pi|n|-K)^2}$$

1. Pour $z \in \mathbb{C}$ et $\tau \in \mathbb{H} := \{v \in \mathbb{C}, \mathscr{I}(v) > 0\}$, on a

$$\theta(z,\tau) = \sum_{n=-\infty}^{+\infty} \exp(i\pi n\tau + 2i\pi nz)$$

qui est un terme positif de série convergente. Donc

$$\sum_{n\in\mathbb{Z}} \|f(.+2\pi n)\|_{\infty,K} \text{ converge}$$

Ainsi $\sum_{n\in\mathbb{Z}} f(.+2\pi n)$ converge normalement sur tout compact. Donc

$$\text{pour tout } x\in\mathbb{R},\quad \sum_{n\in\mathbb{Z}} f(x+2\pi n) \text{ converge}$$

On notera cette somme $F(x)$.

Étape 2 : *F est de classe $\mathcal{C}^1$.*

On peut faire la même chose avec f' car on a les mêmes hypothèses sur f et sur f' (on n'a pas utilisé le caractère $\mathcal{C}^1$ de f). Puisque $f\in\mathcal{C}^1$, $\sum f(.+2\pi n)$ converge simplement et $\sum f'(.+2\pi n)$ converge uniformément sur tout compact. On a $F\in\mathcal{C}^1$.

Étape 3 : *F est 2π-périodique.*

$$\text{Pour tout } x\in\mathbb{R},\ \sum_{n=-N}^{N} f(x+2\pi+2\pi n) = \sum_{n=-N-1}^{N+1} f(x+2\pi n) - f(x-2\pi N) - f(x-(N+1)2\pi)$$

Le membre de gauche tend vers $F(x+2\pi)$ et le membre de droit tend vers $F(x)$ quand N tend vers l'infini. Donc $F(x)=F(x+2\pi)$ pour tout $x\in\mathbb{R}$. Ainsi F est 2π-périodique.

Étape 4 : *Utilisation du théorème de Dirichlet sur F.*

On a $F\in\mathcal{C}^1$ et 2π-périodique, donc on peut appliquer le théorème de Dirichlet.
Ainsi $F(x)=\sum_{n\in\mathbb{Z}} c_n(F)e^{inx}$.

On calcule donc les coefficients de Fourier de F. Pour tout $n\in\mathbb{Z}$,

$$\begin{aligned}
c_n(F) &= \frac{1}{2\pi}\int_{-\pi}^{\pi} F(x)e^{-inx}dx \\
&= \frac{1}{2\pi}\int_{-\pi}^{\pi} \sum_{k=-\infty}^{+\infty} f(x+2\pi k)e^{-inx}dx \\
&= \frac{1}{2\pi}\sum_{k=-\infty}^{+\infty}\int_{-\pi}^{\pi} f(x+2\pi k)e^{-inx}dx \\
&= \frac{1}{2\pi}\sum_{k=-\infty}^{+\infty}\int_{(2k-1)\pi}^{(2k+1)\pi} f(u)e^{-inu}du \\
&= \frac{1}{2\pi}\int_{-\infty}^{+\infty} f(u)e^{-inu}du \\
&= \frac{1}{2\pi}\hat{f}(n)
\end{aligned}$$

D'où l'égalité pour tout $x\in\mathbb{R}$,

$$\sum_{n\in\mathbb{Z}} f(x+2\pi n) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} \hat{f}(n)e^{inx}$$

□

Définition 1. On définit $\Theta(u) = \sum_{n\in\mathbb{Z}} e^{-\pi u n^2}$

Théorème 2. Pour tout $u > 0$, on a

$$\Theta(u) = \sqrt{\frac{1}{u}}\Theta\Big(\frac{1}{u}\Big)$$

Démonstration. On pose la fonction $f : x \mapsto e^{-\pi\omega x^2}$ pour $\omega > 0$. La fonction f vérifie les hypothèses du théorème précédent, donc on peut appliquer la formule sommatoire de Poisson au point $x = 0$. On a

$$\sum_{n\in\mathbb{Z}} f(2\pi n) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} \hat{f}(n)$$

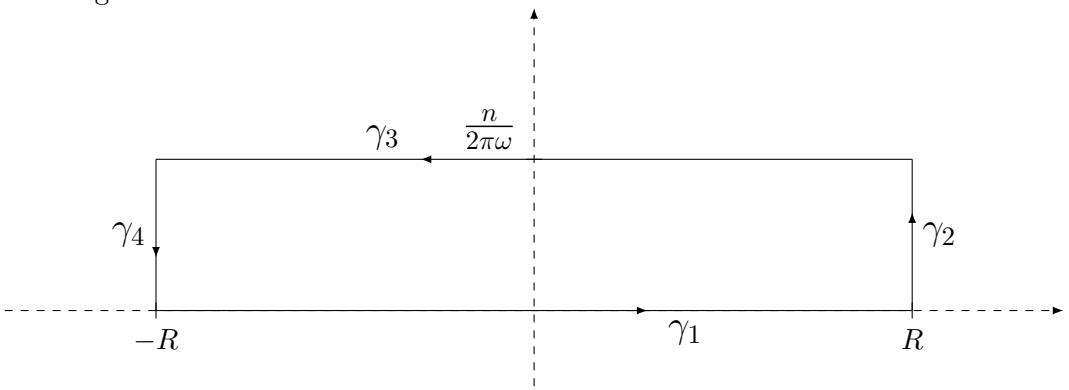
Or on a

$$\sum_{n\in\mathbb{Z}} f(2\pi n) = \sum_{n\in\mathbb{Z}} e^{-\pi\omega 4\pi^2 n^2} = \Theta(4\pi^2\omega)$$

On veut donc calculer $\hat{f}(n)$

$$\begin{aligned}
\hat{f}(n) &= \int_{-\infty}^{+\infty} f(x)e^{-inx}dx \\
&= \int_{-\infty}^{+\infty} e^{-\pi\omega x^2}e^{-inx}dx \\
&= \int_{-\infty}^{+\infty} e^{-\pi\omega(x+\frac{in}{2\pi\omega})^2}e^{-\frac{n^2}{4\pi\omega}}dx \\
&= e^{-\frac{n^2}{4\pi\omega}}\int_{-\infty}^{+\infty} e^{-\pi\omega(x+\frac{in}{2\pi\omega})^2}dx
\end{aligned}$$

On veut calculer donc $\int_{-\infty}^{+\infty} e^{-\pi\omega(x+\frac{in}{2\pi\omega})^2}dx$ en posant la fonction holomorphe $g : z \mapsto e^{-\pi\omega z^2}$ et en l'intégrant sur le contour suivant



On trouve donc $\int_{-\infty}^{+\infty} e^{-\pi\omega(x+\frac{in}{2\pi\omega})^2}dx = \int_{-\infty}^{+\infty} e^{-\pi\omega x^2}dx = \sqrt{\frac{1}{\omega}}$.

Ainsi

$$\Theta(4\pi^2\omega) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} e^{-\frac{n^2}{4\pi\omega}}\sqrt{\frac{1}{\omega}} = \sqrt{\frac{1}{4\pi^2\omega}}\Theta\Big(\frac{1}{4\pi^2\omega}\Big)$$

On fait le changement de variable $u = 4\pi^2\omega$, on trouve alors

$$\Theta(u) = \sqrt{\frac{1}{u}}\Theta\Big(\frac{1}{u}\Big)$$

□

Astuces de l'agrégatif :

Il faut faire attention à la définition de la convergence de la somme $\sum_{n\in\mathbb{Z}} f(.+2\pi n)$.

J'ai changé la formule sommatoire de Poisson par rapport à celle qu'on a l'habitude de voir car je voulais que la convention que j'ai prise pour la transformée de Fourier soit la même que celle de mon plan. (voir l'appendice sur les conventions de Fourier)

Dans un soucis de temps, je ne détaille pas l'intégration sur le contour dans le développement.

On revient sur le calcul de l'intégrale sur le contour : g est holomorphe sur $\mathbb{C}$, donc

$$\underbrace{\int_{\gamma_1} g(z)dz}_{I_1} + \underbrace{\int_{\gamma_2} g(z)dz}_{I_2} + \underbrace{\int_{\gamma_3} g(z)dz}_{I_3} + \underbrace{\int_{\gamma_4} g(z)dz}_{I_4} = 0$$

On pose :

$$\gamma_1 : \begin{cases} [-R;R] & \to & \mathbb{C} \\ t & \mapsto & t \end{cases} \qquad \gamma_2 : \begin{cases} [0;\frac{n}{2\pi\omega}] & \to & \mathbb{C} \\ t & \mapsto & R+it \end{cases}$$

$$\gamma_3 : \begin{cases} [-R;R] & \to & \mathbb{C} \\ t & \mapsto & -t+\frac{in}{2\pi\omega} \end{cases} \qquad \gamma_4 : \begin{cases} [0;\frac{n}{2\pi\omega}] & \to & \mathbb{C} \\ t & \mapsto & -R+i(\frac{n}{2\pi\omega}-t) \end{cases}$$

$$I_1 = \int_{\gamma_1} g(z)dz = \int_{-R}^{R} e^{-\pi\omega t^2}dt \qquad I_2 = \int_{\gamma_2} g(z)dz = \int_0^{\frac{n}{2\pi\omega}} e^{-\pi\omega(R+it)^2}idt$$

$$I_3 = \int_{\gamma_3} g(z)dz = -\int_{-R}^{R} e^{-\pi\omega(t-\frac{in}{2\pi\omega})^2}dt \qquad I_4 = \int_{\gamma_4} g(z)dz = -\int_0^{\frac{n}{2\pi\omega}} e^{-\pi\omega(R-i(\frac{n}{2\pi\omega}-t))^2}idt$$

Or I_2 et I_4 convergent vers 0 quand R tend vers $+\infty$ par convergence dominée car $e^{-\pi\omega(R-i(\frac{n}{2\pi\omega}-t))^2}i$ tend vers 0 et on a $|e^{-\pi\omega(R-i(\frac{n}{2\pi\omega}-t))^2}i| \leqslant e^{-\pi\omega R}$ intégrable sur $[0;\frac{n}{2\pi\omega}]$.

De plus, I_1 tend vers $\int_{-\infty}^{+\infty} e^{-\pi\omega t^2}dt$ par convergence dominée avec $|\mathbb{1}_{-R;R}e^{-\pi\omega t^2}| \leqslant e^{-\pi\omega t^2}$ intégrable.

De même, I_3 tend vers $\int_{-\infty}^{+\infty} e^{-\pi\omega(t-\frac{in}{2\pi\omega})^2}dt$ par convergence dominée par une majoration similaire.

En conclusion, $\int_{-\infty}^{+\infty} e^{-\pi\omega t^2}dt - \int_{-\infty}^{+\infty} e^{-\pi\omega(t-\frac{in}{2\pi\omega})^2}dt = 0$.

D'où,

$$\int_{-\infty}^{+\infty} e^{-\pi\omega t^2}dt = \int_{-\infty}^{+\infty} e^{-\pi\omega(t-\frac{in}{2\pi\omega})^2}dt$$

3.5 Développements d'informatiques

Tri par tas

Leçons : 901 ; 903 ; 926

Références : CORMEN–LEISERSON–RIVEST–STEIN, *Introduction à l'algorithmique* (p.139) [CLRS10] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 634) [LMLBP20]

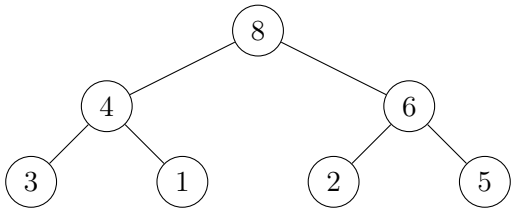
Introduction :

On va présenter ici un algorithme de tri par comparaisons dont la complexité est en $O(n \log n)$, donc c'est un tri optimal pour les tris par comparaisons puisque la complexité minimale est en $O(n \log n)$. Il a la même complexité que les tris fusion et rapide. [1] Le tri par tas n'est pas un tri stable, mais il est en place.

Définition 1 (Tas)**.** Un tas est un arbre binaire où chaque noeud est supérieur ou égal à chacun de ses fils, tous les niveaux de l'arbre doivent être remplis et le dernier niveau est tassé vers la gauche.

On parle en réalité de tas-max, on pourrait définir le tas-min si la relation d'ordre était "inférieur ou égal", mais ici, on ne considèrera que des tas-max.

On implémente le tas dans une structure de tableau indexé en commençant par 1. Ainsi les fils du noeud en case i sont en cases $2i$ pour le fils gauche et $2i+1$ pour le fils droit et le père d'un noeud i est en case $\lfloor i/2 \rfloor$.



Représenté dans le tableau $[\![8;\ 4;\ 6;\ 3;\ 1;\ 2;\ 5]\!]$ avec une taille 7.

Un tas est la donnée de son tableau associé et de sa taille : $T = (tab, taille)$.

On va présenter trois algorithmes : le premier est une fonction auxiliaire, le deuxième construit la structure de tas et le troisième est le tri en lui-même.

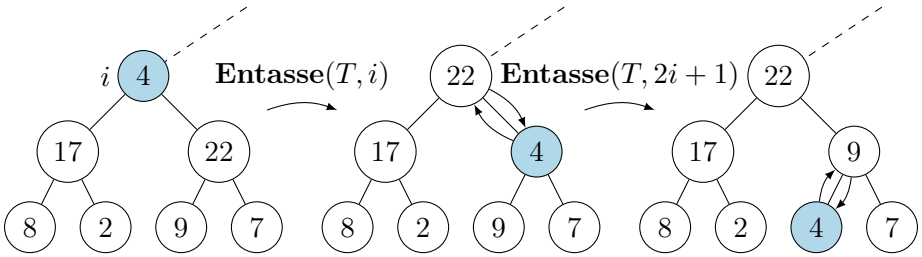
Le premier algorithme est **Entasse**(T, i) qui transforme le sous-arbre de racine i en un tas, en supposant que les deux fils de i sont bien des tas.

1. attention toutefois à quelle complexité on regarde, on parle de temporelle au pire ? en moyenne ?

Algorithme 1 Entasse

```
Procédure Entasse(T, i)
    max ← i ;
    g ← 2i ;        #gauche(i)
    d ← 2i + 1   #droite(i)
    Si (g ⩽ T.taille et T.tab[g] > T.tab[max]) alors
        max ← g
    Fin Si
    Si (d ⩽ T.taille et T.tab[d] > T.tab[max]) alors
        max ← d
    Fin Si
    Si (max ≠ i) alors
        échanger T.tab[i] et T.tab[max] ;
        Entasse(T, max)
    Fin Si

Fin
```



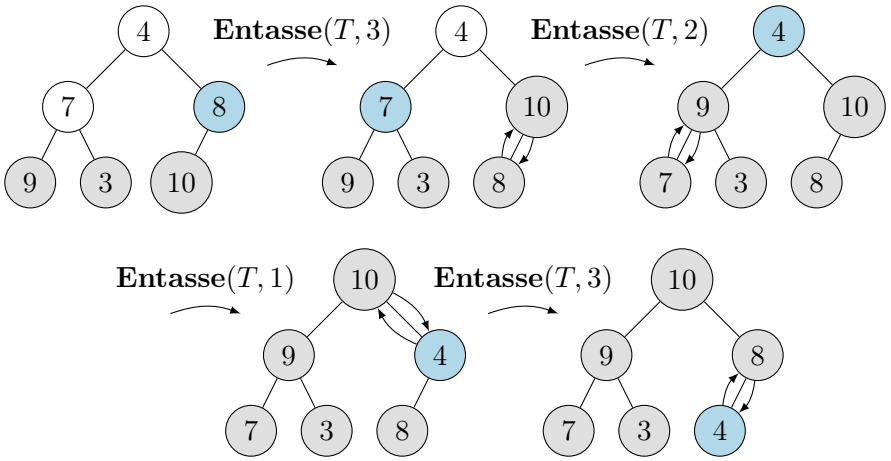
L'algorithme termine car la hauteur est finie. L'algorithme est correct car il place l'élément maximal en position i donc le sous tas inchangé (par exemple $2i$) reste un tas et possède comme père un élément plus grand que tous ses éléments et l'autre sous tas ($2i+1$ dans l'exemple) va avoir l'élément maximal en père et comme ses propres fils sont des tas car $2i+1$ était supposé être un tas, on peut effectuer l'algorithme sur $2i+1$.

Cet algorithme effectue seulement des comparaisons, des affectations ou des échanges (donc en coût constant) puis effectue de nouveau l'algorithme sur un seul de ses fils au pire des cas, donc l'algorithme est en $\mathcal{O}(h - p(i))$ en notant h la hauteur du tas et $p(i)$ la hauteur du noeud i dans le tas. Or $h = \log n$ car le tas est presque complet, donc la complexité de **Entasse** est en au pire $\mathcal{O}(\log n)$.

Le deuxième algorithme **Constuit**(T) sert à construire un tas à partir d'un tableau désordonné. On utilise la programmation dynamique car on va commencer par construire des tas à partir des feuilles et remonter petit à petit jusqu'à la racine en utilisant les tas déjà fabriqués et la fonction **Entasse**.

Algorithme 2 Construit

```
Procédure Construit(T)
    Pour i de ⌊T.taille/2⌋ à 1 faire
        Entasse(T, i)
    Fin Pour
Fin
```



Il suffit de faire une boucle décroissante à partir de $taille/2$ car avant tous les éléments sont des feuilles et donc des tas.

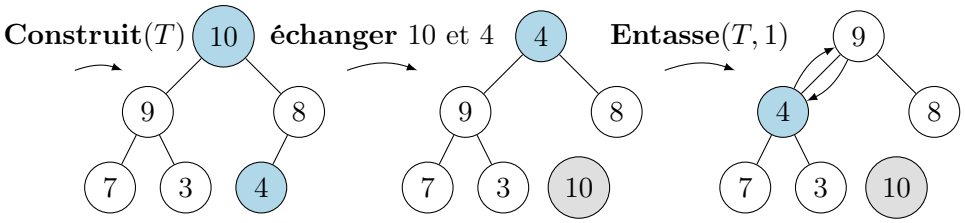
La complexité de **Construit** est naïvement en $\mathcal{O}(n \log n)$ car pour chaque élément on appelle **Entasse**, mais on peut calculer plus finement pour avoir une complexité linéaire.

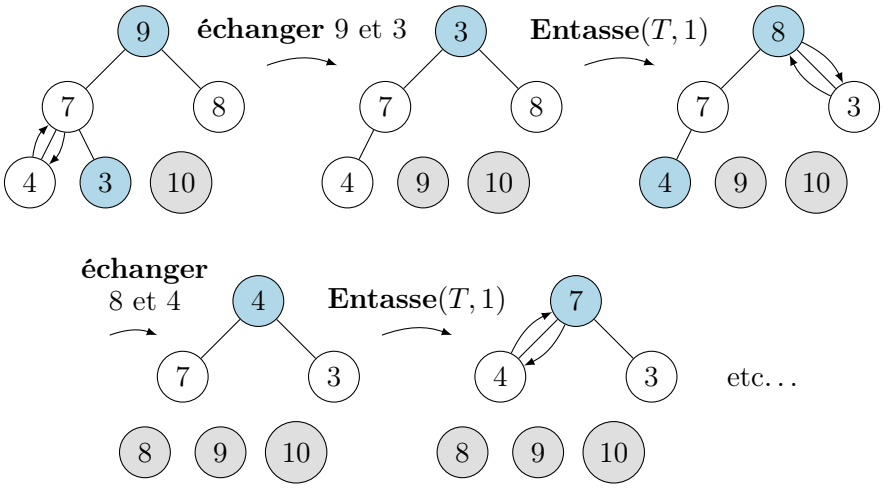
Chaque noeud qui est de profondeur p s'entasse en $\mathcal{O}(h-p)$ et il y a au plus 2^p noeuds de profondeur p dans le tas, donc la complexité de **Construit** est en $\mathcal{O}\big(\sum_{p=0}^{h-1} 2^p(h-p)\big) = \mathcal{O}\big(\sum_{k=1}^{h} 2^{h-k}k\big) = \mathcal{O}\big(n\sum_{k=1}^{h}(1/2)^k k\big) = \mathcal{O}(2n) = \mathcal{O}(n)$ car $2^h = n$.

Le troisième algorithme **Tri_par_tas**(T) est l'algorithme qui permettra de trier notre tableau. Pour cela, on va construire notre tas, puis on va inverser l'élément maximal et le dernier élément du tas, diminuer la taille du tas de 1, puis faire redescendre la racine dans le tas avec la fonction **Entasse**. Ainsi à la fin de l'algorithme les éléments seront triés par ordre croissant.

Algorithme 3 Tri_par_tas

```
Procédure Tri_par_tas(T)
    Construit(T)
    Pour i de T.taille à 2 faire
        échanger T.tab[1] et T.tab[i] ;
        T.taille ← T.taille − 1 ;
        textbfEntasse(T, 1)
    Fin Pour
Fin
```





La complexité du **Tri_par_tas** est en $\mathcal{O}(n) + \mathcal{O}(n \log n) = \mathcal{O}(n \log n)$. Ce tri possède l'avantage d'être un tri en place, il ne demande pas d'allocation mémoire supplémentaire.

Astuces de l'agrégatif :

Le développement peut-être assez long, je choisis de dérouler les algorithmes sur des exemples pour chaque algorithme, cependant il faut bien avoir conscience des preuves de terminaison et correction des algorithmes. On peut faire différemment et prouver la correction de chaque algorithme par exemple.

J'écris l'algorithme **Entasse** en pseudo-code lors du développement.

Questions possibles :

- Quels sont les invariants pour prouver la correction ?
- Connaissez vous d'autres tris en $O(n \log n)$?

  Réponse : Tri fusion, tri rapide
- Est-ce qu'on peut faire mieux que $O(n \log n)$?

  Réponse : pour un tri par comparaison, c'est la borne inférieure, mais avec plus d'hypothèses, on peut avoir des tris linéaires (par dénombrement, par base, par paquets)
- En considérant $([\![5, 7, 4, 4, 6, 2]\!], 6)$, montrer que le tri par tas n'est pas stable.

Master Theorem

(rédigé par Clarence Kineider)

Leçons : (903) ; 926 ; 931

Références : BEAUQUIER–BERSTEL–CHRÉTIENNE, *Éléments d'algorithmique* (p.30) [BBC92]

Introduction :

On va présenter un théorème essentiel qui permet de donner la complexité d'algorithmes utilisant le paradigme "diviser pour régner". Cependant, on ne peut pas donner la complexité de tous les algorithmes de "diviser pour régner" avec ce théorème.

Théorème 1. Soit $T : \mathbb{N} \to \mathbb{R}_+$ croissante à partir d'un certain rang. On suppose qu'il existe un rang $n_0 \geqslant 1$, des entiers $b \geqslant 2$ et $k \geqslant 0$ ainsi que des réels $a, c, d > 0$ tels que la relation de récurrence suivante soit vérifiée :

$$\begin{cases} T(n_0) = d \\ T(n) = aT\left(\frac{n}{b}\right) + cn^k \text{ pour tout entier de la forme } n = b^p n_0 \text{ avec } p \in \mathbb{N} \end{cases}$$

Alors on a la disjonction de cas suivante :

(i) Si $a < b^k$ alors $T(n) = \Theta(n^k)$

(ii) Si $a = b^k$ alors $T(n) = \Theta(n^k \log_b(n))$

(iii) Si $a > b^k$ alors $T(n) = \Theta(n^{\log_b(a)})$

Démonstration. **Étape 1 :** *Cas $n = n_0 b^p$*

Soit $p \in \mathbb{N}$, $n = b^p n_0$. Par récurrence, on a :

$$T(n) = da^p + \sum_{i=0}^{p-1} ca^i \left(\frac{n}{b^i}\right)^k = \underbrace{da^p}_{\delta(n)} + cn^k \underbrace{\sum_{i=0}^{p-1} \left(\frac{a}{b^k}\right)^i}_{\gamma(n)}$$

On a $\delta(n) = da^p = da^{\log_b(n) - \log_b(n_0)} = \dfrac{d}{a^{\log_b(n_0)}} b^{log_b(a) log_b(n)} = \dfrac{d}{a^{\log_b(n_0)}} n^{\log_b(a)} = \Theta(n^{\log_b(a)})$.

De plus, $\gamma(n)$ est une somme partielle d'une série géométrique. On distingue trois cas :

— Si $a < b^k$, la série géométrique de raison $\frac{a}{b^k}$ converge, donc $\gamma(n)$ est bornée. On a donc

$$T(n) = \Theta(n^{\log_b(a)}) + \Theta(n^k) = \Theta(n^k)$$

car $\log_b(a) < k$.

— Si $a = b^k$, alors $\gamma(n) = p = \log_b(n) - \log_b(n_0) = \Theta(\log_b(n))$. Donc

$$T(n) = \Theta(n^{\log_b(a)}) + \Theta(n^k \log_b(n)) = \Theta(n^k \log_b(n))$$

car $\log_b(a) = k$.

— Si $a > b^k$, alors $\gamma(n) \sim \alpha \dfrac{a^p}{b^{kp}}$ avec $\alpha = \dfrac{1}{\frac{a}{b^k} - 1}$. Donc $cn^k \gamma(n) \sim c\alpha \left(\dfrac{n}{b^p}\right)^k a^p \sim c\alpha n_0^k a^p$. Or $a^p = \Theta(n^{\log_b(a)})$, donc on a

$$T(n) = \Theta(n^{\log_b(a)}) + \Theta(n^{\log_b(a)}) = \Theta(n^{\log_b(a)})$$

On a donc le résultat pour n de la forme $n = b^p n_0$ avec $p \in \mathbb{N}$.

Étape 2 : *Cas $n \in \mathbb{N}$*

Soit $n \geq n_0$ et $p \in \mathbb{N}$ tel que $b^p n_0 \leq n < b^{p+1} n_0$. Puisque T est croissante à partir d'un certain rang, pour n assez grand on a

$$T(b^p n_0) \leq T(n) < T(b^{p+1} n_0)$$

Or pour $f \in \left\{m \mapsto m^k, m \mapsto m^k \log_b(m), m \mapsto m^{\log_b(a)}\right\}$, on a $f(bm) = \Theta(f(m))$. Par encadrement, on a le résultat pour tout n à partir d'un certain rang. □

Astuces de l'agrégatif :

Suivant votre vitesse, vous pouvez ajouter une application à l'algorithme de votre choix (tri fusion pour la leçon 903 par exemple).

Si on a seulement une majoration dans l'hypothèse de récurrence (i.e. $T(n) \leq aT\left(\frac{n}{b}\right) + cn^k$), on a le même résultat mais avec des O à la place des Θ. En effet, il suffit de voir qu'on a $T(n) \leq \delta(n) + cn^k\gamma(n)$ pour les mêmes δ et γ que dans la démonstration. Cela permet d'appliquer le théorème à des relations de type $T(n) = aT\left(\frac{n}{b}\right) + O(n^k)$.

Remarques :

Voici une technique pour se passer de l'hypothèse de croissance de T :
Je la rédige pour le tri fusion, mais elle devrait s'adapter à n'importe quel algorithme.
On note $T(n)$ le temps d'exécution dans le cas le pire pour une entrée de taille n. On pose $T_m(n) = \max_{k \leq n} T(n)$ le temps d'exécution dans le cas le pire pour une entrée de taille inférieure ou égale à n. On a alors T_m croissante. On montre que T_m vérifie les hypothèses du Master Theorem avec une inégalité :

$$T_m(n) \leq T_m\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + T_m\left(\left\lceil \frac{n}{2} \right\rceil\right) + cn \leq 2T_m\left(\left\lceil \frac{n}{2} \right\rceil\right) + cn$$

Donc pour $n = 2^k$ on a :

$$T_m(2^k) \leq 2T_m(2^{k-1}) + cn$$

Par le Master Theorem, on a donc $T_m(n) = O(n \log(n))$ car T_m est croissante.
Donc $T(n) \leq T_m(n) = O(n \log(n))$.

Remarques :

Voilà quelques problèmes qui utilisent ce théorème :

- Tri fusion ($a = 2, b = 2, k = 1$) (cas (ii))
- Multiplication de Matrices par Strassen ($a = 7, b = 2, k = 2$) (cas (iii))
- Dichotomie sur tableau trié ($a = 1, b = 2, k = 0$) (cas (ii))
- Multiplication d'entiers par la relation de Karatsuba ($a = 3, b = 2, k = 1$) (cas (iii))
- Dichotomie sur une liste triée ($a = 1, b = 2, k = 1$) (cas (i))

Attention, on ne peut pas utiliser ce théorème pour le tri rapide (car on ne divise pas la taille de notre objet par une quantité constante (la constante b))

Indécidabilité de la validité d'une formule en logique du premier ordre

Leçons : 914 ; 924

Références : HUTH–RYAN, *Logic in computer science* (p.133) [HR04] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 812) [LMLBP20]

Remarques :
La référence peut différer de la version que j'écris ci-dessous, car j'ai écris le développement en faisant la réduction moi-même (en m'appuyant tout de même sur le polycopié de François Schwarzentruber). Puis durant l'année, on a trouvé une référence, donc je la mets ici mais je ne m'en suis pas servi pour écrire le développement.

On utilise ici un schéma de preuve classique (la réduction) pour montrer l'indécidabilité de la validité en logique du premier ordre, ce qui permet d'illustrer la leçon 914. Ce problème s'intègre aussi dans la leçon 924 puisque d'une part, la preuve de la réduction met en jeu des manipulations de modèles et d'autre part, ce résultat montre l'indécidabilité de la théorie vide.

Prérequis :

- indécidabilité du problème Post
- bien différencier la syntaxe et la sémantique de la logique du premier ordre
- notions de modèles et théorie en logique du premier ordre

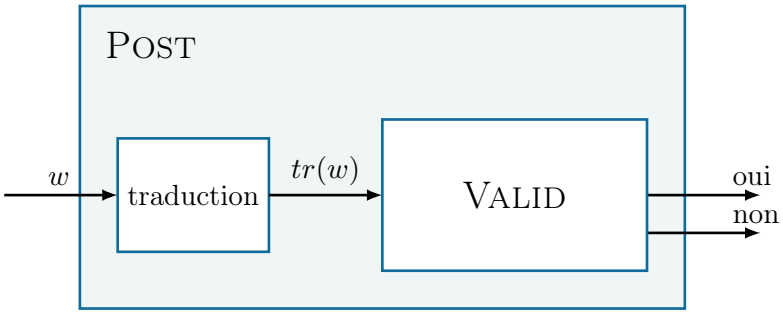
Introduction :
On va montrer que la validité d'une formule close en logique du premier ordre est un problème indécidable. Pour cela on va réduire Post à Valid.

Théorème 1. Le problème

Valid { entrée : une formule φ close en logique du premier ordre
sortie : oui si φ est valide, non sinon

est indécidable

Démonstration : On va réduire le problème Post au problème Valid. On sait que le problème Post est indécidable[1], donc si on réduit le problème Post au problème Valid, il sera lui aussi indécidable, car s'il était décidable, on rendrait le problème Post décidable, ce qui serait absurde.



1. voir appendice

On se place sur l'alphabet $\Sigma = \{a, b\}$. Soit w une instance du problème de Post, autrement dit un ensemble fini de N tuiles de la forme $\boxed{\begin{array}{|c|}\hline u_i \\ \hline v_i \\ \hline \end{array}}$, pour i allant de 1 à N avec u_i et v_i des mots sur l'alphabet Σ. On suppose que la tuile $\boxed{\begin{array}{|c|}\hline \varepsilon \\ \hline \varepsilon \\ \hline \end{array}}$ n'est pas dans w[2]. On rappelle que le problème de Post est de savoir s'il existe ou non une suite de tuiles telle qu'en les concaténant, les mots du haut et du bas formés par la concaténation des tuiles sont les deux mêmes.

On pose $tr(w) = (\varphi \to \psi)$ avec :

$$\varphi = p(\varepsilon, \varepsilon) \wedge \bigwedge_{i=1}^{N} \Big(\forall x \forall y \big(p(x, y) \to p(u_i(x), v_i(y)) \big) \Big)$$

$$\psi = \exists x \Big(p(a(x), a(x)) \vee p(b(x), b(x)) \Big)$$

Notation :

- pour chaque mot $m = m_1 m_2 \dots m_n$, on notera $m(.) = m_1 m_2 \dots m_n(.) = m_n(m_{n-1}(\dots m_1(.) \dots))$ (pour justifier l'écriture $u_i(x)$)
- on notera $\boxed{\boxed{\begin{array}{|c|}\hline x \\ \hline y \\ \hline \end{array}}}$ une succession de tuiles de w telle que le mot du haut soit x et celui du bas y. Cela sous entend qu'en écrivant $\boxed{\boxed{\begin{array}{|c|}\hline x \\ \hline y \\ \hline \end{array}}}$, il existe une succession de tuiles de w qui forme les mots x en haut et y en bas.

Il y a deux résultats à prouver :

— $tr(.)$ est une fonction calculable, c'est bien le cas car tr effectue un calcul fini pour toute instance de Post (il y a toujours un nombre fini de tuiles, et donc cela prend un temps fini pour créer la formule $\varphi \to \psi$).

— $tr(w)$ valide SSI w est une instance positive du problème de Post.

$\boxed{\Longrightarrow}$ Pour le sens direct :

La formule $\varphi \to \psi$ est valide donc pour tout modèle $\mathcal{M}$, on a $\mathcal{M} \vDash (\varphi \to \psi)$.

On choisit le modèle $\mathcal{M}$ suivant :

- le domaine est $\mathcal{D}_{\mathcal{M}} = \Sigma^*$
- $\varepsilon^{\mathcal{M}}$ correspond à ε_{Σ^*}
- $a^{\mathcal{M}}(.) : \begin{cases} \Sigma^* & \to & \Sigma^* \\ x & \mapsto & xa \end{cases}$
- $b^{\mathcal{M}}(.) : \begin{cases} \Sigma^* & \to & \Sigma^* \\ x & \mapsto & xb \end{cases}$
- $p^{\mathcal{M}}(.,.) : \begin{cases} (\Sigma^*)^2 & \to & \{0,1\} \\ (x, y) & \mapsto & \begin{cases} 1 & \text{si } \boxed{\boxed{\begin{array}{|c|}\hline x \\ \hline y \\ \hline \end{array}}} \text{ existe} \\ 0 & \text{sinon} \end{cases} \end{cases}$

2. Cela ne serait pas très interessant car toute instance du problème de Post qui contient $\boxed{\begin{array}{|c|}\hline \varepsilon \\ \hline \varepsilon \\ \hline \end{array}}$ est positive, il suffit de mettre la tuile $\boxed{\begin{array}{|c|}\hline \varepsilon \\ \hline \varepsilon \\ \hline \end{array}}$ pour avoir une solution. Il suffit alors de donner une formule valide comme traduction de cette instance de Post

Montrons que $\mathcal{M} \vDash \varphi$:

On a $\mathcal{M} \vDash p(\varepsilon, \varepsilon)$ [3].

Puis pour tout mot $u, v \in \Sigma^*$, on a si $\mathcal{M} \begin{bmatrix} x := u \\ y := v \end{bmatrix} \vDash p(x, y)$ cela veut dire que $\left\| \begin{array}{|c|} \hline u \\ \hline v \\ \hline \end{array} \right\|$ existe. Donc en concaténant $\left\| \begin{array}{|c|} \hline u \\ \hline v \\ \hline \end{array} \right\|$ et $\begin{array}{|c|} \hline u_i \\ \hline v_i \\ \hline \end{array}$, il existe bien $\left\| \begin{array}{|c|} \hline uu_i \\ \hline vv_i \\ \hline \end{array} \right\|$ pour tout $i \in \{1, \dots, N\}$, alors $\mathcal{M} \begin{bmatrix} x := u \\ y := v \end{bmatrix} \vDash p(u_i(x), v_i(y))$.
Donc pour tout $i \in \{1, \dots, N\}$, $\mathcal{M} \vDash \Big(\forall x \forall y \big(p(x, y) \to p(u_i(x), v_i(y))\big)\Big)$ Ainsi $\mathcal{M} \vDash \varphi$.

Or la formule $\varphi \to \psi$ est valide donc en particulier $\mathcal{M} \vDash (\varphi \to \psi)$ ainsi puisque $\mathcal{M} \vDash \varphi$ alors $\mathcal{M} \vDash \psi$. Sans perte de généralité, on peut dire que $\mathcal{M} \vDash \exists x \; p(a(x), a(x))$ (le cas pour b serait similaire). Donc il existe $\alpha \in \Sigma^*$ tel que $\mathcal{M} \big[x := \alpha\big] \vDash p(a(x), a(x))$. Donc $\left\| \begin{array}{|c|} \hline \alpha a \\ \hline \alpha a \\ \hline \end{array} \right\|$ existe. Ainsi par définition, il existe une succession de tuiles telle que le mot du haut et celui du bas soit le même. L'instance w est bien une instance positive du problème Post.

$\boxed{\Longleftarrow}$ Pour le sens indirect :

On suppose que w est une instance positive de Post donc il existe $m \geqslant 1$ tel qu'il existe $i_1, \dots, i_m \in \{1, \dots, N\}$ avec $u_{i_1} u_{i_2} \dots u_{i_m} = v_{i_1} v_{i_2} \dots v_{i_m}$.

Soit $\mathcal{M}$ un modèle. On suppose que $\mathcal{M} \vDash \varphi$, montrons que $\mathcal{M} \vDash \psi$.

Prouvons par récurrence sur k que $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_k}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_k}(\varepsilon) \end{bmatrix} \vDash p(x, y)$.

Initialisation : pour $k = 0$, on a $\mathcal{M} \vDash p(\varepsilon, \varepsilon)$ car $\mathcal{M} \vDash \varphi$.

Hérédité : On suppose que l'on a $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_k}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_k}(\varepsilon) \end{bmatrix} \vDash p(x, y)$. On veut prouver que $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_{k+1}}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_{k+1}}(\varepsilon) \end{bmatrix} \vDash p(x, y)$.
On sait que $\mathcal{M} \vDash \forall x \forall y \big(p(x, y) \to p(u_i(x), v_i(y))\big)$ pour tout $i \in \{1, \dots, N\}$, en particulier, pour $i = i_{k+1}$, on a $\mathcal{M} \vDash \forall x \forall y \big(p(x, y) \to p(u_{i_{k+1}}(x), v_{i_{k+1}}(y))\big)$. Donc $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_k}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_k}(\varepsilon) \end{bmatrix} \vDash \big(p(x, y) \to p(u_{i_{k+1}}(x), v_{i_{k+1}}(y))\big)$.
Ainsi $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_{k+1}}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_{k+1}}(\varepsilon) \end{bmatrix} \vDash p(x, y)$.

Conclusion : On a, pour tout $k \in \{1, \dots, m\}$,

$$\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_k}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_k}(\varepsilon) \end{bmatrix} \vDash p(x, y).$$

Sans perte de généralité, on suppose que $u_{i_1} u_{i_2} \dots u_{i_m}$ finit par un a. On écrit $u_{i_1} u_{i_2} \dots u_{i_m} = \tilde{u}a$ et $v_{i_1} v_{i_2} \dots v_{i_m} = \tilde{v}a$. On veut prouver que $\mathcal{M} \vDash \psi$ et on a $\mathcal{M} \begin{bmatrix} x := u_{i_1} u_{i_2} \dots u_{i_m}(\varepsilon) \\ y := v_{i_1} v_{i_2} \dots v_{i_m}(\varepsilon) \end{bmatrix} \vDash p(x, y)$, donc $\mathcal{M} \begin{bmatrix} x := \tilde{u}a(\varepsilon) \\ y := \tilde{v}a(\varepsilon) \end{bmatrix} \vDash p(x, y)$, d'où $\mathcal{M} \begin{bmatrix} x := \tilde{u}a(\varepsilon) \\ y := \tilde{u}a(\varepsilon) \end{bmatrix} \vDash p(x, y)$. De ce fait il existe $\tilde{u}$ tel que $\mathcal{M} \big[x := \tilde{u}(\varepsilon)\big] \vDash p(a(x), a(x))$. Donc $\mathcal{M} \vDash \psi$. Ainsi $\mathcal{M} \vDash (\varphi \to \psi)$. Ce qui prouve que $(\varphi \to \psi)$ est valide.

□

3. car si l'on ne met aucune tuile, par définition, on a $\left\| \begin{array}{|c|} \hline \varepsilon \\ \hline \varepsilon \\ \hline \end{array} \right\|$ (on rappelle que l'on a considéré que la tuile $\begin{array}{|c|} \hline \varepsilon \\ \hline \varepsilon \\ \hline \end{array}$ n'est pas dans notre instance w)

Remarques :

Le problème de savoir si une formule du calcul propositionnel est valide est décidable, c'est le dual du problème SAT que l'on étudie dans le Théorème de Cook.

Astuces de l'agrégatif :

Je présente ce développement dans la leçon 924, en disant que la théorie vide n'est pas décidable, en effet dire qu'une formule est satisfaite par la théorie vide est une autre formulation de la validité d'une formule

On rappelle qu'on dit qu'une théorie T satisfait une formule φ, que l'on note $T \vDash \varphi$, si, pour tout modèle $\mathcal{M}$, on a

$$\mathcal{M} \vDash T \text{ implique } \mathcal{M} \vDash \varphi$$

Comme tout modèle satisfait le vide, on a

$$\emptyset \vDash \varphi \text{ est équivalent à } \varphi \text{ est valide}$$

cela justifie le fait que la validité de φ est parfois notée $\vDash \varphi$

Questions possibles :

- VALID est-il dans RE ?

  Réponse : oui

- qu'en est-il de SATFO ?

  Réponse : il est aussi indécidable mais est dans co-RE

On a appelé SATFO le problème

SATFO
- entrée : un formule φ close en logique du premier ordre
- sortie : oui si φ est satisfiable, non sinon

Machine de Turing $\Longrightarrow$ μ-recursif

Leçons : 912 ; 913

Références : WOLPER, *Introduction à la calculabilité* (p.135) [WOL06] et CARTON, *Langages formels, calculabilité et complexité* (p.185) [CAR14] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 687) [LMLBP20]

Prérequis :

- Savoir coder les fonctions de base en μ-récursif (voir appendice sur les fonctions μ-récursives)

Introduction :

On va montrer que toute fonction calculable par une machine de Turing est une fonction μ-récursive, c'est un étape pour valider la thèse de Church qui nous dit que toute fonction calculable par une procédure effective est en fait une fonction calculable par une machine de Turing. En effet, on va pouvoir remplacer machine de Turing par λ-calcul ou fonctions μ-récursives quand on aura prouver que ces trois modèles de calcul sont équivalents. On prouve ici une implication de cette équivalence.

Théorème 1. Tout fonction (totale) calculable par une machine de Turing est calculable par une fonction (totale) μ-récursive.

Démonstration. Soit $M = (Q, \Sigma, \Gamma, \delta, q_0, F, \#)$ une machine de Turing déterministe à ruban bi-infini qui boucle sur ces états finals [1] telle que si n est écrit en unaire sur son ruban, à la fin de l'exécution, il y a écrit $f(n)$ en unaire.

On représente :

— l'ensemble des états Q par des entiers $\{0, \dots, m\}$ où l'état initial $q_0 = 0$

— l'alphabet de lecture $\Sigma = \{1\}$ [2]

— l'alphabet d'écriture $\Gamma = \{0, \dots, k-1\}$ où $k = |\Gamma|$ et le symbole blanc $\#$ est représenté par 0.

On représente la configuration

							$\downarrow$						
$\dots$	$\#$	$\#$	g_j	$\dots$	g_1	g_0	d_0	d_1	$\dots$	d_i	$\#$	$\#$	$\dots$

par le triplet d'entiers (g, q, d) où $q \in \{0, \dots, m\}$ et g, d sont les entiers en base k des mots avant et après la tête de lecture de M. [3]

$$g = \overline{g_0 \dots g_j}^k = \sum_{p=0}^{j} g_p k^p \quad \text{et} \quad d = \overline{d_0 \dots d_i}^k = \sum_{p=0}^{i} d_p k^p$$

La fonction $\mathbb{1}_F$ est primitive récursive car c'est une somme finie d'indicatrice.

La fonction δ est primitive récursive car elle est aussi à support fini.

1. pour permettre à la fonction config_suivante d'être totale, car toutes les fonctions primitives récursives sont totales
2. car n est écrit en unaire
3. avec bit de poids faible au niveau de la tête de lecture

On va maintenant décrire le fonctionnement de la machine de Turing par des fonctions primitives récursives et μ-récursives et donc écrire la fonction f sous la forme d'une fonction μ-récursive.

$$\mathsf{init} : \begin{cases} \mathbb{N} & \to & \mathbb{N}^3 \\ n & \mapsto & \left(0, 0, \sum_{p=0}^{n-1} k^p\right) \end{cases}$$

La fonction init est primitive récursive car la somme et l'exponentiation sont primitives récursives. [4]

$$\mathsf{config_suivante} : \begin{cases} \mathbb{N}^3 & \to & \mathbb{N}^3 \\ (g, q, d) & \mapsto & \begin{cases} (g * k + \alpha, q', d//k) & \text{si } dir = \rightarrow \\ (g//k, q', g_0 + k * (\alpha + (d//k) * k)) & \text{si } dir = \leftarrow \end{cases} \end{cases}$$

pour $\delta(q, d_0) = (q', \alpha, dir)$. [5]

La fonction config_suivante est primitive récursive car on utilise que des fonctions primitives récursives (mod, //, +,∗).

$$\mathsf{config} : \begin{cases} \mathbb{N}^3 \times \mathbb{N} & \to & \mathbb{N}^3 \\ (\vec{x}, k) & \mapsto & \begin{cases} \vec{x} & \text{si } k = 0 \\ \mathsf{config_suivante}(\mathsf{config}(\vec{x}, k-1)) & \text{sinon} \end{cases} \end{cases}$$

La fonction config est primitive récursive en utilisant le principe de récursion.

$$\mathsf{temps_arret} : \begin{cases} \mathbb{N}^3 & \to & \mathbb{N} \\ \vec{x} & \mapsto & \mu_i(\mathbb{1}_F(\pi_2^3(\mathsf{config}(\vec{x}, i)))) \end{cases}$$

La fonction temps_arret est μ-récursive car utilise une minimisation non bornée.

$$\mathsf{somme} : \begin{cases} \mathbb{N} & \to & \mathbb{N} \\ p & \mapsto & \mu(i \leqslant p)(k^i > p) \end{cases}$$

La fonction somme est primitive récursive, elle permet de retrouver l'entier en unaire qui correspond au nombre en base k.

Ainsi on pose la fonction

$$\begin{aligned} f(n) =& \mathsf{somme}(\pi_1^3(\mathsf{config}(\mathsf{init}(n), \mathsf{temps_arret}(\mathsf{init}(n))))) \\ &+ \mathsf{somme}(\pi_3^3(\mathsf{config}(\mathsf{init}(n), \mathsf{temps_arret}(\mathsf{init}(n)))))\end{aligned}$$

La fonction $\mathsf{config}(\mathsf{init}(n), \mathsf{temps_arret}(\mathsf{init}(n)))$ renvoie une configuration, il faut ensuite récupérer le g et d correspondant d'où l'utilisation de projections.

On a donc réussi à simuler la machine de Turing avec une fonction μ-récursive.

□

4. Elle représente le ruban au début de l'exécution de la machine car la tête de lecture est sur la première case du mot (donc $g = 0$), dans l'état initial $q_0 = 0$ et il y a n fois le symbole 1 sur le ruban donc représenté par $\sum_{p=0}^{n-1} k^p$ en base k.

5. où $g_0 = g \bmod k$ et $d_0 = d \bmod k$

Remarques :

C'est en fait une équivalence de modèle de calcul et on prouve l'autre sens par induction, en simulant les fonctions de base des fonctions μ-récursives par une machine de Turing.

Le symbole # est représenté par 0 ce qui coïncide bien avec le fait que $\underbrace{\#\#\#\dots\#}_{r} g_j \dots g_0$ s'écrit $g = \sum_{l=1}^{j} g_l k^l + \sum_{l=1}^{r} 0 k^{i+l}$. Autrement dit, cela ne change rien d'ajouter des 0 à gauche (ou à droite si on pense à d) des nombres que l'on écrit en base k.

Astuces de l'agrégatif :

Cette preuve existe aussi avec des codages de Gödel mais elle est plus compliquée pour les notations, ici ce qui facilite c'est que l'on code tout en unaire pour l'entrée et sortie de la machine de Turing.

Questions possibles :

- Justifier que l'on peut considérer une machine de Turing qui vérifie les hypothèses de l'énoncé (déterminisme, ruban bi-infini, unaire, unique état initial et final, boucle sur l'état final).
- Montrer que toute fonction μ-récursive est calculable par une machine de Turing en explicitant les machines de Turing.
- Montrer que les fonctions arithmétiques utilisées dans ce développement sont primitives récursives.
- Montrer que la comparaison est un prédicat primitif récursif.
- Montrer que la conditionnelle est une fonction primitif récursif, *i.e.* si P est un prédicat primitif récursif et f, g deux fonctions primitives récursives, alors la fonction qui a n associe $\mathsf{if}\ P(n)\ \mathsf{then}\ f(n)\ \mathsf{else}\ g(n)$ est primitive récursive.
- Montrer que la minimisation bornée est une fonction primitive récursive.

Transformation de Tseitin

Leçons : 916 ; 928

Références : BEN ARI, *Mathematical Logic for computer Science* (p.91) [BA12] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 797) [LMLBP20]

Introduction :

On peut transformer tout formule en une formule en CNF équivalente, mais la transformation est exponentielle. Pour montrer que CnfSat est NP-dur, on veut une transformation polynomiale. La transformation de Tseitin que l'on présente ci-dessous permet de trouver une formule en CNF qui soit équisatisfiable à la formule de départ. On a de l'équisatisfiabilité car les formules ne sont pas sur les mêmes variables propositionnelles donc on ne peut pas espérer avoir équivalence. Ainsi cette transformation qui est polynomiale en la taille de la formule de départ, permet de prouver que CnfSat est NP-dur. Comme il est aussi dans NP, il est alors NP-complet.

Théorème 1. Pour toute formule φ du calcul propositionnel, il existe une formule $T(\varphi)$ en forme normale conjonctive (CNF) de taille linéaire en celle de φ et telle que φ et $T(\varphi)$ sont équisatisfiables.

Démonstration.

Étape 1 : *Notation et énonciation de la formule $T(\varphi)$.*

On appelle *taille d'une formule* φ, notée $|\varphi|$, le nombre de connecteurs logiques de la formule φ.

On suppose que φ ne possède que les connecteurs suivants $\wedge, \vee, \neg$. [1]

On note $SF(\varphi)$ l'ensemble des sous-formules de φ (y compris φ). On note VAR l'ensemble des variables de φ.

Pour toute sous-formule $\psi \in SF(\varphi)$, on définit une nouvelle variable a_ψ (a_ψ veut dire "ψ est vraie").

On pose

$$\boxed{T(\varphi) = a_\varphi \wedge \bigwedge_{\psi \in SF(\varphi) \setminus VAR} t(\psi)} \quad [2]$$

où l'on définit $t(.)$ comme ci-dessous. La transformation $t(\psi)$ doit donner le sens que l'on voudrait [3] à chaque a_ψ tout en étant en CNF (puisque l'on veut que $T(\varphi)$ soit en CNF) donc on procède comme suit

$t(\neg\psi)$:

$$\begin{aligned} & a_{\neg\psi} \longleftrightarrow \neg a_\psi \\ \sim\ & (a_{\neg\psi} \to \neg a_\psi) \wedge (\neg a_\psi \to a_{\neg\psi}) \end{aligned}$$

1. puisque l'on peut remplacer $\psi_1 \to \psi_2$ par $\neg\psi_1 \vee \psi_2$ et $\psi_1 \leftrightarrow \psi_2$ par $(\neg\psi_1 \vee \psi_2) \wedge (\neg\psi_2 \vee \psi_1)$ ce qui n'augmente la formule d'au plus 5 fois sa taille donc cela restera linéaire en $|\varphi|$
2. si φ est juste une variable propositionnelle, elle est déjà sous forme normale conjonctive
3. a_ψ veut dire "ψ est vraie"

$$\sim \ (\neg a_{\neg\psi} \vee \neg a_{\psi}) \wedge (a_{\psi} \vee a_{\neg\psi})$$

On pose donc $t(\neg\psi) = (\neg a_{\neg\psi} \vee \neg a_{\psi}) \wedge (a_{\psi} \vee a_{\neg\psi})$ de taille 5.

$\underline{t(\psi_1 \wedge \psi_2)}$:

$$\begin{aligned} & a_{\psi_1\wedge\psi_2} \longleftrightarrow a_{\psi_1} \wedge a_{\psi_2} \\ \sim \ & (a_{\psi_1\wedge\psi_2} \to a_{\psi_1} \wedge a_{\psi_2}) \wedge (a_{\psi_1} \wedge a_{\psi_2} \to a_{\psi_1\wedge\psi_2}) \\ \sim \ & (\neg a_{\psi_1\wedge\psi_2} \vee a_{\psi_1}) \wedge (\neg a_{\psi_1\wedge\psi_2} \vee a_{\psi_2}) \wedge (\neg a_{\psi_1} \vee \neg a_{\psi_2} \vee a_{\psi_1\wedge\psi_2}) \end{aligned}$$

On pose donc $t(\psi_1 \wedge \psi_2) = (\neg a_{\psi_1\wedge\psi_2} \vee a_{\psi_1}) \wedge (\neg a_{\psi_1\wedge\psi_2} \vee a_{\psi_2}) \wedge (\neg a_{\psi_1} \vee \neg a_{\psi_2} \vee a_{\psi_1\wedge\psi_2})$ de taille 10.

$\underline{t(\psi_1 \vee \psi_2)}$:

$$\begin{aligned} & a_{\psi_1\vee\psi_2} \longleftrightarrow a_{\psi_1} \vee a_{\psi_2} \\ \sim \ & (a_{\psi_1\vee\psi_2} \to a_{\psi_1} \vee a_{\psi_2}) \wedge (a_{\psi_1} \vee a_{\psi_2} \to a_{\psi_1\vee\psi_2}) \\ \sim \ & (\neg a_{\psi_1\vee\psi_2} \vee a_{\psi_1} \vee a_{\psi_2}) \wedge (\neg a_{\psi_1} \vee a_{\psi_1\vee\psi_2}) \wedge (\neg a_{\psi_2} \vee a_{\psi_1\vee\psi_2}) \end{aligned}$$

On pose donc $t(\psi_1 \vee \psi_2) = (\neg a_{\psi_1\vee\psi_2} \vee a_{\psi_1} \vee a_{\psi_2}) \wedge (\neg a_{\psi_1} \vee a_{\psi_1\vee\psi_2}) \wedge (\neg a_{\psi_2} \vee a_{\psi_1\vee\psi_2})$ de taille 9.

Étape 2 : *Montrons que $|T(\varphi)|$ est linéaire en $|\varphi|$.*

Remarquons que

$$\#SF(\varphi) \leqslant 2|\varphi|$$

car chaque connecteur donne naissance à au plus 2 sous-formules de φ.

De plus, pour tout $\psi \in SF(\varphi)$, on a

$$|t(\psi)| \leqslant 10$$

En conclusion, on a

$$\begin{aligned} |T(\varphi)| &\leqslant |a_\varphi \wedge \bigwedge_{\psi\in SF(\varphi)\setminus VAR} t(\psi)| \\ &\leqslant 1 + |\bigwedge_{\psi\in SF(\varphi)\setminus VAR} t(\psi)| \\ &\leqslant 1 + 11\#SF(\varphi)\setminus VAR \text{ [4]} \\ &\leqslant 1 + 11\#SF(\varphi) \\ &\leqslant 1 + 22|\varphi| \end{aligned}$$

Donc $|T(\varphi)|$ est linéaire en taille de φ.

Étape 3 : *Montrons que $T(\varphi)$ et φ sont équisatisfiables.*

$\boxed{\Longrightarrow}$ Supposons que φ est satisfiable, il existe donc une valuation ν telle que $\nu(\varphi) = 1$. On pose la valuation $\tilde{\nu}$ telle que pour tout $\psi \in SF(\varphi)$, $\tilde{\nu}(a_\psi) = \nu(\psi)$. On regarde maintenant $\tilde{\nu}(T(\varphi))$.

$$T(\varphi) = \underbrace{a_\varphi}_{\tilde{\nu}(a_\varphi)=1} \wedge \bigwedge_{\psi_1\wedge\psi_2\in SF(\varphi)} t(\psi_1 \wedge \psi_2) \wedge \bigwedge_{\psi_1\vee\psi_2\in SF(\varphi)} t(\psi_1 \vee \psi_2) \wedge \bigwedge_{\neg\psi\in SF(\varphi)} t(\neg\psi)$$

4. on a mis 11 car on compte 1 pour chaque $\wedge$ entre chaque clause

On va regarder juste pour $\psi_1 \wedge \psi_2 \in SF(\varphi)$, on ferait pareil pour les autres.

$$\begin{aligned}\tilde{\nu}(t(\psi_1 \wedge \psi_2)) &= \tilde{\nu}(a_{\psi_1\wedge\psi_2} \leftrightarrow a_{\psi_1} \wedge a_{\psi_2}) \\ &= \mathbb{1}_{\tilde{\nu}(a_{\psi_1\wedge\psi_2})=\tilde{\nu}(a_{\psi_1}\wedge a_{\psi_2})} \\ &= \mathbb{1}_{\tilde{\nu}(a_{\psi_1\wedge\psi_2})=\tilde{\nu}(a_{\psi_1})\tilde{\nu}(a_{\psi_2})} \\ &= \mathbb{1}_{\nu(\psi_1\wedge\psi_2)=\nu(\psi_1)\nu(\psi_2)} \\ &= 1\end{aligned}$$

Ainsi la valuation $\tilde{\nu}$ rend vrai chaque clause, donc $\tilde{\nu}(T(\varphi)) = 1$. Ainsi $T(\varphi)$ est satisfiable.

$\boxed{\Longleftarrow}$ Supposons que $T(\varphi)$ est satisfiable, il existe donc une valuation ν telle que $\nu(T(\varphi)) = 1$.

On pose la valuation $\tilde{\nu}$ telle que pour tout $p \in VAR$, $\tilde{\nu}(p) = \nu(a_p)$.

Or $\nu(T(\varphi)) = 1$, donc $\nu(a_\varphi) = 1$ ce qui implique que $\tilde{\nu}(\varphi) = 1$ car la variable associée à une sous-formule est équivalente à cette sous-formule par construction [5].

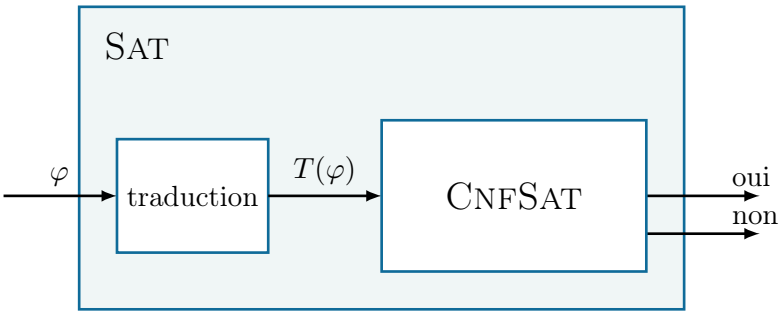
Donc φ est satisfiable. □

Astuces de l'agrégatif :

Il peut être intéressant de faire un exemple pour illustrer cette méthode, mais le temps ne le permet pas forcément. On peut couper l'explication $t(\psi_1 \vee \psi_2)$ pour gagner du temps car cela fonctionne comme $t(\psi_1 \wedge \psi_2)$.

Remarques :

On peut voir ce théorème comme réduction du problème Sat au problème CnfSat [6]



La transformation de Tseitin est donc la traduction de φ en $T(\varphi)$ qui est bien polynomiale. Ainsi CnfSat est NP-dur. De plus comme CnfSat est dans NP pour les mêmes raisons que Sat, on a alors que CnfSat est NP-complet.

Questions possibles :

- Que se passe-t-il si φ est juste une variable propositionnelle ?
- Montrer que l'on a en fait la majoration plus fine

$$|F_\varphi| \leqslant |\varphi| + |V_\varphi|.$$

- Montrer rigoureusement la réduction de CnfSat à 3Sat.
- Pourrait-on trouver une transformation similaire pour les formules sous forme normale disjonctive ? Quelles en seraient les conséquences ?

5. on peut le prouver par induction

6. CnfSat : entrée : une formule φ du calcul propositionnel sous forme normale conjonctive ; sortie : oui si φ est satisfiable, non sinon

- Montrer qu'une formule sous CNF équivalente à

$$(x_1 \wedge y_1) \vee (x_2 \wedge y_2) \vee \cdots \vee (x_n \wedge y_n)$$

  est de taille exponentielle en la taille de la formule de départ.
- Montrer que le système $\{\leftrightarrow, \neg\}$ n'est pas complet.
- Donner un système complet de connecteurs logiques qui ne contient qu'un seul connecteur logique.

Théorème de Cook

Leçons : 913 ; 915 ; 916 ; 928

Références : CARTON, *Langages formels, calculabilité et complexité* (p.203) [CAR14] et WOLPER, *Introduction à la calculabilité* (p.185) [WOL06] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 791) [LMLBP20]

Le théorème de Cook est un résultat fondamental en théorie de la complexité car il montre la NP-complétude du problème Sat *en logique propositionnelle. Il est d'autant plus important que c'est la brique élémentaire qui sert à montrer la NP-difficulté de nombreux problèmes, comme celui de la 3-coloration d'un graphe, le problème du voyageur de commerce ou le problème du sac à dos. On effectue une réduction en simulant une machine de Turing, ce qui justifie le placement de ce développement dans la leçon 913. Le résultat en lui-même est un pilier de la classe de complexité des problèmes NP-complets, ce qui en fait une bonne illustration des leçons 915 et 928. De plus, le problème de satisfiabilité d'une formule en calcul propositionnel est une question récurrente ; le fait de savoir qu'il s'agit d'un problème NP-complet permet de comprendre sa difficulté, ce qui justifie son placement dans la leçon 916.*

Introduction :

On rappelle qu'un problème est dit NP -complet, s'il est NP [1] et NP-dur [2]. Le problème Sat est le premier problème que l'on prouve être NP-complet. Ce qui nous permet ensuite de pouvoir réduire Sat d'autres problèmes et ainsi prouver qu'ils sont aussi NP-dur. (voir Appendice)

Théorème 1. Le problème Sat $\begin{cases} \text{entrée : une formule } \varphi \text{ en calcul propositionnel} \\ \text{sortie : oui si } \varphi \text{ est satisfiable, non sinon} \end{cases}$ est NP-complet.

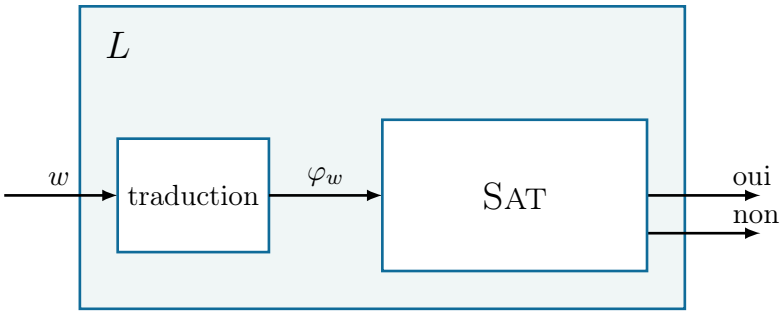
Démonstration.

Étape 1 : Sat $\in$ *NP*

Une valuation est un certificat polynomial, car on peut vérifier en temps polynomial qu'elle satisfait ou non la formule φ. Donc Sat $\in$ NP.

Étape 2 : Sat *est NP-dur*

Soit L un problème NP, on veut réduire L à Sat.



1. décidé par une machine de Turing non déterministe en temps polynomial
2. tout problème NP se réduit à lui en temps polynomial

On sait que L est décidé par une machine de Turing $M = (Q, \Sigma, \Gamma, q_0, q_f, \#, \delta)$ non déterministe. On suppose qu'elle a un seul état final q_f et qu'elle boucle sur cet état final. [3] De plus, M s'arrête en temps polynomial, donc il existe $P \in \mathbb{R}[X]$ tel que, pour tout $w \in L$ de taille n, le temps d'exécution de M sur w est inférieur à $P(n)$.

Pour tout $w = w_1 w_2 \dots w_n \in \Sigma^*$ tel que $|w| = n$,

$$w \in L \iff M \text{ s'arrête sur } w \iff M \text{ est dans l'état } q_f \text{ à l'étape } P(n)+1$$

On représente l'exécution de la machine M sur w par un tableau des configurations que l'on peut borner par $P(n)+1$ lignes (par définition de P) mais aussi par $P(n)+1$ colonnes car la complexité spatiale est inférieure à la complexité temporelle. [4] Chaque configuration est représentée dans le tableau par gqd où $q \in Q$ et $g, d \in \Gamma^*$, la tête de lecture de M est sur le premier caractère de d. Ainsi, on a un tableau de taille $(P(n)+1) \times (P(n)+1)$ avec des caractères de $A := \Gamma \cup Q$ dans chaque case. Par exemple :

q_0	w_1	w_2	$\cdots$	w_n	$\#$	$\cdots$	$\#$
γ_1	q_1	w_2	$\cdots$	w_n	$\#$	$\cdots$	$\#$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
γ_k	$\cdots$	γ_l	q_f	γ_m	$\cdots$	$\cdots$	γ_p

Tableau typique représentant la suite des configurations de la machine M

On veut construire une formule φ_w de calcul propositionnel de taille polynomiale telle que

$$\varphi_w \text{ est satisfiable} \iff w \in L \iff M \text{ est dans l'état } q_f \text{ à l'étape } P(n)+1$$

On introduit les variables popositionnelles $x_{i,j,a}$ pour $i, j \in [\![0, P(n)]\!]$ et $a \in A$ qui signifie "la case (i,j) du tableau contient le symbole a".

On pose la formule

$$\varphi_w = \underbrace{E}_{\text{Existence}} \wedge \underbrace{U}_{\text{Unicité}} \wedge \underbrace{I}_{\text{Initialisation}} \wedge \underbrace{F}_{\text{État final}} \wedge \underbrace{T}_{\text{Transition}}$$

avec

$$E \wedge U = \bigwedge_{i,j} \Big(\bigvee_{a \in A} x_{i,j,a} \wedge \bigwedge_{\substack{a,a' \in A \\ a \neq a'}} \neg(x_{i,j,a} \wedge x_{i,j,a'}) \Big)$$

qui est de taille $O((P(n)+1)^2(|A| + |A|^2))$

$$I = x_{0,0,q_0} \wedge \bigwedge_{j=1}^{n} x_{0,j,w_j} \wedge \bigwedge_{j=n+1}^{P(n)} x_{0,j,\#}$$

qui est de taille $O(P(n)+1)$

$$F = \bigvee_{j=0}^{P(n)} x_{P(n),j,q_f}$$

qui est de taille $O(P(n)+1)$

$$T = \bigwedge_{i=0}^{P(n)-1} \Big(\bigwedge_{j=0}^{P(n)} \big([(i,j) \notin C_{i,j}] \wedge [x_{i,j} = x_{i+1,j}] \big) \vee x_{i,j-1 \in Q}$$

3. il suffit de rajouter des transitions d'un ensemble d'états finals vers un état q_f pour chaque élément de Γ et de rajouter des transitions de q_f vers q_f pour chaque lettre de Γ pour faire boucler sur q_f

4. en effet, on ne pourrait pas atteindre la case $P(n)+2$ du ruban en $P(n)$ étapes

$$\vee \left(x_{i,j\in Q} \wedge [\delta^{\rightarrow}(i,j) \vee \delta^{\leftarrow}(i,j)]\right) \vee x_{i,j+1\in Q}\Big)$$

où $C_{i,j}$ correspond aux 6 cases $\begin{array}{c|ccc} i & * & q & * \\ i+1 & * & * & * \end{array}$ des lignes i et $i+1$.

On a utilisé les notations suivantes :

— $(i,j) \in C_{i,j} := x_{i,j-1\in Q} \vee x_{i,j\in Q} \vee x_{i,j+1\in Q}$ avec $x_{i,j\in Q} := \bigvee_{q\in Q} x_{i,j,q}$ (pour savoir si on est ou non dans $C_{i,j}$) qui est de taille $O(3|Q|)$

— $(i,j) \notin C_{i,j} := \neg[(i,j) \in C_{i,j}]$

— $x_{i,j} = x_{k,l} := \bigvee_{a\in A} (x_{i,j,a} \wedge x_{k,l,a})$ (pour tester l'égalité entre les caractères de deux cases) qui est de taille $O(|A|)$

— $\delta^{\leftarrow}(i,j) := \bigvee_{\substack{\gamma_1,\gamma_2\in\Gamma \\ q\in Q \\ \delta(q,\gamma_2)=(q',\gamma_3,\leftarrow)}} \left(x_{i,j-1,\gamma_1} \wedge x_{i,j,q} \wedge x_{i,j+1,\gamma_2} \wedge x_{i+1,j-1,q'} \wedge x_{i+1,j,\gamma_1} \wedge x_{i+1,j+1,\gamma_3}\right)$
qui est de taille $O(|\Gamma|^2|Q||\delta|)$

— $\delta^{\rightarrow}(i,j) := \bigvee_{\substack{\gamma_1,\gamma_2\in\Gamma \\ q\in Q \\ \delta(q,\gamma_2)=(q',\gamma_3,\rightarrow)}} \left(x_{i,j-1,\gamma_1} \wedge x_{i,j,q} \wedge x_{i,j+1,\gamma_2} \wedge x_{i+1,j-1,\gamma_1} \wedge x_{i+1,j,\gamma_3} \wedge x_{i+1,j+1,q'}\right)$
(pour simuler la fonction de transition)

Donc T est de taille $O((P(n)+1)^2(3|Q| + |A| + 3|Q| + 2|Q||\Gamma|^2|\delta|))$.

Ainsi φ_w est satisfiable si et seulement si $w \in L$. De plus, φ_w est de taille polynomiale par rapport à n donc la réduction est de taille polynomiale.

En effet si φ_w est satisfiable, alors $w \in L$, car il suffit de remplir le tableau avec le caractère a en case (i,j) si $x_{i,j,a}$ est évaluée à vrai. Par existence et unicité, pour tout (i,j) il y a exactement un caractère a qui va dans la case (i,j) et par $I \wedge F \wedge T$, le tableau représente bien une suite de configurations valides de M qui accepte w, d'où $w \in L$.

Réciproquement, si $w \in L$, on pose $\nu(x_{i,j,a}) = 1$ si et seulement si a est dans la case (i,j) ($\nu(x_{i,j,a}) = 0$ sinon). La valuation ν satisfait donc la formule φ_w car U, E, I, F, T sont satisfaite par ν car on a bien l'exécution de la machine M décrite dans le tableau.

□

Remarques :

— À partir de ce problème, on peut prouver que Cnf-Sat et 3-Sat sont NP-complets (on explicite ces problèmes dans la partie dédiée aux questions). Pour la réduction à Cnf-Sat, on utilise la Transformation de Tseitin. Pour la réduction de Cnf-Sat à 3-Sat, il suffit de trouver des conjonctions de clauses à 3 littéraux qui sont équivalentes aux clauses initiales. En voici un exemple :

$$x \simeq (x \vee y \vee z) \wedge (x \vee \neg y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee \neg z),$$

$$x \vee y \simeq (x \vee y \vee z) \wedge (x \vee y \vee \neg z),$$

$$x_1 \vee \cdots \vee x_n \simeq (x_1 \vee x_2 \vee y_2) \wedge (\neg y_2 \vee x_3 \vee y_3) \wedge (\neg y_3 \vee x_4 \vee y_4) \wedge \cdots \wedge (\neg x_{n-2} \vee x_{n-1} \vee x_n),$$

où toutes les nouvelles variables que l'on utilise sont des variables fraiches (*i.e.* qui n'apparaissent pas dans la formule initiale).

— Le problème 3-Sat est important car c'est à partir de lui que l'on prouve la NP-complétude d'autres problèmes comme des problèmes sur les graphes, des problèmes de paquets, etc. Voir [GJ79].

— Aujourd'hui, on utilise des SAT-solvers qui sont des algorithmes tentant de se rapprocher d'algorithmes polynomiaux afin de résoudre la question de satisfiabilité d'une formule. Par exemple, les algorithmes DPLL utilisent le backtracking pour résoudre SAT. Leur complexité peut être constante pour certaines entrées, mais exponentielles pour d'autres.

Astuces de l'agrégatif :

Il faut bien comprendre que dans la formule T lorsqu'on parcourt les lignes si (i, j) n'est pas dans $C_{i,j}$, on vérifie l'égalité entre les cases (i, j) et $(i + 1, j)$, puis si à la case (i, j) on a un état q, on vérifie les formules de transition ($\delta^{\rightarrow}$ et $\delta^{\leftarrow}$) sur les 6 cases de $C_{i,j}$, et pour les deux cases mitoyennes de l'état, on ne vérifie rien, puisque les vérifications sont effectuées avec les formules de transition sur les 6 cases de $C_{i,j}$ à la fois.

La formule T est valide à l'intérieur du tableau, il en faudrait une légèrement différente pour traiter les bords.

Bien comprendre les formules, pour bien les retrouver. Il y a d'autres présentations possibles mais il faut faire attention au temps que l'on a pour bien mettre en avant la structure du développement (NP puis NP-dur) sans perdre trop temps pour ne pas bacler les derniers points. Je pense qu'il faut au moins mettre une des deux formules $\delta^{\rightarrow}$ et $\delta^{\leftarrow}$.

Questions possibles :

- Le problème SAT est-il décidable ?
- Une machine de Turing non déterministe qui décide un problème s'arrête-t-elle sur toutes ses entrées ?
- Comment transformer une machine de Turing quelconque en la machine de Turing considérée dans ce développement ?
- Comment prouver que le problème CNF-SAT ci-dessous est NP-complet ?

  CNF-SAT
  - entrée : une formule φ en calcul propositionnel sous forme normale conjonctive ;
  - sortie : oui si φ est satisfiable, non sinon.

- Comment prouver que le problème 3-SAT ci-dessous est NP-complet ?

  3-SAT
  - entrée : une formule φ en calcul propositionnel sous forme normale conjonctive avec 3 littéraux par clause ;
  - sortie : oui si φ est satisfiable, non sinon.

- Ecrire la formule T sur les bords.

B-arbres

(inspiré de la version de Julie Parreaux)

Leçons : 901 ; 921 ; 932

Références : CORMEN–LEISERSON–RIVEST–STEIN, *Introduction à l'algorithmique* (p.425) [CLRS10] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 658) [LMLBP20]

Prérequis :

- les opérations élémentaires [1] pour les arbres binaires de recherche.

On donne la définition d'un B-arbre :

Définition 1. Un B-arbre est un arbre T possédant les propriétés suivantes :

1. Chaque noeud x contient les attributs ci-après :
   (a) $x.n$ le nombre de clés conservées dans le noeud (le noeud est alors d'arité $n+1$) ;
   (b) les $x.n$ clés $x.cle_1, \dots x.cle_n$ stockées dans un ordre croissant (structure de donnée associée : liste) ;
   (c) un booléen, $x.feuille$ marquant si le noeud est une feuille ;
   (d) les $n+1$ pointeurs des fils, $\{x.c_1, \dots x.c_{n+1}\}$;
2. Les clés et les valeurs dans les arbres fils vérifient la propriété suivante :
$$k_0 \leq x.cle_1 \leq \cdots \leq x.cle_n \leq k_n$$
3. toutes les feuilles ont la même profondeur, qui est la hauteur h de l'arbre ;
4. Le nombre de clé d'un noeud est contenu entre $t-1 \leq n \leq 2t-1$. (Pour la racine on n'a que la borne supérieure, la borne inférieure est 1 : on demande qu'il y ait au moins une clé dans la racine) où t est le degré minimal du B-arbre.

Remarques :
Ne pas réécrire la définition au tableau, il faut qu'elle figure dans le plan.

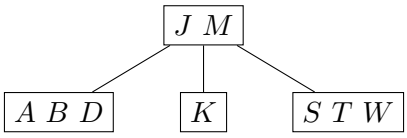
Introduction :

On se place dans le cadre d'une recherche de clé dans une base de données stockée sur un disque dur externe. On cherche à minimiser le nombre d'action sur un disque externe (c'est ce qui prend le plus de temps, facteur d'un million entre un accès au disque et d'une opération sur processeur). La structure de données que l'on privilégie est un arbre de recherche. On cherche alors un arbre avec une ramification importante ce qui nous permet de minimiser le nombre d'appel au disque (hauteur plutôt faible ce qui minimise les quantités recherchées). En pratique on stocke une page (unité de transfert avec le disque dur) sur un noeud. Dans ce cas, on maximise l'impact de l'accès au disque.

Lors de ce développement, on se donne deux opérations atomiques : Ecriture-Disque et Lecture-Disque. On veut montrer l'optimalité de la structure de donnée face à l'utilisation de ces deux opérations.

1. recherche, insertion, suppression

Exemple avec $t = 2$:



Dans la vraie vie, t est choisi en fonction du nombre de tuples que peut contenir une page du disque.

Recherche dans un B-arbre

La recherche dans un B-arbre est analogue à la recherche dans un ABR en rajoutant des intervalles dans les nœuds. On commence alors à chercher dans quel intervalle on se trouve, puis on descend.

L'algorithme prend en paramètre l'élément recherché k et le noeud courant x. On retourne alors le noeud x et la place de k dans le noeud x, si k est dans l'arbre. Sinon, on retourne Nil.

Hypothèses pour le calcul de la complexité :

- La racine du B-arbre se trouve toujours en mémoire principal : on n'a pas de Lire-Disque ; cependant, il faudra effectuer un Écriture-Disque lors de la modification de la racine.
- Tout noeud passé en paramètre devra subir un Lire-Disque.

Algorithme 1 Recherche B-arbre

```
Procédure Recherche-BArbre(x, k)
    [x a subi une lecture dans le disque Lire-Disque]
    i ← 1 ;
    Tant que (i ≤ x.n et k > x.cle_i) faire
        [Recherche de l'intervalle dans lequel se trouve k]
        i ← i + 1 ;
    Fait
    Si (i ≤ x.n et k = x.cle_i) alors
        [On a trouvé k]
        Retourne (x, i)
    Sinon
        [On n'a pas trouvé k]
        Si (x.feuille) alors
            [On a fini l'arbre et k n'y est pas]
            Retourne Nil
        Sinon
            [On peut continuer à descendre dans l'arbre : récursivité sur le fils de x]
            Lire-Disque(x.c_i)
            Retourne Recherche-BArbre(x.c_i, k)
        Fin Si
    Fin Si
Fin
```

Théorème 1. Soit T un B-arbre à n éléments de degré minimal $t \geq 2$. Alors la hauteur h vérifie

$$h \leq \log_t \frac{n+1}{2}$$

Démonstration. — La racine a au moins une clé et les autres nœuds $t-1$.

— T possède 2 nœuds à la profondeur 1, $2t$ à la profondeur 2,... Par récurrence, on montre que T possède $2t^{h-1}$ nœuds à la profondeur h.

— On en déduit $n \geq 1 + (t-1)\sum_{i=1}^{h} 2t^{i-1} = 1 + 2(t-1)(\frac{t^h-1}{t-1}) = 2t^h - 1$.

— $t^h \leq \frac{(n+1)}{2}$ et on conclut en passant au $\log_t$.

□

Complexité en accès au disque : $O(h)$ où h est la hauteur de l'arbre. Donc en $O(log_t n)$ lecture-écriture sur le disque (on ne fait que des lectures). Comme $n < 2t$, la boucle **while** s'effectue en $O(t)$, le temps processeur total est $O(th) = O(t \log n)$.

Insertion dans un B-arbre

L'insertion dans un B-arbre est plus délicate que dans une ABR. Comme dans un ABR, on commence par chercher la feuille sur laquelle on doit insérer cette nouvelle clé. Cependant, on ne peut pas juste créer une nouvelle feuille (on obtient un arbre illicite). On est alors obligé d'insérer l'élément dans un noeud déjà existant.

L'opération de l'ajout consiste en la recherche de la place de la clé dans les feuilles de l'arbre puis on insère dans la feuille de l'arbre correspondant.

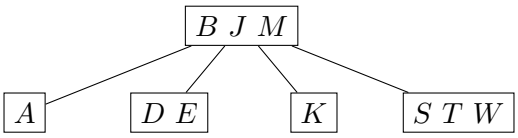
On peut avoir le **problème** suivant : on peut violer la capacité du nœud.

Pour palier ce problème, on pourrait séparer le nœud en deux et on fait remonter la clé médiane dans le noeud du dessus tant qu'on n'a pas trouvé de nœud capable de garder la clé. Cependant, il nous faut deux passages dans l'arbre : un pour trouver l'emplacement de la nouvelle clé et un pour remonter le superflu. Ce n'est pas optimal.

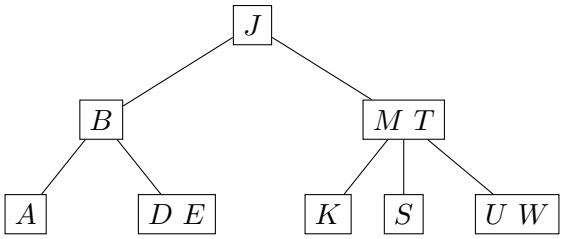
On peut faire **mieux** : si le nœud est plein lors de la descente de l'arbre (recherche de l'emplacement), on sépare le nœud (on garanti qu'il n'y a aucun nœud plein sur notre parcours de l'arbre). On alors un unique passage.

On peut avoir un **nouveau problème** si la racine est pleine, alors on partagera la racine ce qui aura pour effet d'augmenter la hauteur de l'arbre de 1.

Insertion de E dans l'arbre précédent :



Partage de la racine qui augmente la hauteur de l'arbre dû à l'ajout de U :



Complexité en accès au disque : $O(h) = O(\log_t n)$ où h est la hauteur de l'arbre.

Remarques :

La suppression est encore plus compliquée à mettre en place que l'insertion, lire les pages du Cormen [CLRS10].

Astuces de l'agrégatif :

Ce développement est assez long surtout si on veut donner l'algorithme d'insertion, j'ai fait le choix d'essayer d'expliquer le plus clairement possible, comment on insère, quelles sont les difficultés liées à l'insertion pour préserver la structure, etc. Je ne pense pas que ce soit faisable de traiter la suppression en plus.

Questions possibles :

- Donner les algorithmes de recherche, d'insertion et de suppression pour un arbre binaire de recherche.

Cocke–Younger–Kasami

Leçons : 907 ; 915 ; 923 ; (926) ; (927) ; 931

Références : CARTON, *Langages formels, calculabilité et complexité* (p.199) [CAR14] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 779) [LMLBP20]

Introduction :

L'algorithme Cocke–Younger–Kasami permet de résoudre le problème du mot pour les langages algébriques et permet de dire que ce problème est dans P.

Définition 1. Une grammaire algébrique G est dite sous forme normale de Chomsky si elle ne contient que des règles de la forme $A \to a$ (avec a un terminal) ou $A \to A_1 A_2$ (avec A_1, A_2 deux non-terminaux).

Théorème 1. L'algorithme CYK permet de répondre au problème du mot pour les grammaires algébriques

MOT : entrée : un mot $w = w_1 w_2 \dots w_n$, une grammaire G sous forme normale de Chomsky ; sortie : oui si $w \in \mathrm{L}(G)$, non sinon

Démonstration. Pour tous indices $1 \leqslant i \leqslant j \leqslant n$, on note

$$E_{i,j} = \{\text{non-terminaux qui engendrent } w_i \dots w_j\}$$

Ainsi on a donc $w \in \mathrm{L}(G)$ si et seulement si $S \in E_{1,n}$.[1] On veut donc calculer $E_{1,n}$.

Pour cela, on va calculer tous les $E_{i,j}$ en utilisant le lemme suivant :

Lemme 1. (i) Pour tout $i \in \{1, \dots, n\}$,

$$E_{i,i} = \{A, A \to w_i \text{ est une règle de production de } G\}$$

(ii) Pour tout $1 \leqslant i < j \leqslant n$, on a

$$E_{i,j} = \bigcup_{\substack{A \to B_1 B_2 \\ B_1 \in E_{i,k} \\ B_2 \in E_{k+1,j} \\ i \leqslant k < j}} \{A\}$$

Démonstration du lemme. (i) Immédiat puisque la grammaire est sous forme normale de Chomsky.

(ii) $\supset$ S'il existe B_1, B_2, k tels que

$$B_1 \to^* w_i \dots w_k, \quad B_2 \to^* w_{k+1} \dots w_j \quad \text{et} \quad A \to B_1 B_2$$

Alors on a $A \to^* w_i \dots w_j$ d'où $A \in E_{i,j}$.

$\subset$ Réciproquement, si $A \to^* w_i \dots w_j$ (i.e $A \in E_{i,j}$) (avec au moins 2 lettres car $i \neq j$) alors par le lemme de factorisation, il existe B_1, B_2, k tels que $B_1 \in E_{i,k}$, $B_2 \in E_{k+1,j}$ et $i \leqslant k < j$ car G est sous forme normale de Chomsky.

□

1. S est l'axiome de la grammaire G

Pour calculer $E_{i,j}$ (avec $i < j$), on a besoin des $E_{i,k}$ et $E_{k+1,j}$ pour tout $i \leqslant k < j$.

$$\begin{pmatrix} E_{1,1} & \cdots & E_{1,i} & \cdots & E_{1,j} & \cdots & E_{1,n} \\ & \ddots & \vdots & & \vdots & & \vdots \\ & & E_{i,i} & \to & E_{i,j} & \cdots & E_{i,n} \\ & & & \ddots & \uparrow & & \vdots \\ & & & & E_{j,j} & \cdots & E_{j,n} \\ & \emptyset & & & & \ddots & \vdots \\ & & & & & & E_{n,n} \end{pmatrix}$$

On utilise la programmation dynamique en commençant par les coefficients diagonaux et en remontant à chaque étape.

Ordre de calcul :

$$\begin{matrix} 1 & 2 & \dots & \dots & n \\ & \ddots & \ddots & & \vdots \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & 2 \\ & & & & 1 \end{matrix}$$

Procédure CYK(un mot w, une grammaire G)
- initialiser $E_{i,j} = \emptyset$;
- **Pour** i **de** 1 **à** n **faire**
  - **Pour** $A \to a \ \in G$ **faire**
    - **Si** $(a = w_i)$ **alors**
      - $E_{i,i} = E_{i,i} \cup \{A\}$
    - **Fin Si**
  - **Fin Pour**
- **Fin Pour**
- **Pour** d **de** 2 **à** n **faire**
  - **Pour** $E_{i,j}$ sur la diagonale d **faire**
    - **Pour** k **de** i **à** $j-1$ **faire**
      - **Pour** $A \to B_1 B_2 \ \in G$ **faire**
        - **Si** $(B_1 \in E_{i,k}$ et $B_2 \in E_{k+1,j})$ **alors**
          - $E_{i,j} = E_{i,j} \cup \{A\}$
        - **Fin Si**
      - **Fin Pour**
    - **Fin Pour**
  - **Fin Pour**
- **Fin Pour**
- **Renvoyer** $S \in E_{1,n}$

Fin

Pour implémenter les ensembles $E_{i,j}$, on voudrait pouvoir *ajouter les non-terminaux* et *vérifier si des non-terminaux sont dans un certain ensemble* $E_{i,j}$ en temps constant. Pour faire cela, on peut construire une matrice qui contient à la case (i, j) un tableau indexé par les non-terminaux et valant "vrai" si le non-terminal est dans $E_{i,j}$, "faux" sinon.

Complexité : $O(n^3|G|)$ où $|G|$ est le nombre de règles de G. □

Proposition 1. Pour toute grammaire algébrique G, il existe une grammaire algébrique G' sous forme normale de Chomsky telle que $\mathrm{L}(G') = \mathrm{L}(G)\backslash\{\varepsilon\}$.

Démonstration.
Étape 1 : *Obtenir les règles $A \to a$*
On a $G = (\Sigma, S, V, T, P)$.[2] On pose alors $G'' = (\Sigma, S, V', T, P')$ où

$$V' = V \cup \{V_a, a \in \Sigma\}$$

et

$$P' = \tilde{P} \cup \{V_a \to a, a \in \Sigma\}$$

où $\tilde{P}$ sont les mêmes règles que P mais où l'on a remplacé le terminal a par le non-terminal V_a.
On obtient alors une grammaire telle que $\mathrm{L}(G') = \mathrm{L}(G)\backslash\{\varepsilon\}$ et avec des règles de la forme :

$$T \to T_1 \dots T_n \text{ et } T \to a$$

où les lettres majuscules sont des non-terminaux et les minuscules sont des terminaux.

Étape 2 : *Transformer les règles $T \to U$*
Pour chaque règle $T \to U$, on duplique toutes les règles qui contiennent des T à droite, et, pour les copies, on remplace T par U. On peut maintenant supprimer la règle $T \to U$ sans changer le langage engendré par la grammaire.

Étape 3 : *Transformer les règles $T \to T_1 \dots T_n$ pour $n > 2$*
Pour chaque règle $T \to T_1 \dots T_n$ (avec $n > 2$) de G'', on la remplace par

$$T \to T_1 T_2', \quad T_i' \to T_i T_{i+1}' \text{ et } \quad T_{n-1}' \to T_{n-1} T_n$$

où $i \in \{2, \dots, n-2\}$. On obtient ainsi une grammaire G' équivalente à G'' et qui est sous forme normale de Chomsky. □

Remarques :
Ainsi on peut résoudre le problème du mot pour n'importe quelle grammaire algébrique car la complexité de la transformation que l'on a faite est linéaire.
Une grammaire sous forme de Chomsky ne peut pas produire ε mais on peut ajouter aux règles la règle $S \to \varepsilon$ (à l'axiome) pour pouvoir produire ε (cependant, souvent on veut travailler avec des grammaires "propres" donc qui ne produisent pas ε)

Astuces de l'agrégatif :
En tournant l'algorithme comme solution au problème du mot pour les langages algébriques, je fais rentrer ce développement dans le leçon classe de complexité, exemple de problème P.
Je passe assez rapidement sur la transformation de la grammaire en forme normale de Chomsky, en fonction du temps qui me reste.

2. Σ est l'alphabet, S est l'axiome, V est l'ensemble des non-terminaux (ou variables), T est l'ensemble des terminaux et P est l'ensemble des règles de production de G

Questions possibles :

- Est-ce que cela marche pour le mot vide ε ?
- Donner un algorithme qui vérifie si ε appartient au langage engendré par une grammaire G ou non.
- Quelle est la définition de $|G|$?
- Quelle est la taille de l'entrée ? puisqu'on considère un mot w et une grammaire G
- Est ce que la version récursive de cet algorithme est mieux ?
- En pratique, est-ce qu'on utilise cet algorithme ?

  Une réponse possible est que pour l'analyse syntaxique, on utilise plutôt des algorithmes linéaires mais ce sont des algorithmes qui ne marchent que pour des grammaires $LL(1)$ et $LR(0)$ et toute grammaire n'est pas forcément de ce type
- Après avoir mis sous forme normale de Chomsky la grammaire suivante $G = (\Sigma, \mathcal{N}, \mathcal{T}, S, \mathcal{R})$ où $\Sigma = \{a, b, c, d\}$, $\mathcal{N} = \{S, A, B, C\}$, $\mathcal{T} = \Sigma$ et $\mathcal{R}$ est décrit par

$$\begin{aligned} S &\to AB \mid Ca \\ A &\to aAb \mid \varepsilon \\ B &\to bB \mid b \\ C &\to cC \mid d, \end{aligned}$$

  appliquer l'algorithme CYK afin de savoir si les mots *aabbbb*, *ccddda* et *aabb* sont dans L(G). Comprendre l'intérêt de l'analyse LL(1), voir Caractérisation de Premier pour l'analyse $LL(1)$.
- En réduisant le problème de Post, montrer l'indécidabilité de Inter, Univ et Egal.

Tri topologique

(inspiré de la version de Clarence Kineider)

Leçons : 903 ; 925 ; 927

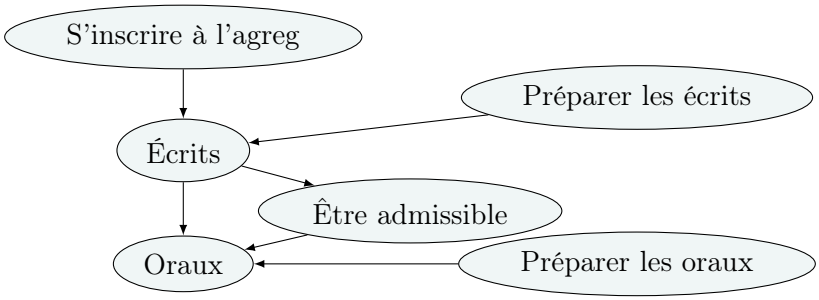
Références : CORMEN–LEISERSON–RIVEST–STEIN, *Introduction à l'algorithmique* (p.566) [CLRS10] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 743) [LMLBP20]

Introduction :

Le problème du tri topologique est un problème d'ordonnancement des tâches : on a une liste de choses à faire, certaines ont besoin d'être faites avant d'autres. On représente ces contraintes par un graphe orienté dont les sommets sont les tâches et les arêtes sont les couples (u, v) tels que la tâche u doit être effectuée avant la tâche v. On cherche alors un ordre sur les sommets tel que si (u, v) est une arête, alors u apparait avant v dans l'ordre. Le problème n'a pas de solution s'il y a un cycle dans le graphe, on va donc supposer que le graphe est acyclique.

But : Ordonnancer des tâches dont certaines doivent être faites avant d'autres.

Exemple :



Ordre possible : [Préparer les écrits, S'inscrire à l'agreg, Préparer les oraux, Écrits, Être admissible, Oraux]

Cadre : Un graphe acyclique orienté $G = (S, A)$

Tri topologique
- Entrée : Un graphe orienté acyclique $G = (S, A)$
- Sortie : Une liste L constituée des sommets de G telle que si $(u, v) \in A$, alors u apparaît avant v dans L

Remarques :

Il n'y a pas unicité de la solution (contrairement à un tri classique sur des valeurs distinctes).

Une façon de réaliser un tri topologique de G est de faire un parcours en profondeur, et de placer les sommets dans la liste dans l'ordre inverse de l'ordre de visite. Ce développement consiste à donner cet algorithme et à justifier sa correction. Sa terminaison et sa complexité sont élémentaires et seront données également.

On commence par donner l'algorithme principal, qui utilise la fonction auxiliaire **Visite** donnée immédiatement après. Pour alléger les notations, on supposera que **Visite** a accès aux variables définies dans le corps de **Tri_topo** (il suffit de définir **Visite** à l'intérieur de **Tri_topo**).

Algorithme 1

```
Fonction Tri_topo(G) : L ← [ ]                                    :
Colorier tous les sommets en blanc
[Par exemple avec un tableau de couleurs indexé par les sommets de G]
Pour u ∈ V faire
    Si (u est blanc) alors
        Visite(u)
    Fin Si
Fin Pour
Retourner L

Fin
Tri_topo
```

Algorithme 2 : Visite

```
Procédure Visite(u)
    Colorier u en gris
    Pour (u, v) ∈ A faire
        Si (v est blanc) alors
            Visite(v)
        Fin Si
    Fin Pour
    Colorier u en noir
    L ← u :: L
Fin
```

Proposition 1. L'algorithme **Tri_topo** termine et a une complexité en $\Theta(|S| + |A|)$.

Démonstration. Le nombre de sommets blancs diminue strictement à chaque appel à **Visite**, donc l'algorithme termine. De plus, chaque sommet est visité exactement une fois, et chaque arête est traitée exactement une fois aussi, d'où une complexité en $\Theta(|S| + |A|)$. □

Pour démontrer la correction, on va utiliser le lemme suivant.

Lemme 1.
- Pour tout $v \in S$, v est visité une unique fois, donc v est ajouté une unique fois à L.
- Au début et à la fin de chaque appel à **Visite**, L contient exactement l'ensemble des sommets noirs.
- Si au moment de l'appel à **Visite**(v), le sommet u est gris, alors il existe un chemin de u à v dans G.

Démonstration. Seul le troisième point n'est pas immédiat. Pour le démontrer proprement, faire une récurrence sur la profondeur de l'appel à **Visite**(v) dans l'exécution de **Visite**(u). □

Théorème 1. L'algorithme **Tri_topo** est correct.

Démonstration. Soit L la liste renvoyée par **Tri_topo**(G), et soit $(u, v) \in A$. Au moment de l'unique appel à **Visite**(u), il y a trois possibilités :

— Si v est noir, alors v est déjà dans L. Donc u est placé avant v dans L.

— Si v est gris, alors il existe un chemin de v à u dans G, et $(u, v) \in A$ ce qui contredit l'acyclicité de G. Absurde.

— Si v est blanc, alors v sera visité lors de la boucle sur les voisins de u. L'appel à **Visite**(v) sera donc terminé à la sortie de la boucle, donc v sera déjà dans L au moment où u y sera ajouté. Donc u est avant v dans L.

□

Remarques :

On peut voir le tri topologique comme un "vrai" algorithme de tri : on trie un ensemble muni d'un ordre partiel.

Astuces de l'agrégatif :

Souvent, l'exemple classique de cet algorithme est l'ordre dans lequel il faut s'habiller [1]. Dans la version de Clarence Kineider, il avait représenté une recette de cuisine. Pour ma part, sous l'influence de Lilian Besson, j'ai mis un exemple méta pour l'agrégation.

Questions possibles :

- Donner la solution que l'algorithme **Tri_Topo** renvoie sur l'exemple en partant de « S'inscrire à l'agrégation ».

1. il faut mettre son caleçon avec de mettre son pantalon, mais on peut mettre son tshirt avant/après le pantalon, etc.

Automate des occurrences

Leçons : 907 ; 909 ; 921

Références : CORMEN–LEISERSON–RIVEST–STEIN, *Introduction à l'algorithmique* (p.915) [CLRS10] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 763) [LMLBP20]

Définition 1. Un automate complet et déterministe qui reconnait un langage L est dit minimal, s'il a un nombre minimal d'états parmi tous les automates complets et déterministes qui reconnaissent L.

Prérequis :

- Un automate complet et déterministe, dont le nombre d'état vaut le nombre de résiduels, est minimal.

Introduction :

On va présenter ici un automate qui permet de trouver les occurrences d'un motif dans un texte, il est notamment utile dans l'algorithme de Morris Pratt. Cet algorithme peut être amélioré en l'algorithme de Knuth–Morris–Pratt qui ne retient pas l'automate des occurrences mais seulement la longueur des bords des préfixes du motif m.

But : Trouver un algorithme qui cherche un motif dans un texte

Soit Σ un alphabet fini, soit $m \in \Sigma^*$ le motif que l'on veut chercher. On veut construire un automate fini qui reconnait les mots se finissant par m.

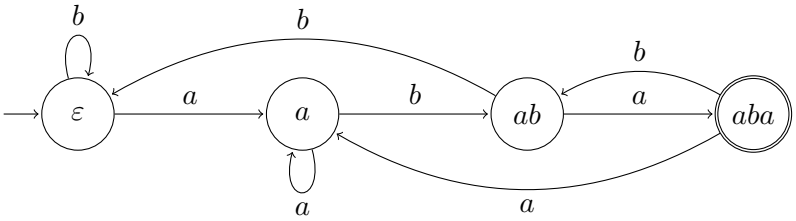
On pose $\mathcal{P}$ l'ensemble des préfixes du mot m. Pour tout $u \in \Sigma^*$, on pose $\sigma_m(u)$ le plus grand suffixe de u qui est dans $\mathcal{P}$ [1].

On va construire l'automate $\mathcal{A}_m$ de la manière suivante :

$$\mathcal{A}_m = (\mathcal{P}, \{\varepsilon\}, \{m\}, \delta, \Sigma)$$

où δ est définie telle que, pour tout $p \in \mathcal{P}$, $a \in \Sigma$, on ait $\boxed{\delta(p,a) = \sigma_m(pa)}$.

Exemple : Pour $m = aba$, l'automate $\mathcal{A}_m$ est de la forme



Théorème 1. L'automate $\mathcal{A}_m$ reconnait le langage $\Sigma^* m$ et cet automate est minimal.

1. i.e. qui est aussi suffixe de m

Démonstration. On prolonge la fonction δ aux mots. [2]

Étape 1 : *Montrons que* $\delta(p,u) = \sigma_m(pu)$

Pour tout $p = p_1 \dots p_k \in \mathcal{P}$, on va prouver par récurrence sur la longueur du mot u, que $\delta(p,u) = \sigma_m(pu)$.

Initialisation : $|u| = 1$, par définition de δ, on a $\delta(p,u) = \sigma_m(u)$ car $u \in \Sigma$.

Hérédité : Supposons que le résultat est vrai pour w avec $|w| \geqslant 1$. Soit $a \in \Sigma$, on veut prouver le résultat pour aw.

Par définition de δ, on a $\delta(p,aw) = \delta(\delta(p,a),w) = \delta(\sigma_m(pa),w) = \sigma_m(\sigma_m(pa)w)$ (par hypothèse de récurrence). Il faut donc prouver que $\sigma_m(\sigma_m(pa)w) = \sigma_m(paw)$.

— Si $\sigma_m(pa) \neq \varepsilon$, il existe donc $i \in \{1,\dots,k\}$ tel que $\sigma_m(pa) = p_i \dots p_k a$ et pour tout $j < i$, $p_j \dots p_k a$ n'est pas préfixe de m. Ainsi

$$\sigma_m(\sigma_m(pa)w) = \sigma_m(p_i \dots p_k aw) = \sigma_m(p_1 \dots p_k aw) \text{ [3]} = \sigma_m(paw)$$

— Si $\sigma_m(pa) = \varepsilon$, aucun suffixe de pa n'est préfixe de m, donc les suffixes de paw qui sont préfixes de m sont exactement les suffixes de w qui sont préfixes de m. Ainsi

$$\sigma_m(\sigma_m(pa)w) = \sigma_m(w) = \sigma_m(paw)$$

Ainsi on a prouvé que

$$\sigma_m(\sigma_m(pa)w) = \sigma_m(paw)$$

Conclusion : Pour tout mot $u \in \Sigma^*$, $\delta(p,u) = \sigma_m(pu)$.

Étape 2 : $L(\mathcal{A}_m) = \Sigma^* m$

Par double inclusion,

$\boxed{\subset}$ Si $w \in \mathrm{L}(\mathcal{A}_m)$, alors $\delta(\varepsilon,w) \in \{m\}$, d'où par l'étape 1, $\sigma_m(w) = m$. Donc, par définition, m est un suffixe de w, autrement dit, $w \in \Sigma^* m$.

$\boxed{\supset}$ Si $w \in \Sigma^* m$, alors $\sigma_m(w) = m$ car m est suffixe de w. Or $\sigma_m(w) = \delta(\varepsilon,w) = m$, donc $w \in \mathrm{L}(\mathcal{A}_m)$.

Étape 3 : *Montrons que* $\mathcal{A}_m$ *est minimal*

On note $L = \Sigma^* m$. Comme $\mathcal{A}_m$ est déterministe, complet et reconnait L, il suffit de prouver que $|\mathcal{P}|$ est égal au nombre de résiduels. On notera $\{u^{-1}L\}$ l'ensemble des résiduels du langage L. On sait que le nombre de résiduels est inférieur au nombre d'états de $\mathcal{A}_m$ [4] On a donc déjà

$$|\{u^{-1}L\}| \leqslant |\mathcal{P}|$$

2. pour un mot aw (avec $a \in \Sigma$ et $w \in \Sigma^*$) et $p \in \mathcal{P}$, on pose $\tilde{\delta}(p,aw) = \begin{cases} \delta(p,a) & \text{si } w = \varepsilon \\ \tilde{\delta}(\delta(p,a),w) & \text{sinon} \end{cases}$ bien définie car l'automate est déterministe et qu'on applique l'hypothèse de récurrence sur un mot de longueur strictement plus petite. On continuera de noter cette fonction δ

3. car pour tout $j < i$, $p_j \dots p_k a$ n'est pas préfixe de m donc $p_j \dots p_k aw$ n'est pas préfixe de m non plus

4. car pour tout $u \in \Sigma^*$, on note q l'unique (car déterministe) état dans lequel l'automate sera après avoir lu u (existe car complet), on a

$$u^{-1}L = \{v \in Q, q \xrightarrow{v} f, f \in F\}$$

Donc, $u^{-1}L$ ne dépend que de q, ainsi le nombre de résiduel est inférieur au nombre d'états de l'automate. Plus rigoureusement, l'application

$$\varphi : \left\{ \begin{array}{ccc} \{u^{-1}L\} & \to & Q \\ u^{-1}L & \mapsto & \delta(i,u) \end{array} \right.$$

est injective (où i est l'état initial de l'automate).

D'autre part, l'application

$$f : \begin{cases} \mathcal{P} & \to & \{u^{-1}L\} \\ p & \mapsto & p^{-1}L \end{cases}$$

est injective, car si $m_1 \dots m_i \neq m_1 \dots m_j$ avec $i < j$, alors $m_{j+1} \dots m_{|m|} \in (m_1 \dots m_j)^{-1}L$, or $m_{j+1} \dots m_{|m|} \notin (m_1 \dots m_i)^{-1}L$.[5] Ainsi $(m_1 \dots m_i)^{-1}L \neq (m_1 \dots m_j)^{-1}L$. Donc f est bien injective et l'on a

$$|\mathcal{P}| \leqslant |\{u^{-1}L\}|$$

Donc

$$|\mathcal{P}| = |\{u^{-1}L\}|$$

Ce qui permet de conclure sur le fait que $\mathcal{A}_m$ est minimal. □

Astuces de l'agrégatif :

On pourrait initialiser la récurrence à 0.

Il faut bien comprendre ce que sont les résiduels d'un langage et la construction de l'automate des résiduels pour maitriser ce développement. On a utilisé de manière cruciale que le nombre de résiduels d'un langage est inférieur au nombre d'états de tout automate déterministe complet reconnaissant le langage.

5. car on a lu moins de $|m|$ caractères donc on ne peut pas atteindre l'état final

3–Coloration d'un graphe

(rédigé par David Xu)

Leçons : 915 ; 925 ; 928

Références : CORMEN–LEISERSON–RIVEST–STEIN, *Introduction à l'algorithmique* (p.1014) [CLRS10]

Prérequis :

- la NP-complétude de 3Sat $\begin{cases}\text{entrée : une formule } \varphi \text{ en 3-Cnf (calcul propositionnel)}\\ \text{sortie : oui si } \varphi \text{ est satisfiable, non sinon}\end{cases}$

Introduction :

On va montrer dans ce développement que le problème de 3 coloration d'une graphe est NP-complet. Pour cela, on va réduire le problème 3Sat à 3Col. C'est une des arêtes du graphe en appendice sur les problèmes NP-complets.

Définition 2. On dit qu'une graphe $G = (S, A)$ est 3−coloriable s'il existe une application

$$c : S \to \{1, 2, 3\}$$

telle que, pour tout $(u, v) \in A$, $c(u) \neq c(v)$.

Théorème 1. Le problème de 3−coloration de graphe

3Col $\begin{cases}\text{entrée : un graphe } G = (S, A) \text{ non orienté}\\ \text{sortie : oui si } G \text{ est 3−coloriable, non sinon}\end{cases}$

est NP-complet.

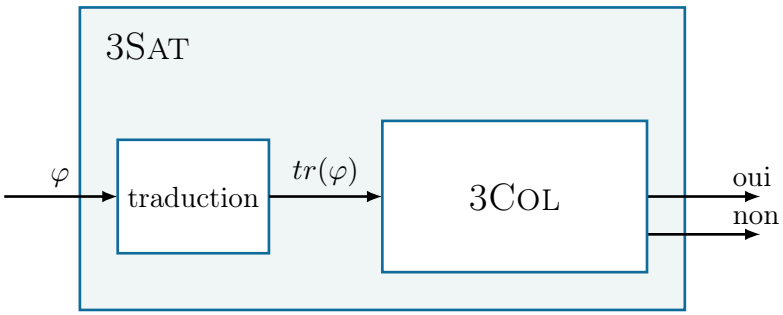
Démonstration.

Étape 1 : 3Col $\in$ *NP*

Ce problème est bien dans NP car on peut vérifier en temps polynomial (en le nombre d'arêtes du graphe) qu'une coloration d'un graphe vérifie bien les propriétés voulues.

Étape 2 : 3Col *est NP-dur*

Pour montrer cela, on va définir une réduction à partir du problème 3Sat qui est NP-dur (et même NP-complet). [1]

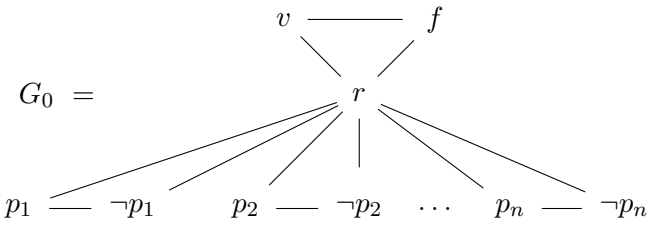


1. On utilise le théorème de Cook et la transformation de Tseitin pour avoir la NP-complétude de CnfSat puis on peut réduire le nombre de littéraux dans chaque clause en ajoutant des nouvelles variables et des nouvelles clauses

Soit donc φ une formule du calcul propositionnel en 3-CNF possédant m clauses,

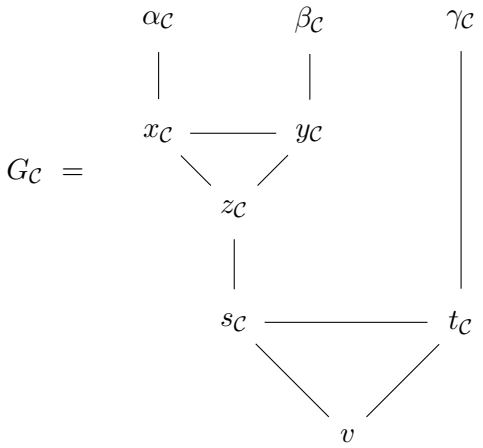
$$\varphi = \bigwedge_{j=1}^{m} \mathcal{C}_j.$$

Notons $p_1, \ldots, p_n$ les variables propositionnelles qui apparaissent dans φ. On va construire un graphe $tr(\varphi)$ qui repose sur le squelette G_0 suivant :



On peut remarquer que dans une coloration de ce graphe, la couleur d'une variable propositionnelle p sera toujours différente de celle de $\neg p$ et qu'un littéral aura toujours la couleur de v ou de f mais pas celle de r.

Puis, pour chaque clause $\mathcal{C} = (\alpha_\mathcal{C} \vee \beta_\mathcal{C} \vee \gamma_\mathcal{C})$ de φ, on va "connecter" le gadget suivant à G_0 pour former le graphe G :



Ainsi le graphe $G = tr(\varphi)$ possède $3+2n+5m$ sommets. La réduction $tr(\varphi)$ est donc calculable en temps polynomial en m, le nombre de clauses de ϕ (car $n \leqslant 3m$).
Pour montrer que tr définit bien une réduction de 3SAT à 3COL, nous utiliserons les deux lemmes suivants :

Lemme 1. On peut compléter toute coloration partielle d'un gadget $G_\mathcal{C}$ où les sommets $\alpha_\mathcal{C}$, $\beta_\mathcal{C}$ et $\gamma_\mathcal{C}$ sont de la couleur de f ou v et où l'un d'eux est de la couleur de v en une coloration licite de $G_\mathcal{C}$.

Démonstration. Il suffit de traiter tous les cas, il y en a $2^3 - 1 = 7$. □

Lemme 2. Dans toute coloration d'un gadget de la forme $G_\mathcal{C}$, l'un des sommets $\alpha_\mathcal{C}$, $\beta_\mathcal{C}$ ou $\gamma_\mathcal{C}$ a la couleur de v.

Démonstration. Par l'absurde, supposons que $\alpha_\mathcal{C}$, $\beta_\mathcal{C}$ et $\gamma_\mathcal{C}$ ont tous la couleur de f (on rappelle qu'ils ont soit la couleur de v, soit celle de f). Comme $\alpha_\mathcal{C}$ et $\beta_\mathcal{C}$ ont la couleur de f, les sommets

$x_\mathcal{C}$ et $y_\mathcal{C}$ ont les couleurs de r ou v et leur couleur est différente car ils sont liés par une arête. $z_\mathcal{C}$ a donc nécessairement la couleur de f. De même, comme $z_\mathcal{C}$ et $\gamma_\mathcal{C}$ ont la couleur de f, on en déduit que v a la couleur de f. Contradiction. □

Proposition 1. Pour toute formule φ en 3-CNF, φ est satisfiable si et seulement si $tr(\varphi)$ est 3−coloriable.

Démonstration. Soit φ une formule en 3-CNF.
$\boxed{\Longrightarrow}$ Soit ν une valuation qui satisfait φ, $\nu \models \varphi$. On fixe des couleurs différentes pour les sommets v, f et r de $tr(\varphi)$, $c(v)$, $c(f)$ et $c(r)$, et on colorie les sommets associés aux variables propositionnelles de φ de la façon suivante :
pour tout $i \in \{1, \dots, n\}$, $c(p_i) = \begin{cases} c(v) & \text{si } \nu(p_i) = 1 \\ c(f) & \text{sinon} \end{cases}$ et $c(\neg p_i) = \begin{cases} c(v) & \text{si } \nu(p_i) = 0 \\ c(f) & \text{sinon} \end{cases}$.
Comme $\nu \models \varphi = \bigwedge_{j=1}^{m} \mathcal{C}_j$, on a $\forall j \in \{1, \dots, m\}$ $\nu \models \mathcal{C}_j = (\alpha_{\mathcal{C}_j} \vee \beta_{\mathcal{C}_j} \vee \gamma_{\mathcal{C}_j})$, donc dans chacun des gadgets $G_\mathcal{C}$, l'un des sommets $\alpha_\mathcal{C}$, $\beta_\mathcal{C}$ ou $\gamma_\mathcal{C}$ est de la couleur de v. Donc d'après le lemme 1, on peut compléter les colorations partielles des $G_\mathcal{C}$ en une coloration de $tr(\varphi)$. Donc $tr(\varphi)$ est 3−coloriable.
$\boxed{\Longleftarrow}$ Soit c une 3−coloration de $tr(\varphi)$. On définit une valuation ν par :
pour tout $i \in \{1, \dots, n\}$, $\nu(p_i) = \begin{cases} 1 & \text{si } c(p_i) = c(v) \\ 0 & \text{sinon} \end{cases}$.
D'après le lemme 2, dans chaque gadget $G_\mathcal{C}$, l'un des sommets $\alpha_\mathcal{C}$, $\beta_\mathcal{C}$ ou $\gamma_\mathcal{C}$ a la couleur de v, donc pour tout $j \in \{1, \dots, m\}$ $\nu \models \mathcal{C}_j$, donc $\nu \models \varphi$. La formule φ est satisfiable.

□

Ce qui prouve que 3COL est NP-dur et donc NP-complet. □

Remarques :
On a supposé que les instances de 3SAT sont des formules ayant exactement 3 littéraux par clauses, mais si considère que les clauses ont au plus 3 littéraux, alors on construit les gadgets $G_\mathcal{C}$ en mettant des f à la place de $\gamma_\mathcal{C}$ si $\mathcal{C} = \alpha_\mathcal{C} \vee \beta_\mathcal{C}$ ou $\beta_\mathcal{C}$ et $\gamma_\mathcal{C}$ si $\mathcal{C} = \alpha_\mathcal{C}$.

Astuces de l'agrégatif :
Pendant le développement, je ne donnais pas de nom aux sommets intérieurs de $G_\mathcal{C}$ et pour prouver le lemme 2, je notais les couleurs des sommets sur le dessin de $G_\mathcal{C}$ directement.
Parfois, on parle de coloration propre pour désigner une coloration telle que deux sommets qui sont adjacents sont de couleurs différentes.

μ-recursive $\Longrightarrow$ λ-définissable

Leçons : 912 ; 929

Références : LASSAIGNE, DE ROUGEMONT, *Logique et fondements de l'informatique* (p.193) [LDR93] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 696) [LMLBP20]

Prérequis :

- la définition de fonctions μ-récursives
- combinateurs de point fixe (Turing [1], Curry [2] par exemple) [3]

Introduction :

On va montrer que toute fonction μ-récursive est λ-définissable, c'est un étape pour valider la thèse de Church qui nous dit que toute fonction calculable par une procédure effective est en fait une fonction calculable par une machine de Turing. En effet, on va pouvoir remplacer machine de Turing par λ-calcul ou fonctions μ-récursives quand on aura prouver que ces trois modèles de calcul sont équivalents. On prouve ici une implication de cette équivalence.

On représentera les entiers par [4]

$$[\![0]\!] := \lambda x.x$$
$$[\![n+1]\!] := \langle F, [\![n]\!]\rangle$$

avec

$$F := \lambda xy.y$$
$$\langle M, N\rangle := \lambda x.xMN$$

Définition 1. On dit qu'une fonction $f : \mathbb{N}^p \to \mathbb{N}$ est λ-définissable si et seulement si il existe un terme F de λ-calcul tel que

$$\forall n_1, \dots, n_p \in \mathbb{N}, \quad F[\![n_1]\!][\![n_2]\!]\dots[\![n_p]\!] = [\![f(n_1, \dots, n_p)]\!]$$

On dira que F représente f.

Théorème 1. Toute fonction μ-récursive est λ-définissable.

Démonstration.

Étape 1 : *Les fonctions de base* [5] *sont λ-définissables.*

La fonction zero est représentée par

$$\lambda x.[\![0]\!]$$

La fonction succ est représentée par

$$\lambda x.\langle F, x\rangle$$

La fonction π_i^n est représentée par

$$\lambda x_1 x_2 \dots x_n.x_i$$

1. $\Theta := AA$ où $A := \lambda xf.f(xxf)$
2. $Y := \lambda f.(\lambda x.f(xx))(\lambda x.f(xx))$
3. L'avantage du point fixe de Turing sur celui de Curry, c'est qu'on a une β-réduction directe, alors que pour celui de Curry, il faut réduire dans des sens différents (c'est une β-équivalence)
4. c'est une définition que l'on trouve dans le Barendregt [BAR12]
5. La fonction nulle zero, la fonction qui donne le successeur succ et la projection sur la $i^{\text{ème}}$ coordonnée d'un vecteur à n éléments π_i^n.

Étape 2 : *Clos par composition*

Si f une fonction à p arguments est représentée par un terme F et les p fonctions $g_1, \dots, g_p$ sont représentées par $G_1, \dots, G_p$, alors

$$\begin{aligned}[\![f(g_1(\vec{n}), \dots, g_p(\vec{n}))]\!] &= F[\![g_1(\vec{n})]\!] \dots [\![g_p(\vec{n})]\!] \\ &= F(G_1[\![\vec{n}]\!]) \dots (G_p[\![\vec{n}]\!])\end{aligned}$$

Donc

$$\lambda\vec{x}.F(G_1\vec{x}) \dots (G_p\vec{x})$$

représente la composition de f avec les fonctions g_i.

Étape 3 : *Clos par récursion primitive*

Soit φ le schéma de récursion primitive :

$$\varphi(\vec{n}, 0) = f(\vec{n})$$

$$\varphi(\vec{n}, k) = g(\vec{n}, k, \varphi(\vec{n}, k-1)$$

On se donne F qui représente f et G qui représente g.

On veut montrer que φ est λ-définissable.

On voudrait trouver un terme H tel que

$$H\ \vec{x}\ k = \ \mathsf{if}\ (\mathsf{is_zero}\ k)\ \mathsf{then}\ F\ \vec{x}\ \mathsf{else}\ G\ \vec{x}\ k\ (H\ \vec{x}\ (\mathsf{pred}\ k))$$

avec

$$\mathsf{if.then.else} = \lambda xtf.xtf$$

$$\mathsf{is_zero} = \lambda x.(xT)$$

$$\mathsf{pred} = \lambda x.(xF)$$

On va donc avoir besoin d'un combinateur de point fixe θ tel que

$$\forall K, \quad \theta K = K(\theta K)$$

La fonction φ est donc représentée par

$$\theta\ H$$

avec

$$H := (\lambda h\vec{x}k.\ \mathsf{if}\ (\mathsf{is_zero}\ k)\ \mathsf{then}\ F\ \vec{x}\ \mathsf{else}\ G\ \vec{x}\ k\ (h\ \vec{x}\ (\mathsf{pred}\ k))$$

En effet

$$\begin{aligned}[\![\varphi(\vec{n}, 0)]\!] &= \theta\ H\ [\![\vec{n}]\!]\ [\![0]\!] \\ &= H\ (\theta\ H)\ [\![\vec{n}]\!]\ [\![0]\!] \\ &= F\ [\![\vec{n}]\!] \\ &= [\![f(\vec{n})]\!]\end{aligned}$$

et pour tout $k > 0$,

$$\begin{aligned}[\![\varphi(\vec{n}, k)]\!] &= \theta\ H\ [\![\vec{n}]\!]\ [\![k]\!] \\ &= H\ (\theta\ H)\ [\![\vec{n}]\!]\ [\![k]\!] \\ &= G\ [\![\vec{n}]\!]\ [\![k]\!]\ (\theta\ H\ [\![\vec{n}]\!]\ (\mathsf{pred}\ [\![k]\!])) \\ &= G\ [\![\vec{n}]\!]\ [\![k]\!]\ (\theta\ H\ [\![\vec{n}]\!]\ [\![k-1]\!]) \\ &= G\ [\![\vec{n}]\!]\ [\![k]\!]\ [\![\varphi(\vec{n}, k-1)]\!] \\ &= [\![g(\vec{n}, k, \varphi(\vec{n}, k-1))]\!]\end{aligned}$$

Étape 4 : *Clos par minimisation non bornée*

Soit $\varphi(\vec{n}) = \mu_i(f(\vec{n}, i) = 0)$ le schéma de minimisation non bornée. On se donne F qui représente f.

Montrons que φ est λ-définissable.

Il faut trouver un terme qui fait un test sur le prédicat $f(\vec{n}, i) = 0$ et qui renvoit i si le prédicat est évalué à vrai et sinon teste sur $i + 1$, etc.

Soit P un prédicat, on pose

$$H_P = \lambda hk.\ \mathsf{if}\ (P\ k)\ \mathsf{then}\ k\ \mathsf{else}\ h\ (\mathsf{succ}\ k))$$

On utilise à nouveau un combinateur de point fixe

$$\begin{aligned} \theta\ H_P\ [\![0]\!] &= H_P\ (\theta\ H_P)\ [\![0]\!] \\ &= \mathsf{if}\ (P\ [\![0]\!])\ \mathsf{then}\ [\![0]\!]\ \mathsf{else}\ \theta\ H_P\ (\mathsf{succ}\ [\![0]\!]) \\ &= \mathsf{if}\ (P\ [\![0]\!])\ \mathsf{then}\ [\![0]\!]\ \mathsf{else}\ \theta\ H_P\ [\![1]\!] \end{aligned}$$

On pose

$$\mu\ P = \theta\ H_P\ [\![0]\!]$$

Ainsi on peut représenter φ par le terme

$$\lambda\vec{x}.\Big(\mu\big(\lambda k.(\mathsf{is_zero}\ (F\ \vec{x}\ k))\big)\Big)$$

□

Remarques :

Ce théorème est une implication dans l'équivalence des modèles de calcul entre Machines de Turing, fonctions μ-récursives et λ-calcul. En effet, combiné avec le développement Machine de Turing $\Longrightarrow$ μ-recursif, il suffit de prouver que toute fonction λ-définissable est calculable par une Machine de Turing.

Astuces de l'agrégatif :

Il faut bien comprendre le sens des termes notamment pour la minimisation non bornée qui n'est pas forcément la partie la plus immédiate.

Il faut voir les λ-termes T et F comme les booléens true et false. En effet, pour la conditionnelle if then else : $\lambda btf.btf$, le booléen b qui sera soit T soit F renverra soit t soit f puisque T renvoie le premier argument et F le deuxième argument.

Le combinateur de point fixe permet de simuler une boucle while, car il permet de réitérer une fonction sans connaitre le nombre d'itérations. On a utilisé un combinateur de point fixe pour simuler la récursion primitive mais l'expressivité du combinateur de point fixe est plus grande puisqu'elle peut simuler la minimisation non bornée. On peut prendre comme combinateur de point fixe celui de Curry Y ou celui de Turing Θ avec

$$Y := \lambda f.(\lambda x.f(xx))(\lambda x.f(xx)) \quad \text{et} \quad \Theta := AA \text{ où } A := \lambda xf.f(xxf)$$

par exemple. Un des avantages du point fixe de Turing réside dans le fait qu'on a une β-réduction directe, alors que pour celui de Curry, il faut réduire dans des sens différents (c'est une β-équivalence). L'avantage de celui de Curry est qu'il est plus naturel à définir. En effet,

$$\begin{aligned} \lambda f.(\lambda x.f(xx))(\lambda x.f(xx))K &\to_\beta (\lambda x.K(xx))(\lambda x.K(xx)) \\ &\to_\beta K((\lambda x.K(xx))(\lambda x.K(xx))) \\ &\leftarrow_\beta K(\lambda f.(\lambda x.f(xx))(\lambda x.f(xx))K) \end{aligned}$$

Questions possibles :

- Montrer que à $\vec{x}$ fixé, $\lambda k.(\mathsf{is_zero}\ (X\ [\![\vec{x}]\!]\ [\![k]\!]))$ représente $\chi(\vec{x}, k) = 0$.
- Donner un λ-terme qui additionne deux entiers.
- Donner une autre représentation des entiers. entiers de Church
- Montrer que toute fonction λ-définissable est Turing-calculable.
- Montrer que les combinateurs de Curry et de Turing sont bien des combinateurs de point fixe.

Décidabilité de l'arithmétique de Presburger

Leçons : 909 ; 914 ; 924

Références : CARTON, *Langages formels, calculabilité et complexité* (p.178) [CAR14]

Introduction :

On va prouver que la théorie de Presburger est décidable, c'est à dire que, pour toute formule close (écrite sur la signature [1] comprenant les constantes 0 et 1, la fonction *successeur* et le prédicat d'égalité), on peut dire si $\mathbb{N}$ est un modèle de cette formule ou non.

Théorème 1. Le problème

$PRES$ $\begin{cases} \text{entrée :} & \text{une formule } \varphi \text{ close sur la signature } \sigma = \{0, 1, +, =\} \\ \text{sortie :} & \text{oui si } \mathbb{N} \vDash \varphi, \text{ non sinon} \end{cases}$

est décidable.

Démonstration.

Étape 1 : *On veut construire un automate $\mathcal{A}$ telle que $\mathbb{N} \vDash \varphi$ si et seulement si $L(\mathcal{A}) \neq \emptyset$*

Pour tout $k \in \mathbb{N}^*$, on va se donner un alphabet pour représenter les $k-$uplet $(n_1, \dots, n_k) \in \mathbb{N}^k$. On pose $\Sigma_k = \{0, 1\}^k$. On représente les entiers en binaire avec le bit de poids faible à gauche. On ajoute des 0 à droite pour que l'on ait des représentations qui font toutes la même taille.

$$\begin{array}{ccccc} n_1 & = & \alpha_1^1 & \dots & \alpha_1^r \\ n_2 & = & \alpha_2^1 & \dots & \alpha_2^r \\ \vdots & \vdots & \vdots & & \vdots \\ n_k & = & \alpha_k^1 & \dots & \alpha_k^r \end{array}$$

Chaque colonne appartient à Σ_k, donc on peut représenter un $k-$uplet $(n_1, \dots, n_k)$ par un mot w sur l'alphabet Σ_k.

Soit φ une formule sur la signature σ.

On commence par remplacer tous les $\forall x \psi(x)$ par la formule $\neg(\exists x \neg\psi(x))$ qui est sémantiquement équivalente, cela a pour avantage d'enlever tous les quantificateurs $\forall$ de φ.

On va construire pour toute sous-formule ψ de φ un automate $\mathcal{A}_\psi$ tel que

$$L(\mathcal{A}_\psi) = \{(n_1, \dots, n_k) \in \mathbb{N}^k, \mathbb{N}[x_1 = n_1, \dots, x_k = n_k] \vDash \psi \\ \text{où } x_1, \dots, x_k \text{ sont les variables libres de } \psi\}$$

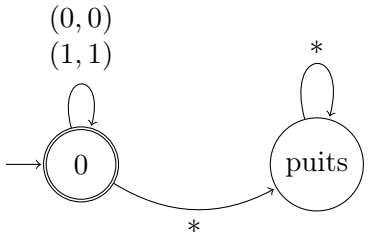
Procédons par induction sur la structure de la formule φ :

— cas où ψ est une formule atomique, deux cas se présentent : [2]

  — $\psi := x_i = x_j$

1. on parle parfois de langage qui comprend des fonctions qui ont chacune une arité positive (on parle de constantes pour les fonctions d'arité nulle) et des relations qui ont chacune une arité strictement positive.
2. on peut traiter les cas $x_i = 0$, $x_i = 1$ de manière similaire.

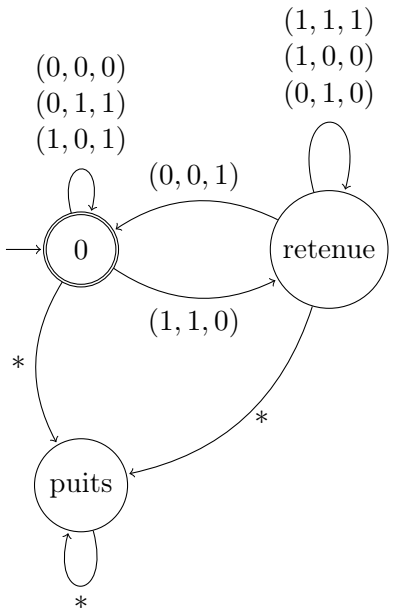
On pose $\mathcal{A}_\psi :=$



En notant $(0,0)$ et $(1,1)$ sur les transitions, on ne donne que les indices i et j des étiquettes, mais ce sont en réalité des étiquettes sur l'alphabet Σ_k. De plus, les étoiles $*$ désignent toutes les autres étiquettes possibles sur Σ_k.

— $\psi := x_i + x_j = x_k$

On pose $\mathcal{A}_\psi :=$



— cas $\psi := \psi_1 \vee \psi_2$, on dispose des automates $\mathcal{A}_{\psi_1}$ et $\mathcal{A}_{\psi_2}$, on construit alors l'automate $\mathcal{A}_\psi$ comme l'automate de l'union des automates $\mathcal{A}_{\psi_1}$ et$\mathcal{A}_{\psi_2}$.

— cas $\psi := \psi_1 \wedge \psi_2$, similaire en prenant l'automate de l'intersection.

— cas $\psi := \neg\psi_1$, similaire en prenant l'automate du complémentaire [3].

— cas $\psi := \exists x \psi_1(x)$ si $x \notin FV(\psi)$, on peut prendre $\mathcal{A}_\psi := \mathcal{A}_{\psi_1}$.

— cas $\psi := \exists x \psi_1(x)$ si $x \in FV(\psi)$, on note $\mathcal{A}_{\psi_1} = (Q, I, F, \delta)$. On pose l'automate

$$\mathcal{A}_\psi := (Q, I, F, \delta')$$

où δ' est telle que

$$p \xrightarrow{(x_1,\dots,x_{k-1})} q \text{ dans } \mathcal{A}_\psi$$

si et seulement si

$$\text{il existe } x \text{ tel que } p \xrightarrow{(x_1,\dots,x_{k-1},x)} q \text{ dans } \mathcal{A}_{\psi_1}$$

3. attention, il faut compléter et déterminiser l'automate, ce qui est coûteux

On obtient à la fin un automate $\mathcal{A}$ sur le langage vide (puisque φ est close) qui est tel que

$\mathbb{N} \vDash \varphi$ si et seulement un état final de $\mathcal{A}$ est accessible en partant de l'état initial.

Comme un parcours d'un graphe[4] est un algorithme d'accessibilité dans un graphe, la théorie de Presburger est donc bien une théorie décidable.

Étape 2 : *Calcul de la complexité*

Lors de la construction de l'automate, l'opération la plus couteuse est la création de l'automate du complémentaire car il faut compléter et déterminiser l'automate précédent. Pour déterminiser et compléter un automate, on passe d'un automate à n états vers un automate à 2^n états. Ainsi si la formule φ contient k symboles $\neg$ et m symboles $\forall$, on va devoir déterminiser $k + 2m$ fois et donc cela coutera $2^{2^{\cdot^{\cdot^{\cdot^{2^n}}}}}$ où on itère l'exponentielle $k + 2m$ fois et là, on ne compte même pas l'expansion de l'automate dûe aux autres opérateurs (union, intersection). Donc l'algorithme que l'on décrit ici est dans $(k + 2m)$ExpTime. On a donc un problème décidable mais avec une complexité non élémentaire, qui n'est pas calculable par une machine efficacement. □

Remarques :

- L'arithmétique de Presburger est cohérente et complète.
- L'arithmétique de Presburger est décidable, mais si on ajoute le symbole $\times$, on obtient l'arithmétique de Peano qui est indécidable.
- Le problème de décidabilité de Presburger est en réalité dans 3ExpTime et est 2ExpTime-dur.

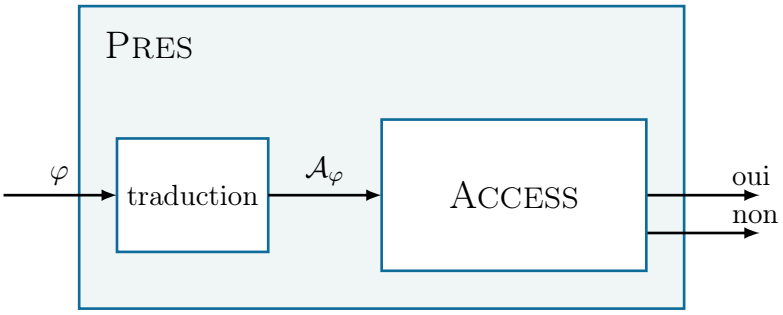
Astuces de l'agrégatif :

Il y a plein de rédaction de ce développement, je mets en page suivante un exemple de rédaction qu'il ne faut pas faire, au début je l'avais rédigé comme ci-après mais après un passage en leçon avec certains encadrants, ils nous avaient mis en garde contre cette rédaction car ce n'était vraiment pas propre.

Remarques :

On peut voir ce résultat comme une réduction de Pres à Access où

Access $\begin{cases} \underline{\text{entrée :}} \text{ un graphe } G = (S, A) \text{ et deux sommets } u, v \in S \\ \underline{\text{sortie :}} \text{ oui si il existe un chemin de } u \text{ à } v \text{ dans le graphe } G, \text{ non sinon} \end{cases}$



Comme Access est décidable, alors Pres est bien décidable.

4. en largeur ou en profondeur par exemple

Décidabilité de l'arithmétique de Presburger (Version à ne pas faire)

Leçons : 909 ; 914 ; 924

Références : CARTON, *Langages formels, calculabilité et complexité* (p.178)

Introduction :

Le développement qui suit est un exemple de ce qu'il ne faut pas faire, il est tiré du *Carton* qui est un mauvaise référence pour ce développement. Je l'avais tapé en pensant qu'il était bien mais en fait il y a plein de choses bizarres dedans. Ainsi j'ai tapé une meilleure version (à mon sens) de ce développement, cela peut donc faire la différence à l'agreg avec des candidats qui auraient "bêtement" recopié le *Carton*. Les problèmes les plus flagrants sont : la mise sous forme prénexe inutile (en effet les formules en elle-même sont définies par induction, pourquoi séparer les cas inductifs ?), le fait de s'arrêter à 1 et non à 0 (cela rajoute une disjonction de cas inutile) et on ne parle pas de complexité (alors que c'est primordial ici puisque décidable est équivalent à avoir un algorithme sauf que celui-ci est de complexité très médiocre il est dans kExpTime où k est le nombre de négations (après avoir fait le changement des $\forall$ en $\exists$)).

Enfin bref tout cela pour dire qu'il faut faire attention à ce développement qui est sournois.

Prérequis :

- la décidabilité de Vide pour un langage rationnel [1]
- la décidabilité de Univ pour un langage rationnel [2]
- Théorème de Kleene

Théorème 1. Le problème Pres $\begin{cases} \text{entrée : une formule } \varphi \text{ close sur le langage } L = \{0, 1, +, =\} \\ \text{sortie : oui si } \mathbb{N} \vDash \varphi, \text{ non sinon} \end{cases}$ est décidable.

Démonstration.

Étape 1 : *Se ramener à un problème de vacuité ou d'universalité d'un langage*

Pour tout $k \in \mathbb{N}^*$, on va se donner un alphabet pour représenter les $k-$uplet $(n_1, \dots, n_k) \in \mathbb{N}^k$. On pose $\Sigma_k = \{0, 1\}^k$. On représente les entiers en binaire avec le bit de poids faible à gauche. On ajoute des 0 à droite pour que l'on ait des représentations qui font toutes la même taille.

$$\begin{array}{ccccc} n_1 & = & \alpha_1^1 & \dots & \alpha_1^r \\ n_2 & = & \alpha_2^1 & \dots & \alpha_2^r \\ \vdots & \vdots & \vdots & & \vdots \\ n_k & = & \alpha_k^1 & \dots & \alpha_k^r \end{array}$$

Chaque colonne appartient à Σ_k, donc on peut représenter un $k-$uplet $(n_1, \dots, n_k)$ par un mot w sur l'alphabet Σ_k. On notera $[\![w]\!] = (n_1, \dots, n_k)$ le décodage du mot.

1. Vide $\begin{cases} \text{entrée : un langage rationnel } L \text{ sur un alphabet } \Sigma \\ \text{sortie : oui si } L = \emptyset, \text{ non sinon} \end{cases}$
2. Univ $\begin{cases} \text{entrée : un langage rationnel } L \text{ sur un alphabet } \Sigma \\ \text{sortie : oui si } L = \Sigma^*, \text{ non sinon} \end{cases}$

Soit φ une formule sur le langage L, on peut la supposer sous forme prénexe[3].

$$\varphi = Q_1 x_1 \dots Q_n x_n \psi$$

où $Q_i \in \{\exists, \forall\}$ et ψ est une formule sans quantificateur.

On pose

$$\varphi_k = Q_{k+1} x_{k+1} \dots Q_n x_n \psi$$

D'où $\varphi_0 = \varphi$ et $\varphi_n = \psi$. Les variables $x_1, \dots, x_k$ sont libres dans φ_k.

On introduit, pour tout $k \in \mathbb{N}^*$,

$$\mathcal{N}_k = \{(n_1, \dots, n_k) \in \mathbb{N}^k, \mathbb{N}[x_1 = n_1, \dots, x_k = n_k] \vDash \varphi_k\}$$

et

$$\mathcal{L}_k = \{w \in \Sigma_k^*, [\![w]\!] \in \mathcal{N}_k\}$$

On remarque que

— Si $\varphi = \exists x_1 \varphi_1$, alors $\big(\mathbb{N} \vDash \varphi \iff \mathcal{N}_1 \neq \emptyset \iff \mathcal{L}_1 \neq \emptyset\big)$.

— Si $\varphi = \forall x_1 \varphi_1$, alors $\big(\mathbb{N} \vDash \varphi \iff \mathcal{N}_1 = \mathbb{N} \iff \mathcal{L}_1 = \Sigma_1^*\big)$.

Étape 2 : *Prouver que le langage $\mathcal{L}_1$ est rationnel*

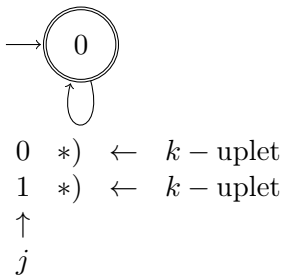
Montrons par récurrence sur k allant de n à 1 que

"il existe un automate $\mathcal{A}_{\varphi_k}$ tel que $\mathrm{L}(A_{\varphi_k}) = \mathcal{L}_k$"

Initialisation : On veut montrer qu'il existe A_ψ tel que $\mathrm{L}(A_\psi) = \mathcal{L}_n$. On va le montrer par induction structurelle sur la forme de ψ

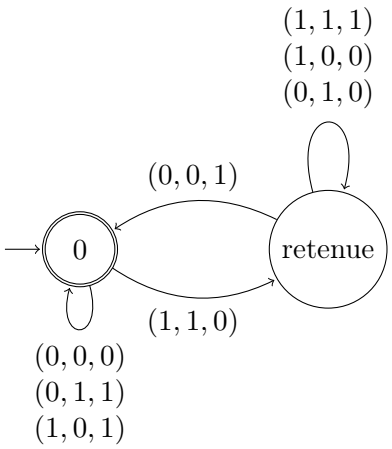
— cas $\psi := x_i = x_j$

On pose $\mathcal{A}_\psi :=$



— cas $\psi := x_i + x_j = x_l$ (on va mettre juste les indices qui nous intéressent)

On pose $\mathcal{A}_\psi :=$



3. c'est-à-dire tous les quantificateurs précèdent la formule

— cas $\psi := \psi_1 \vee \psi_2$ en prenant l'automate de l'union

— cas $\psi := \psi_1 \wedge \psi_2$ en prenant l'automate de l'intersection

— cas $\psi := \neg\psi_1$ en prenant l'automate du complémentaire [4]

Ainsi on peut construire A_ψ tel que $\mathrm{L}(A_\psi) = \mathcal{L}_n$.

Hérédité : On suppose que l'on a $A_{\varphi_{k+1}}$, on veut construire A_{φ_k}.

— Si $Q_{k+1} = \forall$, on se ramène à un $\exists$ par l'automate du complémentaire. [5]

— Si $Q_{k+1} = \exists$, on sait que l'on dispose de

$$\mathcal{A}_{\varphi_{k+1}} = (Q_{k+1}, I_{k+1}, F_{k+1}, T_{k+1}, \Sigma_{k+1})$$

On note $\pi_k : \left\{ \begin{array}{ccc} \Sigma_{k+1} & \to & \Sigma_k \\ (x_1, \dots, x_{k+1}) & \mapsto & (x_1, \dots, x_k) \end{array} \right.$.

On pose alors

$$\mathcal{A}_{\varphi_k} = (Q_{k+1}, I_k, F_{k+1}, T_k, \Sigma_k)$$

où T_k est définie par

$$\text{si } p \xrightarrow{x} q \text{ est dans } \mathcal{A}_{\varphi_{k+1}} \text{ alors on met } p \xrightarrow{\pi_k(x)} q \text{ dans } \mathcal{A}_{\varphi_k}$$

et $I_k = I_{k+1} \cup \{T_k(i, \underbrace{(0, \dots, 0)}_{k \text{ fois}}), \forall i \in I_{k+1}\}$

On trouve en fait x_{k+1} de manière non déterministe mais il se pourrait que l'entier à "deviner" soit plus grand et nécessite plus de lettres de Σ_{k+1} et donc il faut que l'état qui viendrait d'un état initial de $\mathcal{A}_{\varphi_{k+1}}$ où, sur la transition, on aurait lu que des 0 soit un état initial de $\mathcal{A}_{\varphi_k}$, d'où la modification des états initiaux.

Conclusion : On a donc construit $\mathcal{A}_{\varphi_1}$ tel que $\mathrm{L}(\mathcal{A}_{\varphi_1}) = \mathcal{L}_1$.

Donc $\mathcal{L}_1$ est rationnel en vertu du théorème de Kleene.

Ainsi savoir $\mathcal{L}_1 \neq \emptyset$ et $\mathcal{L}_1 = \Sigma_1^*$ sont des problèmes décidables. Donc PRES est décidable, d'après la remarque de la fin de l'étape 1. □

Remarques :

L'arithmétique de Presburger est décidable, mais si on ajoute le symbole $\times$, on obtient l'arithmétique de Peano qui est indécidable.

Astuces de l'agrégatif :

On pourrait juste parler de langages reconnaissables et ne pas utiliser le théorème de Kleene mais souvent on énonce les problèmes UNIV et VIDE plutôt pour les langages rationnels donc j'ai préféré garder les utilisations usuelles de ces problèmes.

4. attention, il faut compléter et déterminiser l'automate
5. puisque $\forall x \psi(x)$ est sémantique équivalent à $\neg\exists x(\neg\psi(x))$.

Équivalence entre sémantiques opérationnelles

Leçons : 930

Références : NIELSON & NIELSON, *Semantics with applications* (p.40) [NN07] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 830) [LMLBP20]

On notera $\langle S, s\rangle \to s'$ pour la sémantique à grands pas (NS) (voir appendice)
On notera $\langle S, s\rangle \Longrightarrow s'$ pour un pas de la sémantique à petits pas (SOS) (voir appendice)

Introduction :

Nous allons prouver que la sémantique opérationnelle à petits pas et la sémantique opérationnelle à grands pas sont équivalentes. Elles sont équivalentes mais ont toutes deux des avantages différents. [1]

Théorème 1. Pour toute instruction S, on a $\mathscr{S}_{SOS}[\![S]\!] = \mathscr{S}_{NS}[\![S]\!]$

Lemme 1. Si $\langle S_1, s\rangle \Longrightarrow^* s'$, alors

$$\langle S_1; S_2, s\rangle \Longrightarrow^* \langle S_2, s'\rangle$$

Démonstration. Par récurrence sur le nombre de pas.
Initialisation : Si $k = 1$, alors $\langle S_1, s\rangle \Longrightarrow s'$, d'où par la règle de composition [comp $_{SOS}$], on a

$$\langle S_1; S_2, s\rangle \Longrightarrow \langle S_2, s'\rangle$$

ce qui prouve le cas d'initialisation.
Hérédité : Supposons que l'on ait le résultat pour tout $k \in \mathbb{N}^*$. Si $\langle S_1, s\rangle \Longrightarrow^{k+1} s'$, on a alors $\langle S_1, s\rangle \Longrightarrow \langle S_1', s''\rangle$. Ainsi $\langle S_1', s''\rangle \Longrightarrow^k s'$ puis, en appliquant l'hypothèse de récurrence, cela donne

$$\langle S_1'; S_2, s''\rangle \Longrightarrow^* s'$$

On utilise alors la règle de composition [comp $_{SOS}$] puisque l'on a $\langle S_1, s\rangle \Longrightarrow \langle S_1', s''\rangle$ pour avoir

$$\langle S_1; S_2, s\rangle \Longrightarrow \langle S_1'; S_2, s''\rangle \Longrightarrow^* s'$$

D'où le résultat souhaité.
Conclusion : Ainsi, pour tout $k \in \mathbb{N}^*$, si $\langle S_1, s\rangle \Longrightarrow^k s'$, alors

$$\langle S_1; S_2, s\rangle \Longrightarrow^* \langle S_2, s'\rangle$$

□

1. par exemple, la sémantique à grands pas permet d'être plus concis car on n'explique pas chaque pas de calcul, cependant sur un langage qui aurait des exceptions (division par zero par exemple) la sémantique à petit pas permet d'aller calculer jusqu'à l'exception dans une boucle while alors que la sémantique à grands pas bloquera dès le début de la boucle while car il ne trouverait pas le résultat final.

Lemme 2. Si $\langle S_1; S_2, s\rangle \Longrightarrow^k s'$ alors il existe $k_1, k_2 \in \mathbb{N}$ tels que $k_1 + k_2 = k$ et

$$\langle S_1, s\rangle \Longrightarrow^{k_1} s'' \text{ et } \langle S_2, s''\rangle \Longrightarrow^{k_2} s'$$

Démonstration. Par récurrence sur le nombre de pas.
Initialisation : On ne peut pas avoir $k = 1$[2], donc on initialise la récurrence pour $k = 2$.Si $\langle S_1; S_2, s\rangle \Longrightarrow^2 s'$ c'est que $\langle S_1, s\rangle \Longrightarrow s''$ et $\langle S_2, s''\rangle \Longrightarrow s'$ (par la règle de composition [comp $_{SOS}$]). Donc on a bien $k_1 = 1$ et $k_2 = 1$ avec $k_1 + k_2 = 2$, ce qui prouve le cas d'initialisation.
Hérédité : Soit $k > 2$, on suppose que la propriété est vraie pour tout $l < k$. On suppose que $\langle S_1; S_2, s\rangle \Longrightarrow^k s'$.

- Si $\langle S_1, s\rangle \Longrightarrow s''$, alors, par [comp $_{SOS}$], on a $\langle S_2, s''\rangle \Longrightarrow^{k-1} s'$ et comme $(k-1)+1 = k$, on a le résultat souhaité
- Si $\langle S_1, s\rangle \Longrightarrow \langle S_1', s''\rangle$, alors, par [comp $_{SOS}$], on a $\langle S_1' S_2, s''\rangle \Longrightarrow^{k-1} s'$. Par hypothèse de récurrence, on a

  $$\langle S_1', s''\rangle \Longrightarrow^{k_1} s''' \text{ et } \langle S_2, s'''\rangle \Longrightarrow^{k_2} s'$$

  avec $k_1 + k_2 = k - 1$. Ce qui donne

  $$\langle S_1, s\rangle \Longrightarrow \langle S_1', s''\rangle \Longrightarrow^{k_1} s'''$$

  D'où

  $$\langle S_1, s\rangle \Longrightarrow^{k_1+1} s'''$$

  De plus, on a $k_1 + 1 + k_2 = (k-1) + 1 = k$. Donc on a le résultat souhaité

Conclusion : Pour tout $k \in \mathbb{N}$[3] si $\langle S_1; S_2, s\rangle \Longrightarrow^k s'$ alors il existe $k_1, k_2 \in \mathbb{N}$ tels que $k_1 + k_2 = k$ et

$$\langle S_1, s\rangle \Longrightarrow^{k_1} s'' \text{ et } \langle S_2, s''\rangle \Longrightarrow^{k_2} s'$$

□

Démonstration du théorème.
Étape 1 : *Montrons que* $\langle S, s\rangle \to s'$ *implique* $\langle S, s\rangle \Longrightarrow^* s'$

On va prouver cela par induction sur la structure de l'arbre de dérivation[4].
cas de base : La propriété est vraie car les règles pour skip et l'assignation sont les mêmes dans les deux sémantiques.
cas inductif :

→ cas *comp* : Par la règle [comp $_{NS}$], on a $\dfrac{\langle S_1, s\rangle \to s_1' \qquad \langle S_2, s_1'\rangle \to s'}{\langle S_1; S_2, s\rangle \to s'}$

Par hypothèse d'induction, on a $\langle S_1, s\rangle \Longrightarrow^{k_1} s_1'$ et $\langle S_2, s_1'\rangle \Longrightarrow^{k_2} s'$
On a donc

$$\langle S_1; S_2, s\rangle \Longrightarrow^{k_1} \langle S_2, s_1'\rangle \Longrightarrow^{k_2} s'$$

On a utilisé le lemme 1 pour la première flèche. On a donc ainsi

$$\langle S_1; S_2, s\rangle \Longrightarrow^* s'$$

2. car il faut au moins 2 pas pour transformer $S_1; S_2, s$ en un état s'
3. on peut dire que $k \in \mathbb{N}$ car la propriété sera vraie puisque l'hypothèse ne se produit jamais
4. attention, on ne peut pas le faire par induction sur la formule directement car pour le cas *while*, on a le même terme qui réapparaît .

→ cas *if* : Par la règle [if $^{tt}_{NS}$], on a $\dfrac{\langle S_1, s\rangle \to s'}{\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \to s'}$ si $\mathcal{B}[\![b]\!]_s = tt$

Par hypothèse d'induction, on a

$$\langle S_1, s\rangle \Longrightarrow^k s'$$

Or la règle [if $^{tt}_{SOS}$] nous donne $\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \Longrightarrow \langle S_1, s\rangle$, d'où

$$\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \Longrightarrow \langle S_1, s\rangle \Longrightarrow^* s'$$

Par la règle [if $^{ff}_{NS}$], on a $\dfrac{\langle S_2, s\rangle \to s'}{\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \to s'}$ si $\mathcal{B}[\![b]\!]_s = ff$

Par hypothèse d'induction, on a

$$\langle S_2, s\rangle \Longrightarrow^k s'$$

Or la règle [if $^{ff}_{SOS}$] nous donne $\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \Longrightarrow \langle S_2, s\rangle$, d'où

$$\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \Longrightarrow \langle S_2, s\rangle \Longrightarrow^* s'$$

→ cas *while* : Par la règle [while $^{tt}_{NS}$], on a $\dfrac{\langle S, s\rangle \to s' \ \langle \text{while } b \text{ do } S, s'\rangle \to s''}{\langle \text{while } b \text{ do } S, s\rangle \to s''}$ si $\mathcal{B}[\![b]\!]_s = tt$

Par hypothèse d'induction, on a

$$\langle S, s\rangle \Longrightarrow^* s' \text{ et } \langle \text{while } b \text{ do } S, s'\rangle \Longrightarrow^* s''$$

Or la règle du [while $_{SOS}$] nous donne

$$\langle \text{while } b \text{ do } S, s\rangle \Longrightarrow \langle \text{ if } b \text{ then } (S; \text{while } b \text{ do } S) \text{ else skip}, s\rangle$$

D'où

$$\begin{aligned}
\langle \text{while } b \text{ do } S, s\rangle &\Longrightarrow \langle \text{ if } b \text{ then } (S; \text{while } b \text{ do } S) \text{ else skip}, s\rangle \\
&\Longrightarrow \langle S; \text{while } b \text{ do } S, s\rangle \quad \text{car } \mathcal{B}[\![b]\!]_s = tt \\
&\Longrightarrow^* \langle \text{while } b \text{ do } S, s'\rangle \quad \text{en appliquant le lemme 1 et en utilisant} \\
&\qquad\qquad\qquad\qquad \text{l'hypothèse } \langle S, s\rangle \Longrightarrow^* s' \\
&\Longrightarrow^* s'' \quad \text{en utilisant l'hypothèse } \langle \text{while } b \text{ do } S, s'\rangle \Longrightarrow^* s''
\end{aligned}$$

Par la règle [while $^{ff}_{NS}$], on a $\langle \text{while } b \text{ do } S, s\rangle \to s$ si $\mathcal{B}[\![b]\!]_s = ff$

Or la règle du [while $_{SOS}$] nous donne

$$\langle \text{while } b \text{ do } S, s\rangle \Longrightarrow \langle \text{ if } b \text{ then } (S; \text{while } b \text{ do } S) \text{ else skip}, s\rangle$$

D'où

$$\begin{aligned}
\langle \text{while } b \text{ do } S, s\rangle &\Longrightarrow \langle \text{ if } b \text{ then } (S; \text{while } b \text{ do } S) \text{ else skip}, s\rangle \\
&\Longrightarrow \langle \text{skip}, s\rangle \quad \text{car } \mathcal{B}[\![b]\!]_s = ff \\
&\Longrightarrow s \quad \text{en utilisant [skip } _{SOS}]
\end{aligned}$$

Ce qui conclut l'induction.

Étape 2 : *Montrons que* $\langle S, s\rangle \Longrightarrow^k s'$ *implique* $\langle S, s\rangle \to s'$

Par récurrence sur le nombre de pas.

Initialisation : Pour $k = 1$, les seuls cas possibles sont : skip et l'assignation qui ont les mêmes règles dans les deux sémantiques donc cela justifie l'initialisation.

Hérédité : Soit $k \in \mathbb{N}^*$, supposons que la propriété est vraie pour tous les rangs $l < k$.

→ cas *comp* : Si $\langle S_1; S_2, s\rangle \Longrightarrow^k s'$, alors en utilisant le lemme 2, on a

$$\langle S_1, s\rangle \Longrightarrow^{k_1} s'' \text{ et } \langle S_2,'' \rangle \Longrightarrow^{k_2} s' \text{ avec } k_1 + k_2 = k$$

Or $k_1, k_2 \geqslant 1$, donc $k_1, k_2 < k$, on peut donc appliquer l'hypothèse de récurrence pour obtenir

$$\langle S_1, s\rangle \to s'' \text{ et } \langle S_2, s''\rangle \to s'$$

Ainsi par la règle [comp $_{NS}$], on a

$$\langle S_1; S_2, s\rangle \to s'$$

→ cas *if* : On suppose que $\langle$ if b then S_1 else $S_2, s\rangle \Longrightarrow^k s'$.
Si $\mathcal{B}[\![b]\!]_s = tt$, alors, par la règle [if $^{tt}_{SOS}$], on a

$$\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \Longrightarrow \langle S_1, s\rangle \Longrightarrow^{k-1} s'$$

Ainsi, par hypothèse de récurrence, on a $\langle S_1, s\rangle \to s'$.
Donc par la règle [if $^{tt}_{NS}$], on a

$$\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \to s'$$

Si $\mathcal{B}[\![b]\!]_s = ff$, alors, par la règle [if $^{ff}_{SOS}$], on a

$$\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \Longrightarrow \langle S_2, s\rangle \Longrightarrow^{k-1} s'$$

Ainsi, par hypothèse de récurrence, on a $\langle S_2, s\rangle \to s'$.
Donc par la règle [if $^{ff}_{NS}$], on a

$$\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \to s'$$

→ cas *while* : On suppose que $\langle$while b do $S, s\rangle \Longrightarrow^k s'$.
Par la règle [while $_{SOS}$], on a

$$\langle \text{while } b \text{ do } S, s\rangle \Longrightarrow \langle \text{ if } b \text{ then } (S; \text{while } b \text{ do } S) \text{ else skip}, s\rangle$$

Ainsi, si $\mathcal{B}[\![b]\!]_s = tt$, on a

$$\langle \text{while } b \text{ do } S, s\rangle \Longrightarrow^2 \langle S; \text{while } b \text{ do } S, s\rangle \Longrightarrow^{k-2} s'$$

On a utilisé la règle [if $^{tt}_{SOS}$].
On utilise le lemme 2, pour obtenir

$$\langle S, s\rangle \Longrightarrow^{k_1} s'' \text{ et } \langle \text{while } b \text{ do } S, s''\rangle \Longrightarrow^{k_2} s' \text{ avec } k_1 + k_2 = k - 2 < k$$

Ainsi par hypothèse de récurrence, on a

$$\langle S, s\rangle \to s'' \text{ et } \langle \text{while } b \text{ do } S, s''\rangle \to s'$$

On peut conclure en utilisant la règle [while $^{tt}_{NS}$], pour avoir

$$\langle \text{while } b \text{ do } S, s\rangle \to s'$$

Et si $\mathcal{B}[\![b]\!]_s = ff$, on a

$$\langle \text{while } b \text{ do } S, s\rangle \Longrightarrow^2 \langle \text{skip}, s\rangle \Longrightarrow s$$

On a utilisé la règle [if $^{ff}_{SOS}$]. Ainsi, on avait en fait $s' = s$.
Or la règle [while $^{ff}_{NS}$] nous donne

$$\langle \text{while } b \text{ do } S, s\rangle \to s$$

Ce qui conclut le cas ff.

Conclusion : Ainsi pour tout $k \in \mathbb{N}^*$, si $\langle S, s\rangle \Longrightarrow^k s'$, alors $\langle S, s\rangle \to s'$.

□

Remarques :

On a aussi une équivalence entre la sémantique dénotationnelle et la sémantique opérationnelle à petits pas donc grâce au théorème que l'on vient de prouver, on a une équivalence entre la sémantique dénotationnelle et la sémantique opérationnelle à grands pas.

Astuces de l'agrégatif :

Il est mieux d'écrire les lemmes dans le plan et donc de s'affranchir de cette partie lors du développement.

Il faut bien comprendre qu'on ne peut pas faire la première induction sur la structure de l'instruction mais qu'il faut le faire sur la structure de l'arbre.

Questions possibles :

- Montrer que les instructions while b do S et if b then S; while b do S else skip sont équivalentes pour la sémantique opérationnelle à grands pas.
- Écrire des règles de sémantique à grands et petits pas pour gérer les instructions repeat S until b, et montrer que l'équivalence est préservée.
- Montrer que le langage IMP muni de la sémantique opérationnelle à petits pas (ou à grands pas) est déterministe, *i.e.* il y a unicité de l'état sortant s' après exécution d'une instruction S à partir d'un état s.

Complétude de la logique de Hoare

Leçons : 927 ; 930

Références : NIELSON & NIELSON, *Semantics with applications* (p.186) [NN07] et WINSKEL, *The Formal Semantics of Programming Languages : An Introduction* [WIN93] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 824) [LMLBP20]

Prérequis :

- Connaître différentes sémantiques du langage IMP (voir Appendice)

Définition 1. On notera

$$\vdash_p \{P\}S\{Q\}$$

s'il existe un arbre de dérivation aboutissant à $\{P\}S\{Q\}$ en utilisant les règles de la logique de Hoare (notée $[\dots]_H$). (voir Appendice)

Définition 2. On notera

$$\vDash_p \{P\}S\{Q\}$$

si $\forall s$ tel que $P\ s = tt$ on ait $\langle S, s\rangle \to s'$ implique $Q\ s' = tt$

Dans la deuxième définition, on utilise les règles de la sémantique opérationnelle à grands pas (notée $[\dots]_{NS}$ pour "sémantique naturelle") (voir Appendice).

Introduction :

La logique de Hoare est un outil qui permet de prouver la correction de certains programmes. Pour cela, on a des règles de dérivation que l'on va utiliser pour démontrer (à l'aide d'une preuve) la correction d'un programme et une sémantique (celle opérationnelle à grands pas) qui va être le sens que l'on donne au programme. On veut donc prouver un théorème de correction et complétude face aux règles que l'on s'est donné. La correction consiste à vérifier que les règles que l'on utilise vérifient bien la sémantique que l'on a (on n'abordera pas cet aspect dans ce développement). La complétude consiste à trouver, pour tout programme ayant une certaine sémantique, un arbre de dérivation des règles qui démontre le résultat (c'est ce que l'on va faire dans ce développement).

Théorème 1. Pour tous prédicats P, Q et toute instruction S,

$$\vdash_p \{P\}S\{Q\} \iff \vDash_p \{P\}S\{Q\}$$

Démonstration de la complétude. $\boxed{\Longleftarrow}$

Définition 3. $\mathrm{wlp}(S, Q)$ est la plus faible précondition donnant Q en exécutant S, i.e.

$$\mathrm{wlp}(S, Q)\ s = tt \text{ si et seulement si } \forall s'\ \langle S, s\rangle \to s' \text{ implique } Q\ s' = tt$$

Lemme 1. $\vDash_p \{P\}S\{Q\}$ implique $(P \implies \mathrm{wlp}(S, Q))$.

Démonstration du lemme. On suppose $P\ s = tt$, on veut prouver que $\text{wlp}(S,Q) = tt$. Par définition de $\vDash_p$ et puisque $P\ s = tt$, on a $\langle S, s\rangle \to s'$ implique $Q\ s' = tt$. D'où $\text{wlp}(S,Q)\ s = tt$ par définition de wlp. □

On veut prouver que $\vdash_p \{P\}S\{Q\}$
On va pouvoir utiliser la règle de la conséquence [cons $_H$] avec $P \implies \text{wlp}(S,Q)$.
Donc il faut prouver que $\vdash_p \{\text{wlp}(S,Q)\}S\{Q\}$.

Montrons que $\vdash_p \{\text{wlp}(S,Q)\}S\{Q\}$ par induction sur la structure de S.

→ cas *skip* : On a $\text{wlp}(\mathsf{skip}, Q) = Q$

Preuve. — On suppose que $Q\ s = tt$. Si on a $\langle \mathsf{skip}, s\rangle \to s'$ c'est que $s' = s$ (par définition de la règle [skip $_{NS}$]) d'où $Q\ s' = tt$ et donc $\text{wlp}(\mathsf{skip}, Q)\ s = tt$ par définition de wlp. Ainsi

$$Q \implies \text{wlp}(\mathsf{skip}, Q)$$

— On suppose que $\text{wlp}(\mathsf{skip}, Q)\ s = tt$. Si on a $\langle \mathsf{skip}, s\rangle \to s'$, c'est aussi que $s' = s$ et donc $Q\ s = tt$. Ainsi

$$\text{wlp}(\mathsf{skip}, Q) \implies Q$$ [1]

□

Or on a $\vdash_p \{Q\}\mathsf{skip}\{Q\}$ par la règle [skip $_H$] d'où

$$\vdash_p \{\text{wlp}(\mathsf{skip}, Q)\}\mathsf{skip}\{Q\}$$

→ cas *affectation* : On a $\text{wlp}(x := a, Q) = Q[x \mapsto \mathcal{A}[\![a]\!]]$

Preuve. — On suppose que $Q[x \mapsto \mathcal{A}[\![a]\!]]\ s = tt$. Si on a $\langle x := a, s\rangle \to s'$ c'est que $s' = s[x \mapsto \mathcal{A}[\![a]\!]]$ (par définition de la règle de l'affectation [ass $_{NS}$]) d'où $Q\ s' = Q[x \mapsto \mathcal{A}[\![a]\!]]\ s = tt$ et donc $\text{wlp}(x := a, Q)\ s = tt$ par définition de wlp. Ainsi

$$Q[x \mapsto \mathcal{A}[\![a]\!]] \implies \text{wlp}(x := a, Q)$$

— On suppose que $\text{wlp}(x := a, Q)\ s = tt$. Si on a $\langle x := a, s\rangle \to s'$, c'est aussi que $s' = s[x \mapsto \mathcal{A}[\![a]\!]]$ et donc $Q\ s' = Q[x \mapsto \mathcal{A}[\![a]\!]]\ s = tt$. Ainsi

$$\text{wlp}(x := a, Q) \implies Q[x \mapsto \mathcal{A}[\![a]\!]]$$ [2]

□

Or on a $\vdash_p \{Q[x \mapsto \mathcal{A}[\![a]\!]]\}x := a\{Q\}$ par la règle de l'affectation [ass $_H$] d'où

$$\vdash_p \{\text{wlp}(x := a, Q)\}x := a\{Q\}$$

→ cas *composition* : Par induction, on a

$$\vdash_p \{\text{wlp}(S_2, Q)\}S_2\{Q\} \text{ et } \vdash_p \{\text{wlp}(S_1, \text{wlp}(S_2, Q))\}S_1\{\text{wlp}(S_2, Q)\}$$

Montrons que $\text{wlp}(S_1; S_2, Q) \implies \text{wlp}(S_1, \text{wlp}(S_2, Q))$

1. en réalité, cette implication est suffisante, en utilisant la règle de la conséquence(hoare)
2. de même, cette implication est suffisante, en utilisant la règle de la conséquence [cons $_H$]

On suppose que $\text{wlp}(S_1; S_2, Q)\ s = tt$. Ainsi par définition si on a $\langle S_1; S_2, s\rangle \to s'$ alors $Q\ s' = tt$. Mais si on a $\langle S_1; S_2, s\rangle \to s'$, c'est que, par la règle de la composition [comp $_{NS}$], l'on avait

$$\langle S_1, s\rangle \to s'' \text{ et } \langle S_2, s''\rangle \to s'$$

Donc $\text{wlp}(S_2, Q)\ s'' = tt$ (par la deuxième assertion) et ainsi $\text{wlp}(S_1, \text{wlp}(S_2, Q))\ s = tt$ (par la première assertion). On a utilisé le fait que ce sont des wlp.

On utilise la règle de la conséquence(hoare) :
Comme $\vdash_p \{\text{wlp}(S_1, \text{wlp}(S_2, Q))\}S_1; S_2\{Q\}$ par la règle de la composition [comp $_H$] et $\text{wlp}(S_1; S_2, Q) \implies \text{wlp}(S_1, \text{wlp}(S_2, Q))$, on a donc

$$\vdash_p \{\text{wlp}(S_1; S_2, Q)\}S_1; S_2\{Q\}$$

→ cas *if* : Par induction, on a

$$\vdash_p \{\text{wlp}(S_1, Q)\}S_1\{Q\} \text{ et } \vdash_p \{\text{wlp}(S_2, Q)\}S_2\{Q\}$$

On pose $P = \big(\mathcal{B}[\![b]\!] \wedge \text{wlp}(S_1, Q)\big) \vee \big(\neg B[\![b]\!] \wedge \text{wlp}(S_2, Q)\big)$
Ainsi on a $\vdash_p \{P \wedge \mathcal{B}[\![b]\!]\}S_1\{Q\}$ et $\vdash_p \{P \wedge \neg\mathcal{B}[\![b]\!]\}S_2\{Q\}$. Donc, par la règle [if $_H$], on a

$$\vdash_p \{P\}\textsf{if } b \textsf{ then } S_1 \textsf{ else } S_2\{Q\}$$

Montrons que $\text{wlp}(\textsf{if } b \textsf{ then } S_1 \textsf{ else } S_2, Q) \implies P$

On suppose que $\text{wlp}(\textsf{if } b \textsf{ then } S_1 \textsf{ else } S_2, Q)\ s = tt$.
Ainsi par définition si on a $\langle \textsf{if } b \textsf{ then } S_1 \textsf{ else } S_2, s\rangle \to s'$ alors $Q\ s' = tt$.

- si $\mathcal{B}[\![b]\!]\ s = tt$, alors on a $\langle S_1, s\rangle \to s'$ d'où $\text{wlp}(S_1, Q)\ s = tt$
- si $\mathcal{B}[\![b]\!]\ s = ff$, alors on a $\langle S_2, s\rangle \to s'$ d'où $\text{wlp}(S_2, Q)\ s = tt$

Ainsi $P\ s = tt$.

On utilise la règle de la conséquence [cons $_H$] :
Comme $\vdash_p \{P\}\textsf{if } b \textsf{ then } S_1 \textsf{ else } S_2\{Q\}$ par la règle [if $_H$] et
$\text{wlp}(\textsf{if } b \textsf{ then } S_1 \textsf{ else } S_2, Q) \implies P$, on a donc

$$\vdash_p \{\text{wlp}(\textsf{if } b \textsf{ then } S_1 \textsf{ else } S_2, Q)\}\textsf{if } b \textsf{ then } S_1 \textsf{ else } S_2\{Q\}$$

→ cas *while* : On veut montrer que $\vdash_p \{\text{wlp}(\textsf{while } b \textsf{ do } S, Q)\}\textsf{while } b \textsf{ do } S\{Q\}$.
On note $P = \text{wlp}(\textsf{while } b \textsf{ do } S, Q)$.
Par induction , on a $\vdash_p \{\text{wlp}(S, P)\}S\{P\}$.
Montrons que $(\neg\mathcal{B}[\![b]\!] \wedge P) \implies Q$

On suppose que $(\neg\mathcal{B}[\![b]\!] \wedge P)\ s = tt$, c'est-à-dire $\mathcal{B}[\![b]\!]\ s = ff$ et $P\ s = \text{wlp}(\textsf{while } b \textsf{ do } S, Q)\ s = tt$. Donc si on a $\langle \textsf{while } b \textsf{ do } S, s\rangle \to s'$, c'est que $s = s'$ et donc $Q\ s = tt$. Ainsi

$$(\neg\mathcal{B}[\![b]\!] \wedge P) \implies Q$$

Montrons que $(\mathcal{B}[\![b]\!] \wedge P) \implies \text{wlp}(S, P)$

On suppose que $(\mathcal{B}[\![b]\!] \wedge P)\ s = tt$, c'est-à-dire $\mathcal{B}[\![b]\!]\ s = tt$ et $P\ s = \text{wlp}(\textsf{while } b \textsf{ do } S, Q)\ s = tt$. Donc si on a $\langle \textsf{while } b \textsf{ do } S, s\rangle \to s'$, c'est que, par les règles [while $_{NS}$]), on avait

$$\langle S, s\rangle \to s'' \text{ et } \langle \textsf{while } b \textsf{ do } S, s''\rangle \to s'$$

On a donc

$$Q\ s' = tt$$

car $\text{wlp}(\mathsf{while}\ b\ \mathsf{do}\ S, Q)\ s = tt$.
De ce fait, on a

$$\text{wlp}(\mathsf{while}\ b\ \mathsf{do}\ S, Q)\ s'' = tt$$

car $Q\ s' = tt$.
Et donc

$$\text{wlp}(S, P) = \text{wlp}(S, \text{wlp}(\mathsf{while}\ b\ \mathsf{do}\ S, Q))\ s = tt$$

car $\text{wlp}(\mathsf{while}\ b\ \mathsf{do}\ S, Q)\ s'' = tt$.
Ce qui prouve que

$$(\mathcal{B}[\![b]\!] \wedge P) \implies \text{wlp}(S, P)$$

On a dit que, par induction, on avait

$$\vdash_p \{\text{wlp}(S, P)\} S \{P\}$$

On utilise la règle de la conséquence [cons $_H$] pour avoir :

$$\vdash_p \{\mathcal{B}[\![b]\!] \wedge P)\} S \{P\}$$

Ainsi, par la règle du while [while $_H$], on a :

$$\vdash_p \{P\} \mathsf{while}\ b\ \mathsf{do}\ S \{\neg\mathcal{B}[\![b]\!] \wedge P\}$$

Puis, de nouveau par la règle de la conséquence [cons $_H$], on a :

$$\vdash_p \{P\} \mathsf{while}\ b\ \mathsf{do}\ S \{Q\}$$

□

Remarques :

On ne parle ici que de correction partielle, d'où le p en indice du symbole $\vdash$, c'est-à-dire que l'on n'a pas d'information sur la terminaison. Il existe des règles pour la correction totale avec un théorème de complétude associé.

Pour la correction, la preuve se fait par induction sur la structure de l'arbre. (Nielson & Nielson (p.184))

Astuces de l'agrégatif :

Attention, il faut bien maitriser toutes les règles que l'on utilise (que ce soit celles de la logique de Hoare ou celles de la sémantique opérationnelle à grands pas) pour expliquer de manière claire au jury et ne pas perdre du temps dessus. (C'est déjà un développement relativement long).

Je fais un point sur les bases de quelques sémantiques que l'on peut mettre sur le langage IMP dans l'appendice sur la sémantique.

Questions possibles :

- Justifier que $Q[x \to \mathcal{A}[\![a]\!]]\ s = Q\ s[x \mapsto \mathcal{A}[\![a]\!]_s]$.

- Représenter l'arbre de **Factorielle**(2) pour la sémantique à grands pas.

Algorithme 1 Factorielle(n)

$x \leftarrow n$
$y \leftarrow 1$
Tant que $(x > 0)$ **faire**
    $y \leftarrow y \times x$
    $x \leftarrow x - 1$
Fait
Renvoyer y

- Prouver la correction de **Factorielle** grâce à la logique de Hoare, c'est-à-dire montrer que le triplet de Hoare « $\{n \geqslant 0\}$**Factorielle**$(n)\{y = n!\}$ »est vrai.
- Montrer la correction de la logique de Hoare.

Théorème de Scott–Curry

Leçons : 929

Références : HINDLEY, SELDIN, Lambda-Calculus and Combinators (p.65) [HS08] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 700) [LMLBP20]

Prérequis :

- notions de λ-calcul (notamment la β-réduction)
- équivalence entre fonctions μ-récursives et λ-calcul

Notations :

- $[\![n]\!]$ désigne le λ-terme qui représente l'entier n
- les lettres majuscules représentent les λ-termes (sauf pour A et B)
- les lettres grecques représentent les fonctions μ-récursives
- T représente le booléen vrai $T := \lambda xy.x$
- F représente le booléen faux $F := \lambda xy.y$

Introduction :

Le théorème suivant est un théorème qui peut servir à prouver que le problème qui est de savoir si un terme de λ-calcul possède une forme normale est indécidable. Pour cela, on va prouver que des ensembles disjoints ne sont pas séparables par une fonction μ-récursive.

Définition 1 (Récursivement séparable)**.** On dit que deux ensembles $A \subset \mathbb{N}$ et $B \subset \mathbb{N}$ disjoints sont récursivement séparables, s'il existe une fonction μ-récursive φ telle que

$$x \in A \implies \varphi(x) = 0$$

$$x \in B \implies \varphi(x) = 1$$

Définition 2. On dit qu'une fonction $f : \mathbb{N}^p \to \mathbb{N}$ est λ-définissable si et seulement si il existe un terme M de λ-calcul tel que

$$\forall n_1, \dots, n_p \in \mathbb{N}, \quad M[\![n_1]\!][\![n_2]\!] \dots [\![n_p]\!] = [\![f(n_1, \dots, n_p)]\!]$$

On dira que M représente f.

Théorème 1 (Scott–Curry)**.** Aucune paire (A, B) d'ensembles non vides disjoints de λ-termes clos par β-équivalence n'est récursivement séparable.

On veut donc définir "récursivement séparable" pour les λ-termes. Pour cela, on va avoir recours au codage de Gödel $gd(X)$ pour X un λ-terme.

La fonction

$$gd : \Lambda \to \mathbb{N}$$

doit être injective (avec Λ l'ensemble des λ-termes)

Ainsi on peut poser la définition suivante :

Définition 3. On dit que deux ensembles A et B de λ-termes sont récursivement séparables si les ensembles

$$\mathcal{A} = \{gd(X), X \in A\} \text{ et } \mathcal{B} = \{gd(X), X \in B\}$$

sont récursivement séparables.

Démonstration du théorème. Soit A et B deux ensembles non vides de λ-termes clos par β-équivalence.

Par l'absurde, supposons qu'il existe une fonction μ-récursive φ qui sépare les ensembles $\mathcal{A}$ et $\mathcal{B}$. On note M le λ-terme qui représente la fonction φ.

On va poser les deux fonctions suivantes :

$$\gamma : \begin{cases} \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ (gd(X), gd(Y)) & \mapsto & gd(XY) \end{cases}$$

$$\nu : \begin{cases} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & gd([\![n]\!]) \end{cases}$$

Ces deux fonctions peuvent être trouvées μ-récursives. [1]

On note G la représentation de γ et N la représentation de ν.

On prend $X \in A$ un λ-terme de A et $Y \in B$ un λ-terme de B.

On pose le λ-terme suivant

$$H := \lambda x.((\mathsf{is_zero}\ M\ (G\ x\ (N\ x)))\ Y\ X)$$

On notera

$$[Z] := [\![gd(Z)]\!]$$

On veut montrer une absurdité en cherchant dans quel ensemble (A ou B) le terme $J := H\ [H]$ se trouve

$$\begin{aligned} J &\to_\beta ((\mathsf{is_zero}\ M\ (G\ [H]\ (N\ [H])))\ Y\ X) \\ &\to_\beta ((\mathsf{is_zero}\ M\ (G\ [H]\ [[H]]))\ Y\ X) \\ &\to_\beta ((\mathsf{is_zero}\ M\ [H\ [H]])\ Y\ X) \\ &\to_\beta ((\mathsf{is_zero}\ M\ [J])\ YX) \\ &\to_\beta ((\mathsf{is_zero}\ M\ [\![gd(J)]\!])\ Y\ X) \end{aligned}$$

On a utilisé les résultats suivants

$$\begin{aligned} N\ [H] &= N\ [\![gd(H)]\!] \\ &= [\![\nu(gd(H))]\!] \\ &= [\![gd([\![gd(H)]\!])]\!] \\ &= [[H]] \\ G\ [W]\ [Z] &= [\![\gamma(gd(W), gd(Z))]\!] \\ &= [\![gd(W\ Z)]\!] \\ &= [W\ Z] \end{aligned}$$

On peut maintenant faire une disjonction de cas sur la valeur de $\varphi(gd(J))$:

1. je dis "peuvent être" car cela dépend du codage de gd, donc si on numérote les λ-termes par tailles croissantes de termes et en ajoutant des variables différentes au fur et à mesure. Ainsi on peut retrouver pour chaque n le terme correspondant puis la concaténation de deux termes et la représentation des entiers (de Barendregt ou de Church par exemple) sont bien calculables. Donc on a bien des fonctions μ-récursives.

— Si $\varphi(gd(J)) = 0$, alors on a $J \in A$ par définition de φ et on a aussi

$$(\mathsf{is_zero}\ M\ [\![gd(J)]\!]) \to_\beta T$$

De ce fait,

$$J \to_\beta T\ Y\ X \to_\beta Y \in B\ ^{2}$$

Or B est clos par β-réduction donc $J \in B$ (contradiction avec le fait que $J \in A$)

— Si $\varphi(gd(J)) > 0$, alors on a $J \notin A$ par définition de φ et on a aussi

$$(\mathsf{is_zero}\ M\ [\![gd(J)]\!]) \to_\beta F$$

De ce fait,

$$J \to_\beta F\ Y\ X \to_\beta X \in A\ ^{3}$$

Or A est clos par β-réduction donc $J \in A$ (contradiction avec le fait que $J \notin A$)

Ainsi on a une contradiction, donc la fonction φ n'existe pas et l'on ne peut pas séparer récursivement les ensembles A et B □

Remarques :

On peut poser A l'ensemble des termes clos qui possèdent une forme normale et B l'ensemble des termes clos qui ne possèdent pas de forme normale. Ces ensembles sont bien disjoints et clos par β-réduction, on peut donc appliquer le théorème de Scott–Curry qui nous dit qu'il n'existe pas de fonction μ-récursive qui sépare ces deux ensembles.

Ainsi le probleme de terminaison (de la β-réduction)

TERMINAISON { entrée : un terme clos X de λ-calcul ; sortie : oui si X possède une forme normale, non sinon

est indécidable.

Cette preuve finalement ressemble beaucoup à la preuve de l'indécidabilité du problème de l'arrêt pour les machines de Turing, on crée une machine/un λ-terme qui est paradoxal(e).

Astuces de l'agrégatif :

Je mets dans le plan la définition de récursivement séparable (la première en gris), puis au cours du développement, je définis cette notion pour les λ-termes. Quant à la définition de λ-définissable, elle serait aussi dans mon plan avant le théorème d'équivalence avec les fonctions μ-récursives.

Pendant mon développement, je mettais les calculs de $N\ [H]$ et $G\ [W]\ [Z]$ en les intercalant avec la β-réduction de J, je changeais de couleur au tableau pour bien faire comprendre la continuité de la β-réduction de J.

Questions possibles :

- Montrer que l'ensemble des termes clos qui possèdent une forme normale et l'ensemble des termes clos qui ne possèdent pas de forme normale sont tous les deux non vides.
- Où utilise-t-on que A et B sont non vides ?
- Pourquoi l'ensemble A des termes clos qui possèdent une forme normale et l'ensemble B des termes clos qui ne possèdent pas de forme normale sont non vides ?

2. car dès le début on avait pris $X \in A$ et $Y \in B$
3. car dès le début on avait pris $X \in A$ et $Y \in B$

Caractérisation de PREMIER pour l'analyse $LL(1)$

LEÇONS : 923

RÉFÉRENCES : LEGENDRE, SCHWARZENTRUBER, *Compilation : analyse lexicale et syntaxique* (p.63) [LS15] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 783) [LMLBP20]

Notations :

- $G = (\Sigma, \mathcal{N}, \mathcal{T}, S, \mathcal{R})$ désigne une grammaire où Σ est l'alphabet utilisé, $\mathcal{N}$ est l'ensemble des non-terminaux, $\mathcal{T}$ l'ensemble des terminaux, S l'axiome de G et $\mathcal{R}$ est l'ensemble des règles de production.
- les minuscules seront utilisées pour les terminaux et les majuscules pour les non-terminaux
- $\vec{\alpha}$ désigne une concaténation d'éléments de $\mathcal{N}$ et $\mathcal{T}$
- $\to^k$ désigne une dérivation de longueur k

Introduction :

On va prouver un théorème qui permet de donner une caractérisation de la fonction PREMIER et grâce à cette caractérisation, on pourra donner un algorithme de saturation qui calcule cette fonction PREMIER. Cette fonction est un outil clé dans l'analyse LL(1), analyse syntaxique descendante durant la compilation d'un programme.

Définition 1. (PREMIER) Pour $\vec{\alpha} \in (\mathcal{N} \cup \mathcal{T})^*$, on pose

$$\text{PREMIER}(\vec{\alpha}) = \begin{cases} \{a, \vec{\alpha} \to^* a\vec{\beta}\} & \text{si } \vec{\alpha} \not\to^* \varepsilon \\ \{a, \vec{\alpha} \to^* a\vec{\beta}\} \cup \{\bowtie\} & \text{si } \vec{\alpha} \to^* \varepsilon \end{cases}$$

On peut voir PREMIER comme une partie de $(\mathcal{N} \cup \mathcal{T})^* \times (\mathcal{T} \cup \bowtie)$
Si $\text{PREMIER}(\vec{\alpha}) = \{a, +, \bowtie\}$, on écrit alors

$$\text{PREMIER} = \{(\vec{\alpha}, a), (\vec{\alpha}, +), (\vec{\alpha}, \bowtie)\}$$

Théorème 1. La fonction PREMIER est la plus petite partie P de $(\mathcal{N} \cup \mathcal{T})^* \times (\mathcal{T} \cup \bowtie)$ telle que

(i) $a \in P(a)$
(ii) $\bowtie \in P(\varepsilon)$
(iii) si $N \to \alpha_1\alpha_2 \dots \alpha_n$, alors $P(\alpha_1 \dots \alpha_n) \subset P(N)$
(iv) si $N \to \varepsilon$, alors $\bowtie \in P(N)$
(v) si $\bowtie \notin P(\alpha_1)$, alors $P(\alpha_1) \subset P(\alpha_1 \dots \alpha_n)$
(vi) si $\bowtie \in P(\alpha_1)$, alors $(P(\alpha_1) \setminus \{\bowtie\}) \cup P(\alpha_2) \subset P(\alpha_1 \dots \alpha_n)$

Démonstration. On procède par double inclusion pour prouver que $P = \text{PREMIER}$
$\boxed{\subset}$ inclusion simple puisque PREMIER vérifie les 6 propriétés du théorème et que P est la plus petite partie qui vérifie ses 6 propriétés.

(i) Comme $a \to^0 a$, on a $a \in \textsc{Premier}(a)$

(ii) Comme $\varepsilon \to^0 \varepsilon$, on est dans le deuxième cas de la définition de Premier et ainsi

$$\bowtie \in \textsc{Premier}(\varepsilon)$$

(iii) Supposons que $N \to \alpha_1\alpha_2 \dots \alpha_n$. Soit $a \in \textsc{Premier}(\alpha_1 \dots \alpha_n)$, ainsi $\alpha_1 \dots \alpha_n \to^* a\vec{\beta}$, ainsi par hypothèse $N \to^* a\vec{\beta}$, ce qui permet de conclure $a \in \textsc{Premier}(N)$

(iv) Supposons que $N \to \varepsilon$. On est dans le deuxième cas de la définition de Premier et ainsi

$$\textsc{Premier}(\varepsilon) = \{\bowtie\} \subset\subset P(N)$$

(v) Supposons que $\bowtie \notin \textsc{Premier}(\alpha_1)$. Si $a \in \textsc{Premier}(\alpha_1)$, alors $\alpha_1 \to^* a\vec{\beta}$. Ainsi

$$\alpha_1\alpha_2 \dots \alpha_n \to^* a\vec{\beta}\alpha_2 \dots \alpha_n$$

Donc $a \in \textsc{Premier}(\alpha_1 \dots \alpha_n)$

(vi) Supposons que $\bowtie \in \textsc{Premier}(\alpha_1)$. Si $a \in \textsc{Premier}(\alpha_1) \setminus \{\bowtie\}$, alors $\alpha_1 \to^* a\vec{\beta}$. Ainsi

$$a \in \textsc{Premier}(\alpha_1 \dots \alpha_n)$$ [1]

Si $a \in \textsc{Premier}(\alpha_2 \dots \alpha_n)$, et comme $\alpha_1 \to^* \varepsilon$ [2], alors

$$\alpha_1\alpha_2 \dots \alpha_n \to^* \varepsilon\alpha_2 \dots \alpha_n$$

Donc $a \in \textsc{Premier}(\alpha_1 \dots \alpha_n)$

$\boxed{\supset}$ On veut montrer que $\textsc{Premier} \subset P$
On va établir ce résultat par récurrence forte sur la longueur de la dérivation

$$HR_n : \begin{array}{ll} \text{“} & \text{si } \vec{\alpha} \to^n a\vec{\beta} \text{ alors } a \in P(\vec{\alpha}) \\ \text{et} & \text{si } \vec{\alpha} \to^n \varepsilon \text{ alors } \bowtie \in P(\vec{\alpha}) \text{ ”} \end{array}$$

Initialisation :

- Si $\vec{\alpha} \to^0 a\vec{\beta}$, alors $\vec{\alpha} \in \mathcal{T}$ et $\vec{\alpha} = a$. D'où

$$a \in P(\vec{\alpha}) \text{ par (i)}$$

- Si $\vec{\alpha} \to^0 \varepsilon$, alors $\vec{\alpha} = \varepsilon$. D'où

$$\bowtie \in P(\vec{\alpha}) \text{ par (ii)}$$

Hérédité : Soit $n \in \mathbb{N}^*$. Supposons que HR_l soit vraie pour tout $l < n$, montrons HR_n.

- Si $\vec{\alpha} \to^n a\vec{\beta}$, on veut montrer que $a \in P(\vec{\alpha})$
  - ☞ Si le premier caractère de $\vec{\alpha}$ est un terminal, on a forcément $\vec{\alpha}[1] = a$. D'où

$$a \underbrace{\in}_{\text{(i)}} P(a) \underbrace{\subset}_{\text{(v)}} P(\vec{\alpha})$$

  - ☞ Si le premier caractère de $\vec{\alpha}$ est un non-terminal, notons $N := \vec{\alpha}[1]$ et $\vec{\gamma}$ tel que $\vec{\alpha} = N\vec{\gamma}$.

1. pour les mêmes raisons que (v)
2. car $\bowtie \in \textsc{Premier}(\alpha_1)$

✪ Si $N \to^j \varepsilon$, on a $j < n$ [3] et

$$N\vec{\gamma} \to^j \vec{\gamma} \to^{n-j} a\vec{\beta}$$

Donc $\bowtie \in P(N)$ par HR_j et $a \in P(\vec{\gamma})$ par HR_{n-j}. Ainsi

$$a \underbrace{\in}_{HR_{n-j}} P(\vec{\gamma}) \underbrace{\subset}_{\text{(vi)}} P(N\vec{\gamma}) = P(\vec{\alpha})$$

✪ Sinon, on a $N \to x_1 \dots x_k$ avec un des (x_i) qui produit la lettre a. Soit i l'indice minimale tel que $x_i \to^{<n} a$. [4] Ainsi, pour tout $j < i$, $x_j \to^{<n} \varepsilon$. Par $HR_{<n}$, on a $\bowtie \in P(x_j)$ pour tout $j < i$ et $a \in P(x_i)$

$$N\vec{\gamma} \to^{<n} x_i x_{i+1} \dots x_k \vec{\gamma} \to^{<n} a\vec{\beta}$$

$$a \underbrace{\in}_{HR_{<n}} P(x_i) \underbrace{\subset}_{\text{(v) ou (vi)}} P(x_i \dots x_k) \underbrace{\subset}_{\text{(vi)}} P(x_{i-1} \dots x_k) \underbrace{\subset}_{\text{(vi)}} \dots \underbrace{\subset}_{\text{(vi)}} P(x_1 \dots x_k)$$

$$P(x_1 \dots x_k) \underbrace{\subset}_{\text{(iv)}} P(N) \underbrace{\subset}_{\text{(v) ou (vi)}} P(N\vec{\gamma}) = P(\vec{\alpha})$$

- Si $\vec{\alpha} \to^n \varepsilon$, on veut montrer que $\bowtie \in P(\vec{\alpha})$.
  On est forcément dans le cas où $\vec{\alpha}$ commence par un non-terminal [5] que l'on continue d'appeler N et $\vec{\alpha} = N\vec{\gamma}$

  $$N\vec{\gamma} \to x_1 \dots x_k \vec{\gamma} \to^{n-1} \varepsilon$$

  Ainsi $x_1 \dots x_n \to^{<n} \varepsilon$, d'où par $HR_{<n}$, on a

  $$\bowtie \in P(x_1 \dots x_k) \underbrace{\subset}_{\text{(iii)}} P(N)$$

  Or $\vec{\gamma} \to^{<n} \varepsilon$, d'où par $HR_{<n}$, on a

  $$\bowtie \in P(\vec{\gamma}) \underbrace{\subset}_{\text{(vi)}} P(N\vec{\gamma}) = P(\vec{\alpha})$$

Conclusion : On a HR_n pour tout $n \in \mathbb{N}$
Donc ainsi Premier $\subset P$.
Ce qui achève la preuve du théorème

□

Remarques :
Ce théorème permet de donner un algorithme par saturation pour calculer Premier.

Astuces de l'agrégatif :
Je ne fais pas le cas $\vec{\alpha} \to^n \varepsilon$ pendant le développement car il se traite de manière similaire. J'essaye de bien expliquer les cas, en faisant bien référence aux règles à chaque fois que je les utilise.
Je prononce "noeud papillon" pour le symbole $\bowtie$ lors du développement.

3. car il faut que $N\vec{\gamma} \to^n a\vec{\beta}$
4. notation pour dire que la dérivation a strictement moins de n étapes
5. car si on commençait avec un terminal a, on n'engendrerait pas le mot vide à la fin de la dérivation

L'algorithme suivant n'est pas à écrire dans le développement mais est essentiel à comprendre pour savoir à quoi ce théorème peut bien servir. C'est donc cet algorithme qui est utilisé en pratique pour calculer PREMIER.

Algorithme 1 Calcul_PREMIER

Procédure Calcul_PREMIER($\vec{\alpha}$)
  Pour $a \in \mathcal{T}$ **faire**
    PREMIER(a) $\leftarrow \{a\}$
  Fin Pour
  PREMIER(ε) $\leftarrow \{\bowtie\}$
  Pour $N \to \varepsilon \in \mathcal{R}$ **faire**
    PREMIER(N) $\leftarrow \{\bowtie\}$
  Fin Pour
  Tant que (PREMIER est modifié) **faire**
    PREMIER(N) $\leftarrow$ PREMIER(N) $\cup \bigcup_{N \to \alpha_1 \dots \alpha_n}$ PREMIER($\alpha_1 \dots \alpha_n$)
    Si ($\bowtie \notin$ PREMIER(α_1)) **alors**
      PREMIER($\alpha_1 \dots \alpha_n$) $\leftarrow$ PREMIER($\alpha_1 \dots \alpha_n$) $\cup$ PREMIER(α_1)
    Fin Si
    Si ($\bowtie \in$ PREMIER(α_1)) **alors**
      PREMIER($\alpha_1 \dots \alpha_n$) $\leftarrow$ PREMIER($\alpha_1 \dots \alpha_n$) $\cup$ (PREMIER(α_1) $\setminus \{\bowtie\}$) $\cup$ PREMIER($\alpha_2 \dots \alpha_n$)
    Fin Si
  Fait
Fin

Questions possibles :

- Calculer la fonction PREMIER pour la grammaire suivante $G = (\Sigma, \mathcal{N}, \mathcal{T}, S, \mathcal{R})$ où $\Sigma = \{a, b, c, d\}$, $\mathcal{N} = \{S, A, B, C\}$, $\mathcal{T} = \Sigma$ et $\mathcal{R}$ est décrit par

$$S \to AB \mid Ca$$
$$A \to aAb \mid \varepsilon$$
$$B \to bB \mid b$$
$$C \to cC \mid d.$$

- Donner la table d'analyse syntaxique de la grammaire précédente.
- Donner une grammaire qui n'est pas LL(1).
- Calculer la fonction SUIVANT pour la grammaire suivante $G = (\Sigma, \mathcal{N}, \mathcal{T}, S, \mathcal{R})$ où $\Sigma = \{a, b\}$, $\mathcal{N} = \{S\}$, $\mathcal{T} = \Sigma$ et $\mathcal{R}$ est décrit par

$$S \to \varepsilon \mid aSb.$$

Indécidabilité de la satisfiabilité d'une requête

Leçons : 914 ; 932

Références : ABITEBOUL–HULL–VIANU, *Foundations of Database* (p.123) [AHV95] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 817) [LMLBP20]

Notations :

- pour $u_{i_1} \dots u_{i_n}$, on note $u^{(k)}$ pour $u_{i_1} \dots u_{i_k}$ avec $k \in [\![1, n]\!]$
- pour $v_{i_1} \dots v_{i_n}$, on note $v^{(k)}$ pour $v_{i_1} \dots v_{i_k}$ avec $k \in [\![1, n]\!]$

Introduction :

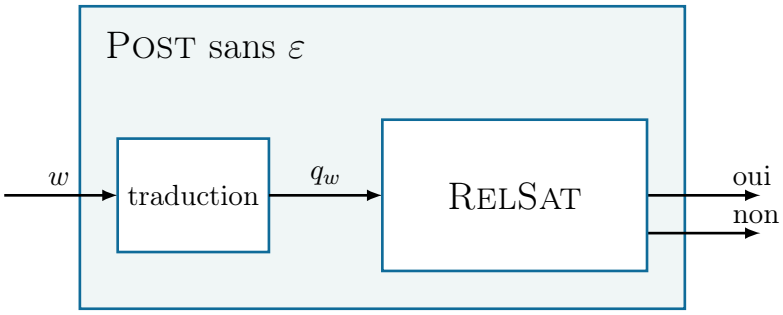
On veut montrer que le problème qui est de savoir si une requête du calcul relationnel est satisfiable est un problème indécidable. On va pour le prouver montrer une réduction du problème Post à RelSat.

Théorème 1. Le problème

RelSat $\begin{cases} \text{entrée :} & \text{une requête } q \text{ du calcul relationnel} \\ \text{sortie :} & \text{oui si il existe une base de donnée } \mathcal{I} \text{ telle que } q(\mathcal{I}) \neq \emptyset, \text{ non sinon} \end{cases}$

est indécidable.

Démonstration. On va réduire le problème Post sans ε [1] à RelSat.



Soit w une instance de Post, c'est à dire un nombre fini de tuiles $\boxed{\begin{matrix} u_1 \\ v_1 \end{matrix}}, \dots, \boxed{\begin{matrix} u_N \\ v_N \end{matrix}}$ sur l'alphabet $\Sigma = \{a, b\}$.

On prend le schéma de base de données suivant

$$\mathcal{R} = \{\text{Enc}(pos1, pos2, mot, u, v), \text{Sync}(debut_u, debut_v)\}$$

Je note Enc pour Encoder et Sync pour Synchroniser

Les colonnes $pos1$ et $pos2$ servent à mettre un ordre sur les tuples. Pour une instance positive de Post, on écrira le mot qui figure en haut et en bas d'une concaténation de tuiles valide dans la colonne mot. La colonne u (respectivement v) sert à donner l'indice de la tuile du haut (resp. du bas) à laquelle correspond la lettre qui est dans la colonne mot. (voir les exemples de remplissage du tableau plus bas)

1. Post sans ε $\begin{cases} \text{entrée :} & \text{des tuiles du problème de Post sans tuile contenant des } \varepsilon \\ \text{sortie :} & \text{oui si on peut trouver une suite de tuiles ayant le même mot en haut et en bas, non sinon} \end{cases}$
(pour la réduction du problème de Post original voir l'appendice ici).

On pose la requête suivante

$$q_w = \{\langle\rangle, \varphi_w\}$$

où φ_w est la conjonction des 5 formules suivantes :

— φ_{ENC} qui traduit le fait que
  - les éléments de $pos1$ sont disjoints
  - les colonnes $pos1, pos2$ forment un cycle de longueur > 1
  - $pos1$ contient le symbole \$

  Cette formule sert à forcer les tuples de la relation ENC à être dans un certain ordre [2] et donc de retrouver cet ordre même si une relation est un ensemble de tuples (donc sans ordre a priori). C'est pour ça que l'on a besoin de deux colonnes. La première colonne est une clé pour retrouver le début de chaque tuile (d'où la nécessité d'avoir des éléments distincts). Le symbole \$ est un symbole spécial pour marquer le début.

— φ_{SYNC} qui traduit le fait que les éléments de $debut_u$ sont disjoints et les éléments de $debut_v$ sont disjoints

  On a les indices de début de chaque tuile, donc il faut que les éléments soient distincts.

— φ_u qui traduit le fait que pour tout $x \in debut_u$, il existe $i \in [\![1, N]\!]$ avec $u_i = z_1 \dots z_k$ et $x_1, \dots, x_{k+1}$ avec $x = x_1$ tels que

$$\langle x_1, x_2, z_1, i, * \rangle \in \text{ENC}$$

$$\langle x_2, x_3, z_2, i, * \rangle \in \text{ENC}$$

$$\vdots$$

$$\langle x_k, x_{k+1}, z_k, i, * \rangle \in \text{ENC}$$

  avec $x_1, x_{k+1} \in debut_u$ et $x_2, \dots, x_k \notin debut_u$
  (où $*$ peut être choisi indifféremment)

  Cette formule permet de dire que pour chaque indice de début de tuile dans SYNC, on a une tuile $\boxed{\begin{array}{|c|}\hline u_i \\ \hline v_i \\ \hline \end{array}}$ et que (dans l'ordre imposé par la formule φ_{ENC}) on a bien une succession de tuples qui correspond au mot u_i de la tuile $\boxed{\begin{array}{|c|}\hline u_i \\ \hline v_i \\ \hline \end{array}}$ puis que les lettres du mot correspondent bien à u_i entre les indices $x = x_1$ et x_k. De plus, on oblige à ne pas avoir de début de tuile pendant les indices intermédiaires, et que l'indice suivant (x_{k+1}) soit un début de tuile.

— φ_v similaire à φ_u
  φ_v qui traduit le fait que pour tout $x \in debut_v$, il existe $i \in [\![1, N]\!]$ avec $v_i = z_1 \dots z_k$ et $x_1, \dots, x_{k+1}$ avec $x = x_1$ tels que

$$\langle x_1, x_2, z_1, *, i \rangle \in \text{ENC}$$

$$\langle x_2, x_3, z_2, *, i \rangle \in \text{ENC}$$

$$\vdots$$

$$\langle x_k, x_{k+1}, z_k, *, i \rangle \in \text{ENC}$$

  avec $x_1, x_{k+1} \in debut_v$ et $x_2, \dots, x_k \notin debut_v$
  (où $*$ peut être choisi indifféremment)

2. l'ordre que l'on donne dans les tables que l'on dessine dans le développement, c'est en fait l'ordre dans lequel on lit le mot qui est en haut et en bas d'une concaténation valide de tuiles du problème POST

Cette formule permet de dire que pour chaque indice de début de tuile dans SYNC, on a une tuile $\boxed{\begin{array}{|c|}\hline u_i \\ \hline v_i \\ \hline \end{array}}$ et que (dans l'ordre imposé par la formule φ_{ENC}) on a bien une succession de tuples qui correspond au mot v_i de la tuile $\boxed{\begin{array}{|c|}\hline u_i \\ \hline v_i \\ \hline \end{array}}$ puis que les lettres du mot correspondent bien à v_i entre les indices $x = x_1$ et x_k. De plus, on oblige à ne pas avoir de début de tuile pendant les indices intermédiaires, et que l'indice suivant (x_{k+1}) soit un début de tuile.

— $\varphi_{\text{SYNC_}u_v}$ définie par

$$\begin{aligned}
&\text{SYNC}(\$, \$) \\
&\wedge \forall x \forall y \left(\text{SYNC}(x, y) \to \bigvee_{i=1}^{N} \exists t_1 t_2 t_3 s_1 s_2 s_3 \text{ENC}(x, t_1, t_2, i, t_3) \wedge \text{ENC}(y, s_1, s_2 s_3, i) \right) \\
&\wedge \forall x \forall y \left(\text{SYNC}(x, y) \ \wedge \ \neg(x = \max(\mathit{debut_u})) \ \wedge \ \neg(y = \max(\mathit{debut_v})) \to \text{SYNC}(x', y') \right)
\end{aligned}$$

avec $x' = \min_{a \in \mathit{debut_u}} a > x$ et $y' = \min_{a \in \mathit{debut_v}} a > y$

Cette formule force à commencer par une première tuile (par le fait que SYNC($\$, \$$)), puis à synchroniser le reste des tuiles, c'est-à-dire que après la tuile $\boxed{\begin{array}{|c|}\hline u_{i_1} \\ \hline v_{i_1} \\ \hline \end{array}}$, on accède à la tuile suivante (3ème sous-formule), et que c'est une tuile licite (car il faut que ce soit une tuile $\boxed{\begin{array}{|c|}\hline u_i \\ \hline v_i \\ \hline \end{array}}$ où l'indice du haut est le même que l'indice du bas et non une tuile $\boxed{\begin{array}{|c|}\hline u_3 \\ \hline v_4 \\ \hline \end{array}}$ qui ne serait pas licite) (par la 2ème sous-formule).

Il faut montrer que

$$\boxed{q_w \text{ est satisfiable SSI } w \text{ est une instance positive de POST}}$$

$\boxed{\Longrightarrow}$ Soit une instance $\mathcal{I}$ telle que $\mathcal{I} \vDash q_w$.
On note $r = |\text{SYNC}|$ (ce sera le nombre de tuiles)
On veut montrer par récurrence sur $k \in [\![1, r]\!]$ que

$$HR_k : \begin{cases} u^{(k)} = mot[1 \dots |u^{(k)}|] \\ v^{(k)} = mot[1 \dots |v^{(k)}|] \end{cases}$$

On prouve cela grâce aux formules de φ_w qui est satisfiable [3].

Ainsi, on peut conclure que $u^{(r)} = v^{(r)}$ et donc que w est une instance positive de POST.

$\boxed{\Longleftarrow}$ w est une instance positive de POST, donc il existe $i_1, \dots, i_r$ tels que

$$m = u_{i_1} \dots u_{i_r} = v_{i_1} \dots v_{i_r}$$

On construit alors la table ENC et SYNC comme ci-dessous

3. les arguments sont en fait les explications en gris sous chaque formule

ENC

$pos1$	$pos2$	mot	u	v
\$	1	m_1	i_1	i_1
1	2	m_2	i_1	i_1
⋮	⋮	⋮	i_1	i_1
$\|v^{(1)}\|$	$\|v^{(1)}\|+1$	$m_{\|v^{(1)}\|}$	i_1	i_2
⋮	⋮	⋮	i_1	⋮
⋮	⋮	⋮	i_1	⋮
$\|u^{(1)}\|$	$\|u^{(1)}\|+1$	$m_{\|u^{(1)}\|}$	i_2	⋮
⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮
$\|m\|-2$	$\|m\|-1$	⋮	⋮	⋮
$\|m\|-1$	\$	$m_{\|m\|}$	i_r	i_r

SYNC

$debut_u$	$debut_v$
\$	\$
$\|u^{(1)}\|$	$\|v^{(1)}\|$
$\|u^{(2)}\|$	$\|v^{(2)}\|$
⋮	⋮
⋮	⋮
$\|u^{(r-1)}\|$	$\|v^{(r-1)}\|$

Cette instance de base de données $\mathcal{I}$ (sur le schéma de base de données $\mathcal{R}$) satisfait la requête q_w [4]. Il suffit de vérifier qu'elle vérifie chaque formule que l'on a énoncé.

□

Remarques :

Il existe d'autres problèmes indécidables sur les bases de données comme :

RelEqu :
- entrée : deux requêtes q et q' du calcul relationnel
- sortie : oui si q et q' sont sémantiquement équivalentes, non sinon

RelSure :
- entrée : une requête q du calcul relationnel
- sortie : oui si q est sûre, non sinon

Pour montrer l'indécidabilité de RELEQU, il suffit de réduire co-RELSAT à RELEQU. En effet, une requête est insatisfiable si et seulement si elle est équivalente à la requête vide.

Astuces de l'agrégatif :

- Ce développement est très long, je ne pense pas qu'il soit faisable d'écrire toutes les formules et de prouver la réduction tout en faisant comprendre au jury ce que l'on est en train de faire. J'ai fait le choix d'essayer de faire comprendre au jury la réduction en donnant le sens des formules.
- J'écris la base de données à droite du tableau dès que j'introduis ENC et SYNC en expliquant comment les remplir, pour que le sens des formules soit compréhensible quand je les énonce ensuite. Je dis que le but des formules est que la seule façon de remplir la base de données soit celle que j'ai présenté.
- Lors du développement je dis juste POST, en effet ce n'est qu'une variante de POST.
- Je mets les formules ci-dessous, il peut être intéressant de donner une formule d'unicité sur la formule φ_{ENC} pour convaincre le jury que l'on maitrise aussi l'écriture rigoureuse des formules.
- On a prouvé ici que ce problème n'est pas dans R, mais il est quand même dans RE. En effet, on peut dénombrer les bases de données qui sont des ensembles finis de tuples sur un domaine dénombrable.

4. i.e. $q_w(\mathcal{I}) \neq \emptyset$

— φ_{ENC}

$$\begin{aligned}
&\exists t\Big(\psi(\$,t)\wedge\neg(t=\$)\Big)\wedge\exists t\Big(\psi(t,\$)\wedge\neg(t=\$)\Big) && \text{existence \$}\\
&\wedge\forall x\forall y\exists z\Big(\psi(x,y)\to\psi(y,z)\Big) && \text{cycle}\\
&\wedge\forall x\forall y\exists z\Big(\psi(y,x)\to\psi(z,y)\Big) && \text{cycle}\\
&\wedge\forall x\forall y\forall z\Big((\psi(x,y)\wedge\psi(x,z))\to(y=z)\Big) && \text{unicité}\\
&\wedge\forall x t_1t_2t_3t_4s_1s_2s_3s_4\Big((\text{ENC}(x,t_1,t_2,t_3,t_4)\\
&\qquad\wedge\text{ENC}(x,s_1,s_2,s_3,s_4))\to(t_1=s_1\\
&\qquad\qquad\wedge t_2=s_2\\
&\qquad\qquad\wedge t_3=s_3\\
&\qquad\qquad\wedge t_4=s_4)\Big) && \text{unicité } pos1
\end{aligned}$$

avec $\psi(x,y):=\exists z\exists t\exists s\text{ENC}(x,y,z,t,s)$

— φ_{SYNC}

$$\begin{aligned}
&\forall x\forall y\forall z\Big((\text{SYNC}(x,y)\wedge\text{SYNC}(x,z))\to y=z\Big) && \text{unicité } debut_u\\
&\wedge\forall x\forall y\forall z\Big((\text{SYNC}(x,y)\wedge\text{SYNC}(z,y))\to x=z\Big) && \text{unicité } debut_v
\end{aligned}$$

— φ_u

$$\begin{aligned}
\forall x\Big(\exists y\text{SYNC}(x,y)\to\Big(\bigvee_{i=1}^{N}\big(&\exists x_1x_2\dots x_{|u_i|}x_{|u_i|+1}j_1\dots j_{|u_i|}\\
&\big(\bigwedge_{k=1}^{|u_i|}\text{ENC}(x_k,x_{k+1},u_i[k],i,j_k)\big)\\
&\wedge(x=x_1)\wedge(\exists z\text{SYNC}(x_{|u_i|+1},z))\\
&\wedge\bigwedge_{k=2}^{|u_i|}\neg\exists y\text{SYNC}(x_k,y)\big)\big)\Big)
\end{aligned}$$

— φ_v similaire

— $\varphi_{\text{SYNC_u_v}}$ il faut coder $x<y$, pour cela il faut borner le nombre d'intermédiaire entre x et y, on n'a a priori pas de borne, mais on sait que l'indice de début de tuile suivante est forcément à moins de "taille maximum des mots sur les tuiles" de x, donc on peut faire un disjonction sur le nombre d'intermédiaires qui sera donc borné puisqu'on regarde toujours la différence entre x et y sur des tuiles qui se suivent. Pour faire l'égalité avec le maximum, il faut regarder si dans le tableau ENC, le dernier caractère de la tuile possède une $pos2$ égale à \$.

$$x<y:=\neg(x=y)\wedge\bigvee_{k=1}^{\text{borne}}\exists z_1z_2\dots z_k\big(\psi(x,z_1)\wedge\psi(z_1,z_2)\wedge\dots\wedge\psi(z_k,y)\big)$$

$$x=\max(debut_u):=\bigvee_{k=0}^{|u_x|}\exists z_1\dots z_k\big(\psi(x,z_1)\wedge\psi(z_1,z_2)\wedge\dots\wedge\psi(z_k,\$)\big)$$

(Je ne suis pas sûr de ces dernières formules, il faudrait écrire vraiment rigoureusement tout cela pour être vraiment propre, mais je pense que cette idée marche [5]).

Je mets un exemple concret de tables pour $m = aabbbab = u_{i_1}u_{i_2}u_{i_3} = v_{i_1}v_{i_2}v_{i_3}$ avec les tuiles

$$i_1 \begin{array}{|c|}\hline aab \\ \hline a \\ \hline \end{array} ; i_2 \begin{array}{|c|}\hline b \\ \hline abbb \\ \hline \end{array} ; i_3 \begin{array}{|c|}\hline bab \\ \hline ab \\ \hline \end{array}$$

ENC

$pos1$	$pos2$	mot	u	v
\$	1	a	i_1	i_1
1	2	a	i_1	i_2
2	3	b	i_1	i_2
3	4	b	i_2	i_2
4	5	b	i_3	i_2
5	6	a	i_3	i_3
6	\$	b	i_3	i_3

SYNC

$debut_u$	$debut_v$
\$	\$
3	1
4	5

Questions possibles :

- Montrer que le problème de POST sans ε est indécidable.
- Écrire explicitement la récurrence de la question **c)** (i).

5. envoie moi un mail, si tu réussis à écrire ça proprement

3.6 Autres développements

Prolongement de la fonction Zéta de Riemann

(rédigé par Émilie Tezenas)

Leçons : 207 ; 245 ; 265

Références : CONWAY, *Functions of one complex variable* (p.183) [CON95]

Introduction :

La fonction ζ de Riemann est définie facilement sous forme d'une série pour les complexes de partie réelle strictement plus grande que 1. L'objet de ce développement est de montrer que cette fonction se prolonge en fait en une fonction méromorphe sur $\mathbb{C}$, dont l'unique pôle se situe en 1 et est simple. Cette preuve est décrite dans le livre de Conway.

On utilisera pour ce développement les deux lemmes suivants :

Lemme 1. Pour $t \in \mathbb{R}_+^*$,

$$\operatorname{cotan}\left(\frac{it}{2}\right) = \frac{2}{it} - 4it\sum_{n\geq 1}\frac{1}{t^2+4n^2\pi^2}$$

Ce lemme est démontré après le développement. Il repose essentiellement sur le théorème des Résidus, appliqué à un contour bien choisi.

Lemme 2. Pour tout $z \in \{\mathrm{Re}(z) \in]0,1[\}$,

$$\int_0^{+\infty}\frac{1}{t^z(1+t)}\mathrm{d}t = \frac{\pi}{\sin(\pi z)}$$

Ce dernier lemme est démontré dans la preuve de la formule des compléments, dans l'étape 2.

On cherche donc à démontrer le théorème suivant

Théorème 1. ζ admet un prolongement méromorphe à $\mathbb{C}$ admettant un pôle simple en 1.

Démonstration.

Étape 1 : *Relation fonctionnelle avec Gamma*

Soit $x \in]1,+\infty[$. On a vu dans la partie II de la leçon que pour un tel x, la fonction Gamma est bien définie sous sa forme intégrale.
On a $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}\mathrm{d}t$.

Soit maintenant $n \in \mathbb{N}^*$. On a $n^{-x}\Gamma(x) = \int_0^\infty \left(\frac{t}{n}\right)^x \frac{1}{t}e^{-t}\mathrm{d}t$.

Le changement de variable $u = \frac{t}{n}$ donne alors

$$n^{-x}\Gamma(x) = \int_0^\infty u^{x-1}e^{-nu}\mathrm{d}u$$

On somme alors sur les $n \geq 1$, et on intervertit l'intégrale et la somme en appliquant le théorème de Fubini-Tonelli (l'intégrande est positive). On obtient :

$$\zeta(x)\Gamma(x) = \int_0^\infty u^{x-1}\sum_{n\geq 1} e^{-nu}\mathrm{d}u = \int_0^\infty \frac{u^{x-1}}{e^u-1}\mathrm{d}u \tag{3.4}$$

Or, la fonction $z \mapsto \int_0^\infty \frac{u^{z-1}}{e^u-1}\mathrm{d}u$ est holomorphe sur $\mathrm{Re}(z) > 1$.

En effet, pour tout $z \in \mathbb{C}$ tel que $\mathrm{Re}(z) > 1$, il existe $A > \delta > 1$ tel que $A > \mathrm{Re}(z) > \delta > 1$. Alors

$$\left|\frac{u^{z-1}}{e^u-1}\right| = \frac{u^{\mathrm{Re}(z)-1}}{e^u-1} \leq \begin{cases} \frac{u^{A-1}}{e^u-1} & \text{Si } u \geq 1 \\ \frac{u^{\delta-1}}{e^u-1} & \text{Si } 0 < u < 1 \end{cases}$$

Or, ce dernier terme est intégrable sur $\mathbb{R}_+^*$, car d'une part $\frac{u^{\delta-1}}{e^u-1} \underset{u\to 0}{\sim} u^{\delta-2}$ qui est intégrable sur $]0,1[$ puisque $\delta - 2 > 1 - 2 = -1$, et d'autre part $\frac{u^{A-1}}{e^u-1} \underset{u\to\infty}{\sim} u^{A-2}e^{-u}$ qui est intégrable sur $]1,+\infty[$.

Donc l'intégrale à paramètre est holomorphe sur tout domaine de $\mathbb{C}$ de la forme $A > \mathrm{Re}(z) > \delta$, donc sur $\mathrm{Re}(z) > 1$.

Par ailleurs, les fonctions ζ et Γ sont également holomorphes sur ce domaine, donc leur produit l'est aussi.

L'équation (3.4) nous donne alors l'égalité de deux fonctions holomorphes sur un ensemble admettant l'axe $]1,+\infty[$ pour points d'accumulation, donc le théorème de prolongement analytique nous assure que

$$\zeta(z)\Gamma(z) = \int_0^\infty \frac{u^{z-1}}{e^u-1}\mathrm{d}u \qquad \text{pour tout } z \text{ tel que } \mathrm{Re}(z) > 1$$

Étape 2 : *Prolongement à* $0 < \mathrm{Re}(z) < 1$

Le problème à un prolongement immédiat avec la formule obtenue en (3.4) se situe dans l'intégration au voisinage de 0 lorsque z est proche de 1.

On cherche donc à s'affranchir de ce problème en découpant l'intégrale : Pour tout $z \in \mathrm{Re}(z) > 1$

$$\zeta(z)\Gamma(z) = \int_0^\infty \frac{u^{z-1}}{e^u-1}\mathrm{d}u = \int_0^1 \frac{u^{z-1}}{e^u-1}\mathrm{d}u + \int_1^\infty \frac{u^{z-1}}{e^u-1}\mathrm{d}u$$

On va maintenant utiliser le développement limité de l'exponentielle au voisinage de 0 pour écrire

$$\frac{1}{e^u-1} \underset{u\mapsto 0}{=} \frac{1}{u} - \frac{1}{2} + o(1) \tag{3.5}$$

En particulier, cela nous permet d'affirmer que $\frac{1}{e^u-1} - \frac{1}{u}$ est bornée au voisinage de 0.

Ainsi, on écrit

$$\begin{aligned}\int_0^1 \frac{u^{z-1}}{e^u-1}\mathrm{d}u &= \int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u + \int_0^1 u^{z-1}\frac{1}{u}\mathrm{d}u \\ &= \int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u + \frac{1}{z-1}\end{aligned}$$

On a donc finalement

$$\zeta(z)\Gamma(z) = \underbrace{\int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u}_{\text{(a)}} + \underbrace{\frac{1}{z-1}}_{\text{Pôle en 1}} + \underbrace{\int_1^\infty \frac{u^{z-1}}{e^u-1}\mathrm{d}u}_{\text{(b)}} \qquad \text{pour } \mathrm{Re}(z)>1.$$

— (a) : Ce terme est holomorphe sur $\{\mathrm{Re}(z)>0\}$. En effet, pour $z\in\{\mathrm{Re}(z)>0\}$, il existe $\delta>0$ tel que $\delta\leq\mathrm{Re}(z)$. Alors $|u^{z-1}|\left|\frac{1}{e^u-1}-\frac{1}{u}\right|\leq u^{\delta-1}M$ où M est une borne de $\frac{1}{e^u-1}-\frac{1}{u}$ sur $]0,1[$. Cette borne existe bien car on a vu que la fonction était bornée au voisinage de 0, et qu'elle est de plus continue sur $]0,1]$. On peut donc appliquer le théorème d'holomorphie sous le signe intégral, qui nous donne l'holomorphie du terme (a).

— (b) : Ce terme est également holomorphe sur $\{\mathrm{Re}(z)>0\}$. Pour le montrer, on applique le théorème d'holomorphie sous l'intégrale en dominant sur des domaines de $\mathbb{C}$ de la forme $0<\mathrm{Re}(z)\leq A$.

Par prolongement analytique, $\zeta.\Gamma$ est donc méromorphe sur $\mathrm{Re}(z)>0$, avec un pôle simple en 1. De plus, Γ est holomorphe et ne s'annule pas sur $\mathrm{Re}(z)>0$ donc pour tout $z\in\{\mathrm{Re}(z)>0\}$,

$$\zeta(z) = \underbrace{\frac{1}{\Gamma(z)}}_{Holomorphe} \times \underbrace{\left(\int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u + \frac{1}{z-1} + \int_1^\infty \frac{u^{z-1}}{e^u-1}\mathrm{d}u\right)}_{\text{Méromorphe}}$$

.

On a donc prolongé ζ en une fonction méromorphe sur $\mathrm{Re}(z)>0$, avec un pôle simple en 1, de Résidu 1.

Étape 3 : *Prolongement à* $-1<\mathrm{Re}(z)<0$

On réutilise la relation fonctionnelle obtenue à l'étape précédente pour $z\in\{0<\mathrm{Re}(z)<1\}$. On remarque que pour $-1<\mathrm{Re}(z)<1$, la fonction $u\mapsto u^{z-2}$ est intégrable sur $]1,+\infty[$ et que $-\int_1^\infty u^{z-2}\mathrm{d}u = \frac{1}{z-1}$.

On utilise cette remarque dans la relation fonctionnelle : pour $0<\mathrm{Re}(z)<1$, on a

$$\begin{aligned}\zeta(z)\Gamma(z) &= \int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u - \int_1^\infty u^{z-2}\mathrm{d}u + \int_1^\infty \frac{u^{z-1}}{e^u-1}\mathrm{d}u \\ &= \int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}+\frac{1}{2}\right)\mathrm{d}u - \int_0^1 \frac{u^{z-1}}{2}\mathrm{d}u + \int_1^\infty u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u\end{aligned}$$

où on a, pour la dernière égalité, rajouté le terme suivant du développement de $\frac{1}{e^u-1}$ au voisinage de 0.

On développe à un ordre supérieur l'expression (3.5) : $\frac{1}{e^u-1}\underset{u\mapsto 0}{=}\frac{1}{u}-\frac{1}{2}+O(u)$ qui nous permet d'affirmer que

$$u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}+\frac{1}{2}\right)\underset{u\to 0}{\sim} Mu^z$$

qui est intégrable sur $]0,1[$. Ainsi la fonction

$$z \mapsto \int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}+\frac{1}{2}\right)\mathrm{d}u$$

est holomorphe sur le domaine $-1 < \mathrm{Re}(z) < 1$ (Appliquer le théorème d'holomorphie sous l'intégrale en dominant sur un domaine de la forme $-1 < \delta \leq \mathrm{Re}(z) \leq 1$).

Par ailleurs, $\int_0^1 \frac{u^{z-1}}{2}\mathrm{d}u = -\frac{1}{2z}$.

Enfin, la fonction $z \mapsto \int_1^\infty u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u$ est holomorphe sur le domaine $\mathrm{Re}(z) < 1$ (séparer la fraction en deux, et appliquer le théorème d'holomorphie. On domine l'intégrande de la première en majorant simplement u^{z-1} par 1, et la seconde sur des domaines de la forme $Re(z) \leq \delta < 1$).

On obtient donc, pour $-1 < \mathrm{Re}(z) < 1$, et puisque Γ ne s'annule pas sur $\mathbb{C}$:

$$\begin{aligned}
\zeta(z) &= \frac{1}{\Gamma(z)} \times \left(\int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}+\frac{1}{2}\right)\mathrm{d}u - \int_0^1 \frac{u^{z-1}}{2}\mathrm{d}u + \int_1^\infty u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u\right) \\
&= \frac{1}{\Gamma(z)}\int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}+\frac{1}{2}\right)\mathrm{d}u - \frac{1}{2\Gamma(z)z} + \frac{1}{\Gamma(z)}\int_1^\infty u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u \\
&= \underbrace{\frac{1}{\Gamma(z)}\int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}+\frac{1}{2}\right)\mathrm{d}u}_{\text{Holomorphe}} - \underbrace{\frac{1}{2\Gamma(z+1)}}_{\text{Holomorphe car Re}(z+1)>0} + \underbrace{\frac{1}{\Gamma(z)}\int_1^\infty u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u}_{\text{Holomorphe}}
\end{aligned}$$

On a donc prolongé ζ au domaine $-1 < \mathrm{Re}(z) < 0$.

Étape 4 : *Prolongement à* $\mathrm{Re}(z) < -1$

On a obtenu à l'étape précédente la formule suivante pour tout $-1 < \mathrm{Re}(z) < 0$:

$$\zeta(z)\Gamma(z) = \int_0^1 u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}+\frac{1}{2}\right)\mathrm{d}u - \frac{1}{2z} + \int_1^\infty u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}\right)\mathrm{d}u$$

On remarque que pour $-1 < \mathrm{Re}(z) < 0$, $u \mapsto u^{z-1}$ est intégrable sur $]1,+\infty[$, et que $-\frac{1}{2z} = \int_1^\infty \frac{1}{2}u^{z-1}\mathrm{d}u$.

On a alors, en regroupant les termes,

$$\zeta(z)\Gamma(z) = \int_0^\infty u^{z-1}\left(\frac{1}{e^u-1}-\frac{1}{u}+\frac{1}{2}\right)\mathrm{d}u.$$

On remarque que pour tout $u \in \mathbb{R}_+$,

$$\frac{1}{e^u-1}+\frac{1}{2} = \frac{i}{2}\mathrm{cotan}\left(\frac{iu}{2}\right)$$

On utilise ensuite la formule de la cotangente énoncée au lemme 1. On a donc

$$\frac{1}{e^u-1}+\frac{1}{2} = \frac{1}{u}+2u\sum_{n\geq 1}\frac{1}{u^2+4n^2\pi^2}$$

Soit maintenant $x \in]-1,0[$. En combinant l'équation fonctionnelle précédemment obtenue, valable pour de tels x, et le calcul sur la cotangente, on obtient :

$$\zeta(x)\Gamma(x) = \int_0^\infty u^{x-1}\left(2u\sum_{n\geq 1}\frac{1}{u^2+4n^2\pi^2}\right)\mathrm{d}u$$

L'intégrande étant positive, on applique Fubini-Tonnelli, puis on réalise le changement de variable $t = \frac{u}{2n\pi}$, à n fixé :

$$\zeta(x)\Gamma(x) = 2\sum_{n\geq 1}\int_0^\infty \frac{u^x}{u^2+4n^2\pi^2}\mathrm{d}u \overset{F.T}{=} 2\int_0^\infty \frac{t^x}{1+t^2}\mathrm{d}t \times \underbrace{\sum_{n\geq 1}(2n\pi)^{x-1}}_{=(2\pi)^{x-1}\zeta(1-x)}$$

Par ailleurs, le changement de variable $v = t^2$ et le lemme 2 donnent pour l'intégrale restante :

$$\int_0^\infty \frac{t^x}{1+t^2}\mathrm{d}t = \frac{1}{2}\int_0^\infty \frac{v^{\frac{1}{2}(x-1)}}{1+v}\mathrm{d}v = \frac{1}{2}\frac{\pi}{\sin(\frac{\pi}{2}(1-x))}$$

On termine le calcul à l'aide de formules trigonométriques :

$$\frac{1}{2}\frac{\pi}{\sin(\frac{\pi}{2}(1-x))} = \frac{\pi}{\sin(\pi x)}\sin(\frac{\pi}{2}x)$$

Revenons maintenant à ζ. On a obtenu, toujours pour $x \in]-1,0[$,

$$\zeta(x) = \frac{2}{\Gamma(x)}\frac{\pi}{\sin(\pi x)}\sin(\frac{\pi}{2}x)(2\pi)^{x-1}\zeta(1-x)$$

La formule des compléments, valable sur $\mathbb{C}$ privé des entiers, donc sur $]-1,0[$, donne encore $\frac{1}{\Gamma(x)}\frac{\pi}{\sin(\pi x)} = \Gamma(1-x)$.

D'où finalement

$$\zeta(x) = 2\Gamma(1-x)\sin(\frac{\pi}{2}x)(2\pi)^{x-1}\zeta(1-x)$$

Or, $\mathrm{Re}(z) < 0 \Leftrightarrow \mathrm{Re}(1-z) > 1$, et la fonction $z \mapsto 2\Gamma(1-z)\sin(\frac{\pi}{2}z)(2\pi)^{z-1}\zeta(1-z)$ est holomorphe sur $\mathrm{Re}(z) < -1$ (on utilise ici en particulier le fait que ζ est une fonction holomorphe sur $\mathrm{Re}(z) > 1$).

La théorème de prolongement analytique nous permet de conclure, et de prolonger ζ en une fonction holomorphe sur $\mathrm{Re}(z) < 0$.

On a donc bien prolongé ζ en une fonction méromorphe sur $\mathbb{C}$, admettant un unique pôle, en 1, de résidu 1.

□

Démonstration du lemme 1.
Soit $a \in \mathbb{C} \setminus \mathbb{Z}$. On va appliquer le théorème des résidus à la fonction

$$\mathrm{f} : z \mapsto \frac{\pi}{z^2-a^2}\mathrm{cotan}(\pi z)$$

qui est méromorphe de pôles a, $-a$, et tous les entiers, sur le contour rectangulaire ci-après, où n est choisi de façon à ce que le point a se trouve à l'intérieur du contour. En faisant ensuite tendre n vers $+\infty$, on obtiendra le résultat souhaité.

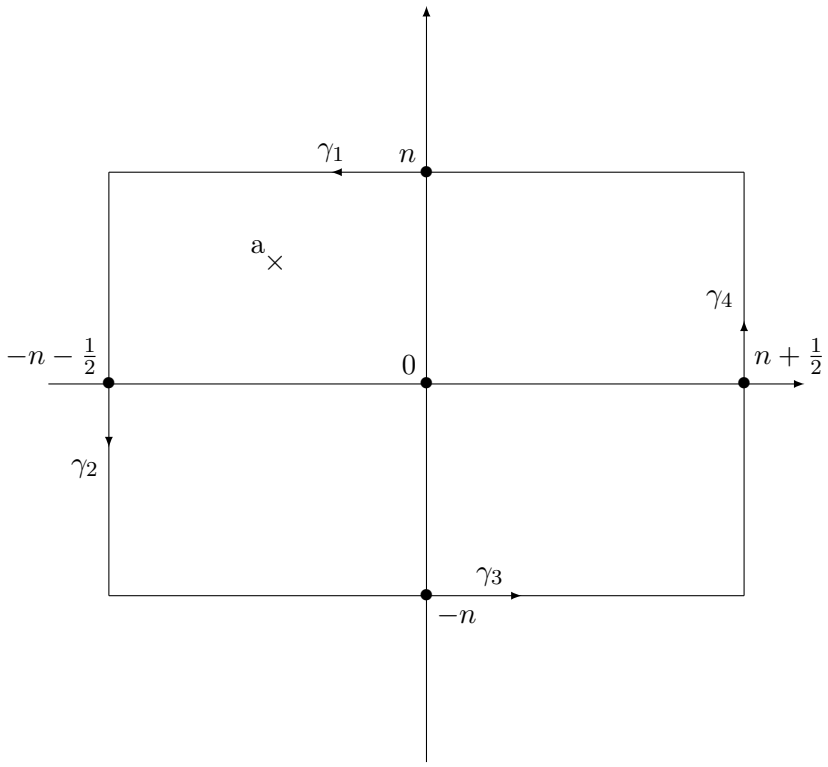


FIGURE 3.1 – Contour d'intégration pour la formule de la cotangente

Ces choix sont motivés par le fait qu'ainsi, le contour englobe plusieurs pôles de la fonction f sans en rencontrer : a, $-a$, et les entiers compris entre $-n$ et n inclus.

Le théorème des Résidus donne alors :

$$\frac{1}{2i\pi}\int_{\gamma_n} f(z)\mathrm{d}z = \mathrm{Res}(f,a) + \mathrm{Res}(f,-a) + \sum_{|k|\leq n} \mathrm{Res}(f,k)$$

On calcule :

— a est un pôle simple de f. Donc $\mathrm{Res}(f,a) = (z-a)f(z)|_{z=a} = \frac{\pi}{2a}\mathrm{cotan}(\pi a)$

— $-a$ est également un pôle simple de f, donc $\mathrm{Res}(f,-a) = -\frac{\pi}{2a}\mathrm{cotan}(-\pi a) = \frac{\pi}{2a}\mathrm{cotan}(\pi a)$

— soit $k \in [\![0,n]\!]$, k est un pôle simple de cotan, car c'est un zéro simple de la fonction sin. Donc $\mathrm{Res}(f,k) = \lim\limits_{z\to k}(z-k)f(z) = \frac{\pi\cos(\pi k)}{k^2-a^2} \lim\limits_{z\to k} \frac{z-n}{\sin(\pi z)}$
Or, $\sin(\pi z) = \sin(\pi(z-n)+\pi n) = (-1)^n\sin(\pi(z-n))$.
Donc $\lim\limits_{z\to k} \frac{z-n}{\sin(\pi z)} = (-1)^n \lim\limits_{z\to k} \frac{z-n}{\sin(\pi(z-n))} = \frac{(-1)^n}{\pi}$.
D'où finalement $\mathrm{Res}(f,k) = \frac{1}{k^2-a^2} = \mathrm{Res}(f,-k)$. On va donc, dans la somme, isoler le terme $k=0$ et regrouper les opposés.

On a alors obtenu

$$\frac{1}{2i\pi}\int_{\gamma_n} f(z)\mathrm{d}z = \frac{\pi}{a}\mathrm{cotan}(\pi a) - \frac{1}{a^2} + \sum_{k=1}^{n} \frac{2}{k^2-a^2}$$

Étape 1 : *Majoration de cotan sur le contour*

Soit $z \in \mathbb{C}$. On note $z = x+iy$, avec $x, y \in \mathbb{R}$.

Alors, grâce à la formule de Moivre, on a $\cos(z) = \frac{e^{iz}+e^{-iz}}{2} = \frac{\cos(x)\left(e^{-y}+e^{y}\right)+i\sin(x)\left(e^{-y}-e^{y}\right)}{2} = \cos(x)\cosh(y) + i\sin(x)\sinh(-y)$. On passe au module pour obtenir $|\cos(z)|^2 = \cos(x)^2 + \sinh(y)^2$

De même, on a $\sin(z) = i\sin(x)\cosh(y) + \cos(x)\sinh(-y)$, donc $|\sin(z)|^2 = \sin(x)^2 + \sinh(y)^2$.

On obtient donc $|\text{cotan}(\pi z)|^2 = \frac{\cos(\pi x)^2+\sinh(\pi y)^2}{\sin(\pi x)^2+\sinh(\pi y)^2}$.

Soit $n \in \mathbb{N}$.

— Si $|x| = n + \frac{1}{2}$, c'est à dire si z est sur γ_2 ou γ_4, alors $\cos(\pi x) = \cos(\pm\pi(n+\frac{1}{2})) = 0$. Donc $|\text{cotan}(\pi z)|^2 = \frac{\sinh(\pi y)^2}{1+\sinh(\pi y)^2} \leq 1$

— Si $|y| = n$, c'est à dire si z est sur γ_1 ou γ_3, alors on minore $\sin(\pi x)^2+\sinh(\pi y)^2 \geq \sinh(\pi y)^2$, et on majore $\cos(\pi y)^2 \leq 1$ pour obtenir $|\text{cotan}(\pi z)|^2 \leq \frac{1+\sinh(\pi n)^2}{\sinh(\pi n)^2} \underset{n\to+\infty}{\longrightarrow} 1$. Ainsi, cotan est bornée sur le contour.

Donc il existe $M > 0$ telle que pour tout $n \in \mathbb{N}$ et $z \in \gamma_n$, $|\text{cotan}(\pi z)| \leq M$.

Étape 2 : *Convergence des intégrales sur le contour*

On va pouvoir grâce à la majoration effectuée précédemment, contrôler la valeur des intégrales sur le contour lorsque $n \to \infty$.

▷ Sur γ_1, on paramètre le segment comme suit :

$$\begin{array}{rccc} \gamma & : & [-n-\frac{1}{2}, n+\frac{1}{2}] & \longrightarrow & \mathbb{C} \\ & & t & \longmapsto & in - t \end{array}$$

On a alors, en appliquant l'inégalité triangulaire et en utilisant la majoration démontrée précédemment :

$$\left|\int_{\gamma_1} f(z)\mathrm{d}z\right| \leq \int_{-n-\frac{1}{2}}^{n+\frac{1}{2}} \frac{\pi}{|in-t|^2-|a|^2} M\mathrm{d}t \leq \pi M \frac{2n+1}{n^2-|a|^2} \underset{n\to\infty}{\longrightarrow} 0$$

Car n est choisi tel que $|a| < n$.

▷ On traite de la même façon les intégrales sur les autres segments, pour obtenir

$$\int_{\gamma_k} f(z)\mathrm{d}z \underset{n\to\infty}{\longrightarrow} 0, \quad \forall k \in \{1,2,3,4\}$$

Étape 3 : *Conclusion*

On a donc

$$\lim_{n\to\infty} \frac{1}{2i\pi}\int_{\gamma_n} f(z)\mathrm{d}z = \lim_{n\to\infty}\left(\frac{\pi}{a}\text{cotan}(\pi a) - \frac{1}{a^2} + \sum_{k=1}^{n}\frac{2}{k^2-a^2}\right)$$

Et la série converge, donc

$$0 = \frac{\pi}{a}\text{cotan}(\pi a) - \frac{1}{a^2} + \sum_{k=1}^{\infty}\frac{2}{k^2-a^2}$$

Ce qui donne encore

$$\boxed{\text{Pour tout } a \in \mathbb{C}\setminus\mathbb{Z}, \quad \text{cotan}(\pi a) = \frac{1}{\pi a} - \frac{2a}{\pi}\sum_{n=0}^{\infty}\frac{1}{n^2-a^2} \qquad \text{Pour tout } a \in \mathbb{C}\setminus\mathbb{Z}}$$

Pour le prolongement de ζ, on cherche à calculer $\frac{i}{2}\text{cotan}(i\frac{u}{2})$, avec $u \in \mathbb{R}$. On peut donc appliquer la formule que l'on vient de démontrer, puisque pour tout $u \in \mathbb{R}$, $i\frac{u}{2} \notin \mathbb{Z}$. On pose alors $i\frac{u}{2} = \pi a$, et simplifiant les expressions, on trouve bien

$$\frac{i}{2}\text{cotan}(i\frac{u}{2}) = \frac{1}{u} + 2u\sum_{n\geq 1}\frac{1}{4n^2\pi^2 + u^2}$$

□

Générateurs de $GL_n(\mathbb{Z})$

(rédigé par Émilie Tezenas)

Leçons : 108 ; 142

Références : COGNET, *Algèbre Linéaire* [COG00]

Introduction :

Le but de ce développement est d'obtenir un système de générateurs du groupe $\mathrm{GL}_n(\mathbb{Z})$, en le faisant agir sur $\mathbb{Z}^n$. On commence par exhiber une famille de représentants de l'action, avant de s'attaquer à la génération du groupe.

On considère l'action naturelle de $\mathrm{GL}_n(\mathbb{Z})$ sur $\mathbb{Z}^n$:

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{Z}) \times \mathbb{Z}^n & \longrightarrow & \mathbb{Z}^n \\ (P, X) & \longmapsto & P.X \end{array}$$

On note pour $X \in \mathbb{Z}^n$, et $a \in \mathbb{Z}$,

— ω_X l'orbite de X sous l'action de $\mathrm{GL}_n(\mathbb{Z})$,

— ρ_X le pgcd des coordonnées de X,

— C_a la colonne $\begin{pmatrix} a \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ de $\mathbb{Z}^n$.

Introduisons également les matrices suivantes :

— $T_n(i, j, \varepsilon)$: matrice de transvection avec $\varepsilon = \pm 1$.

— $D_n(i)$: matrice de dilatation, avec un -1 à la $i^{\text{ème}}$ ligne.

— $P_n(\tau)$: la matrice de permutation associée à τ, avec $\tau \in \mathfrak{S}_n$.

On note alors G_n le groupe engendré par toutes ces matrices. G_n est en particulier inclus dans $\mathrm{GL}_n(\mathbb{Z})$, car les déterminants des générateurs valent ± 1.

Théorème 1. Pour tout $X \in \mathbb{Z}^n$, $\omega_X = \omega_{C_{\rho_X}}$. Autrement dit, l'orbite de X est confondue avec l'orbite de la colonne contenant le pgcd des coordonnées de X.

Démonstration. Soit $X \in \mathbb{Z}^n$. Les orbites sous une actions sont soit disjointes, soit égales. Il nous suffit donc de trouver un élément dans l'intersection

$$\omega_X \cap \omega_{C_{\rho_X}}$$

pour montrer que ces deux orbites sont égales.
Montrons que $C_{\rho_X} \in \omega_X \cap \omega_{C_{\rho_X}}$.

On va en fait montrer un Lemme plus fort, qui nous sera utile pour trouver ensuite un système de générateurs de $\mathrm{GL}_n(\mathbb{Z})$.

Lemme 1. Pour tout $X \in \mathbb{Z}^n$, il existe $P \in G_n$ tel que $P.X = C_{\rho_X}$

Une fois ce lemme démontré, il est immédiat que C_{ρ_X} se trouve dans l'orbite de X, et donc que les deux orbites sont confondues.

□

Démonstration du Lemme. L'idée est de réaliser des opérations qui ne changent pas le pgcd, en s'inspirant de l'algorithme d'Euclide additif.

On note, pour $X \in \mathbb{Z}^n$, $S_X = \sum_{i=1}^n |x_i|$. On raisonne par récurrence sur S_X.

Pour $k \in \mathbb{N}$, on note : HR(k) : "Si $S_X = k$, alors il existe $P \in G_n$ tel que $P.X = C_{\rho_X}$"

▷ $S_X = 0$: Alors $P = I_n$ convient.

▷ Soit $k \geq 1$. Supposons HR(m) vérifiées pour $m < k$. Soit $X \in \mathbb{Z}^n$ tel que $S_X = k$.

— Si X a un seul coefficient non nul, disons à la ligne i, ce coefficient est égal au pgcd de X. Alors si $\tau = (1, i)$, $P_n(\tau).X = C_{\rho_X}$.

— Sinon, X a au moins deux éléments non nuls, aux lignes $i < j$. Quitte à permuter ces deux lignes au moyen d'une matrice de permutation, on peut supposer que $|x_i| > |x_j|$. Soit ε tel que $|x_i + \varepsilon x_j| = |x_i| - |x_j|$ (ε vaut -1 si les deux coefficients sont de même signe, 1 sinon).

On note $\tilde{X} = T_n(i, j, \varepsilon).X$. Alors

$$S_{\tilde{X}} = \sum_{k=1}^{n} |\tilde{x}_k| = \sum_{k \neq i} |x_k| + |x_i + \varepsilon x_j|$$

Or, $|x_i + \varepsilon x_j| = |x_i| - |x_j| < |x_i|$. Donc $S_{\tilde{X}} < S_X$.

On peut donc appliquer l'hypothèse de récurrence à $\tilde{X}$. De plus, $\rho_X = \rho_{\tilde{X}}$ car pour $a, b \in \mathbb{Z}$, $\text{pgcd}(a, b) = \text{pgcd}(a, b - a)$.

Finalement, il existe $\tilde{P} \in G_n$ tel que $\tilde{P}.\tilde{X} = C_{\rho_{\tilde{X}}} = C_{\rho_X}$. D'où

$$\tilde{P}.T(i, j, \varepsilon).X = C_{\rho_X}$$

.

□

Corollaire 3. L'ensemble $(C_a)_{a \in \mathbb{Z}}$ est une famille de représentants de l'action.

Démonstration. Le théorème précédent montre que pour tout $X \in \mathbb{Z}^n$, il existe $a \in \mathbb{Z}$ tel que $\omega_X = \omega_{C_a}$.

Il reste à montrer que si $a \neq b$, alors $\omega_{C_a} \cap \omega_{C_b} = \varnothing$.

Soit a et $b \in \mathbb{Z}$ tels que $\omega_{C_a} \cap \omega_{C_b} \neq \varnothing$. Alors il existe $P \in \text{GL}_n(\mathbb{Z})$ tel que $P.C_a = C_b$.

$P \in \text{GL}_n(\mathbb{Z})$ donc $\det(P) = \pm 1$. En particulier, en développant par rapport à la première colonne, la valeur du déterminant donne une relation de Bézout entre les coefficients de la première colonne de P - que l'on note maintenant P_1. Donc $\rho_{P_1} = 1$.

On a alors $C_b = a.P_1$ donc $b = \rho_{C_b} = a.\rho_{P_1} = a$. Donc si $a \neq b$, les orbites sont disjointes, et on a bien trouvé un système de représentants de l'action. □

Théorème 2. $\text{GL}_n(\mathbb{Z}) = G_n$

Démonstration. On procède par récurrence sur n.

▷ $n = 1$: OK, $\text{GL}_n(\mathbb{Z}) = \pm 1$

▷ Soit $n \geq 2$. Supposons que le théorème soit vrai en dimension $n - 1$.

Soit $P \in \mathrm{GL}_n(\mathbb{Z})$. Le pgcd des coefficients de la première colonne vaut 1 (vu dans la preuve du corollaire). Donc il existe $G \in G_n$ tel que $G.P_1 = C_1$ (P_1 désigne la première colonne de la matrice P). Autrement dit, il existe $G \in G_n$ tel que

$$G.P = \begin{pmatrix} 1 & \star \\ \vdots & \star \\ 0 & \end{pmatrix}$$

Au moyen d'une multiplication à droite par des matrices de transvection, dont on notera le produit $\tilde{T}$, on annule les coefficients de la première ligne pour se ramener à une matrice de la forme suivante :

$$G.P.\tilde{T} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \tilde{P} & \\ 0 & & & \end{pmatrix}$$

$\tilde{P}$ est une matrice de taille $n-1 \times n-1$, donc l'hypothèse de récurrence s'y applique : $\tilde{P} \in G_{n-1}$.

La matrice $\tilde{G} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \tilde{P} & \\ 0 & & & \end{pmatrix}$ est donc dans G_n car les matrices de transpositions, permutations et dilatations en dimenson $n-1$ donnent des matrices de transposition, permutation et dilatation en dimension n lorsqu'on leur rajoute un point fixe.

On a donc $P = G^{-1}.\tilde{G}.\tilde{T}^{-1} \in G_n$, et le théorème est démontré.

□

Théorème de Structure des groupes abéliens finis

(rédigé par Émilie Tezenas)

Leçons : 104 ; 108 ; 110

Références : COLMEZ, *Éléments d'analyse et d'algèbre (et de théorie des nombres)* [COL11]

Théorème 1 (Théorème de structure des groupes abéliens finis)**.** Soit G un groupe abélien fini. Alors il existe un entier r et des entiers $n_1, n_2, \dots, n_r$ tels que $n_r | \dots | n_2 | n_1$ et

$$G \simeq \mathbb{Z}_{/n_1\mathbb{Z}} \times \dots \times \mathbb{Z}_{/n_r\mathbb{Z}}$$

L'idée est d'exhiber un sous-groupe de G d'ordre n_1 et un morphisme faisant intervenir ce sous-groupe. La notion d'exposant d'un groupe abélien fini va permettre de préciser cette idée.

Définition 1. On appelle exposant de G le maximum des ordres des éléments de G. On le note dorénavant m.

Lemme 1. Pour tout $g \in G$, $o(g)|m$. En particulier, l'exposant d'un groupe abélien fini est le ppcm des ordres de ses éléments.

Démonstration du lemme. Soit $x \in G$ tel que $o(x) = m$. Soit $y \in G$ différent de x. On note l son ordre. Le but est de montrer que $\text{ppcm}(l, m) = m$. Ainsi, on aura montré que $l|m$.

Notons $\text{ppcm}(l, m) = p_1^{\alpha_1} \dots p_q^{\alpha_q}$ la décomposition en facteurs premiers du ppcm.

Alors par construction de cette décomposition en utilisant les valuations de chaque nombre premier, pour tout $i \in \| 1, q \|$, deux cas peuvent se produire :

— soit $p_i^{\alpha_i} | m$, et alors $x^{\frac{m}{\alpha_i}}$ est d'ordre $p_i^{\alpha_i}$ (à vérifier, mais pas difficile)

— soit $p_i^{\alpha_i} | l$, et alors $y^{\frac{l}{\alpha_i}}$ est d'ordre $p_i^{\alpha_i}$ (à vérifier, mais pas difficile)

Dans tous les cas, on trouve un élément $z_i \in G$ d'ordre $p_i^{\alpha_i}$.

On note $z = z_1 \dots z_q$. Alors z est d'ordre $\text{ppcm}(l, m)$ (Par récurrence, le cas à deux éléments repose sur la commutativité des éléments, et le fait que leurs ordres sont premiers entre eux).

Or, par définition de m, $o(z) \leq m$. Mais par définition du ppcm, $\text{ppcm}(l, m) \geq m$. Donc $\text{ppcm}(l, m) = m$ et $l|m$. □

Démonstration du théorème de structure. Soit G un groupe abélien fini. On note toujours m son exposant.

Soit $x \in G$ d'ordre m (existe, m est le maximum des ordres). On note $H = \langle x \rangle$. Alors $H \simeq \mathbb{Z}_{/m\mathbb{Z}}$.

On pose

$$\begin{array}{rccc} \chi & : & H & \longrightarrow & \mathbb{C}^* \\ & & z = x^k & \longmapsto & e^{\frac{2i\pi}{m}k} \end{array}$$

χ est un caractère de H. C'est même un isomorphisme entre H et $\mathbb{U}_m$.

D'après le théorème de prolongement des caractères que l'on prouvera après, χ peut être prolongé en un caractères sur G, que l'on note χ'.

On a vu que tout ordre d'un élément de G divise l'exposant de G. Donc pour tout $g \in G$, $\chi'(g)^m = \chi'(g^m) = \chi'(e) = 1$. Donc χ' est à valeurs dans $\mathbb{U}_m$. χ' est même surjectif, puisque c'est un prolongement de χ qui était lui-même surjectif.

On obtient donc un morphisme de groupe surjectif entre G et $\mathbb{U}_m$.

On note $N = \mathrm{Ker}(\chi')$. Le but est maintenant de montrer que

$$G \simeq H \times N$$

Posons

$$\begin{array}{rccc} f & : & H \times N & \longrightarrow & G \\ & & (h,n) & \longmapsto & hn \end{array}$$

Alors :

— f est injective : si $hn = h'n'$, alors $h'^{-1}h = n^{-1}n' \in H \cap N$. Or, χ est injectif sur H, donc $H \cap N = H \cap \mathrm{Ker}(\chi) = \{e\}$. D'où $h'^{-1}h = e$ i.e. $h = h'$ et donc $n = n'$.

— f est surjective : $|G| = |\mathrm{Im}(\chi)||\mathrm{Ker}(\chi)| = |H||N|$. Donc en combinant l'injectivité et l'égalité des cardinaux, on a la sujectivité.

— Enfin, f est un morphisme : $f((h,n)(h',n')) = f((hh',nn')) = hh'nn' = hnh'n'$ car G est abélien.

Donc on a bien un isomorphisme

$$G \simeq H \times N \simeq \mathbb{Z}_{/m\mathbb{Z}} \times N$$

.

On itère ensuite le raisonnement sur N pour obtenir les autres invariants. Les relations de divisibilité proviennent du fait que m est l'exposant de G, et que donc tout ordre d'un élément de G divise m. □

Théorème 2 (de prolongement des caractères)**.** Soit G un groupe abélien fini et H un sous-groupe de G. Alors tout caractère linéaire de H peut être prolongé en un caractère linéaire de G.

Démonstration du lemme. On raisonne par récurrence sur l'indice de H.

Initialisation : $[G : H] = 1$ Cela signifie que $G = H$. Donc un caractère de H est déjà un caractère de G.

Hérédité : $[G : H] > 1$ Soit alors $x \in G \setminus H$. On note $K = \langle H, x\rangle$. Soit χ un caractère linéaire de H.

On a $[G : K] < [G : H]$ donc l'hypothèse de récurrence s'applique à K. Il reste donc à prolonger χ à K.

On note $n = \min\{k \in \mathbb{N} \text{ tel que } x^k \in H\}$. Ce *min* existe bien puisque l'ensemble $\{k \in \mathbb{N} \text{ tel que } x^k \in H\}$ est inclus dans $\mathbb{N}$ et est non vide : G est un groupe fini, donc x admet un ordre, et $x^{o(x)} = e \in H$.

Alors pour tout $z \in K$, il existe un unique couple $(y, l) \in H \times [\![0, n-1]\!]$ tel que $z = y.x^l$.

En effet, l'existence est immédiate vu la définition de K, celle de n, et le caractère abélien de G.

Supposons qu'il existe $(y, l), (\tilde{y}, \tilde{l})$ tels que $yx^l = \tilde{y}.x^{\tilde{l}}$. On peut supposer que $l < \tilde{l}$. Alors $\tilde{y}^{-1}.y = x^{\tilde{l}-l} \in H$. Or, $\tilde{l} - l < n$. Par minimalité de n, on a donc $\tilde{l} = l$, et ainsi $y = \tilde{y}$. L'unicité est donc bien démontrée.

Revenons au prolongement de χ. On procède par analyse synthèse.

♦ Analyse : Supposons χ prolongé en un caractère de K, que l'on note $\tilde{\chi}$. Alors on a

— d'une part $\tilde{\chi}(x^n) = \chi(x^n)$, car $x^n \in H$

— d'autre part, $\tilde{\chi}(x^n) = \tilde{\chi}(x)^n$ car $\tilde{\chi}$ est un morphisme.

Finalement, $\tilde{\chi}(x)$ est une racine n^{ème} de $\chi(x^n)$.

♦ Synthèse : Soit ζ une racine n^{ème} de $\chi(x^n)$. Posons

$$\begin{array}{rccc} \tilde{\chi} & : & K & \longrightarrow & \mathbb{C}^* \\ & & z = y.x^l & \longmapsto & \chi(y)\zeta^l \end{array}$$

— $\tilde{\chi}$ est bien à valeurs dans $\mathbb{C}^*$, car χ l'est.

— $\tilde{\chi}$ prolonge χ, vu l'unicité d'écriture des éléments de K démontrée plus tôt.

— Il reste à vérifier que $\tilde{\chi}$ est bien un morphisme.

Soit $z = y.x^l$ et $z' = y'.x^{l'}$. Alors

$$\tilde{\chi}(z.z') = \tilde{\chi}(y.y'.x^{l+l'})$$

Deux cas peuvent se produire :

— Si $l + l' < n$: Alors $\tilde{\chi}(z.z') = \chi(y.y')\zeta^{l+l'} = \chi(y)\chi(y')\zeta^l\zeta^{l'} = \tilde{\chi}(z)\tilde{\chi}(z')$.

— Si $l + l' \geq n$: On ne peut pas appliquer directement la définition de $\tilde{\chi}$. On écrit alors $l + l' = n + k$, avec $k < n$ et ainsi :

$$\begin{aligned} \tilde{\chi}(z.z') &= \tilde{\chi}(y.y'.x^{n+k}) \\ &= \tilde{\chi}(y.y'.x^n.x^k) \\ &= \chi(y.y'.x^n).\zeta^k \\ &= \chi(y)\chi(y')\chi(x^n)\zeta^{l+l'-n} \qquad \text{Car } x^n \in H \\ &= \chi(y)\chi(y')\chi(x^n)\zeta^{-n}\zeta^l\zeta^{l'} \end{aligned}$$

Or, on a choisit ζ comme une racine n^{ème} de $\chi(x^n)$. Donc finalement on a bien :

$$\tilde{\chi}(z.z') = \chi(y)\chi(y')\zeta^l\zeta^{l'} = \tilde{\chi}(z)\tilde{\chi}(z')$$

Donc $\tilde{\chi}$ est un morphisme, donc un caractère de K, qui prolonge χ. Le théorème s'en déduit par la récurrence annoncée : on prolonge $\tilde{\chi}$ à G.

□

Remarques :

L'isomorphisme de la fin existe dans un cadre plus général : il faut que H et N soient distingués dans G, et que leur intersection soit réduite au neutre.

Invariants de similitude

Leçons : 151 ; 153 ; 154

Références : GOURDON, *Algèbre* (p.290) [GOU08a]

Prérequis :

- Lemme des noyaux
- Endomorphismes cycliques
- Notions de dualité (orthogonal, base duale, etc...)

Notations :

- $C(P)$ désigne la matrice compagnon associée au polynôme $P \in \mathbb{K}[X]$
- Π_u désigne le polynôme minimal de l'endomorphisme $u \in \mathcal{L}(E)$ où E est un espace vectoriel

Introduction :

Supposons que l'on fait agir $GL_n(\mathbb{K})$ sur les matrices de $\mathcal{M}_n(\mathbb{K})$ par similitude, on voudrait décrire les orbites. On sait que deux matrices semblables ont même rang, même trace même déterminant, mais cela ne suffit pas à décrire les orbites, puisqu'il existe des matrices de même rang, même trace et même déterminant qui ne sont pas semblables. On va voir ici ce que l'on appelle invariant de similitude qui permet décrire les orbites de cette action. Autrement dit, deux matrices sont semblables si et seulement si elles ont les mêmes invariants de similitude. On va faire ce développement en parlant d'endomorphismes plutôt que de matrices.

Lemme 1. Soit $u \in \mathcal{L}(E)$ avec E de dimension finie. On note Π_u le polynôme minimal de u et Π_u^x le polynôme unitaire qui engendre

$$\{P \in \mathbb{K}[X], P(u)(x) = 0\}$$

Alors il existe $x \in E$ tel que

$$\Pi_u^x = \Pi_u$$

Démonstration du lemme.

Étape 1 : *Étudions le cas où $\Pi_u = P^\alpha$ avec P irréductible*

Pour tout $x \in E$, il existe $n \in [\![0; \alpha]\!]$ tel que

$$P^n(u)(x) = 0$$

On veut trouver un x tel que $P^n(u)(x) \neq 0$ pour tout $n < \alpha$.

Par l'absurde, si pour tout $x \in E$, il existe $n < \alpha$ tel que $P^(u)(x) = 0$, alors

$$P^{\alpha-1}(u) = 0$$

Donc $\Pi_u \mid P^{\alpha-1}$ puisque Π_u est le polynôme minimal de u. On aboutit à une contradiction car $P^{\alpha-1}$ est de degré strictement inférieur à Π_u.

Étape 2 : *Traitons le cas général*

On note

$$\Pi_u = \prod_{i=1}^{r} P_i^{\alpha_i}$$

la décomposition en irréductibles de Π_u. Par le lemme des noyaux, on a

$$E = \ker(\Pi_u(u)) = \bigoplus_{i=1}^{r} \underbrace{\ker(P_i^{\alpha_i}(u)}_{E_i}$$

Par l'étape 1, on a pour tout $i \in [\![1;r]\!]$, un $x_i \in E_i$ tel que

$$\Pi^{x_i}_{u_{|E_i}} = \Pi_{u_{|E_i}}$$

On va montrer le résultat pour $x = x_1 + \cdots + x_r$. On a alors $\Pi_u^x \mid \Pi_u$ car $\Pi_u(u)(x) = 0$. On veut montrer que $\Pi_u \mid \Pi_u^x$, autrement dit $\Pi_u^x(u) = 0$

On a

$$0 = \Pi_u^x(u)(x) = \sum_{i=1}^{r} \Pi_u^x(u)(x_i)$$

Comme les E_i sont en somme directe et que $u(E_i) \subset E_i$ [1], on a alors, pour tout $i \in [\![1;r]\!]$,

$$\Pi_u^x(u)(x_i) = 0$$

Donc

$$\Pi^{x_i}_{u_{|E_i}} = \Pi_{u_{|E_i}} \mid \Pi_u^x$$

Ainsi $\Pi_u^x(u)$ est nul sur chaque E_i donc nul sur E. Ce qui permet de conclure que

$$\Pi_u \mid \Pi_u^x$$

□

Théorème 1. Soit $u \in \mathcal{L}(E)$ avec E de dimension finie n. Alors il existe une suite $F_1, \ldots, F_r$ de sous-espaces vectoriels de E stables par u telle que

- $E = F_1 \oplus \cdots \oplus F_r$
- $\forall i \in [\![1;r]\!]$, $u_i := u_{|F_i}$ est cyclique sur F_i
- En notant P_i le polynôme minimal de u_i, on a

$$\forall i \in [\![1;r-1]\!], \quad P_{i+1} \mid P_i$$

De plus, les (P_i) ne dépendent que de u.

Remarques :

Les F_i sont les invariants de similitude de u.

Démonstration.

Existence : On va raisonner par récurrence sur la dimension de E.

Soit $d = \deg(\Pi_u)$. Par le lemme, il existe $x \in E$ tel que $\Pi_u^x = \Pi_u$. On pose

$$F := \{P(u)(x), P \in \mathbb{K}[X]\}$$

1. il suffit de l'écrire

La dimension de F est alors d puisque

$$\dim(F) = \dim\left(\mathbb{K}[X]/(\Pi_u^x)\right) = \deg(\Pi_u^x) = \deg(\Pi_u) = d$$

La famille des $e_i := u^i(x)$ pour tout $i \in [\![0; d-1]\!]$ forme une base de F. On la complète en $(e_0, \dots, e_{n-1})$ une base de E.

On note $(e_0^*, e_1^*, \dots, e_{n-1}^*)$ sa base duale associée. On pose l'ensemble

$$\begin{aligned} G &= \left\{x \in E, \forall i \in \mathbb{N}, (e_{d-1}^* \circ u^i)(x) = 0\right\} \\ &= \mathrm{Vect}\underbrace{\left\{e_{d-1}^* \circ u^i, i \in \mathbb{N}\right\}}_{\Gamma}^{\perp} \end{aligned}$$

On veut montrer que $F \oplus G = E$.

Soit $y \in F \cap G$. On suppose que $y \neq 0$. On écrit

$$y = a_0 e_0 + \cdots + a_p e_p \text{ avec } a_p \neq 0 \text{ et } p \leqslant d-1$$

Comme $y \in G$, on a

$$e_{d-1}^* \circ u^{d-1-p}(y) = 0$$

Ce qui donne

$$e_{d-1}^*(a_0 e_{d-1-p} + \cdots + a_p e_{d-1}) = a_p = 0$$

On a une contradiction. Donc $F \oplus G$.

On veut montrer que $\dim(\mathrm{Vect}(\Gamma) = d$.

On pose l'application linéaire

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{K}[u] & \to & \mathrm{Vect}(\Gamma) \\ P(u) & \mapsto & e_{d-1}^* \circ P(u) \end{array} \right.$$

qui est bien définie et surjective par définition de Γ. L'application φ est injective par les mêmes techniques que pour montrer que $F \cap G = \{0\}$.

En effet, soit $P(u) \in \ker\varphi$. Si $P(u) \neq 0$, on peut écrire

$$P(u) = a_0 Id + a_1 u + \cdots + a_p u^p \text{ avec } a_p \neq 0 \text{ et } p \leqslant d-1$$

Comme on a

$$e_{d-1}^* \circ P(u) = 0$$

(car $P(u) \in \ker\varphi$), on trouve que $a_p = 0$, donc $P(u) = 0$ et φ est injective.

L'application φ est donc un isomorphisme, ce qui nous permet d'écrire

$$\dim(\mathrm{Vect}(\Gamma)) = \dim\mathbb{K}[u] = \dim(\mathbb{K}[X]/(\Pi_u)) = \deg(\Pi_u) = d$$

Donc $E = F \oplus G$ avec F et G stables par u. De plus, on a

$$\Pi_{u_{|F}} = \Pi_u^x = \Pi_u$$

et comme G est stable par u, on a

$$\Pi_{u_{|G}} \mid \Pi_u = \Pi_{u_{|F}}$$

Car pour tout $x \in G$, on a $\Pi_u(u)(x) = 0$, autrement dit, $\Pi_u(u_{|G}) = 0$.

Si $F = E$, on a le résultat voulue, sinon on effectue le même raisonnement à $u_{|G}$. On obtient le résultat souhaité car E est de dimension finie.

Unicité : Supposons qu'il existe $F_1, \dots, F_r$ et $G_1, \dots, G_s$ qui vérifient le théorème et qui ne sont pas égaux[2]. On pose

$$P_i := \Pi_{u_{|F_i}} \quad \text{et} \quad Q_i := \Pi_{u_{|G_i}}$$

Soit j le premier indice tel que $P_j \neq Q_j$. Cet indice existe car

$$n = \sum_{i=1}^{r} \deg P_i = \sum_{i=1}^{s} \deg Q_i$$

On a

$$E = F_1 \oplus \cdots \oplus F_r = G_1 \oplus \cdots \oplus G_s$$

On a donc

$$P_j(u)(E) = P_j(u)(F_1) \oplus \cdots \oplus P_j(u)(F_{j-1}) \text{ car } \forall i \geqslant j, P_i \mid P_j \tag{3.6}$$
$$P_j(u)(E) = P_j(u)(G_1) \oplus \cdots \oplus P_j(u)(G_s) \tag{3.7}$$

Or $P_i = Q_i$ pour tout $i \in [\![1; j-1]\!]$, en regardant les matrices compagnons, on a donc, pour tout $i \in [\![1; j-1]\!]$,

$$\dim(P_j(u)(F_i) = \operatorname{rg}(P_j(C(P_i))) = \operatorname{rg}(P_j(C(Q_i))) = \dim(P_j(u)(G_i)$$

On passe aux dimensions dans les équations (3.6) et (3.7). On trouve donc

$$\dim(P_j(u)(G_i)) = 0 \text{ pour tout } i \geqslant j$$

Donc $Q_i \mid P_j$ par définition de Q_i. En particulier, on a

$$Q_j \mid P_j$$

On peut faire le même raisonnement pour Q_j. On a donc $Q_j = P_j$, ce qui est absurde. Donc

$$r = s \quad \text{et} \quad (P_1, \dots, P_r = (Q_1, \dots, Q_r)$$

Ce qui conclut la preuve du théorème. □

Remarques :

Ce théorème est parfois appelé théorème de Frobenius.

C'est plus fort que la décomposition de Jordan, car ici on n'a pas besoin que le polynôme caractéristique soit scindé.

On peut montrer ce résultat avec l'algorithme donnant la forme normale de Smith.

Astuces de l'agrégatif :

Il faut bien comprendre où vivent les égalités. Est-ce une inégalité sur E ? sur $\mathcal{L}(E)$?

Le développement est long. Il ne faut pas trainer sur le lemme, pour avoir le temps de montrer le théorème.

2. On n'a pas ($r = s$ et $P_i = Q_i$ pour tout $i \in [\![1; r]\!]$).

Knuth Morris Pratt (Complexité)

Leçons : 907 ; 921 ; 926

Références : CORMEN–LEISERSON–RIVEST–STEIN, *Introduction à l'algorithmique* (p.921) [CLRS10]

But de l'algorithme : trouver toutes les occurences d'un motif P de taille m dans un texte T de taille n.

Par convention, les tableaux commencent à l'indice 1.

Dans l'algorithme, on a besoin d'un tableau auxiliaire π qui pour chaque indice i du tableau donne LA LONGUEUR DU PLUS GRAND SUFFIXE DU SOUS-MOT DE P QUI FINIT À L'INDICE i QUI EST AUSSI PRÉFIXE PROPRE DE P. On peut dire aussi que le tableau π est le tableau qui pour chaque indice i donne LA LONGUEUR DU PLUS GRAND BORD DU SOUS MOT DE P QUI FINIT À L'INDICE i. La définition du bord d'un mot est justement un préfixe propre qui est aussi suffixe du mot.

Exemple : Le motif *abcabd* a pour tableau auxiliaire $\pi = [|0; 0; 0; 1; 2; 0|]$ car pour *a*, *ab*, *abc* leur bord est de longueur nulle (par convention *a* n'est pas suffixe et préfixe propre, donc de bord de longueur nulle). Cependant pour *abca*, *a* est préfixe propre et suffixe et sa longueur est 1, puis *abcab* a pour bord *ab* de longueur 2. Pour finir, *abcabd* n'a pas de bord de longueur non nulle.

Algorithme 1 Calcul-π

```
Fonction Calcul-π(P) :
m = longueur(P)
π = tableau de taille m
π[1] = 0
k = 0  [indice de parcours du motif P]
Pour i de 2 à m faire
    Tant que (k > 0 et π[k+1] ≠ π[i]) faire
        k = π[k]
    Fait
    Si (π[k+1] = π[i]) alors
        k = k + 1
    Fin Si
    π[i] = k
Fin Pour
    π
Fin
```

On veut étudier la complexité de cet algorithme. On a une boucle 'for' de longueur $m-1$ avec des opérations à coup constant à l'intérieur sauf la boucle 'while'.

On va compter le nombre d'itérations maximum de la boucle 'while' quand on exécute le programme. On remarque trois propriétés :

— $k \geqslant 0$ car tout élément de π est positif (car chaque élément représente une longueur de mot)

— $\pi(k) < k$ car $k < i$ donc quand on définit $\pi(i)$, on met un élément strictement inférieur à i.

— k s'incrémente au plus de 1 à chaque fois dans la boucle 'for', donc $m-1$ fois au plus dans le programme

Ainsi on diminue strictement au plus $m-1$ fois la valeur de k dans le programme, donc on passe au plus $m-1$ fois dans la boucle 'while'. Ainsi la complexité est en $\mathcal{O}(m)$.

On peut maintenant donner l'algorithme de Knuth Morris Pratt

Algorithme 2 Knuth Morris Pratt

```
Procédure KMP((T, P))
    n = longueur(T)
    m = longueur(P)
    π = Calcul − π(P)
    k = 0 [indice de parcours du motif P]
    Pour i de 1 à n faire
        Tant que (k > 0 et π[k + 1] ≠ T[i]) faire
            k = π[k]
        Fait
        Si (π[k + 1] = T[i]) alors
            k = k + 1
        Fin Si
        Si (k = m + 1) alors
            Afficher "occurence de P à l'indice i − m + 1"
            k = π(k)
        Fin Si
    Fin Pour
Fin
```

Exemple : Pour le texte $T = abcabcabd$, on veut chercher le motif $P = abcabd$.

i	1	2	3	4	5	6	7	8	9	
T	a	b	c	a	b	c	a	b	d	
	↕	↕	↕	↕	↕	×				
P	a	b	c	a	b	d				
k	1	2	3	4	5					
					2					car $\pi(5) = 2$ et $c \neq d$
P				a	b	c	a	b	d	
k					2	3	4	5	6	

On a modifié 5 en 2 car on entrait une fois dans la boucle 'while'. Il faut faire tourner l'algorithme à la main pour bien se convaincre de sa correction (ce n'est pas une preuve de correction !).

On veut maintenant étudier la complexité de cet algorithme. On raisonne de la même manière que pour le programme **Calcul-π**. Le seul changement est la boucle 'for' de longueur n. Le nombre d'itérations de la boucle 'while' est majoré par n cette fois-ci. On a donc une complexité en $\mathcal{O}(n)$.

Ainsi l'utilisation de l'algorithme de Knuth Morris Pratt utilise une complexité temporelle et spatiale de $\mathcal{O}(m)$ pour le prétraitement, puis pour l'algorithme on a une complexité temporelle en

$\mathcal{O}(n)$. L'algorithme de Knuth Morris Pratt est donc une amélioration de l'algorithme de Morris Pratt qui stockait l'automate des occurrences ($\mathcal{O}(m|\Sigma|)$ en espace où Σ est l'alphabet utilisé).

Remarques :

Pour utiliser des mots précis, on utilise de la complexité amortie, mais il faut savoir exactement comment prouver le résultat avec les techniques style agrégat, potentiel, comptable, ici on raisonne plutôt par agrégat.

Si on parle de Morris Pratt il faut savoir plus en détail cette histoire d'automates des occurrences. Cela tombe bien c'est un développement développé plus haut : Automates des occurrences

Dans ce développement, je développe beaucoup l'exemple pour bien faire comprendre l'algorithme.

Caractérisation de RE

Leçons : 912 ; 913 ; 914

Références : CORI–LASCAR, *Logique Mathématique, tome 2* (p.41) [CL03] et LESESVRE–MONTAGNON–LE BARBENCHON–PIERRON, *131 développements pour l'oral* (p. 692) [LMLBP20]

Prérequis :

- équivalence entre Machine de Turing et fonction μ-récursive

Théorème 1. Soit $A \subset \mathbb{N}$, il y a équivalence entre les propositions suivantes :

(i) $A \in RE$

(ii) $A = \pi_2^2(B)$ pour $B \subset \mathbb{N}^2$ primitive récursive

(iii) $A = \varnothing$ ou A est l'image d'une fonction primitive récursive

(iv) A est l'image d'une fonction μ-récursive

Remarques :

On dit qu'un ensemble $E \subset \mathbb{N}$ est primitif récursif si sa fonction indicatrice est primitive récursive.

Démonstration. $\boxed{(i) \implies (ii)}$ Par définition il existe une machine de Turing M qui accepte A. On pose le prédicat :

$$P(t,x) = \text{“la machine } M \text{ accepte } x \text{ en } t \text{ étapes”}$$

Le prédicat P est primitif récursif car

$$P(t,x) = \mathbb{1}_F(\text{config}(\text{init}(x),t))$$

avec les fonctions définies dans le développement Machine de Turing $\implies$ μ-récursif.

On a supposé ici que la machine de Turing M boucle sur ces états finals.

On pose $B = \{(t,x), P(t,x)\}$, on a alors

$$\begin{aligned} x \in A &\iff \exists t, P(t,x) \\ &\iff \exists t, (t,x) \in B \\ &\iff x \in \pi_2^2(B) \end{aligned}$$

Ainsi on a bien $A = \pi_2^2(B)$.

$\boxed{(ii) \implies (iii)}$ Si $A \neq \varnothing$, il existe $n \in A$

Soit la bijection primitive récursive $\varphi : \mathbb{N} \to \mathbb{N}^2$ définie par :

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N}^2 \\ k & \mapsto & (t_k, x_k) \end{array} \right.$$

où $t_k = \text{diag}(k) - \text{ecart}(k)$ et $x_k = \text{ecart}(k)$ avec $\text{diag}(k) = \mu_i(i \leqslant k+1)(\frac{i(i+1)}{2} > k) - 1$ et $\text{ecart}(k) = k - \frac{\text{diag}(k)(\text{diag}(k)+1)}{2}$. φ est bien primitive récursive et bijective.

On note $B = (t_k, x_k)$ et on pose la fonction :

$$f(k) = (\pi_2^2 \circ \varphi(k))(\mathbb{1}_B \circ \varphi(k) + n(1 - \mathbb{1}_B \circ \varphi(k))$$

On a donc $x \in A \iff \exists t, (t,x) \in B \iff x \in \text{Im}(f)$

$\boxed{(iii) \implies (iv)}$ Si $A = \varnothing$, on a $A = \mathrm{Im}(\mu_i(\mathbb{O}(i)))$ avec $\mu_i(\mathbb{O}(i))$ une fonction μ-récursive. Si A est primitive récursive alors elle est aussi μ-récursive car toute fonction primitive récursive est μ-récursive (on ajoute seulement la minimisation non bornée).

$\boxed{(iv) \implies (i)}$ On a $A = \mathrm{Im}(f)$ avec f μ-récursive. Or f μ-récursive implique f calculable par une machine de Turing.

On peut donner l'algorithme suivant (entrée : x) :

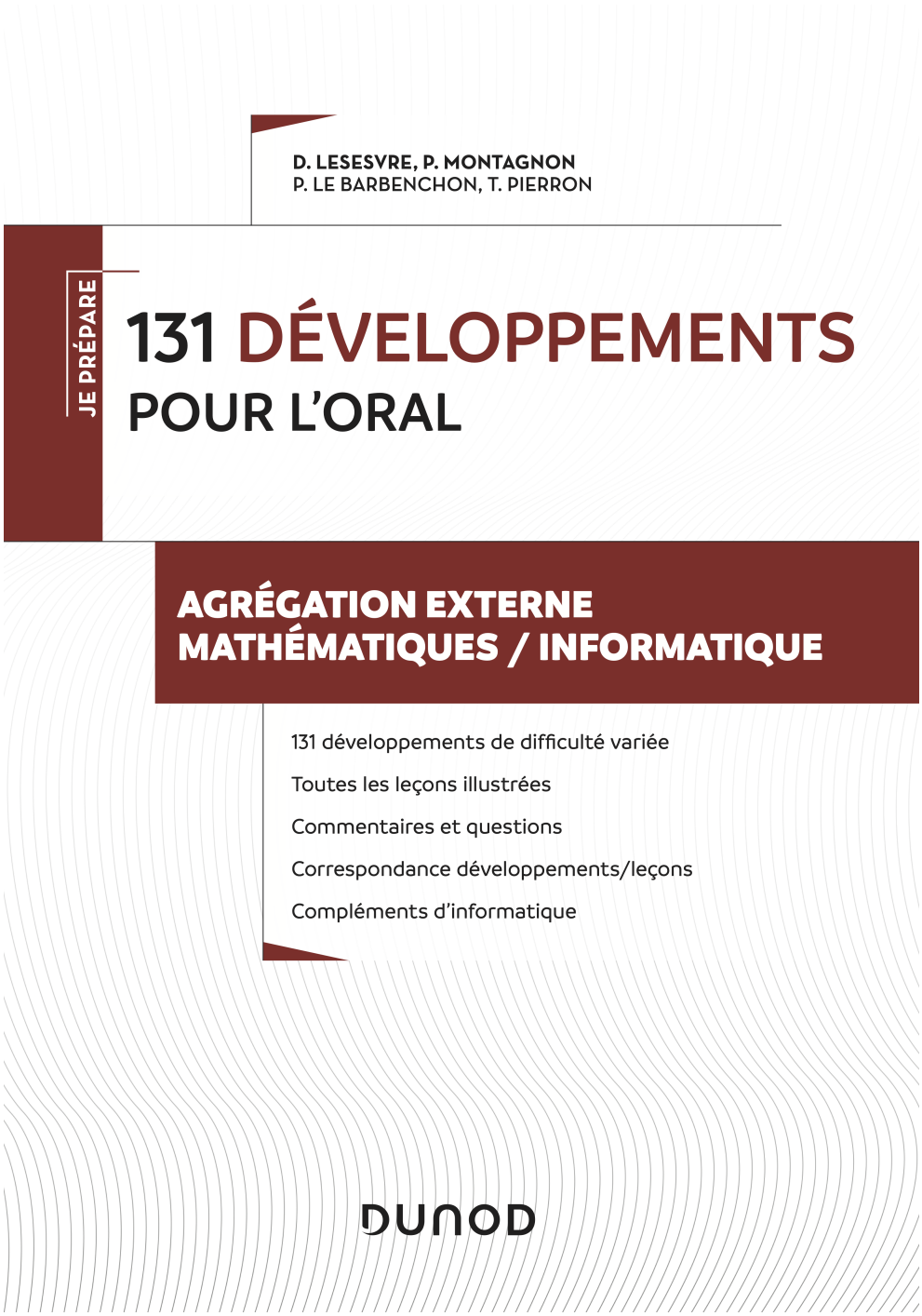
$k = 0$
tant que $f(k) \neq x$:
    $k = k + 1$
ACCEPTER

On peut implémenter cette machine de Turing (puisque f est calculable par une machine de Turing) et elle va accepter les éléments de A car ils seront l'image de f. Donc $A \in RE$. □

3.7 Liste de pleins de développements

3.7.1 Livre coécrit

Tu peux retrouver 131 développements de mathématiques et informatique dans le livre que j'ai co-écrit avec Didier Lesesvre, Pierre Montagnon et Théo Pierron : [LMLBP20]



3.7.2 Développements de mathématiques

Je mets maintenant une liste non exhaustive de nombreux développements en mathématiques et en informatique que j'ai rencontrés, dont j'ai entendu parler, que j'ai étudiés ou que j'ai aperçus chez des camarades. Néanmoins, il faut faire attention aux leçons qui sont indiquées puisque l'insertion d'un développement dépend avant tout du plan. Ainsi, en fonction du plan établi pour une leçon, on pourra faire rentrer tel ou tel développement que ne serait pas rentré sinon.

Groupes d'ordre 105 : 101 ; 103 ; 104 ; 121 ; 190 ([LMLBP20, p.44])
Cyclicité des groupes d'ordre pq : 101 ; 103 ; 104 ([LMLBP20, p.41])
Théorème de Dixon : 103 ; 104 ; 106 ; 160 ; 161 ; 190 ([LMLBP20, p.10])
Sous groupes distingués par les caractères : 102 ; 103 ; 107 ([PEY04])
Table de caractères de $\mathfrak{S}_4$: 105 ; 107 ; 154 ([AUD06])
Table de caractères des groupes diédraux : 101 ; 104 ; 107 ; 108 ([LMLBP20, p.49])
Théorème de Structure des groupes abéliens finis : 104 ; 108 ; 110 (ici)
Théorème $p^\alpha q^\beta$ de Burnside : 101 ; 103 ; 104 ; 107 ; 144 ([LMLBP20, p.54])
Incertitude de Heisenberg pour les groupes : 104 ; 107 ; 246 ([LMLBP20, p.5])
Automorphismes de $\mathfrak{S}_n$: 104 ; 105 ; 108 (ici)
Ensembles de transpositions engendrant $\mathfrak{S}_n$: 105 ; 108 ([LMLBP20, p.18])
Paires génératrices de sous-groupes de $\mathfrak{S}_n$: 101 ; 104 ; 105 ; 108 ; 190 ([LMLBP20, p.23])
Ordre maximum des permutations : 101 ; 104 ; 105 ; 121 ([LMLBP20, p.28])
Commutativité de permutations aléatoires : 101 ; 104 ; 105 ; 190 ([LMLBP20, p.35])
$\mathfrak{A}_n$ est simple pour $n \geqslant 5$: 104 ; 105 ; 108 ([PER96], [ULM12, p.53])
Isométries du cube et du tétraèdre : 101 ; 104 ; 105 ; 161 ; 191 (ici)
Isom. directes des solides de Platon : 101 ; 104 ; 106 ; 108 ; 160 ; 161 ; 190 ; 191 ([LMLBP20, p.251])
Théorème des trois réflexions : 108 ; 160 ; 161 ([LMLBP20, p.239])
Point de Fermat : 161 ; 215 ; 219 ; 229 ; 253 ([FGN13a])
Ellipsoïde de John-Loewner : 152 ; 158 ; 160 ; 170 ; 171 ; 181 ; 203 ; 219 ; 229 ; 253 ([FGN13a, p.229])
Théorème de Killing-Hopf : 101 ; 108 ; 160 ; 161 ; 191 ([LMLBP20, p.243])
Espace des formes modulaires : 151 ; 201 ; 236 ; 239 ; 245 ([LMLBP20, p.477])
Générateurs de $SL_2(\mathbb{Z})$: 101 ; 108 ; 191 (ici)
Groupe circulaire : 108 ; 191 ([AUD06, p.204])
Billard circulaire : 102 ; 108 ; 191 ([LMLBP20, p.219])
Le plongeoir le plus long : 162 ; 181 ; 219 ([LMLBP20, p.226])
Perturbation par des matrices de rang 1 : 152 ; 153 ; 162 ([LMLBP20, p.135])
Dénombrement des matrices diagonalisables de $\mathbb{F}_q$: 101 ; 106 ; 150 ; 155 ;190 (ici)
Cardinal du cône nilpotent sur $\mathbb{F}_q$: 101 ; 104 ; 106 ; 157 ; 190 ([CG17, p.213])
Lemmes de Schwartz-Zippel et de Kakeya : 121 ; 144 ; 151 ; 190 ; 264 ([LMLBP20, p.147])
Générateurs de $GL_n(\mathbb{Z})$: 108 ; 142 (ici)
Théorème de Burnside : 104 ; 106 ; 157 ([FGN09, p.185])
Décomposition polaire : 106 ; 150 ; 155 ; 156 ; 158 ; 160 ; 203 ([LMLBP20, p.185])
Etude du groupe $O(p, s)$: 106 ; 156 ; 158 ; 160 ; 170 ; 171 (ici)
Formes quadratiques semi-réduites : 158 ; 170 ; 171 ([LMLBP20, p.264])
Théorème de Minkowski pour les formes quadratiques : 151 ; 158 ; 170 ; 171 ([LMLBP20, p.268])
Théorème d'Hermite : 158 ; 170 ([LMLBP20, p.260])
Simplicité de $SO_3(\mathbb{R})$: 101 ; 103 ; 106 ; 108 ; 160 ; 161 ([FGN13a, p.67])
$SO_3(\mathbb{R})$ et les quaternions : 101 ; 106 ; 108 ; 154 ; 161 ; 191 ([PER96, p.163],[LMLBP20, p.138])
Théorèmes de Choquet et de Birkhoff : 181 ; 203 ; 219 ; 253 ([LMLBP20, p.423])
Théorème de Carathéodory : 126 ; 151 ; 181 (ici)
Théorèmes de Helly et de Carathéodory : 151 ; 181 ([LMLBP20, p.235])
Endomorphismes conservant le rang : 151 ([LMLBP20, p.167])
Loi de réciprocité quadratique : 121 ; 123 ; 126 ; 170 ; 190 (ici)

Théorème de Frobenius- Zolotarev : 103 ; 105 ; 106 ; 123 ; 152 ([BMP05])
Théorème de Chevalley-Warning : 121 ; 123 ; 126 ([ZAV13, p.32])
Problème de Waring modulo n : 104 ; 108 ;120 ; 121 ; 126 ; 190 ([LMLBP20, p.128])
Nombres de Sophie Germain : 120 ; 121 ; 123 ; 126 ([FGN18])
Théorème de Fermat modulaire : 120 ; 121 ; 126 ; 190 (ici)
Théorème de Fermat et cyclotomie : 102 ; 120 ; 121 ; 122 ; 126 ; 142 ; 144 ([LMLBP20, p.120])
L'unique entier entre un carré et un cube : 122 ; 126 ; 142 ([LMLBP20, p.109])
$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ **est principal mais non euclidien** : 122 ([PER96])
Lemme d'intersection de Krull : 122 ([LMLBP20, p.81])
Théorème d'Artin : 125 ; 141 ; 144 ; 162 ([LMLBP20, p.103])
Primalité des nombres de Mersenne : 120 ; 121 ; 123 ; 125 ; 141 (ici)
Lemme de Hensel : 120 ; 121 ; 126 ; 144 ([LMLBP20, p.69])
Théorème des deux carrés : 120 ; 121 ; 122 ; 123 ; 126 ([PER96, p.56])
Dénombrement des irréductibles de $\mathbb{F}_q[X]$: 123 ; 125 ; 141 ; 144 ([FGN18, p.189])
Irréductibilité des polynômes cyclotomiques : 141 (ici)
Cyclicité de $\mathbb{F}_q^\times$: 104 ; 108 ; 121 ; 123 ([LMLBP20, p.84])
Automorphismes de $\mathbb{F}_q$: 123 ; 125 ; 141 ([LMLBP20, p.89])
Automorphismes d'un corps cyclotomique : 102 ; 120 ; 121 ; 122 ; 125 ; 141 ; 144 ([LMLBP20, p.92])
Automorphismes sauvages de $\mathbb{C}$: 125 ; 141 ; 144 ; 207 ([LMLBP20, p.96])
Valeurs absolues sur $\mathbb{Q}$: 121 ; 122 ; 223 ([LMLBP20, p.114])
Méthode polynomiale en combinatoire : 123 ; 144 ; 190 ; 925 ([LMLBP20, p.73])
Théorème de Cohn : 121 ; 141 ; 144 ([LMLBP20, p.63])
Théorème de Kronecker : 102 ; 144 ([FGN18])
Algorithme de Berlekamp : 122 ; 141 ; 142 ([BMP05, p.244])
Théorème de D'Alembert-Gauss : 125 ; 141 ; 144 ([LMLBP20, p.78])
Théorème de Chebotarev : 102 ; 121 ; 144 ; 152 ([LMLBP20, p.172])
Méthode archimédienne pour approcher π : 223 ; 228 ; 265 ([LMLBP20, p.409])
Aiguille de Buffon : 261 ; 262 ; 266 ([LMLBP20, p.565])
Convergence de polygones vers l'isobarycentre : 152 ; 191 ; 223 ; 226 (ici)
Conv. des polygones vers l'isobarycentre (avec caractères) : 107 ; 110 ; 181 ; 191 ; 226 ([PEY04])
Calculs de polynômes caractéristiques : 144 ; 152 ; 153 ; 162 ([LMLBP20, p.155])
Endomorphismes conservant le déterminant : 106 ; 150 ; 151 ; 152 ([LMLBP20, p.163])
Réduction endomorphismes normaux : 150 ; 151 ; 153 ; 154 ; 157 ; 159 ([GOU08b, p.260],[LMLBP20])
Forme normale de Jordan et résidus : 152 ; 153 ; 154 ; 157 ; 245 ([LMLBP20, p.469])
Invariants de similitude : 150 ; 151 ; 153 ; 154 ; 157 ; 159 (ici)
Forme normale de Smith : 122 ; 142 ; 152 ; 155 ([LMLBP20, p.201])
Décomposition de Dunford : 153 ; 157 (ici)
Sous-algèbres réduites de $\mathcal{M}_n(\mathbb{C})$: 153 ; 155 ([LMLBP20, p.207])
Théorème d'Engel : 151 ; 154 ; 157 ([LMLBP20, p.212])
Cartan Von Neumann : 106 ; 156 ; 214 ; 215 ([GT96, p.81], [LMLBP20, p.313])
Image de l'exponentielle : 153 ; 156 ; 204 ; 214 (ici)
Homéomorphisme $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$: 155 ; 156 ; 158 ([CG17, p.208])
Lemme de Morse : 158 ; 170 ; 171 ; 214 ; 215 ([ROU09])
Théorème des extrema liés : 152 ; 159 ; 214 ; 215 ; 219 (ici)
Théorème des extrema liés (avec Théorème d'inversion locale) : 151 ; 214 ; 219 ([GOU08b])
Formules de Frenet-Serret : 267 ([LMLBP20, p.437])
Morphismes d'algèbre de $\mathcal{C}(K, \mathbb{R})$ sur $\mathbb{R}$: 159 ; 203 (ici)
Logarithme et théorème de Brouwer : 101 ; 204 ; 267 ([LMLBP20, p.296])
Théorème de Nash : 203 ; 223 ; 241 ; 253 ([LMLBP20, p.429])
Compacts d'un espace de Hilbert séparable : 203 ; 205 ; 213 ([LMLBP20, p.277])

Opérateurs compacts d'un espace de Hilbert : 201 ; 203 ; 208 ; 213 ([LMLBP20, p.281])
Décomposition de Mityagin : 208 ; 213 ([LMLBP20, p.285])
Méthode de Kacmarz : 159 ; 162 ; 226 ; 233 ([LMLBP20, p.455])
Méthode QR : 157 ; 162 ; 233 (ici)
Convergence des méthodes itératives : 157 ; 162 ; 233 ([CIA06, p.96])
Méthode de relaxation : 152 ; 153 ; 162 ; 226 ; 233 ([LMLBP20, p.445])
Méthode de Gauss-Seidel : 162 ; 223 ; 226 ; 233 ([LMLBP20, p.451])
Méthode de gradient à pas optimal : 162 ; 219 ; 226 ; 229 ; 233 (ici)
Méthode de Newton : 219 ; 223 ; 226 ; 228 ; 229 ; ; 253 (ici)
Réciproques partielles de Césaro : 223 ; 230 (ici)
Série génératrice des nombres de Bernoulli : 230 ; 243 ; 246 ([FGN13b, 1,p. 308])
Nombres de Bell : 190 ; 230 ; 243 (ici)
Développement asymptotique de la série harmonique : 224 ; 230 ([GOU08b])
Développement asymptotique d'une suite récurrente : 223 ; 224 ; 226 ; 230 ([FGN03, p.102])
Développement en fractions continues : 223 ; 226 ([LMLBP20, p.417])
Translatés d'une fonction $\mathcal{C}^1$: 151 ; 159 ; 221 ; 228 (ici)
Cauchy Lipschitz et lemme de Gronwall : 203 ; 208 ; 220 (ici)
Théorème de Cauchy Peano : 203 ; 215 ; 219 ; 220 ; 228 ; 241 ([LMLBP20, p.332])
Étude qualitative d'une équation de Riccati : 220 ; 228 ; 229 ([LMLBP20, p.367])
Théorème de Lyapunov (stabilité) : 153 ; 154 ; 156 ; 157 ; 215, 220, 221 ([ROU09],[LMLBP20, p.318])
Modèle de croissance de Solow-Swan : 220 ; 228 ; 229 ([LMLBP20, p.341])
Modèle épidémiologique SIS : 220 ; 229 ; 235 ([LMLBP20, p.353])
Modèle épidémiologique SIR : 220 ; 229 ([LMLBP20, p.361])
Modèle de Lotka-Volterra : 220 ; 228 ; 229 ; 265 ; 267 ([LMLBP20, p.372])
Théorème de Hadamard-Levy : 203 ; 204 ; 214 ; 215 ; 220 ([QZ07])
Nombres de zéros des solutions d'une équation différentielle : 220 ; 221 ; 224 (ici)
Loi forte des grands nombres : 260 ; 261 ; 262 ; 266 ([LMLBP20, p.594])
Théorème Central Limite : 260 ; 264 (ici)
Formule de Stirling par la limite centrale : 235 ; 260 ; 262 ; 264 ([LMLBP20, p.580])
Théorème de Cramér-Chernoff : 219 ; 228 ; 229 ; 239 ; 253 ; 262 ; 266 ([LMLBP20, p.617])
Processus de Galton–Watson : 226 ; 229 ; 243 ; 260 ; 261 ; 264 ([CGCDM05, p.72])
Paradoxe de Penney : 153 ; 155 ; 162 ; 226 ; 230 ; 243 ; 261 ; 264 ; 266 ([LMLBP20, p.570])
Marche Aléatoire sur $\mathbb{Z}^d$: 230 ; 241 ; 261 ; 262 ; 264 ([DM85])
Tirage aléatoire de population : 261 ; 264 ; 926 ; 927 ([LMLBP20, p.644])
Un théorème de grandes déviations : 262 ; 264 ; 265 ; 266 ([LMLBP20, p.613])
Théorème de Pólya : 190 ; 230 ; 241 ; 264 ; 266 ([LMLBP20, p.599])
Formule d'inversion de la fonction caractéristique : 236 ; 239 ; 250 ; 260 ; 264 (ici)
Formule de Poisson et Shannon : 239 ; 246 ; 250 (ici)
Formule de Poisson et équivalent Θ : 224 ; 243 ; 246 (ici)
Formule de Poisson et fonction Θ : 228 ; 246 ; 265 (ici)
Théorème de Minkowski pour les réseaux : 190 ; 209 ; 239 ; 250 ([LMLBP20, p.539])
Caractérisation de la fonction Gamma : 229 ; 239 ; 265 ([RUD98, p.179])
Calcul de l'intégrale de Gauss : 228 ; 236 ; 239 ; ([GOU08b, p.163 et 335])
Calcul de l'intégrale de Dirichlet : 235 ; 236 ; 239 ([BB18, p.259])
Calcul des intégrales de Fresnel : 209 ; 228 ; 230 ; 235 ; 236 ; 239 ; 241 ; 245 ; 246 ([LMLBP20, p.487])
Domaines d'holomorphie à une variable : 201 ; 207 ; 245 ([LMLBP20, p.464])
Formule des compléments : 235 ; 236 ; 239 ; 245 ; 265 (ici)
Prolongement de la fonction Zéta de Riemann : 207 ; 245 ; 265 (ici)
Prolongement analytique suivant une courbe : 204 ; 207 ; 245 ([LMLBP20, p.461])
Équation des ondes pour une corde vibrante : 221 ; 222 ; 246 ([LMLBP20, p.381])
Équation de la chaleur : 209 ; 222 ; 228 ; 235 ; 241 ; 246 ([QZ07, p.105])

Caractère bien posé (éq. de transport) : 201 ; 208 ; 213 ; 222 ; 228 ; 234 ; 241 ([LMLBP20, p.388])
Dualité contrôlabilité-observabilité : 201 ; 208 ; 213 ; 222 ; 228 ([LMLBP20, p.396])
Équation de Bessel : 220 ; 221 ; 243 ([FGN12, p.101])
Méthode de Laplace (ou phase stationnaire) : 224 ; 228 ; 239 ([ROU09],[LMLBP20, p.502])
Banach Alaoglu et fonctionnelle convexe : 203 ; 205 ; 208 ; 213 ; 219 ; 229 ; 253 ([BB18, p.27])
Théorème taubérien de Hardy-Littlewood : 207 ; 209 ; 230 ; 243 ([LMLBP20, p.545])
Banach–Steinhaus : 205 ; 208 ; 241 ; 246 (ici)
Théorème de Fejér-Cesàro : 207 ; 209 ; 215 ; 222 ; 235 ; 239 ; 241 ; 246 ([LMLBP20, p.531])
Espace de Bergman : 201 ; 202 ; 205 ; 208 ; 213 ; 234 ; 239 ; 245 ([BB18, p.121])
Théorème de Grothendieck : 201 ; 234 ([BB18, p.127])
Une isométrie de $L^2(\mathbb{R}^+)$ non surjective : 201 ; 202 ; 208 ; 213 ; 234 ([LMLBP20, p.290])
Théorème de Riesz–Fisher : 201 ; 205 ; 208 ; 234 ; 241 ([BRE05], [LMLBP20, p.303])
Théorème de Paley-Wiener : 207 ; 239 ; 245 ; 250 ([LMLBP20, p.509])
Théorème de Fourier–Plancherel : 201 ; 202 ; 207 ; 234 ; 235 ; 236 ; 241 ; 250 ([RUD98])
Optimisation dans un Hilbert : 203, 205, 208, 213, 219, 229, 253 ([CIA06])
Densité des polynômes orthogonaux : 202 ; 209 ; 213 ; 239 ([BMP05])
Meilleure approximation polynomiale : 141 ; 144 ; 209 ([LMLBP20, p.557])
Thrm. de Weierstrass (polynômes Bernstein) : 202 ; 209 ; 228 ; 260 ; 264 ([BL07, p.59], [GOU08b])
Théorème de Weierstrass (par la convolution) : 201 ; 203209 ; 228 ; 239 ; 241 ([GOU08b, p.284])
Racine carrée de la primitivation : 207 ; 208 ; 209 ; 236 ; 239 ; 265 ([LMLBP20, p.496])
Divergence de l'interpolation de Lagrange : 141 ; 209 ; 241 ([LMLBP20, p.552])

3.7.3 Développements d'informatique

Master Theorem : 926 ; 931 (ici)
Hachage parfait : 901 ; 921 ([CLRS10])
Tri par tas : 901 ; 903 ; 926 (ici)
Tri topologique : 903 ; 925 ; 927 (ici)
Tri rapide (complexité) : 903 ; 926 ; 931 ([CLRS10], [BBC92])
Distance de Kendall et tri par insertion : 903 ; 927 ; 931 ([LMLBP20, p.640])
Transformée de Fourier Rapide : 102 ; 901 ; 931 ([LMLBP20, p.651])
Algorithme du lièvre et de la tortue : 927 ([KNU11, p.7])
B-arbres : 901 ; 921 ; 932 ([CLRS10])
Arbres binaires de recherche optimaux : 901 ; 921 ; 931 ([CLRS10])
Arbre couvrant minimal : 925 ; 931 ([CLRS10])
Union Find : 901 ; 921 ; 926 ([CLRS10, p.519])
Cocke-Younger-Kasami : 907 ; 915 ; 923 ; 931 (ici)
Plus longue sous séquence commune : 907 ; 931 ([CLRS10])
Alignement optimal : 907 ; 931 ([CHL01, p.224])
Knuth Morris Pratt (Complexité) : 907 ; 921 ; 926 (ici)
Knuth Morris Pratt (Correction) : 907 ; 921 ; 927 ([CLRS10])
Automate des occurrences : 907 ; 909 (ici)
Théorème de Kleene : 909 ([SAK17])
Algorithme de Hopcroft : 907 ; 927 ; 931 ([BBC92], [CAR14])
Décidabilité de Presburger : 909 ; 914 ; 924 (ici)
Algorithme de l'unificateur principal : 924 ; 927 ([DNR04])
Théorème de Lowenheim-Skolem : 924 ([DNR04], [CL03])
Théorie des ordres denses : 924 ([DNR04])
Complétude de la déduction naturelle pour le premier ordre : 918 ; 924 ([DNR04, p.83])
Complétude de la résolution pour le calcul propositionnel : 916 ([CL03])
Compacité de la logique propositionnelle : 916 ([LMLBP20, p.807])
2Sat $\in$ P : 915 ; 916 ([CAR14], [LMLBP20, p.802])
Complexité du langage des palindromes : 913 ([LMLBP20, p.683])
Transformation de Tseitin : 916 (ici)
Théorème de Cook : 913 ; 915 ; 916 ; 928 (ici)
Problème de séparation par automate : 909 ; 915 ; 928 ([LMLBP20, p.768])
Théorème de Rice : 913 ; 914 ([WOL06])
Problème d'universalité d'un automate : 909 ; 915 ([LMLBP20, p.774])
3-Coloration d'un graphe : 915 ; 925 ; 928 (ici)
Polynôme chromatique : 190 ; 925 ([LMLBP20, p.717])
Formule d'Euler par déchargement : 190 ; 925 ([LMLBP20, p.731])
Séquençage ADN et graphe de De Bruijn : 901 ; 907 ; 925 ([LMLBP20, p.747])
Théorème de Turan : 190 ; 264 ; 925 ([LMLBP20, p.724])
Algorithme de Bellman Ford : 925 ; 931 ([CLRS10])
Algorithme de Floyd-Warshall : 925 ; 926 ; 927 ([CLRS10])
Algorithme de Dijkstra : 901 ; 925 ; 926 ; 927 ; 931 ([CLRS10, p.609])
NP-complétude du chemin hamiltonien : 915 ; 925 ; 928 ([CAR14])
Problème du voyageur de commerce euclidien : 915 ; 925 ; 928 ([LMLBP20, p.738])
Problème de Steiner métrique : 925 ; 928 ([VAZ10])
Indécidabilité de la validité d'une formule du premier ordre : 914 ; 924 (ici)
Indécidabilité de la satisfiabilité d'une requête : 914 ; 932 (ici)
Indécidabilité de quelques problèmes sur les grammaires algébriques : 914 ([CAR14])
Caractérisation de RE : 912 ; 913 ; 914 (ici)
Théorème de Savitch : 913 ; 915 ; 931 ([SIP12, p.335])

NL = co-NL : 915 ; 925 ([SIP12])
Fonction d'Ackermann n'est pas primitive récursive : 912 ([CL03], [WOL06])
Machine de Turing $\Longrightarrow$ μ-recursif : 912 ; 913 (ici)
μ-recursif $\Longrightarrow$ λ-définissable : 912 ; 929 (ici)
Théorème de Scott–Curry : 929 (ici)
Équivalence entre sémantiques opérationnelles : 930 (ici)
Équivalence entre sémantiques opérationnelle et dénotationnelle : 930 ([NN07])
Complétude de la logique de Hoare : 927 ; 930 ([NN07])
Correction de *Factorielle(n)* par la logique de Hoare : 927 ; 930 ([WIN93, p.93])
Caractérisation de Premier pour l'analyse $LL(1)$: 923 (ici)

CHAPITRE 4

MON MÉMOIRE SUR LA LEÇON 223

J'ai effectué mon mémoire sur la leçon 223 : *Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.* J'ai rédigé mon mémoire entre octobre et novembre. Mon plan a ensuite changé comme on peut le voir dans le métaplan **223**. Voici mon mémoire :

Introduction

Les suites numériques sont un outil très utile pour comprendre comment évolue l'itération d'un résultat ou d'une donnée. La notion d'itération est déjà utilisée dans l'Antiquité par Archimède pour approcher la valeur de π. Pour cela, il calculait le périmètre de polygones inscrit et circonscrit dans le cercle, il obtenait alors deux suites de valeurs qui tendaient vraisemblablement vers π. Cette approche reste empirique et non formelle par rapport à ce que l'on utilise de nos jours.

En effet, c'est au XIXème siècle que Gauss et Cauchy définissent rigoureusement la notion de suite, de limite et de convergence (notamment convergence des suites dites de Cauchy).

Les suites sont utilisées notamment dans un cadre topologique, puisque lorsqu'on est dans un cadre métrique, on peut caractériser des propriétés comme la continuité ou la compacité par des suites. On retrouve aussi la notion de suites en analyse, puisque l'on définit même la convergence de fonctions qui se ramène à des suites dans $\mathbb{R}$ pour des normes bien choisies. Cependant ce n'est pas à proprement parler des suites numériques donc cela ne fera pas l'objet de cette leçon. On utilise aussi des suites pour définir l'intégrale de Riemann (la méthode des rectangles, la méthode de Simpson, ...)

Depuis plus d'un siècle, les suites sont utilisées aussi dans l'analyse numérique, notamment pour approcher des zéros de fonctions (dichotomie, méthode de Newton, méthode de la sécante, ...) mais aussi pour approcher des fonctions solutions d'équations différentielles (schéma d'Euler explicite et implicite, méthode de Runge-Kutta (ordre 4), ...).

I. Convergence

Sauf précision contraire, les suites considérées sont à valeurs dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Certains résultats sont vrais juste en prenant un espace métrique, mais le titre de la leçon étant "suites numériques", nous avons préféré présenter les résultats de manière concrète dans $\mathbb{R}$ et $\mathbb{C}$ qui sont deux corps que l'on maîtrise mieux que des espaces métriques abstraits.

Définition 1 (Convergence)**.**

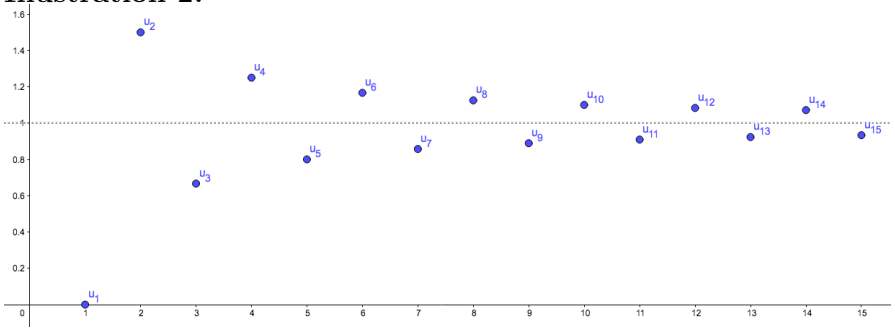
— Une suite réelle $(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ est dite convergente vers $l \in \mathbb{R}$ si :

$$\forall \varepsilon > 0,\ \exists n_0 \in \mathbb{N} \ / \ \forall n \geqslant n_0,\ |u_n - l| < \varepsilon$$

— Une suite complexe $(z_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ est dite convergente vers $u+iv \in \mathbb{C}$ avec $(u,v) \in \mathbb{R}^2$ si :
  (i) $z_n = u_n + iv_n$ où (u_n) et (v_n) sont des suites réelles.
  (ii) (u_n) converge vers u.
  (iii) (v_n) converge vers v.

Quand une suite ne converge pas, on dit qu'elle diverge.

Illustration 2.



Convergence de la suite $\left(u_n = 1 + \frac{(-1)^n}{n}\right)_{n\in\mathbb{N}^*}$ vers 1.

Exemple 3.

— $\left(u_n = \frac{1}{n}\right)_{n\in\mathbb{N}^*}$ converge vers 0.

— $(z_n = n + i\frac{1}{n})_{n\in\mathbb{N}}$ ne converge pas car la partie réelle $(n)_{n\in\mathbb{N}}$ diverge.

Proposition 4. Soit $(u_n)_{n\in\mathbb{N}}$ qui converge vers $l \in \mathbb{K}$ et soit une fonction $f : \mathbb{K} \to \mathbb{K}$ continue en l, alors la suite $(f(u_n))_{n\in\mathbb{N}}$ converge vers $f(l)$.

Exemple 5. Pour $\left(u_n = \frac{1}{n}\right)_{n\in\mathbb{N}^*}$ et $f : x \mapsto x^2$ qui est continue en zéro, on a $\left(f(u_n) = \frac{1}{n^2}\right)_{n\in\mathbb{N}^*}$ qui converge vers $f(0) = 0$.

Proposition 6. Soient deux suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ qui convergent respectivement vers l et l' et λ un élément de $\mathbb{K}$. On a les propriétés suivantes :

(i) $(u_n + v_n)_{n\in\mathbb{N}}$ converge vers $l + l'$

(ii) $(u_n v_n)_{n\in\mathbb{N}}$ converge vers ll'

(iii) $(\lambda u_n)_{n\in\mathbb{N}}$ converge vers λl

(iv) Si $l \neq 0$ alors $\left(\frac{1}{u_n}\right)_{n\in\mathbb{N}}$ converge vers $\frac{1}{l}$, on a $\left(\frac{1}{u_n}\right)_{n\in\mathbb{N}}$ bien définie à partir d'un certain rang.

Remarque 7. L'espace des suites convergentes dans $\mathbb{K}$ est donc un espace vectoriel sur $\mathbb{K}$

Définition 8 (Monotonie)**.** Une suite réelle $(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ est croissante si, pour tout $n \in \mathbb{N}$, $u_{n+1} - u_n$ est positif ou nul. Elle est décroissante si, pour tout $n \in \mathbb{N}$, $u_{n+1} - u_n$ est négatif ou nul. Si la suite est croissante ou décroissante, on dit qu'elle est monotone.

Définition 9 (Borné)**.** Une suite $(u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ est bornée s'il existe $M \geqslant 0$ tel que pour tout $n \in N$, $|u_n| \leqslant M$.

Exemple 10.

— $(u_n = n)_{n\in\mathbb{N}}$ est monotone (croissante), non-bornée.

— $(u_n = (-1)^n)_{n\in\mathbb{N}}$ est bornée, non monotone.

Proposition 11. Une suite réelle monotone bornée est convergente.

Théorème 12 (des gendarmes)**.** Soient $(u_n), (v_n), (w_n)$ trois suites réelles, avec (u_n) et (w_n) qui convergent vers la même limite $l \in \mathbb{R}$. S'il existe un rang n_0 tel que pour tout $n \geqslant n_0$, on ait $u_n \leqslant v_n \leqslant w_n$, alors (v_n) converge vers l.

Preuve. Soit $\varepsilon > 0$, il existe $n_u \in \mathbb{N}$ tel que pour tout $n \geqslant n_u$, $-\varepsilon < u_n - l < \varepsilon$ et il existe $n_w \in \mathbb{N}$ tel que pour tout $n \geqslant n_w$, $-\varepsilon < w_n - l < \varepsilon$. Ainsi en posant $N = \max(n_0, n_u, n_w)$, pour tout $n \geqslant N$, on a $-\varepsilon < u_n - l \leqslant v_n - l \leqslant w_n - l < \varepsilon$, donc $|v_n - l| < \varepsilon$. Ainsi (v_n) converge vers l.

□

Lorsque l'on a une suite qui converge vers une limite l, on observe que ses termes se rapprochent de cette limite et donc qu'ils se rapprochent entre eux. On peut alors se demander si une suite dont la différence des termes va tendre vers 0 converge bien dans l'espace que l'on étudie.

Définition 13 (Suite de Cauchy)**.** La suite $(u_n)_{n\in\mathbb{N}}$ est de Cauchy dans $\mathbb{K}$ si

$$\forall \varepsilon > 0,\ \exists n_0 \in \mathbb{N} \ / \ \forall n, p \geqslant n_0,\ |u_n - u_p| < \varepsilon$$

Proposition 14. Toute suite de Cauchy dans $\mathbb{K}$ converge.

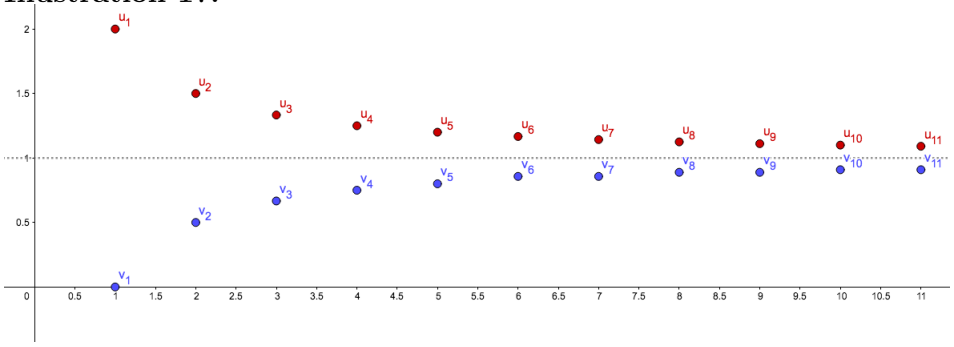
Définition 15 (Suites adjacentes)**.** Soient (u_n), (v_n) deux suites réelles. On dit qu'elles sont adjacentes si :

(i) (u_n) et (v_n) sont monotones de monotonies opposées,

(ii) $(|u_n - v_n|)_{n\in\mathbb{N}}$ converge vers 0.

Exemple 16. Les suites $(u_n = 1 + \frac{1}{n})_{n\in\mathbb{N}^*}$ et $(v_n = 1 - \frac{1}{n})_{n\in\mathbb{N}^*}$ sont adjacentes.

Illustration 17.



Proposition 18. Deux suites adjacentes convergent vers la même limite.

Application 19. Critère spécial des séries alternées : Pour une suite $(u_n)_{n\in\mathbb{N}}$ réelle décroissante vers 0, la série $\sum_{n\geqslant 0}(-1)^n u_n$ converge.

Preuve. On pose $S_N = \sum_{n=0}^{N}(-1)^n u_n$. Montrons que les suites $(S_{2N})_{N\in\mathbb{N}}$ et $(S_{2N+1})_{N\in\mathbb{N}}$ sont adjacentes.

D'une part, pour tout $N \in \mathbb{N}$,

$$S_{2N+2} - S_{2N} = (-1)^{2N+2}u_{2N+2} + (-1)^{2N+1}u_{2N+1} = u_{2N+2} - u_{2N+1} \leqslant 0$$

car la suite (u_n) est décroissante. Donc la suite $(S_{2N})_{N\in\mathbb{N}}$ est décroissante aussi.

D'autre part, pour tout $N \in \mathbb{N}^*$,

$$S_{2N+1} - S_{2N-1} = (-1)^{2N+1}u_{2N+1} + (-1)^{2N}u_{2N} = -u_{2N+1} + u_{2N} \geqslant 0$$

car la suite (u_n) est décroissante. Donc la suite $(S_{2N+1})_{N\in\mathbb{N}}$ est croissante. De plus, pour tout $N \in \mathbb{N}$, $|S_{2N+1} - S_{2N}| = |u_{2N+1}|$ tend vers 0 par hypothèse. Donc les suites $(S_{2N})_{N\in\mathbb{N}}$ et $(S_{2N+1})_{N\in\mathbb{N}}$ sont bien adjacentes.

Ainsi par la propriété 18, les suites $(S_{2N})_{N\in\mathbb{N}}$ et $(S_{2N+1})_{N\in\mathbb{N}}$ convergent vers la même limite l. Montrons que la suite (S_N) converge aussi vers l.
Soit $\varepsilon > 0$, il existe $n_0 \geqslant 0$ tel que si $2N \geqslant n_0$ alors $|S_{2N} - l| < \varepsilon$ et il existe $n_1 \geqslant 0$ tel que si $2N + 1 \geqslant n_1$ alors $|S_{2N+1} - l| < \varepsilon$. Pour $\tilde{n} = \max(n_0, n_1)$, on a, pour tout $n \geqslant \tilde{n}$, l'inégalité $|S_n - l| < \varepsilon$.

Donc (S_N) converge vers l. □

Deux suites peuvent converger vers la même limite, sans pour autant y converger de la même manière, par exemple les suites $(\frac{1}{n})$ et (e^{-n}) convergent toutes les deux vers 0 mais (e^{-n}) tend vers 0 beaucoup plus rapidement, on voudrait donc caractériser cette notion de vitesse de convergence et d'équivalence de convergence pour des suites qui convergeraient à la même vitesse (et évidemment vers la même limite).

Définition 20 (Équivalence de suites)**.** Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites. On dit que $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont équivalentes en $+\infty$ si la suite $\left(\frac{u_n}{v_n}\right)$ converge vers 1, on note $u_n \underset{n\to+\infty}{\sim} v_n$.

Exemple 21. $\frac{1}{n + (-1)^n} \underset{n\to+\infty}{\sim} \frac{1}{n}$

II. Valeurs d'adhérence

On a étudié les suites qui convergent vers une limite l, cette limite est unique comme on l'a énoncé plus haut, mais on pourrait essayer de trouver des outils pour analyser les comportements de suites qui ne convergent pas mais dont il existe des valeurs qui reviennent "souvent" dans la suite, comme par exemple la suite $((-1)^n)_{n\in\mathbb{N}}$ dont les valeurs 1 et -1 reviennent infiniment souvent.

Définition 22 (Borne supérieure/Borne inférieure)**.** Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle.

- On appelle borne supérieure de $(u_n)_{n\in\mathbb{N}}$ le plus petit de ses majorants. Si la suite n'est pas majoré, on dit que sa borne supérieure est $+\infty$. De plus, on la note $\sup_{n\in\mathbb{N}}(u_n) \in \mathbb{R} \cup \{+\infty\}$.
- On appelle borne inférieure de $(u_n)_{n\in\mathbb{N}}$ le plus grand de ses minorants. Si la suite n'est pas minoré, on dit que sa borne inférieure est $-\infty$. De plus, on la note $\inf_{n\in\mathbb{N}}(u_n) \in \mathbb{R} \cup \{-\infty\}$.

Exemple 23. $\sup_{n\in\mathbb{N}}(n) = +\infty$; $\inf_{n\in\mathbb{N}}((-1)^n) = -1$

Définition 24 (Limite supérieure/Limite inférieure)**.** Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle.

- $\limsup_{n_\infty}(u_n) \overset{\text{def}}{=} \inf_{n\in N} \sup_{k\geqslant n}(u_k) \in \mathbb{R} \cup \{\pm\infty\}$
- $\liminf_{n_\infty}(u_n) \overset{\text{def}}{=} \sup_{n\in N} \inf_{k\geqslant n}(u_k) \in \mathbb{R} \cup \{\pm\infty\}$

Exemple 25. Pour $(u_n = (-1)^n)$, on a $\limsup_{n_\infty}(u_n) = 1$ et $\liminf_{n_\infty}(u_n) = -1$.

Proposition 26. Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle.
Alors on a l'inégalité $\liminf_{n_\infty}(u_n) \leqslant \limsup_{n_\infty}(u_n)$ et l'égalité caractérise la convergence.

Application 27. On utilise cette notation pour énoncer le critère d'Hadamard pour les séries entières : $\dfrac{1}{R} = \limsup_{n_\infty}(|a_n|^{1/n})$ où R est le rayon de convergence de la série $\sum a_n z^n$.

Définition 28 (Sous-suite)**.** Soit $(u_n)_{n\in\mathbb{N}}$ une suite dans $\mathbb{K}$. On appelle sous-suite de $(u_n)_{n\in\mathbb{N}}$ les suites $(u_{\varphi(n)})_{n\in\mathbb{N}}$ pour $\varphi : \mathbb{N} \to \mathbb{N}$ fonction strictement croissante.

Exemple 29. La suite (u_{2n}) est une sous-suite de (u_n).

Définition 30 (Valeur d'adhérence)**.** Soit $(u_n)_{n\in\mathbb{N}}$ une suite dans $\mathbb{K}$. On dit que $\alpha \in \mathbb{K}$ est une valeur d'adhérence de (u_n), s'il existe une sous suite $u_{\varphi(n)}$ qui converge vers α. On note $\mathrm{Adh}(u_n)$ l'ensemble des valeurs d'adhérence de (u_n).

Exemple 31. $\mathrm{Adh}((-1)^n) = \{-1,\ 1\}$; $\mathrm{Adh}((e^{ik})_{k\in\mathbb{Z}}) = \mathbb{U} = \{z \in \mathbb{C}/|z| = 1\}$.

Preuve du deuxième exemple. Tous les éléments de (e^{ik}) sont de module 1 donc $\mathrm{Adh}(e^{ik}) \subset \mathbb{U}$, car pour toute sous-suite convergente de (e^{ik}), le module de la limite sera 1.

De plus, $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$, car $\mathbb{Z} + 2\pi\mathbb{Z}$ est un sous groupe additif de $\mathbb{R}$ donc il est soit dense dans $\mathbb{R}$ soit de la forme $r\mathbb{Z}$ avec $r \in \mathbb{R}$. On suppose que $\mathbb{Z} + 2\pi\mathbb{Z}$ est de la forme $r\mathbb{Z}$. Or $1 \in \mathbb{Z} + 2\pi\mathbb{Z}$ et $2\pi \in \mathbb{Z} + 2\pi\mathbb{Z}$ donc on peut écrire $1 = rk$ et $2\pi = rk'$ avec $k,\ k' \in \mathbb{Z}$. D'où $\frac{2\pi}{1} = \frac{rk'}{rk} = \frac{k'}{k} \in \mathbb{Q}$, ce qui est absurde car 2π n'appartient pas à $\mathbb{Q}$. Donc $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$. Soit $e^{i\alpha} \in \mathbb{U}$ et $\varepsilon > 0$ avec $\alpha \in \mathbb{R}$, la fonction $f : \alpha \in \mathbb{R} \mapsto \exp(i\alpha)$ est continue donc il existe $\eta > 0$ tel que pour tout y tel que $|y - \alpha| < \eta$ on ait $|f(\alpha) - f(y)| < \varepsilon$. Par densité, on peut trouver un élément $u + 2\pi v \in \mathbb{Z} + 2\pi\mathbb{Z}$ tel que $|\alpha - (u + 2\pi v)| < \eta$. Ainsi on a $|e^{i\alpha} - e^{i(u+2\pi v)}| < \varepsilon$. Or $e^{i(u+2\pi v)} = e^{iu}$, donc on a prouver que $\mathrm{Adh}((e^{ik})_{k\in\mathbb{Z}}) = \mathbb{U}$. □

Proposition 32. Soit $(u_n)_{n\in\mathbb{N}}$ une suite dans $\mathbb{K}$. Alors $\mathrm{Adh}(u_n) = \bigcap_{n\in\mathbb{N}} \overline{\{u_k, k \geqslant n\}}$.

Proposition 33. Soit $(u_n)_{n\in\mathbb{N}}$ une suite dans $\mathbb{K}$. Alors l'ensemble $\mathrm{Adh}(u_n)$ est un fermé de $\mathbb{K}$.

Proposition 34. Soit $(u_n)_{n\in\mathbb{N}}$ une suite dans $\mathbb{K}$. Si (u_n) converge vers l, alors $\mathrm{Adh}(u_n) = \{l\}$.

Remarque 35. La réciproque est vraie pour une suite (u_n) bornée.

Contre-exemple 36. Soit la suite $(u_n = n(1 + (-1)^n))$, (u_n) ne converge pas car $u_n = 2n$ pour n pair et $u_n = 0$ pour n impair, pourtant on a $\mathrm{Adh}(u_n) = \{0\}$.

Théorème 37 (Bolzano–Weierstrass)**.** De toute suite bornée de $\mathbb{K}$, on peut extraire une sous-suite convergente.

Application 38. Principe des compacts décroissants : toute suite $(K_n)_{n\in\mathbb{N}}$ de compacts décroissante pour l'inclusion donc le diamètre des compacts tend vers 0 est d'intersection réduite à un seul élément, i.e. il existe un élément α tel que $\bigcap_{n\in\mathbb{N}} K_n = \{\alpha\}$.

Preuve. Soit une suite $(K_n)_{n\in\mathbb{N}}$ de compacts telle que pour tout $n \in \mathbb{N}$, $K_{n+1} \subset K_n$ avec $(\mathrm{diam}(K_n))$ qui tend vers 0. On veut prouver qu'il existe un unique α tel que $\bigcap_{n=0}^{\infty} K_n = \{\alpha\}$. Soit une suite d'élément (x_n) telle que pour tout $n \in \mathbb{N}$, $x_n \in K_n$. La suite (x_n) est bornée car elle est dans le compact K_0, ainsi par le théorème de Bolzano–Weierstrass, il existe une sous-suite qui converge vers un élément α qui appartient à chaque compact K_n, car à partir d'un certain rang, la suite (x_n) reste dans K_n pour tout $n \in \mathbb{N}$, grâce à l'hypothèse d'inclusion décroissante. Donc il

existe au moins un élément α dans $\bigcap_{n=0}^{\infty} K_n$. De plus, si on avait deux éléments $a < b$ dans $\bigcap_{n=0}^{\infty} K_n$ (i.e. pour tout $n \in \mathbb{N}$, on a a et b dans K_n), le diamètre des K_n serait au moins $|b-a|$, ce qui contredit l'hypothèse de décroissance vers 0 des diamètres des K_n. Ainsi il y a un unique élément dans $\bigcap_{n=0}^{\infty} K_n$. □

III. Diverses applications

Il peut être interessant de classifier certaines suites pour se ramener à des suites déjà étudiées dont on connait bien le comportement, notamment les suites récurrentes que l'on peut étudier au travers de la fonction f qui les définit.

Définition 39 (Suites récurrentes d'ordre 1)**.** Soient $f : \mathbb{K} \to \mathbb{K}$ une fonction et $x_0 \in \mathbb{K}$. La suite définie par

$$\begin{cases} u_0 = x_0 \\ u_{n+1} = f(u_n) \quad \forall n \in \mathbb{N}^* \end{cases}$$

est une suite récurrente d'ordre 1.

Remarque 40. Dorénavant, on fera l'abus de parler de suites récurrentes pour désigner les suites récurrentes d'ordre 1.

Exemple 41.

- Les suites arithmétiques définies par $u_{n+1} = u_n + a$ pour un certain $a \in \mathbb{K}$ sont des suites récurrentes avec $f(x) = x + a$. On peut les écrire $u_n = u_0 + na$ pour tout $n \in \mathbb{N}$.
- Les suites géométriques définies par $u_{n+1} = q.u_n$ pour un certain $q \in \mathbb{K}$ sont des suites récurrentes avec $f(x) = qx$. On peut les écrire $u_n = u_0.q^n$ pour tout $n \in \mathbb{N}$. Ainsi si $|q| < 1$, alors (u_n) converge vers 0.

Proposition 42. Soit $(u_n)_{n\in\mathbb{N}}$ une suite récurrente de fonction f dans $\mathbb{K}$. Si (u_n) converge vers une limite $l \in \mathbb{K}$ et si f est continue en l, alors l est un point fixe de f, i.e. $f(l) = l$.

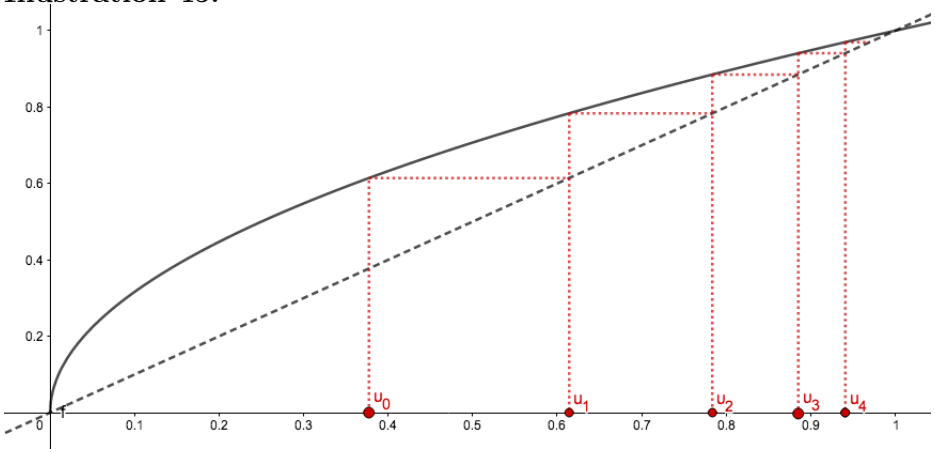
Proposition 43. Soit $(u_n)_{n\in\mathbb{N}}$ une suite récurrente de fonction f dans $\mathbb{K}$. On suppose que $u_0 \in I$ avec I un intervalle stable de f.

(i) Si f est croissante, alors (u_n) est monotone.

(ii) Si f est décroissante, alors (u_{2n}) et (u_{2n+1}) sont monotones, de monotonies opposées.

Exemple 44. Pour $f : x \mapsto \sqrt{x}$ et $I = [0, 1]$, on a (u_n), suite récurrente de premier terme $u_0 = x_0 \in I$, qui converge vers 1.

Illustration 45.



Application 46 (Méthode de Newton)**.** (DEV 1) Soit $f \in \mathcal{C}^2(I, \mathbb{R})$, on suppose qu'il existe $a \in \overset{\circ}{I}$ tel que $f(a) = 0$ et $f'(a) \neq 0$.

(i) Pour u_0 assez proche de a, la suite définie par $u_{n+1} = g(u_n) = u_n - \dfrac{f(u_n)}{f'(u_n)}$ converge vers a de manière quadratique.

(ii) Si on suppose, de plus, que f est convexe sur I et $f'(a) > 0$, alors le résultat précédent est vrai pour tout $u_0 \in I \cap [a, +\infty[$.

Application 47. Le théorème de point fixe de Picard utilise une suite récurrente (u_n) pour une fonction f contractante et on a le résultat $|u_n - l| \leqslant \dfrac{k^n}{1-k}|u_1 - u_0|$ pour tout $n \in \mathbb{N}$ avec k la constante de Lipschitz de f et l la limite de (u_n) qui est l'unique point fixe de f.

IV. Convergence au sens de Césaro

On a étudié les suites convergentes avec la définition de convergence que l'on a donné dans la définition 1 mais on pourrait imaginer une définition plus large que celle de la convergence classique. C'est le cas de la convergence au sens de Césaro, qui va faire converger la suite $((-1)^n)$ par exemple. Il faut s'assurer que la convergence "classique" entraine notre nouvelle notion de convergence, pour être sûr qu'elle est bien plus large que la convergence "classique"

Théorème 48 (Césaro)**.** Soit $(u_n)_{n\in\mathbb{N}^*}$ une suite dans $\mathbb{K}$. Si (u_n) converge vers $l \in \mathbb{K}$, alors $\left(\sigma_n = \dfrac{1}{n}\sum_{k=1}^{n} u_k\right)_{n\in\mathbb{N}^*}$ converge aussi vers l.

Preuve. Soit $\varepsilon > 0$. La suite (u_n) converge vers l, donc il existe n_0 tel que pour tout $n \geqslant n_0$, $|u_n - l| < \varepsilon$. On pose $B = \sum_{k=1}^{n_0} |u_k - l|$, il existe $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, on ait $\dfrac{B}{n} < \varepsilon$.

Pour tout $n \geqslant \max(n_0, N)$, $|\sigma_n - l| = \left|\dfrac{1}{n}\sum_{k=1}^{n}(u_k - l)\right| \leqslant \dfrac{1}{n}\sum_{k=1}^{n}|u_k - l| \leqslant \dfrac{1}{n}\sum_{k=1}^{n_0}|u_k - l| + \dfrac{1}{n}\sum_{k=n_0+1}^{n}|u_k - l| \leqslant \dfrac{B}{n} + \dfrac{1}{n}\sum_{k=n_0+1}^{n}\varepsilon \leqslant \varepsilon + \dfrac{n-n_0}{n}\varepsilon \leqslant 2\varepsilon$.

Donc la suite (σ_n) converge aussi vers la limite l. □

Remarque 49. Le résultat est vrai aussi pour $l = \pm\infty$ (on en donnera une démonstration dans le deuxième développement).

Contre-exemple 50. La suite $(u_n = (-1)^n)_{n\in\mathbb{N}^*}$ ne converge pas et pourtant on a $|\sigma_n| = \left|\dfrac{1}{n}\sum_{k=1}^{n}(-1)^k\right| \leqslant \dfrac{1}{n}$ (terme de suite qui converge vers 0) donc (σ_n) converge vers 0, ce qui prouve que la réciproque est fausse.

Théorème 51 (Réciproque partielle de Césaro)**.** (DEV 2) Soit $(u_n)_{n\in\mathbb{N}^*}$ une suite dans $\mathbb{K}$ telle que $\left(\sigma_n = \dfrac{1}{n}\sum_{k=1}^{n} u_k\right)_{n\in\mathbb{N}^*}$ converge vers $l \in \mathbb{K}$.

(i) Si (u_n) est réelle monotone, alors (u_n) converge vers l.

(ii) Si $u_n - u_{n-1} = O(\dfrac{1}{n})$ (i.e. il existe $A \geqslant 0$ telle que $|u_n - u_{n-1}| \leqslant \dfrac{A}{n}$ pour tout $n \in \mathbb{N}^*$), alors (u_n) converge vers l.

Application 52. Soit $(u_n)_{n\in\mathbb{N}^*}$ une suite réelle strictement positive telle que $\frac{u_{n+1}}{u_n}$ converge vers l. Alors, par le théorème de Césaro, on trouve que la suite $(\sqrt[n]{u_n})_{n\in\mathbb{N}^*}$ converge vers l.

Preuve. On pose la suite $v_n = \ln\left(\frac{u_{n+1}}{u_n}\right)$, on a (v_n) qui converge vers $\ln(l)$ si $l \neq 0$ ou vers $-\infty$ si $l = 0$. On fera l'abus de dire que $\ln(0) = -\infty$. Grâce à la Remarque 49, on peut appliquer le théorème de Césaro à la suite (v_n). Ainsi on a la convergence de $\left(\sigma_n = \frac{1}{n}\sum_{k=0}^{n-1} v_k\right)_{n\in\mathbb{N}^*}$ vers $\ln(l)$ (le théorème de Césaro peut s'énoncer avec la somme allant de 0 à $n-1$ pour les suites indexées sur tout $\mathbb{N}$). Or $\sigma_n = \frac{1}{n}\sum_{k=0}^{n-1} \ln\left(\frac{u_{k+1}}{u_k}\right) = \frac{1}{n}\sum_{k=0}^{n-1}(\ln u_{k+1} - \ln u_k) = \frac{1}{n}(\ln u_n - \ln u_0)$. De plus, $\left(\frac{\ln u_0}{n}\right)$ converge vers 0, donc $\left(\frac{ln u_n}{n}\right)$ converge vers $\ln(l)$. On remarque que $\frac{\ln(u_n)}{n} = \ln(\sqrt[n]{u_n})$. En passant à l'exponentielle, on a $(\exp(\ln(\sqrt[n]{u_n})))$ converge vers $\exp(\ln(l))$. Donc la suite $(\sqrt[n]{u_n})_{n\in\mathbb{N}^*}$ converge vers l. □

Application 53. Régularisation du noyau de Dirichlet :

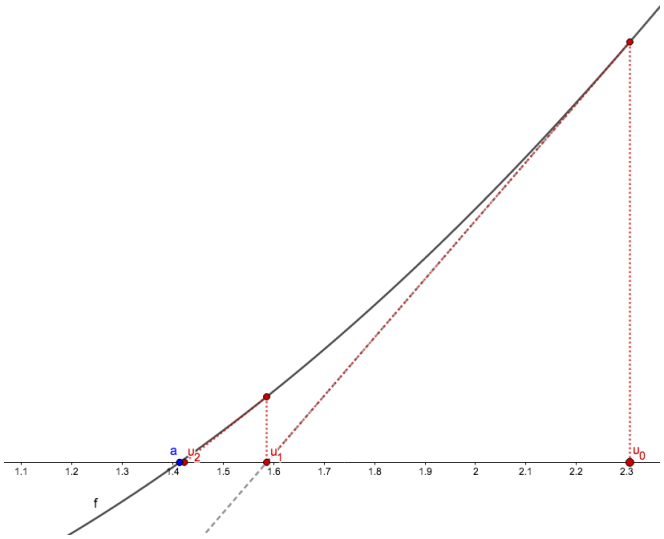
- $\|D_N\|_{L^1}$ diverge vers $+\infty$ alors que $\|K_N\|_{L^1} = 1$ pour tout $N \in \mathbb{N}$ (K_N étant le noyau de Fejer, c'est-à-dire la moyenne de Césaro du noyau de Dirichlet D_N)
- Si $f \in \mathcal{C}^0_{2\pi}$ et que sa série de Fourier converge simplement, alors on peut écrire $f(t) = \sum_{n\in\mathbb{Z}} c_n(f)e^{int}$.

Développement 1 : La méthode de Newton

Lorsque l'on étudie une fonction f, il est naturel de se demander quand est ce que cette fonction s'annule. Parfois, de trouver les zéros explicites d'une fonction est extrêmement difficile voire impossible, on peut alors vouloir approcher des zéros de f. La méthode de Newton est pour cela un bon outil pour avoir une convergence relativement rapide vers un zéro de notre fonction, il faut évidemment se placer dans un bon cadre d'hypothèses pour assurer cette convergence. Dans ce développement, nous nous placerons dans deux cadres différents, un premier qui nécessite d'être assez proche du zéro à approcher et un deuxième qui nous permet de nous affranchir de cette contrainte mais en imposant des hypothèses plus fortes sur la fonction à étudier.

Théorème 1 (Méthode de Newton)**.** (Référence [ROM04]) Soit $f \in \mathcal{C}^2(I, \mathbb{R})$, on suppose qu'il existe $a \in \overset{\circ}{I}$ tel que $f(a) = 0$ et $f'(a) \neq 0$.
Pour u_0 assez proche de a, la suite définie par $u_{n+1} = g(u_n) = u_n - \frac{f(u_n)}{f'(u_n)}$ converge vers a de manière quadratique.

Preuve. Commençons par illustrer le théorème :



Approximation de $\sqrt{2}$ par la méthode de Newton sur $f(x) = x^2 - 2$ avec $u_0 = 2.3$.

Quitte à multiplier f par -1, on peut supposer que $f'(a) > 0$.

Ainsi comme f' est continue, il existe un $\alpha > 0$ tel que f' soit strictement positive sur $J :=]a - \alpha; a + \alpha[\subset I$.

Soit $x \in J$, $|g(x) - a| = \left|x - \dfrac{f(x)}{f'(x)} - a\right| = \left|\dfrac{f(a) - f(x) - (a-x)f'(x)}{f'(x)}\right|$ car $f(a) = 0$.

On utilise Taylor–Lagrange pour avoir un élément $e \in]a, x[$ tel que $f(a) - f(x) - (a-x)f'(x) = \frac{1}{2}f''(e)(a-x)^2$.

Ainsi on a $|g(x) - a| = \dfrac{f''(e)(a-x)^2}{2f'(x)} \leqslant C(x-a)^2$ où on définit C par $C := \dfrac{\sup\limits_J |f''|}{2\inf\limits_J |f'|}$, elle est bien définie car f' et f'' sont continues sur J et sur $\bar{J}$, $f' > 0$.

Quitte à réduire α, on peut supposer que $\alpha < \frac{1}{C}$.

Ainsi pour $x \in J$, $|g(x) - a| < C.\frac{1}{C}\alpha \leqslant \alpha$.

Donc pour $u_0 \in J$, la suite récurrente (u_n) est bien définie. Il faut prouver que (u_n) converge vers a de façon quadratique : pour tout $n \in \mathbb{N}$,
$C|u_{n+1} - a| \leqslant C^2|u_n - a|^2 \leqslant C^4|u_{n-1} - a|^4 \leqslant \cdots \leqslant (C|u_0 - a|)^{(2^n)} \leqslant (C\alpha)^{(2^n)}$.

Or $C\alpha < 1$ donc (u_n) converge vers a car $(C\alpha)^{2^n}$ tend vers 0 quand n tend vers $+\infty$ et de manière quadratique car $|u_{n+1} - a| \leqslant C|u_n - a|^2$ pour tout $n \in \mathbb{N}^*$. □

Théorème 2. Sous les hypothèses du théorème précédent, si on suppose, de plus, que f est convexe sur I et que $f'(a) > 0$, alors le résultat précédent est vrai pour tout $u_0 \in I \cap [a, +\infty[$.

Preuve. Comme f est convexe, f' est croissante, donc puisque $f'(a) > 0$, on a f' positive à droite de a qui implique que f est positive à droite de a.

Soit d la borne supérieure de l'intervalle I. On veut prouver que :

$$a \leqslant g(x) \leqslant x \leqslant d \text{ pour tout } x \in [a, d].$$

Soit $x \in [a, d]$, $x - g(x) = x - x + \dfrac{f(x)}{f'(x)} = \dfrac{f(x)}{f'(x)} \geqslant 0$ car f et f' sont positives à droite de a. D'où $g(x) \leqslant x$.

Soit $x \in [a, d]$, $g(x) - a = x - a - \dfrac{f(x)}{f'(x)} = \dfrac{f''(e)}{2f'(x)}(x-a)^2 \geqslant 0$ par Taylor–Lagrange sur l'intervalle $]x, a[$ (Taylor–Lagrange reste valide même pour un intervalle de bornes décroissantes) et par convexité de f, on a f'' positive (et f' positive à droite de a). Donc $a \leqslant g(x)$.

Ainsi la suite (u_n), définie par récurrence pour $u_0 \in [a,d]$, est décroissante et minorée par a, donc converge vers un point fixe de g (Proposition 11 et Proposition 42). Or les points fixes de g sont les zéros de f et le seul zéro de f sur $[a,d]$ est a. Donc (u_n) converge vers a.

Pour le caractère quadratique, on utilise la même preuve que dans le théorème précédent, car comme (u_n) converge vers a, il existe un rang n_0 tel que pour tout $n \geqslant n_0$, $|u_n - a| < \alpha$ (α définie dans la preuve précédente). □

Développement 2 : Réciproque partielle du théorème de Césaro

On a vu que le théorème de Césaro pouvait s'utiliser pour prouver qu'une suite (v_n) converge. Il suffit de trouver une suite (u_n) qui converge et telle que (v_n) est la moyenne de Césaro de (u_n), de plus si on connait la limite de (u_n), on aura aussi la limite de (v_n). Cependant, on pourrait être intéressé par le phénomène réciproque, c'est à dire connaissant la convergence de la moyenne de Césaro d'une suite (u_n), on voudrait en déduire la convergence de la suite (u_n). Dans ce développement, nous nous placerons dans deux cadres où la réciproque est vraie, le cadre réel monotone et un cadre où l'on a une hypothèse asymptotique sur la proximité des termes successifs de notre suite.

Théorème 1 (Réciproque partielle de Césaro)**.** (Référence [FGN03]) Soit $(u_n)_{n\in\mathbb{N}^*}$ une suite dans $\mathbb{K}$ telle que $\left(\sigma_n = \dfrac{1}{n}\displaystyle\sum_{k=1}^{n} u_k\right)_{n\in\mathbb{N}^*}$ converge vers $l \in \mathbb{K}$.

(i) Si (u_n) est réelle monotone, alors (u_n) converge vers l.

(ii) Si $u_n - u_{n-1} = O(\dfrac{1}{n})$ (i.e. il existe $A \geqslant 0$ telle que $|u_n - u_{n-1}| \leqslant \dfrac{A}{n}$ pour tout $n \in \mathbb{N}^*$), alors (u_n) converge vers l.

Preuve.

(i) Pour (u_n) réelle monotone, on veut prouver l'équivalence :

$$(u_n) \text{ converge vers } l \iff (\sigma_n) \text{ converge vers } l$$

Pour le sens direct $\Longrightarrow$, cela vient du théorème de Césaro.
Pour le sens indirect $\Longleftarrow$, on raisonne par contraposée. Si (u_n) ne converge pas, alors (u_n) tend vers l'infini car (u_n) est supposée monotone. Quitte à prendre $(-u_n)$, on considère que (u_n) est croissante vers $+\infty$.

On va prouver que le théorème de Césaro peut être appliqué pour une limite infinie. Pour tout $A \geqslant 0$, il existe un rang n_0 telle que pour tout $n \geqslant n_0$, $u_n \geqslant A$. On pose la suite (v_n) définie par $v_n = \min(u_n, A)$. On a l'inégalité $v_n \leqslant u_n$ pour tout $n \in \mathbb{N}^*$. De ce fait, on a aussi $\dfrac{1}{n}\displaystyle\sum_{k=1}^{n} v_k \leqslant \dfrac{1}{n}\sum_{k=1}^{n} u_k$ pour tout $n \in \mathbb{N}^*$.

Or la suite (v_n) converge vers A, donc $\left(\dfrac{1}{n}\displaystyle\sum_{k=1}^{n} v_k\right)$ converge aussi vers A (par le théorème de Césaro).

Donc on a $A = \liminf \left(\dfrac{1}{n}\displaystyle\sum_{k=1}^{n} v_k\right) \leqslant \liminf \left(\dfrac{1}{n}\sum_{k=1}^{n} u_k\right) = \liminf \sigma_n$

Ainsi la suite (σ_n) diverge aussi vers $+\infty$.

(ii) On suppose que (σ_n) converge vers une limite l. L'idée va être de prouver que la moyenne des termes entre n et nx avec $x > 1$ converge aussi vers l et ensuite de rapprocher x de 1 pour n'avoir que le terme u_n dans la moyenne, ce qui va nous prouver que la suite (u_n) converge aussi vers l.

On pose, pour tout $t \geqslant 1$, $\sigma_t = \frac{1}{t}\sum_{1\leqslant k\leqslant t} u_k = \frac{E(t)}{t}\sigma_{E(t)}$ où $E(t)$ est la partie entière de t. De plus, $\sigma_{E(t)}$ tend vers l quand t tend vers $+\infty$, et $\frac{E(t)}{t}$ tend vers 1 quand t tend vers $+\infty$. Donc σ_t tend vers l quand t tend vers $+\infty$.

Pour $x > 1$, on pose $M_n(x) = \frac{1}{E(nx-n)}\sum_{n<k\leqslant nx} u_k = \frac{nx\sigma_{nx} - n\sigma_n}{E(n(x-1))} = \frac{n(x-1)}{E(n(x-1))}\frac{(x\sigma_{nx}-\sigma_n)}{(x-1)}$. Or $\frac{n(x-1)}{E(n(x-1))}$ tend vers 1 quand n tend vers $+\infty$ et σ_{nx} et σ_n tendent vers l quand n tend vers $+\infty$ par ce qui précède. Donc $M_n(x)$ tend vers $\frac{xl-l}{x-1} = l$ quand n tend vers $+\infty$.

On veut maintenant comparer le terme u_n avec $M_n(x)$. Or on peut écrire $u_n = \frac{1}{E(nx-n)}\sum_{n<k\leqslant nx} u_n$. Ainsi pour tout $n \in \mathbb{N}^*$,

$$|M_n(x) - u_n| = |\frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}(u_k - u_n)| \leqslant \frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}|u_k - u_n|$$

On va vouloir majorer $u_k - u_n$, on va utiliser l'hypothèse qui nous donne un $C \geqslant 0$ tel que pour tout $j \in \mathbb{N}^*$ on ait $|u_j - u_{j-1}| \leqslant \frac{C}{j}$.

Pour tout $k > n$, on a $|u_k - u_n| = |\sum_{j=n+1}^{k}(u_j - u_{j-1})| \leqslant \sum_{j=n+1}^{k}|u_j - u_{j-1}| \leqslant \sum_{j=n+1}^{k}\frac{C}{j} \leqslant \sum_{j=n+1}^{k}\int_{j-1}^{j}\frac{C}{t}dt \leqslant C\int_n^k \frac{1}{t}dt = C\ln\left(\frac{k}{n}\right)$ (par comparaison avec l'intégrale de $\frac{1}{t}$).

On reprend la majoration précédente,
$|M_n(x) - u_n| \leqslant \frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx}|u_k - u_n| \leqslant \frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx} C\ln\left(\frac{k}{n}\right) \leqslant \frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx} C\ln\left(\frac{nx}{n}\right) \leqslant \frac{1}{E(n(x-1))}\sum_{n<k\leqslant nx} C\ln(x) \leqslant C\ln(x)$. On obtient une majoration indépendante de n.

Soit $\varepsilon > 0$, on choisit $x_0 > 1$ tel que $C\ln(x_0) < \varepsilon$. De plus, on a montré que $M_n(x)$ converge vers l pour tout $x > 1$, donc il existe un rang $n_0 \in \mathbb{N}^*$ tel que pour tout $n \geqslant n_0$, on ait $|M_n(x_0) - l| < \varepsilon$. Ainsi pour tout $n \geqslant n_0$, $|u_n - l| \leqslant |u_n - M_n(x_0)| + |M_n(x_0) - l| \leqslant C\ln(x_0) + \varepsilon < 2\varepsilon$.Donc la suite (u_n) converge vers l. □

Questions

Question 1. Comment caractérise-t-on la convergence quadratique d'une suite $(u_n)_{n\in\mathbb{N}}$ qui converge vers une limite l ?

Réponse 1. Il y a convergence quadratique d'une suite (u_n) vers l lorsqu'il existe une constante $C > 0$ telle que pour tout $n \in \mathbb{N}$, on ait $|u_{n+1} - l| \leqslant C|u_n - l|^2$ et (u_n) converge vers l.

Question 2. Prouver que $\mathrm{Adh}(u_n) = \bigcap_{n\in\mathbb{N}} \overline{\{u_k, k \geqslant n\}}$.

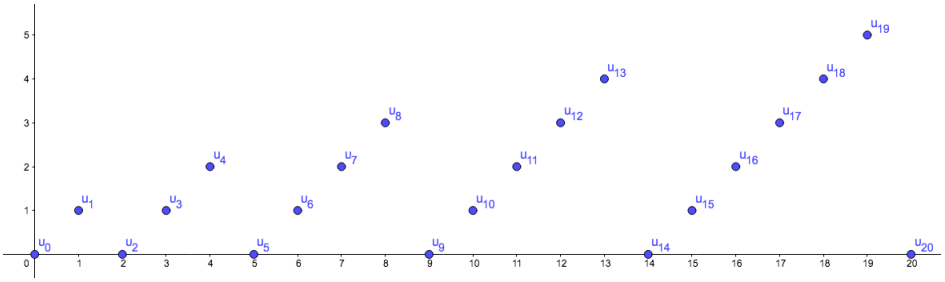
Réponse 2. Soit $l \in \bigcap_{n\in\mathbb{N}} \overline{\{u_k, k \geqslant n\}}$. Par équivalence, pour tout $n \in \mathbb{N}$, $l \in \overline{\{u_k, k \geqslant n\}}$. Ainsi $\forall n \in \mathbb{N}, \forall \varepsilon > 0, \exists k \geqslant n$ tel que $u_k \in \mathrm{B}(l, \varepsilon)$. En permutant les deux quantificateurs $\forall$ du début, on trouve $\forall \varepsilon > 0, \forall n \in \mathbb{N}, \exists k \geqslant n$ tel que $u_k \in \mathrm{B}(l, \varepsilon)$ qui est la définition d'une valeur d'adhérence car on peut alors construire une sous suite qui converge vers l. On a procédé par équivalence, donc l'égalité est vraie.

Question 3. Soit une suite (z_n) dans $\mathbb{C}$ qui est bornée et qui n'admet qu'une seule valeur d'adhérence α. Montrer que (z_n) converge vers cette valeur α.

Réponse 3. On pose la suite $u_n = |z_n - \alpha|$ qui est une suite réelle. On a $\liminf u_n = \limsup u_n = 0$ car α est la seule valeur d'adhérence de z_n qui est supposée bornée. Donc (u_n) converge vers 0. Ainsi $|z_n - \alpha| \xrightarrow[n\to+\infty]{} 0$. Ce qui nous donne $z_n \xrightarrow[n_\infty]{} \alpha$ dans $\mathbb{C}$.

Question 4. Donner une suite ayant $\mathbb{N}$ comme ensemble de valeurs d'adhérence.

Réponse 4. On peut prendre la suite u_n définie par $u_0 = 0$, $u_1 = 1$, $u_2 = 0$, $u_3 = 1$, $u_4 = 2$, $u_5 = 0$, $u_6 = 1$, $u_7 = 2$, $u_8 = 3$, $u_9 = 0 \ldots$



Ainsi, pour chaque $n \in \mathbb{N}$, (u_n) passe une infinité de fois par n.

Question 5. Donner une suite ayant $\mathcal{D}$ un ensemble dénombrable fermé d'éléments comme ensemble de valeurs d'adhérence.

Réponse 5. On s'appuie sur la question précédente. Si $\mathcal{D} = \{x_n, n \in \mathbb{N}\}$, on pose la suite $v_n = x_{u_n}$ avec u_n la suite définie dans la question précédente.

On veut prouver que $\mathcal{D} = \bigcap_{n\in\mathbb{N}} \overline{\{v_k, k \geqslant n\}}$ grâce à la Question 2.

On a $\mathcal{D} \supset \bigcap_{n\in\mathbb{N}} \overline{\{v_k, k \geqslant n\}}$ car $\{v_n, n \in \mathbb{N}\} \subset \{x_n, n \in \mathbb{N}\}$ et que $\mathcal{D}$ est fermé.

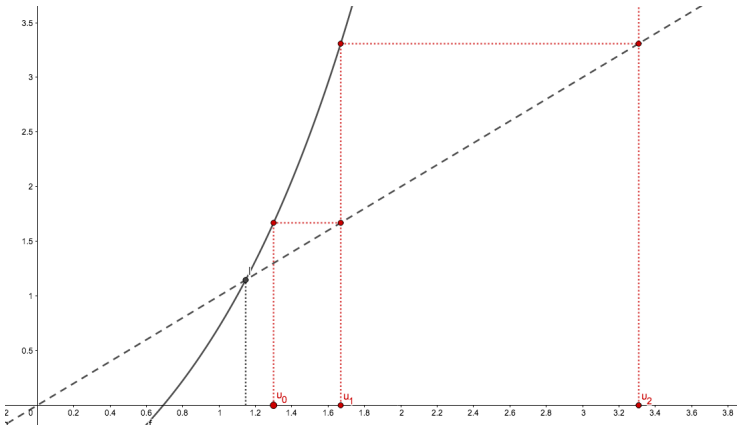
Réciproquement, puisque (u_n) passait une infinité de fois par n pour tout $n \in \mathbb{N}$, (v_n) va passer une infinité de fois par chaque x_n. Donc $\mathcal{D} \subset \bigcap_{n\in\mathbb{N}} \overline{\{u_k, k \geqslant n\}}$, ainsi $\mathrm{Adh}(u_n) = \mathcal{D}$.

Question 6. Donner une suite ayant F un fermé de $\mathbb{R}$ comme ensemble de valeurs d'adhérence.

Réponse 6. Puisque $\mathbb{R}$ est séparable et que F est un sous-ensemble de $\mathbb{R}$, alors F est séparable, donc il existe une famille $\mathcal{D}$ dénombrable et dense dans F. On applique la question précédente, on a donc une suite (w_n) dont les valeurs d'adhérence sont incluses dans F, car F est fermé. De plus, pour tout $x \in F$, pour tout $\varepsilon > 0$, il existe une sous suite de (w_n) qui converge vers une valeur de F qui est proche de ε de la valeur x (car $\mathcal{D}$ est dense dans F). Donc x est valeur d'adhérence de (w_n), donc $F = \mathrm{Adh}(w_n)$.

Question 7. Soit $(u_n)_{n\in\mathbb{N}}$ une suite récurrente bornée définie par un $f \in \mathcal{C}^1$ et telle que (u_n) converge vers une limite l. De plus, $|f'(l)| > 1$, que peut-on dire du comportement de (u_n) lorsque n tend vers l'infini ?

Réponse 7. La situation est la suivante :



Le point fixe l est un point répulsif, donc pour converger vers l, il faut que la suite stationne au bout d'un moment sur l.

Quitte à prendre $-f$, on suppose que $f'(l) > 1$, ainsi comme f' est continue et $f'(l) > 1$, il existe $\alpha > 0$ tel que sur l'intervalle $J :=]l-\alpha; l+\alpha[$, on ait $f' > 1$. Puisque (u_n) converge vers l, il existe un rang n_0 tel que pour tout $n \geqslant n_0$, $|u_n - l| < \alpha$.

Pour $n \geqslant n_0$, on utilise l'égalité des accroissements finis pour f sur $]l, u_n[$, ce qui nous donne $e \in]l, u_n[$ et $|f(u_n) - f(l)| = |f'(e)||u_n - l|$. De plus, on sait que $f'(e) > 1$ car $]l, u_n[\subset J$. Ainsi pour $n \geqslant n_0$, $|u_{n+1} - l| = |f(u_n) - f(l)| = |f'(e)||u_n - l| > |u_n - l|$. On a alors $|u_{n+1} - l| > |u_n - l|$, ce qui est absurde car on sait que (u_n) converge vers l. Donc l'intervalle $]l, u_n[$ est vide. Ainsi pour tout $n \geqslant n_0$, $u_n = l$ car l est un point fixe de f, donc dès que la suite atteint la valeur l, elle stationne.

Question 8. Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_n = \sin\left(\frac{\pi}{2}(2+\sqrt{3})^n\right)$ pour tout $n \in \mathbb{N}$. Montrer que (u_n) converge.

Réponse 8. On calcule $(2+\sqrt{3})^n$:

$$\forall n \in \mathbb{N}, \quad (2+\sqrt{3})^n = \sum_{k=0}^{n} \binom{n}{k} \sqrt{3}^k 2^{n-k} = a_n + \sqrt{3} b_n$$

avec a_n et b_n entiers. En calculant $(2-\sqrt{3})^n$, on trouve $a_n - \sqrt{3}b_n$ (avec les mêmes a_n et b_n). Ainsi, $(2+\sqrt{3})^n = a_n + \sqrt{3}b_n = 2a_n - (a_n - \sqrt{3}b_n) = 2a_n - (2-\sqrt{3})^n$ avec $a_n \in \mathbb{Z}$. Donc $\sin\left(\frac{\pi}{2}(2+\sqrt{3})^n\right) = \sin\left(\frac{\pi}{2}(2a_n - (2-\sqrt{3})^n)\right) = \sin\left(\pi a_n - \frac{\pi}{2}(2-\sqrt{3})^n\right) = (-1)^{a_n+1}\sin\left(\frac{\pi}{2}(2-\sqrt{3})^n\right)$ qui converge vers 0 car $(2-\sqrt{3})^n$ converge vers 0 quand n tend vers $+\infty$. Donc (u_n) converge vers 0.

CHAPITRE 5

COMPTE-RENDU ORAUX

5.1 Oral d'informatique

Samedi 29 Juin 2019, à 12h15 (convoqué à 8h45)

Couplage :

— 903 Algorithmes de tris

— 915 Classes de complexité (celle que j'ai choisi)

Développements proposés :

— CYK (le problème du mot pour les langages algébriques est dans P) (celui que le jury a choisi)

— Théorème de Cook

Plan que j'ai proposé :

I - Outil : Machine de Turing

Définition Machine de Turing

Définition Complexité spatiale et temporelle

Lemme de lien entre les deux complexités

II - Complexité temporelle

1) Changement de modèle de calcul

Théorème d'accélération

Équivalence avec machine de Turing à ruban biinfini (et même complexité temporelle)

Équivalence avec machine de Turing à k rubans (et facteur carré sur la complexité)

Équivalence avec machine de Turing non déterministe (et facteur exponentiel sur la complexité)

2) Classes temporelles

Définition de Time et NTime

Définition de P, NP, ExpTime et NExpTime

Exemple du problème du mot des langages algébriques qui est dans P Cocke-Younger-Kasami

Exemple de SAT qui est NP

3) NP-complétude

Définition réduction polynomiale

Propriété, si A se réduit à B et B est dans P alors A est dans P

Définition NP-dureté

Propriété, si A se réduit à B et A est NP-dur, alors B est NP-dur

Définition NP-complétude

Théorème de Cook

Exemple CNF_SAT et 3_SAT sont NP-complets

Exemple 3_COL, VERTEX_COVER, Circuit Hamiltonien et Voyageur de Commerce sont NP-complets

III - Complexité spatiale

1) Classes spatiales

Théorème de Savitch

Définition de SPACE et NSPACE

Définition de PSPACE, NPSPACE, EXPSPACE et NEXPSPACE

Exemple QBF_SAT est PSPACE

Définition de PSPACE-dureté

Définition de PSPACE-complétude

Exemple QBF_SAT est PSPACE-complet

2) Classe logarithmique

Définition des machines à 3 bandes qui servent à la réduction logarithmique

Définition de L et NL

Exemple PATH est dans NL

IV - Hiérarchie des complexités

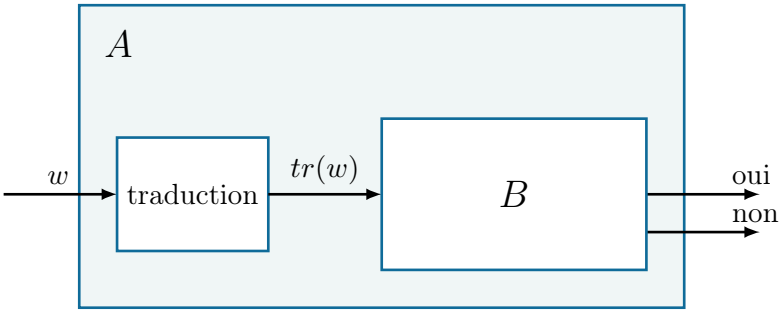
Théorème des hiérarchies

inclusion de toutes les classes avec certaines inclusions strictes

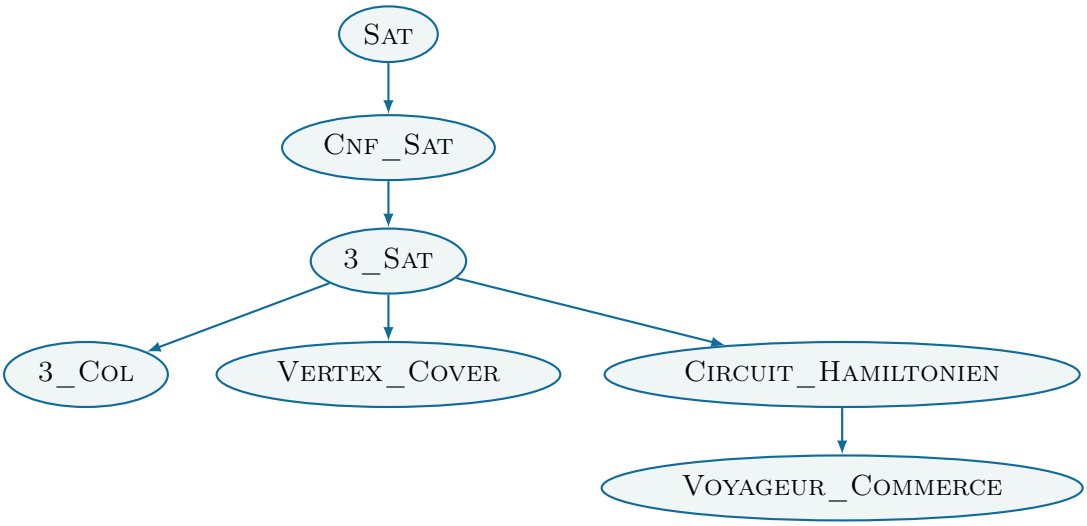
J'ai mis à la fin de mon plan (il me restait une demi page) la liste précise de tous les problèmes de décision que j'ai considérés

J'ai mis en annexe :

— un schéma de réduction



— un graphe possible des réductions des problèmes NP-complets (celui que je maitrise)



— un schéma des inclusions des classes (voir Carton)

Questions du jury :

Sur le développement

— Quelle est la définition de $|G|$?

— Quelle est la taille de l'entrée ? puisqu'on considère un mot w et une grammaire G

— Expliquer en détail la mise sous forme normale de Chomsky

— Est ce que la version récursive de cet algorithme est mieux ?

— En pratique, est-ce qu'on utilise cet algorithme ?

> J'ai dit que pour l'analyse syntaxique, on utilise plutôt des algorithmes linéaires mais ce sont des algorithmes pour des grammaires $LL(1)$ et $LR(0)$ et toute grammaire n'est pas forcément de ce type

Sur le reste

— Donner une autre définition de NP.

> J'ai parlé de certificat en temps polynomial et de l'arbre de choix d'une machine non déterministe

— Connaissez-vous un autre modèle de calcul pour calculer la complexité ?

> J'ai répondu que les fonctions μ-récursvies et le λ-calcul étaient des modèles de calcul équivalent aux machines de Turing et que pour le λ-calcul, on pourrait sans doute parler de complexité temporelle pour le nombre de β-réduction.

— Donner un exemple de problème dans NP dont on ne sait pas s'il est dans P ou NP-dur.

— Expliquer Qbf_Sat. Pourquoi il est PSpace-complet ?

— L'arbre de réduction de l'annexe, qu'est ce qu'il veut dire ?

> J'ai répondu que c'étaient les réductions que je connaissais pour prouver que ces problèmes sont NP-dur mais que comme ils sont NP-dur, le graphe des réductions est un graphe complet.

— Qu'est ce qu'on appelle un problème de décision ?

— Donner une définition de la NP-difficulté d'un problème d'optimisation

> J'ai dit qu'un problème d'optimisation était NP-complet, si son problème de décision associé l'était, mais j'ai l'impression que le jury voulait une autre réponse.

— Pourquoi PSpace $\subset$ ExpTime ?

— Ils m'ont parlé de SubsetSum que j'ai reconnu directement, j'ai dit qu'il était NP-complet, il m'ont demandé un algorithme de programmation dynamique qui résolvait ça, difficilement j'ai écrit l'équation de récurrence, puis on a parlé du problème de codage de l'entrée et des problèmes pseudo-polynomiaux.

Références utilisées :

— Carton (majoritairement)

— Garey Johnson (très peu)

Ressenti :

J'avais l'impression que le jury était très bienveillant, il cherchait à savoir ce que je savais, j'avais évoqué L et NL dans mon plan, je m'attendais à avoir des questions sur la réduction logarithmique, mais je n'en ai pas eu (dommage...) et j'aurais pu leur donner la réduction de 3_Sat à SubsetSum mais ils ont dit que c'était difficile et on est parti sur autre chose. Le jury était souriant et il y a des moments où c'était plus des questions de culture (problème NP, ni P, ni NP-dur).

Jury :

— Sophie Tison

— Marc De Falco

— un troisième dont je ne me souviens pas le nom

5.2 Oral de modélisation

Dimanche 30 Juin 2019, à 14h45 (convoqué à 10h15)

Textes :

— Algorithmique, cryptographie, probabilités

— Graphe, fermeture transitive d'une relation (celle que j'ai choisi)

Plan que j'ai proposé :

Titre : Peut-on serrer la main du président par connaissances interposées ?

I - Lien avec la fermeture transitive d'une relation binaire

II - Calcul de cette fermeture (CODE en Ocaml)

(3 méthodes)

I - Lien avec la fermeture transitive d'une relation binaire

Définition fermeture transitive $\mathcal{R}^+ = \bigcup_{k\geqslant 1} \mathcal{R}^k$ d'une relation $\mathcal{R}$ sur un ensemble $E = \{1, \dots, n\}$ où $\mathcal{R}^k$ est définie par :

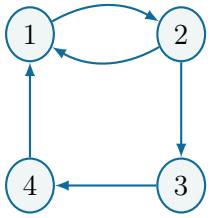
$$\begin{cases} \mathcal{R}^1 = \mathcal{R} \\ \mathcal{R}^{k+1} = \{(x,y) \in E^2, \exists z \in E, x\mathcal{R}z \text{ et } z\mathcal{R}^k y\} \end{cases}$$

Exemple : $x\mathcal{R}y$ si la personne x connait la personne y. La réponse à la question du titre étant de savoir si on est en relation avec le président pour la relation de la fermeture transitive de $\mathcal{R}$

Exemple : β-réduction en λ-calcul

Définition du graphe $G_{\mathcal{R}}$

Exemple qui donne une fermeture transitive où tout sommet a une arête vers tous les autres sommets



Prop : $(x,y) \in R^+$ SSI il y a un chemin de x à y dans $G_{\mathcal{R}}$

preuve : par récurrence (preuve que j'ai écrite très proprement)

II - Calcul de cette fermeture

1) Méthode intuitive

Utilisant la programmation dynamique

Relation de récurrence

$$\begin{cases} A_{i,j}^{(0)} = \begin{cases} 1 & \text{si } (i,j) \in G_{\mathcal{R}} \\ 0 & \text{sinon} \end{cases} \\ A_{i,j}^{(k)} = A_{i,j}^{(k-1)} \vee (A_{i,k}^{(k-1)} \wedge A_{k,j}^{(k-1)}) \end{cases}$$

Limite : à k fixé, il faut regarder la $k^{\text{ième}}$ ligne et la $k^{\text{ième}}$ colonne.

But : trouver un algorithme qui regarde que des lignes car si $G_{\mathcal{R}}$ est trop grand à stocker (par exemple base de données), il faut les mettre sur un disque externe, puis pour récupérer les informations, on veut aller chercher juste des lignes de la matrice d'adjacence du graphe.

2) Méthode minimisant le nombre d'accès au disque

Idée : au lieu de fixer k d'abord puis de faire bouger i, on fixe i d'abord et on fait varier k, il faudra faire attention au sens de calcul, pour bien calculer la fermeture transitive correctement

Algo : si $A_{i,k} = 1$ alors ligne $i \leftarrow$ ligne $i \vee$ ligne k

explication de pourquoi cela renvoie la même chose que la relation de récurrence de la section précédente

deux phases :

— pour i allant de 2 à n, on fait varier k de 1 à $i-1$

— pour i allant de 1 à $n-1$, on fait varier k de $i+1$ à n

explication de la correction

présentation du code

3) Approche matricielle

Remarque : $\mathcal{R}^+ = \bigcup_{k=1}^{n} \mathcal{R}^k$

Prop : la suite S_l définie par

$$\begin{cases} S_1 = \mathcal{R} \\ S_l = S_{l-1} \cup S_{l-1}^2 \end{cases}$$

vérifie $\mathcal{R}^+ = S_{\lceil \log_2(n) \rceil}$

On a $B_{i,j}^{(l)} = B_{i,j}^{(l-1)} \vee \bigvee_{k=1}^{n} (B_{i,k}^{(l-1)} \wedge B_{k,j}^{(l-1)})$

lien avec le produit matriciel $(+, \times)$ remplacé par $(\vee, \wedge)$

Théorème : Si t divise n, la multiplication de matrices booléennes de taille n peut se faire en $O(n^2 2^t + \frac{n^3}{t})$

preuve : j'ai prouvé proprement ce résultat

Code :

```
type graph = bool array array ; ;

let calcul_fermeture (mat : graph) : graph =
    let n = Array.length mat in
    for i = 1 to (n - 1) do
        for k = 0 to (i - 1) do
            if mat.(i).(k) then
                for j = 0 to (n - 1) do
                    mat.(i).(j) ← mat.(i).(j) || mat.(k).(j)
                done ;
        done ;
    done ;
    for i = 0 to (n - 2) do
        for k = (i + 1) to (n - 1) do
            if mat.(i).(k) then
```

```
            for j = 0 to (n - 1) do
                mat.(i).(j) ← mat.(i).(j) || mat.(k).(j)
            done ;
        done ;
    done ;
    mat ; ;


let exemple = [|  [| false ; true ; false ; false |] ;
                  [| true ; false ; true ; false |] ;
                  [| false ; false ; false ; true |] ;
                  [| true ; false ; false ; false |] |] ; ;

calcul_fermeture exemple ; ;
```

L'exemple renvoyait une matrice remplie de true, c'est l'exemple que j'avais mis dans mon plan, et le programme tournait bien.

Questions du jury :

- Est-ce que le dernier théorème est valable pour des entiers ?
  Réponse : non car le 2^t vient du nombre d'éléments de $\{0,1\}^t$
- Ce serait quoi comme complexité ?
  Réponse : si on regarde que des entiers de 0 à k, on a du $(k+1)^t$ à la place du 2^t, mais attention, on ne peut pas remultiplier ensuite car on ne reste pas avec des matrices à coefficients dans $\{0,\dots,k\}$
- Quel est le coût d'une addition matricielle ?
- Quel est le coût d'une addition d'entiers ?
- Quel est le coût de l'ajout de 1 ?
- Si t ne divise pas n comment on fait ?
  Réponse : j'ai dit de rajouter des lignes de 0, et ils m'ont demandé de borner le nombre de lignes de 0, ce que j'ai fait
- Dans mon code la complexité spatiale est en $O(n^2)$ mais ce n'est pas la complexité qui nous intéresse, quelle est-elle ?
  Réponse : on s'intéresse au nombre d'accès aux lignes de notre graphe, c'est aussi en $O(n^2)$
- Comment ça marche dans un ordi ?
  Réponse : j'ai voulu parler de B-arbres et de la minimisation de l'accès au disque, il m'a demandé explicitement où sont les espaces de mémoire, il fallait que je parle de mémoire CACHE, de BUS allant de la RAM au processeur, je n'ai pas su répondre de manière satisfaisante à cette question
- Connaissez-vous d'autres algorithmes de multiplication de matrices ?
  Réponse : Strassen, j'ai expliqué la complexité avec le Master Theorem, etc.
- Comment calculer les puissances d'une matrice et combien ça coûte ?
  Réponse : exponentiation rapide en $O(n^3 \log(n))$
- Que vaut S_k concrètement ?
  Réponse : $S_k = \mathcal{R} \cup \mathcal{R}^2 \cup \cdots \cup \mathcal{R}^{2^{k-1}}$

Ressenti :

Le jury était aussi bienveillant, il y avait surtout un jury qui débitait les questions. Je me suis fait avoir sur la structure de l'ordinateur, je ne savais si la mémoire vive était dans le processeur ou non. Attention, je n'avais pas d'écran pour présenter mon code, le projecteur projetait directement sur le tableau, donc il fallait faire en sorte de pas écrire au milieu du tableau pour qu'on puisse voir le code. Donc j'ai du laisser une fenetre assez étroite et le buffer sous le code. Cependant vu la simplicité du code, je n'ai pas passé mille ans sur le code, donc ça va.

5.3 Oral de mathématiques

Lundi 1er Juillet 2019, à 11h (convoqué à 7h30)

Couplage :

— 141 Polynômes irréductibles, Corps de rupture.

— 162 Systèmes linéaires, opérations élémentaires, aspect algorithmique (celle que j'ai choisi)

Développements proposés :

— Méthode QR pour trouver les valeurs propres

— Méthode du gradient à pas optimal (celui que le jury a choisi)

Plan que j'ai proposé :

I - Systèmes linéaires

Def : avec p équations et q inconnues

Lien avec les matrices, écriture sous la forme $AX = b$

Prop : si matrice carrée et inversible, une unique solution

Prop : solution grâce aux déterminants du système de Cramer

Prop : si matrice carrée, non inversible, deux cas possibles : $b \in \mathrm{Im}(A)$ et infinité de solution, $b \notin \mathrm{Im}(A)$ et pas de solutions

Def : systèmes sur-déterminés et sous-déterminés

II - Pivot de Gauss

1) Opérations élémentaires

Permutation

Dilatation

Transvection

Prop : on peut donc ajouter, à une ligne, une combinaison linéaire des autres lignes

Prop : ces opérations préservent les solutions du système

2) Systèmes échelonnés

Déf de système échelonné

Exemple de deux systèmes échelonné et non échelonné

3) Pivot de Gauss

Définition

Complexité en $O(n^3)$

Application du pivot de Gauss

— résoudre AX=b

— trouver le rang d'une famille de vecteurs

— calculer le déterminant

— calculer l'inverse d'une matrice

— engendrer $GL_n(\mathbb{K})$ par les dilatations et transvections

— engendrer $SL_n(\mathbb{K})$ par les transvections

— savoir si une famille est libre

— savoir si une famille est génératrice

— trouver l'intersection de l'intersection de deux sous-espaces vectoriels

III - Décompositions usuelles

1) Décomposition LU

Théorème de décomposition LU

Complexité $O(n^3)$ pour trouver la décomposition avec pivot de Gauss, mais ensuite résolution en $O(n^2)$ (utile pour résoudre $AX = b$ avec des b différents)

2) Décomposition QR

Théorème de décomposition QR sur $\mathbb{R}$

Théorème de décomposition QR sur $\mathbb{C}$

Complexité $O(n^3)$

Méthode QR

IV - Méthode itérative : méthode du gradient à pas optimal (voir le développement)

Théorème d'équivalence entre $\bar{X}$ est solution de $AX = b$ SSI $\bar{X}$ minimise la fonctionnelle convexe

$$f : \begin{cases} \mathbb{R}^n & \to & \mathbb{R} \\ X & \mapsto & \frac{1}{2}\langle AX, X\rangle - \langle b, X\rangle \end{cases}$$

Algorithme du gradient à pas optimal

Remarque sur comment trouver le α_{k+1}

inégalité de Kantorovich

Méthode de gradient à pas optimal

J'ai mis en annexe :

— un exemple du pivot de Gauss avec les opérations de base et la mise sous forme échelonnée

— une décomposition LU

— une décomposition QR

— un graphe d'une fonction $f : \mathbb{R}^2 \to \mathbb{R}$ avec l'idée du gradient à pas optimal

Questions du jury :

Sur le développement

— Est-ce qu'on peut changer le rôle de μ_1 et μ_n ?

— Vaut-il mieux que les valeurs propres soient rapprochées ou éloignées pour améliorer la vitesse de convergence ?

— Quel est le lien entre cette suite et le théorème qui dit que $\bar{X}$ est solution de $AX = b$ SSI $\bar{X}$ minimise la fonctionnelle convexe

$$f : \begin{cases} \mathbb{R}^n & \to & \mathbb{R} \\ X & \mapsto & \frac{1}{2}\langle AX, X\rangle - \langle b, X\rangle \end{cases}$$

— Ils m'ont fait remarquer une erreur d'indice sur le tableau

Sur le reste

— Quel est le lien entre système linéaire $AX = b$ et l'inverse de A

Réponse : ils voulaient juste que je dise $X = A^{-1}b$

— Combien ça coûte de calculer A^{-1} ?

Réponse : $O(n^3)$

— Combien ça coûte de calculer $A^{-1}b$ une fois que A^{-1} est calculé ?

Réponse : $O(n^2)$

— Donc quel est l'avantage de la décomposition LU ?

Réponse : avantage d'une constante dans le grand O qui est meilleure dans LU que dans l'inverse de A

— Pour une matrice tridiagonale [1], quelle est la complexité de la décomposition LU ?

Réponse : linéaire (j'ai un peu galéré, j'ai dit $O(n^2)$ au début, puis après j'ai rectifié)

— Qu'est ce que vous pouvez me dire sur les systèmes de Cramer ?

— Montrer que pour b fixé, $Ax = b$ admet une unique solution SSI A est inversible

Réponse : il y a une implication immédiate, et l'autre je l'ai faite en utilisant le théorème du rang, et ils m'ont demandé une méthode qui n'utilisait pas d'algèbre linéaire, plutôt des considérations avec le pivot de Gauss

— Comment on calcule l'inverse d'une matrice A avec le pivot de Gauss ?

— On considère $2k+1$ cailloux chacun de masse $(m_i)_1^{2k+1}$, on suppose que dès qu'on enlève un cailloux, parmi les $2k$ restants, il existe un ensemble de k cailloux dont le poids total est le même que les k autres. Montrer que toutes les masses sont égales.

Réponse : il faut poser un système linéaire de taille $(2k+1) \times (2k+1)$,

$$\begin{cases} \varepsilon_{1,1}m1 & + & \varepsilon_{1,2}m_2 & + & \dots & + & \varepsilon_{1,2k+1}m_{2k+1} & = & 0 \\ \varepsilon_{2,1}m1 & + & \varepsilon_{2,2}m_2 & + & \dots & + & \varepsilon_{2,2k+1}m_{2k+1} & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ \varepsilon_{2k+1,1}m1 & + & \varepsilon_{2k+1,2}m_2 & + & \dots & + & \varepsilon_{2k+1,2k+1}m_{2k+1} & = & 0 \end{cases}$$

avec $\varepsilon_{i,j}$ valant 0 si $i = j$, et ± 1 en fonction de si j appartient aux k premiers cailloux ou aux k autres. On a $(1, \dots, 1)$ qui est solution car il y a k cailloux avec des 1 et k cailloux avec des -1. Il faut montrer que la dimension de $\ker A$ est 1, je n'ai pas eu le temps de finir

Références utilisées :

— Grifone (majoritairement)

— Allaire (majoritairement)

— Ciarlet (méthode QR)

— Ramis Warusfel (méthode du gradient)

— Gourdon algèbre (très peu)

— Perrin (très peu, juste pour dilatation, transvection)

Ressenti :

Le jury était encore très bienveillant, il a commencé par des questions très évidentes, parfois ce qui était dur c'était juste de comprendre la question. Beaucoup de questions pour comprendre si j'avais compris la puissance du pivot de Gauss. Un peu déçu de pas avoir abouti sur l'exercice des cailloux mais c'était la fin du temps.

1. juste une diagonale avec une sur-diagonale et une sous-diagonale

CHAPITRE 6

APPENDICE

6.1 Maths

Conventions Transformation de Fourier

Convention 1 : (Celle que j'ai choisie)

$$\boxed{\hat{f}(\xi) = \int_{-\infty}^{+\infty} f(x)e^{-i\xi x}dx}$$

Avantage : ressemble à la convention des coefficients de Fourier pour des fonctions 2π-périodiques qui coïncide avec les séries de Fourier.

$$c_n(f) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)e^{-int}\ dt$$

et quand la série de Fourier coïncide avec la fonction on a

$$f(t) = \sum_{n=-\infty}^{+\infty} c_n(f)e^{inx}$$

On a donc une convention où l'on a jamais de 2π dans l'exponentielle et on peut retrouver la série de fourier grâce au noyau de Dirichlet conventionnel $D_N(t) = \sum_{n=-N}^{N} e^{int}$ avec $S_N(f)(t) = (D_N \star f)(t)$.
En dimension d, la notation est similaire, en mettant un produit scalaire dans l'exponentielle

$$\hat{f}(\xi) = \int_{\mathbb{R}^d} f(x)e^{-i\langle \xi, x\rangle}dx$$

Inconvénient : change la formule sommatoire de Poisson (ou du moins fait apparaitre un facteur 2π au dénominateur), fait apparaitre un 2π au dénominateur pour la transformée de Fourier inverse

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} \hat{f}(\xi)e^{ix\xi}d\xi$$

Convention 2 :

$$\boxed{\hat{f}(\xi) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} f(x) e^{-i\xi x} dx}$$

Avantage : possède le même facteur multiplicatif que la transformée de Fourier inverse

Inconvénient : change la formule sommatoire de Poisson et on a un facteur $\sqrt{2\pi}$ qui se balade tout le temps

Convention 3 :

$$\boxed{\hat{f}(\xi) = \int_{-\infty}^{+\infty} f(x) e^{-i2\pi\xi x} dx}$$

Avantage : la formule sommatoire de Poisson est simple à écrire

$$\sum_{k=-\infty}^{+\infty} f(k) = \sum_{k=-\infty}^{+\infty} \hat{f}(k)$$

Elle est appliquée en $x = 0$ ici, mais en général on a

$$\sum_{k=-\infty}^{+\infty} f(x+k) = \sum_{k=-\infty}^{+\infty} \hat{f}(k) e^{2i\pi nx}$$

Inconvénient : il faut revoir toutes les définitions de noyau de Dirichlet , pour le coefficient de Fourier, on est dans une convention ou la période devient 1 et on a des 2π qui apparaissent un peu partout dans les exponentielles. Le coefficient de Fourier devient

$$c_n(f) = \int_0^1 f(t) e^{-2i\pi nt} dt$$

Remarques :

On s'est occupé de la dimension 1 ici. En dimension d, la convention 1 est très similaire. Pour la convention 2, on met le facteur multiplicatif à la puissance d.

Théorèmes classiques

Voici quelques théorèmes classiques dont il faut avoir connaissance, qu'il faut savoir énoncer, avoir des idées de preuves ou prouver entièrement pour l'agrégation :

1. Lemme de décomposition des noyaux
2. Théorème de prolongement d'une application uniformément continue
3. Théorème de point fixe de Picard
4. Théorème de Cayley–Hamilton
5. Théorème d'Ascoli
6. Lemme de Gronwall
7. Théorème de représentation de Riesz
8. Théorèmes des résidus
9. Décomposition polaire
10. Théorème d'Hahn Banach
11. Théorème de Baire
12. Théorème de Banach–Steinhaus
13. Théorème de l'application ouverte
14. Théorème d'isomorphisme de Banach
15. Théorème de Rolle
16. Théorème de Bolzano–Weierstrass
17. Inégalité de Cauchy–Schwarz
18. Inégalité de Hölder
19. Théorème des accroissements finis
20. Formules de Taylor
21. Théorème de Heine
22. Théorème de Riesz–Fisher
23. Théorème de convergence dominée
24. Théorème de continuité sous le signe intégral
25. Théorème de dérivation sous le signe intégral
26. Lemme de Fatou
27. Théorème de Weierstrass
28. Théorème Spectral
29. Théorème d'inertie de Sylvester
30. Théorème d'Alembert–Gauss
31. Théorème de Maschke
32. Théorème d'arithmétique (Bézout, Gauss, Fermat...)
33. Théorèmes d'isomorphisme
34. Théorème de structure des groupes abéliens de type fini
35. Formule des classes
36. Formule de Burnside
37. Théorème de Sylow
38. Lemme des bases téléscopiques
39. Critère d'Eisenstein
40. Théorème chinois
41. Théorème d'Euclide
42. Théorème de projection sur un convexe fermé
43. Principe des zéros isolés
44. Équivalence des normes
45. Théorème de Riesz (boule unité fermée)
46. Décomposition de Dunford
47. Théorème de Lax–Milgram
48. Formule de Duhamel
49. Théorème de Cauchy–Lipschitz
50. Théorème de sortie de tout compact
51. Théorème d'inversion locale
52. Théorème des fonctions implicites
53. Théorème des extrema liés
54. Théorème de Plancherel
55. Lemme de Borel–Cantelli I et II
56. Théorème de convergence monotone
57. Théorème de Fubini
58. Lemme de Riemann–Lebesgue
59. Théorème de Dirichlet
60. Théorème de Fejer
61. Théorème de Parseval
62. Inégalité de Markov
63. Inégalité de Bienaymé–Tchebychev
64. Loi des grands nombres
65. Théorème Central Limite
66. Théorème de transfert
67. Théorème de Levy
68. Méthode d'Euler
69. Théorème de convergence des méthodes itératives
70. Décomposition LU
71. Décomposition QR
72. Méthode de Newton
73. Méthode de Monte-Carlo

Exercices classiques

Voici quelques exercices classiques qu'il faut savoir faire en arrivant à l'agrégation.

1. Montrer que si $X_n \sim \mathscr{B}(n, p_n)$ avec $np_n \to \lambda$, alors $X_n \xrightarrow[n\to\infty]{Loi} X \sim \mathscr{P}(\lambda)$.
2. Donner tous les automorphismes de corps de $\mathbb{R}$ (attention, ils ne sont pas forcément continus).
3. Montrer que $GL_n(\mathbb{C})$ n'admet pas de sous-groupe arbitrairement petit.
4. Montrer le théorème de point fixe de Picard :
   Soient (E, d) un espace métrique complet et $f : E \to E$ une fonction contractante (qui vérifie $d(f(x), f(y)) \leqslant kd(x, y)$ pour tout $x, y \in E$ avec $k < 1$). Alors f admet un unique point fixe a dans E et pour tout $x_0 \in E$, la suite définie par $x_{n+1} = f(x_n)$ converge vers a et on a
   $$\forall n \in \mathbb{N}, \quad d(x_n, a) \leqslant \frac{k^n}{1-k} d(x_1, x_0).$$
5. Montrer que $\mathbb{F}_q^\times$ est cyclique (pour $q = p^\alpha$ avec p premier et $\alpha \in \mathbb{N}^*$).
6. Montrer la décomposition polaire :
   Soient $O_n(\mathbb{R})$ le groupe orthogonal $\{M \in \mathcal{M}_n(\mathbb{R}), {}^t MM = I_n\}$ et $\mathscr{S}_n^{++}(\mathbb{R})$ l'ensemble des matrices symétriques définies positives.
   $$\phi : \begin{array}{ccc} O_n(\mathbb{R}) \times \mathscr{S}_n^{++}(\mathbb{R}) & \to & GL_n(\mathbb{R}) \\ (O, S) & \mapsto & OS \end{array} \text{ est une bijection.}$$
7. Soit E un espace préhilbertien. Démontrer l'inégalité de Cauchy–Schwarz
   $$\forall x, y \in E, \quad |\langle x, y\rangle| \leqslant \|x\|\|y\|.$$
8. Montrer que les sous groupes additifs de $\mathbb{R}$ sont de la forme $\alpha\mathbb{Z}$ où $\alpha \in \mathbb{R}$ ou sont denses dans $\mathbb{R}$.
9. Montrer le théorème de Riesz : Soit E un espace vectoriel normé, alors les deux assertions suivantes sont équivalentes :
   (i) E est de dimension finie ;
   (ii) la boule unité fermée $\overline{B_E(0,1)}$ est compacte.
10. Montrer qu'un anneau fini commutatif intègre est un corps.
11. On dit qu'un polynôme $P \in \mathbb{Z}[X]$ est primitif si son contenu (pgcd de ses coefficients) vaut 1. Soit $P \in \mathbb{Z}[X]$. Montrer que les deux assertions suivantes sont équivalentes :
   (i) P est irréductible sur $\mathbb{Z}$;
   (ii) P est primitif et P est irréductible sur $\mathbb{Q}$.
12. Calculer la différentielle de $\left\{ \begin{array}{ccc} GL_n(\mathbb{R}) & \to & GL_n(\mathbb{R}) \\ A & \mapsto & A^{-1} \end{array} \right.$.
13. Montrer le théorème de projection sur un convexe fermé [1]
14. Montrer le critère d'irréductibilité d'Eisenstein :
   Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, s'il existe un nombre premier p qui vérifie :
   — $p | a_i, \quad \forall i \in \{0, \dots, n-1\}$
   — $p \nmid a_n$

1. utiliser l'identité du parallélogramme

— $p^2 \nmid a_0$

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

15. Montrer que l'on ne peut pas engendrer $\mathfrak{S}_n$ avec moins de $n-1$ transpositions.
16. Montrer qu'une suite de Cauchy dont une sous-suite converge est convergente.
17. Calculer la valeur de l'intégrale de Dirichlet :
$$\int_0^\infty \frac{\sin x}{x} dx.$$
18. Montrer que
$$\zeta(z) = \sum_{n \geqslant 1} \frac{1}{n^z} = \prod_{p \in \mathcal{P}} \left(1 - p^{-z}\right)^{-1},$$
où $\mathcal{P}$ désigne l'ensemble des nombres premiers.
19. Montrer le théorème de prolongement des fonctions uniformément continues :
Soient (E, d_E) un espace métrique, (F, d_F) un espace métrique complet, D dense dans E et $f : D \to F$ une application uniformément continue. Alors il existe un unique prolongement $\tilde{f} : E \to F$ de f.
20. Montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais réductible sur tous les $\mathbb{F}_p$.[2]
21. Montrer le théorème de Heine : Soient K un espace métrique compact et f une fonction continue de K dans $\mathbb{R}$, alors f est uniformément continue.
22. Montrer le théorème de Wilson :
$$p \text{ premier} \quad \text{si et seulement si} \quad (p-1)! \equiv -1 \ [p].$$
23. Montrer que $\mathfrak{A}_n$ est engendré par les 3-cycles.
24. Donner un développement asymptotique à l'ordre 2 de la suite $(u_n)_{n \in \mathbb{N}}$ définie par
$$u_0 \in]0, \frac{\pi}{2}[\quad \text{et} \quad u_{n+1} = \sin u_n \text{ pour tout } n \in \mathbb{N}.$$
25. Combien il y a de coloriage du cube avec 3 couleurs ?
26. Montrer l'homéomorphisme exp : $\mathscr{S}_n(\mathbb{R}) \to \mathscr{S}_n^{++}(\mathbb{R})$ où $\mathscr{S}_n(\mathbb{R})$ est l'ensemble des matrices symétriques réelles et $\mathscr{S}_n^{++}(\mathbb{R})$ est l'ensemble des matrices symétriques définies positives réelles.
27. Donner un exemple de suite de fonctions telle que l'on ne peut pas intervertir la limite et le signe intégral.
28. Montrer la formule de Stirling :
$$n! \underset{n \to \infty}{\sim} n^n e^{-n} \sqrt{2\pi n}.$$
29. Montrer la décomposition QR :
Soient $U_n(\mathbb{C})$ le groupe unitaire $\{M \in \mathcal{M}_n(\mathbb{C}), M^*M = I_n\}$ et $T_n^{++}(\mathbb{C})$ l'ensemble des matrices triangulaire à diagonale réelle strictement positive.
$$\phi : \begin{array}{ccc} U_n(\mathbb{C}) \times T_n^{++}(\mathbb{C}) & \to & GL_n(\mathbb{C}) \\ (Q, R) & \mapsto & QR \end{array} \text{ est une bijection.}$$
30. Montrer que la fonction de répartition $F_X : t \mapsto \mathbb{P}(X \leqslant t)$ caractérise la loi de X.

2. Ainsi, il n'existe pas de réciproque au critère d'irréductibilité modulaire

31. Montrer les théorèmes de Dini :
    Soit $(f_n)_{n\in\mathbb{N}}$ une suite croissante de fonctions continues de $[a,b]$ dans $\mathbb{R}$ telle que (f_n) converge simplement vers une fonction continue f. Alors (f_n) converge uniformément vers f.
    Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions croissantes de $[a,b]$ dans $\mathbb{R}$ telle que (f_n) converge simplement vers une fonction continue f. Alors (f_n) converge uniformément vers f.
32. Soit X un ensemble fini, soit G un groupe fini agissant sur X. On note $(x_i)_{i=1}^r$ une famille de représentants des orbites. Montrer la formule des classes :
$$|X| = \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}(x_i)|},$$
    où $\mathrm{Stab}(x)$ désigne le stabilisateur de x, autrement dit $\mathrm{Stab}(x) = \{g \in G, g \cdot x = x\}$.
33. Montrer le lemme de Riemann–Lebesgue :
    Soit $f \in L^1(\mathbb{R})$ une fonction 2π périodique. Alors
$$c_n(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-int}dt \xrightarrow[n\to\infty]{} 0.$$
34. Calculer la différentielle du déterminant $\det : \begin{cases} \mathcal{M}_n(\mathbb{R}) & \to & \mathbb{R} \\ A & \mapsto & \det A \end{cases}$.
35. Soient α et β deux réels. On sait que$\{\alpha\mathbb{Z} + \beta\mathbb{Z}\}$ est dense dans $\mathbb{R}$ si et seulement si $\frac{\alpha}{\beta}$ est irrationnel. Utiliser ce résultat pour démontrer que $\{\cos(n) \mid n \in \mathbb{N}\}$ et $\{\sin(n) \mid n \in \mathbb{N}\}$ sont denses dans $[-1,1]$.
36. Montrer le théorème de Liouville :
    Si f est une fonction holomorphe sur $\mathbb{C}$ qui est bornée, alors elle est constante.
37. Montrer que le seul morphisme non trivial de $(\mathfrak{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$ est la signature.
38. Montrer le lemme des noyaux :
    Soient E un espace vectoriel sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $u \in \mathcal{L}(E)$ et $P = \prod_{i=1}^{n} Q_i \in \mathbb{K}[X]$ où les (Q_i) sont deux à deux premiers entre eux, alors on a
$$\ker P(u) = \bigoplus_{i=1}^{n} \ker Q_i(u).$$
39. Montrer que l'on ne peut pas truquer deux dés à 6 faces afin d'obtenir une loi uniforme sur leur somme. [3]
40. Montrer que
$$\sum_{n\geqslant 1} \frac{1}{n^4} = \frac{\pi^4}{90}.$$
41. Soient I un intervalle de $\mathbb{R}$ et $\alpha \in \mathbb{R} \setminus \{1\}$. Résoudre l'équation différentielle $y' = py + qy^\alpha$ pour $p, q : I \to \mathbb{R}$ deux fonctions continues données.
42. Montrer que le groupe orthogonal $O_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}), {}^tMM = I_n\}$ est compact.
43. Montrer le critère des séries alternées :
    Si $(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ est une suite décroissante qui tend vers 0, alors la série $\sum_{n\geqslant 0}(-1)^n u_n$ converge. De plus, son reste $R_n = \sum_{k\geqslant n+1} (-1)^k u_k$ est majoré par $|u_{n+1}|$.

3. utiliser la fonction génératrice

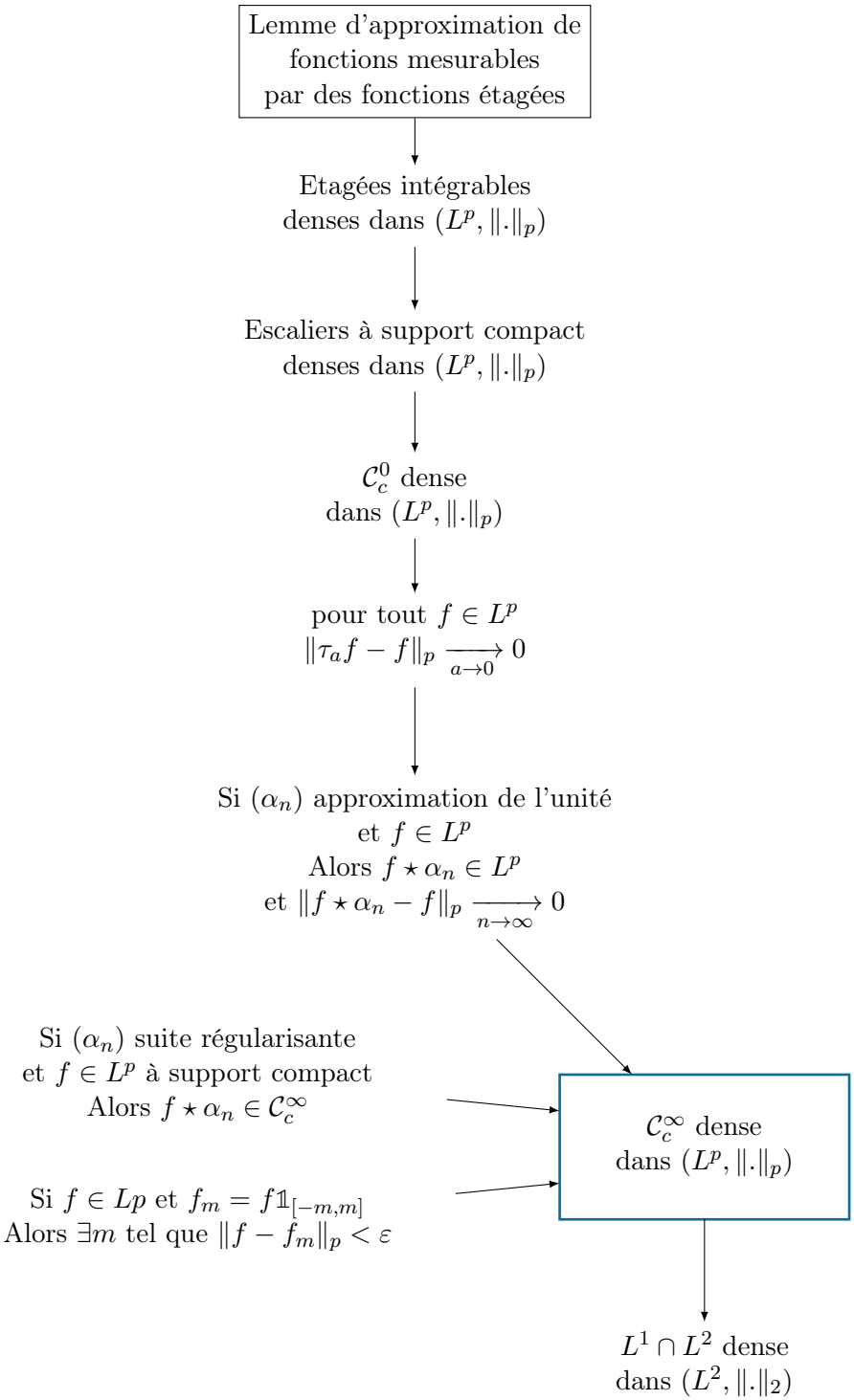
44. Montrer la formule de Burnside :
Soit G un groupe fini (de cardinal $|G|$) agissant sur un ensemble X, on note r le nombre d'orbites de cette action et on note $\mathrm{Fix}(g)$ l'ensemble $\{x \in X, g.x = x\}$. Alors on a
$$r = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g).$$
45. Montrer le théorème spectral :
Si A est une matrice symétrique réelle, alors elle est diagonalisable sur $\mathbb{R}$.
46. Montrer le théorème d'Alembert Gauss [4] :
Si $P \in \mathbb{C}[X]$ n'est pas constant, alors il admet une racine dans $\mathbb{C}$. *i.e.* Tout polynôme de $\mathbb{C}[X]$ est scindé.
47. Calculer
$$I = \int_0^{+\infty} \frac{\cos(\omega t)}{1+t^2} dt \quad \text{pour } \omega > 0. \text{ [5]}$$
48. Montrer le théorème de point fixe compact :
Soit (K, d) un espace métrique compact. Si f est une fonction de K dans K vérifiant
$$d(f(x), f(y) < d(x, y),$$
alors f admet un unique point fixe dans K.
49. Montrer que la limite uniforme d'une suite de polynômes sur $\mathbb{R}$ est un polynôme.
50. Montrer que $\frac{2}{e} < 1$.
51. Combien existe-t-i de collier de perles avec 4 perles bleues, 3 perles blanches et 2 perles rouges ? (sachant qu'on peut faire coulisser les perles sur tout le collier qui est circulaire)
52. Montrer le théorème de Césaro :
Soit $(u_n)_{n \in \mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ une suite qui converge vers l. Alors on a
$$\lim_{n \to \infty} \frac{1}{n} \sum_{k=0}^{n-1} u_k = l$$
53. Montrer que la fonction $x \mapsto \sin\left(\frac{1}{x}\right)$ donne un graphe connexe mais non connexe par arcs dans $\mathbb{R}^2$.
54. Calculer $\sum_{n \in \mathbb{N}} \frac{(-1)^n}{2n+1}$.
55. Montrer le théorème de Cayley–Hamilton :
Soient E un espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Alors $\chi_u(u) = 0$ où χ_u désigne le polynôme caractéristique de u.
56. Montrer que la somme des inverses des nombres premiers diverge.
57. Calculer le déterminant d'une matrice de Van der Monde.
58. Montrer que A/I est un corps si et seulement si I est un idéal maximal de l'anneau A.
Montrer que A/I est intègre si et seulement si I est un idéal premier de l'anneau A.
59. Calculer le rayon de convergence de
$$\sum_{n=1}^{\infty} \frac{(\ln(n!))^a}{(n!)^b} z^n.$$

4. on peut utiliser le théorème d'inversion locale, ou le théorème de Liouville, par exemple...
5. utiliser le théorème des résidus, on doit trouver $\frac{\pi e^{-\omega}}{2}$.

Théorèmes de densité dans les L^p

(rédigé avec Emilie Tezenas)

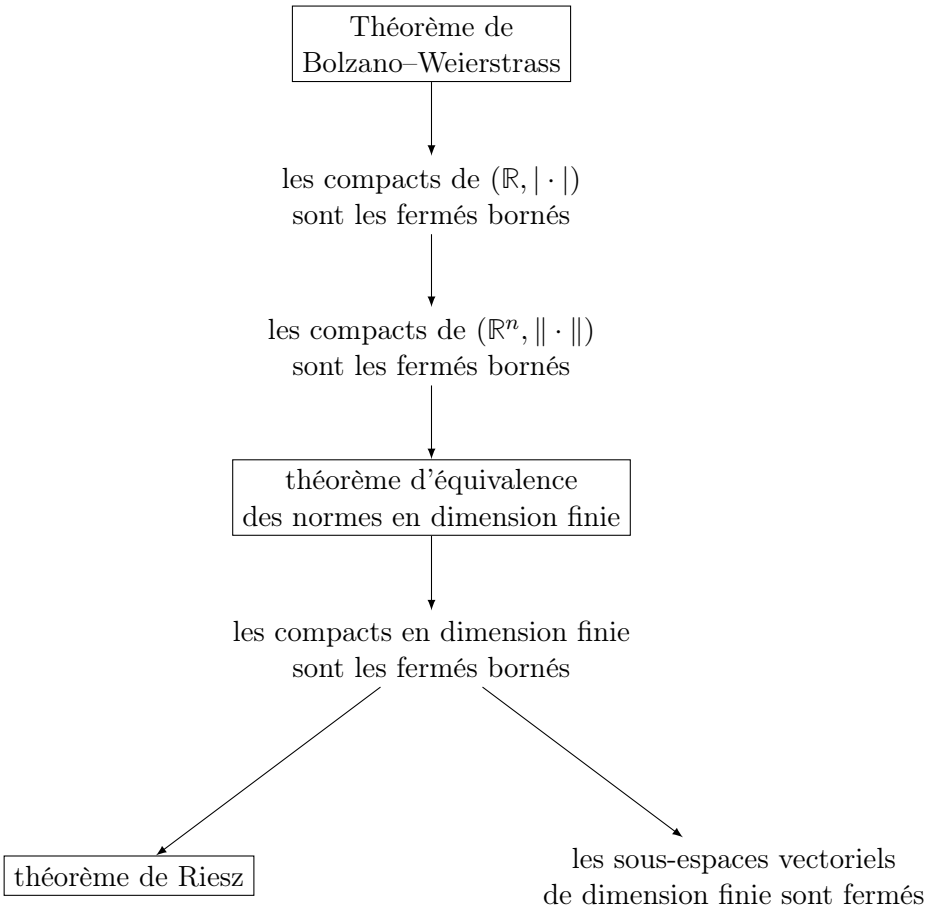
Ce diagramme retranscrit les étapes pour prouver que $\mathcal{C}_c^\infty$ est dense dans $(L^p, \|.\|_p)$. Ici, p appartient à $[1, \infty[$.



La densité de $L^1 \cap L^2$ dans L^2 est utile pour définir la transformée de Fourier sur L^2

Compacité en dimension finie

Ce diagramme retranscrit les étapes par lesquelles on montre les résultats sur la compacité en dimension finie



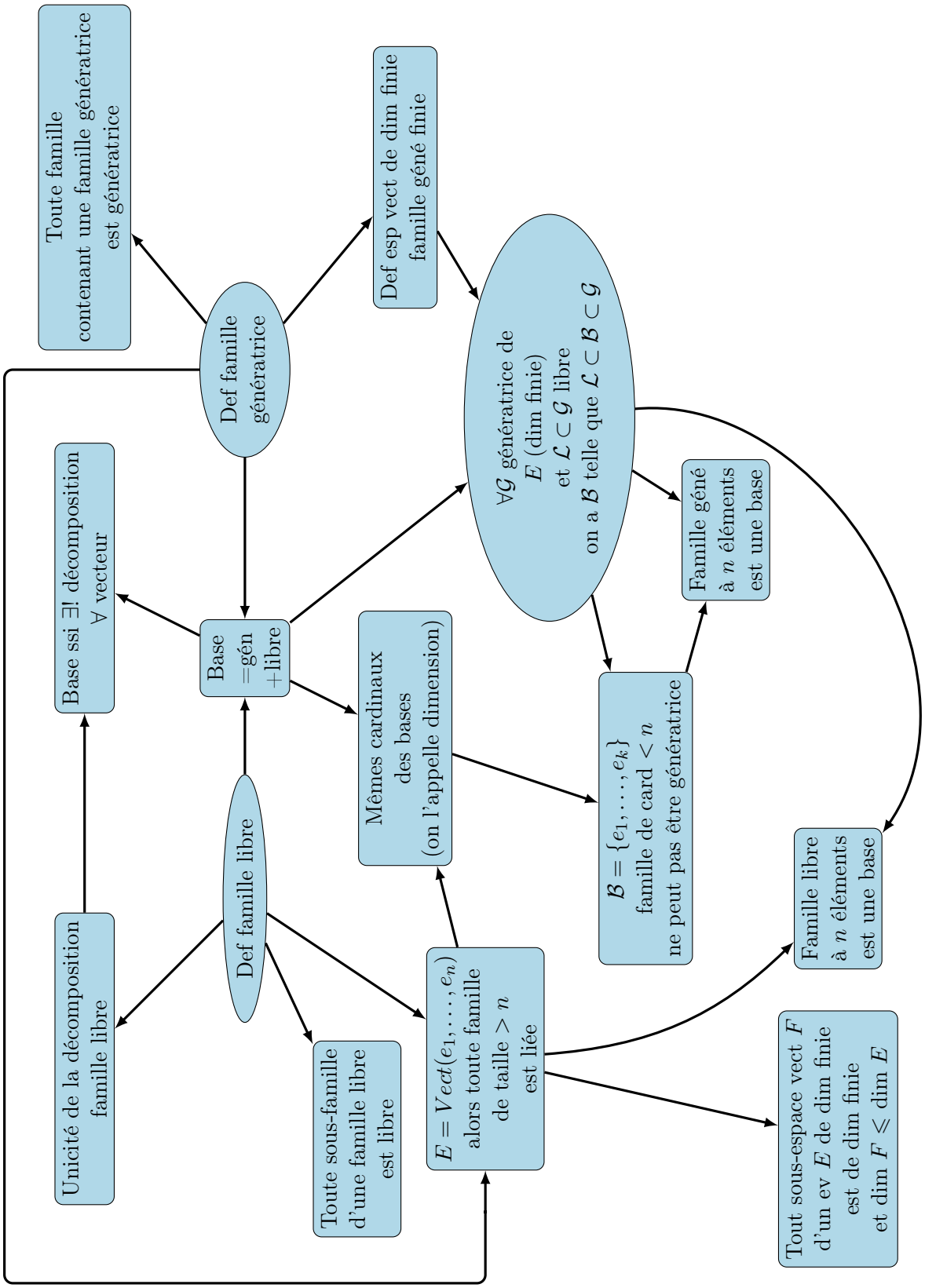
Théorème 1. Sur un $\mathbb{R}$-espace vectoriel de dimension finie, toutes les normes sont équivalentes.

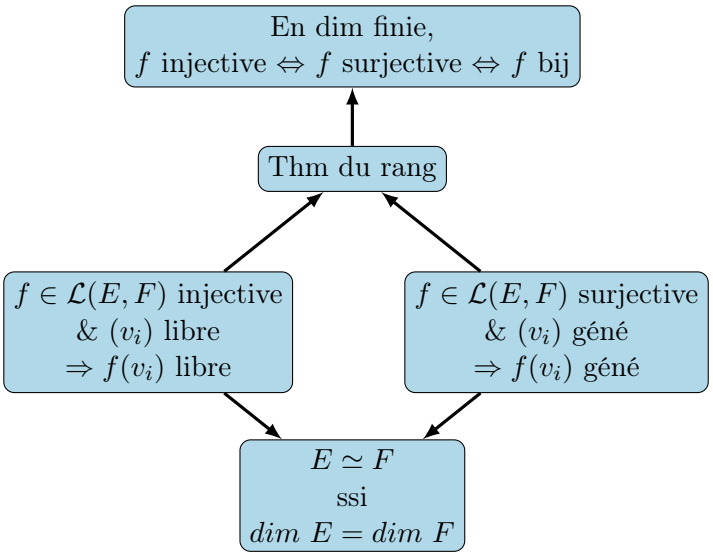
Théorème 2 (Riesz)**.** Soit E un espace vectoriel normé. Il y a équivalence entre les deux assertions suivantes :

- E est de dimension finie
- la boule unité fermée $B_f(0,1)$ est compacte

Théorèmes de dimension d'un espace vectoriel

(créé par Émilie Tezenas et moi et latexifié par David Xu)




En dim finie,
f injective $\Leftrightarrow$ f surjective $\Leftrightarrow$ f bij
Thm du rang
$f \in \mathcal{L}(E,F)$ injective
& (v_i) libre
$\Rightarrow f(v_i)$ libre
$f \in \mathcal{L}(E,F)$ surjective
& (v_i) géné
$\Rightarrow f(v_i)$ géné
$E \simeq F$
ssi
$dim\ E = dim\ F$

D'Alembert Gauss avec Théorème d'Inversion Locale

Théorème 1. Soit $P \in \mathbb{C}[X]$ non constant, alors P est scindé.

Démonstration. On va montrer que $P(\mathbb{C}) = \mathbb{C}$. Ainsi il existe α tel que $P(\alpha) = 0$, on peut donc factoriser P par $(X - \alpha)$, *i.e.* $P = (X - \alpha)Q$. Ensuite on recommence avec Q jusqu'à ce que le polynôme soit constant.

Pour montrer que $P(\mathbb{C}) = \mathbb{C}$, on pose

$$A = \{z \in \mathbb{C}, \quad P'(z) = 0\}$$

Étape 1 : *Montrons que $\mathbb{C}\backslash P(A)$ est connexe.*

Cet ensemble est bien connexe, car il est connexe par arcs. En effet, $P(A)$ est fini car A est fini puisque P est de degré fini. Donc, comme on enlève un nombre fini de points à $\mathbb{C}$, $\mathbb{C}\backslash P(A)$ est connexe par arcs.

Étape 2 : *Montrons que $P(\mathbb{C})\backslash P(A)$ est ouvert dans $\mathbb{C}\backslash P(A)$.*

Soit $P(y) = z \in P(\mathbb{C})\backslash P(A)$. On a $P'(y) \neq 0$ donc il existe, par le théorème d'inversion locale, un voisinage ouvert $\mathcal{V}_y$ contenant y et un voisinage ouvert $\mathcal{V}_z$ contenant z tels que

$$P : \mathcal{V}_y \to \mathcal{V}_z \text{ est un } \mathcal{C}^1\text{-difféomorphisme}$$

Le voisinage $\mathcal{V}_z = P(\mathcal{V}_y) \subset \mathbb{C}\backslash P(A)$ est un ouvert qui contient z. Donc $P(\mathbb{C})\backslash P(A)$ est ouvert dans $\mathbb{C}\backslash P(A)$.

Étape 3 : *Montrons que $P(\mathbb{C})\backslash P(A)$ est fermé dans $\mathbb{C}\backslash P(A)$.*

Soit $(z_n) \in (P(\mathbb{C})\backslash P(A))^{\mathbb{N}}$ telle que $z_n \to z \in \mathbb{C}\backslash P(A)$. On veut montrer que $z \in P(\mathbb{C})\backslash P(A)$. On a $z_n = P(y_n)$ et (z_n) bornée puisque z_n converge. Ainsi (y_n) bornée car $|P(z)| \xrightarrow[|z|\to\infty]{} +\infty$ [1]

Donc il existe une sous-suite $(y_{\phi(n)})$ qui converge vers un certain y. On a, par continuité de P, que $P(y_{\phi(n)}) \xrightarrow[n\infty]{} P(y)$ et $P(y_{\phi(n)}) \xrightarrow[n\infty]{} z$. Ainsi $z = P(y)$, or $z \notin P(A)$, donc $P(y) \notin P(A)$. On peut donc conclure que $z \in P(\mathbb{C})\backslash P(A)$ et $P(\mathbb{C})\backslash P(A)$ est fermé dans $\mathbb{C}\backslash P(A)$.

Étape 4 : *Conclusion.*

Comme $\mathbb{C}\backslash P(A)$ est connexe, que $P(\mathbb{C})\backslash P(A)$ est non vide (puisque $P(A)$ est fini et $P(\mathbb{C})$ est infini) et que $P(\mathbb{C})\backslash P(A)$ est ouvert et fermé dans $\mathbb{C}\backslash P(A)$, alors $P(\mathbb{C})\backslash P(A) = \mathbb{C}\backslash P(A)$.

Ainsi $\mathbb{C}\backslash P(A) \subset P(\mathbb{C})$ et $P(A) \subset P(\mathbb{C})$, donc $\mathbb{C} \subset P(\mathbb{C})$. Puisque $P(\mathbb{C}) \subset \mathbb{C}$, on peut conclure que

$$P(\mathbb{C}) = \mathbb{C}$$

Ce qui achève la preuve. □

1. En effet,

$$\left|\sum_{i=0}^{n} a_i z^i\right| \geqslant \left||a_n||z|^n - \left|\sum_{i=0}^{n-1} a_i z^i\right|\right|$$

$$\geqslant |z|^n \left||a_n| - \underbrace{\left|\frac{1}{|z|^n}\sum_{i=0}^{n-1} a_i z^i\right|}_{\xrightarrow[|z|\to\infty]{} 0}\right| \xrightarrow[|z|\to\infty]{} +\infty$$

Inversion de Pascal et nombre de surjections

Théorème 1 (Formule d'inversion de Pascal)**.** Soit $(a_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$. Si, pour tout $n \in \mathbb{N}$,

$$b_n = \sum_{k=0}^{n} \binom{n}{k} a_k,$$

alors, pour tout $n \in \mathbb{N}$,

$$a_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k.$$

Démonstration. On calcule $\displaystyle\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k$: pour tout $n \in \mathbb{N}$,

$$\begin{aligned}
\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \sum_{j=0}^{k} \binom{k}{j} a_j \\
&= \sum_{j=0}^{n} \sum_{k=j}^{n} (-1)^{n-k} \binom{n}{k} \binom{k}{j} a_j \text{ en intervertissant les deux } \Sigma \\
&= \sum_{j=0}^{n} \sum_{k=j}^{n} (-1)^{n-k} \frac{n!}{\cancel{k!}(n-k)!} \frac{\cancel{k!}}{j!(k-j)!} \frac{(n-j)!}{(n-j)!} a_j \\
&= \sum_{j=0}^{n} \sum_{k=j}^{n} (-1)^{n-k} \binom{n}{j} \binom{n-j}{k-j} a_j \\
&= \sum_{j=0}^{n} \binom{n}{j} a_j \sum_{l=0}^{n-j} (-1)^{n-l-j} \binom{n-j}{l} \text{ par le changement } l = k-j \\
&= \sum_{j=0}^{n} \binom{n}{j} a_j \underbrace{(1-1)^{n-j}}_{\delta_{n,j}} \\
&= a_n
\end{aligned}$$

□

Corollaire 4. Le nombre de surjections de $\{1, \dots, p\}$ vers $\{1, \dots, n\}$ est

$$\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} p^k.$$

Démonstration. Tout d'abord, on remarque qu'il faut $p \geqslant n$. On note $a_{p,k}$ le nombre de surjections de $\{1, \dots, p\}$ vers $\{1, \dots, k\}$.

Il y a n^p applications de $\{1, \dots, p\}$ vers $\{1, \dots, n\}$. On les dénombre en les partitionnant selon le cardinal de leur image. On note k le cardinal de l'image. Ainsi k varie entre 1 et n. Il y a $\binom{n}{k}$ façons de choisir k éléments parmi n. On remarque que les applications sont surjectives sur leur image. D'où

$$n^p = \sum_{k=0}^{n} \binom{n}{k} a_{p,k}$$

Ainsi, par la formule d'inversion de Pascal, on a

$$a_{p,n} = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^p.$$

□

La fonction de répartition F_X caractérise la loi de X

Ce résultat sert dans le développement sur la Formule d'inversion de la fonction caractéristique.

Définition 1 (Tribu)**.** On dit que $\mathcal{A} \subset \mathcal{P}(\Omega)$ est une tribu sur Ω si

(i) $\Omega \in \mathcal{A}$

(ii) $\mathcal{A}$ est stable par complémentaire (*i.e.* si $A \in \mathcal{A}$, alors $A^{\complement} \in \mathcal{A}$)

(iii) $\mathcal{A}$ est stable par réunion dénombrable.

Définition 2 (Classe monotone)**.** On dit que $\mathcal{M} \subset \mathcal{P}(\Omega)$ est une classe monotone sur Ω si

(i) $\Omega \in \mathcal{M}$

(ii) Si $A, B \in \mathcal{M}$ et $B \subset A$ alors $A \backslash B \in \mathcal{M}$

(iii) $\mathcal{M}$ est stable par réunion monotone croissante (*i.e.* si $A_i \in \mathcal{M}$, $A_i \subset A_{i+1}$, alors $\bigcup_{i \in \mathbb{N}} A_i \in \mathcal{M}$)

Théorème 1 (des classes monotones)**.** Soit $\mathcal{E}$ une famille de parties de Ω stable par intersection finie. Alors

$$m(\mathcal{E}) = \sigma(\mathcal{E})$$

où $m(\mathcal{E})$ est la classe monotone engendrée par $\mathcal{E}$ [1]et $\sigma(\mathcal{E})$ est la tribu engendrée par $\mathcal{E}$ [2].

Démonstration. On a l'inclusion $m(\mathcal{E}) \subset \sigma(\mathcal{E})$ car $\sigma(\mathcal{E})$ est une classe monotone qui contient $\mathcal{E}$. [3]

En effet,

(i) $\Omega \in \sigma(\mathcal{E})$ car $\sigma(\mathcal{E})$ est une tribu.

(ii) $A \setminus B = A \cap B^{\complement} \in \sigma(\mathcal{E})$.

(iii) stable par union monotone croissante car stable par union dénombrable.

Si $m(\mathcal{E})$ est stable par intersection finie, alors $m(\mathcal{E})$ est une tribu.

En effet,

(i) $\Omega \in m(\mathcal{E})$.

(ii) Si $A \in m(\mathcal{E})$, $A \subset \Omega$, alors $\Omega \setminus A = A^{\complement} \in m(\mathcal{E})$.

(iii) Si $A_i \in m(\mathcal{E})$, alors

$$\bigcup_{j \leqslant i} A_j \in m(\mathcal{E})$$

car c'est une réunion finie que l'on peut obtenir par intersections finies et complémentaires (deux opérations qui laissent stables l'ensemble $m(\mathcal{E})$). On peut alors écrire

$$\bigcup_{i \in \mathbb{N}} A_i = \bigcup_{i \in \mathbb{N}} \left(\bigcup_{j \leqslant i} A_j \right)$$

union croissante donc appartient à $m(\mathcal{E})$.

1. la plus petite classe monotone qui contient $\mathcal{E}$
2. la plus petite tribu qui contient $\mathcal{E}$
3. donc la plus petite classe monotone qui contient $\mathcal{E}$, autrement dit $m(\mathcal{E})$, est inclus dans $\sigma(\mathcal{E})$

Il faut maintenant montrer que $m(\mathcal{E})$ est stable par intersection finie.

Montrons que si $A, B \in m(\mathcal{E})$ alors $A \cap B \in (E)$. On pose l'ensemble

$$\mathcal{M}_1 := \{A \in m(\mathcal{E}), \quad \forall B \in \mathcal{E},\, A \cap B \in m(\mathcal{E})\}$$

On a $\mathcal{E} \subset \mathcal{M}_1$ (par hypothèse du théorème) et $\mathcal{M}_1$ est une classe monotone.

En effet,

(i) $\Omega \in \mathcal{M}_1$ puisque pour tout $B \in \mathcal{E}$, on a $\Omega \cap B \in \mathcal{E} \subset m(\mathcal{E})$.

(ii) Soit $A_1, A_2 \in \mathcal{M}_1$ avec $A_1 \subset A_2$. Soit $B \in \mathcal{E}$. On a $A_1 \cap B \in m(\mathcal{E})$ et $A_2 \cap B \in m(\mathcal{E})$ par définition de $\mathcal{M}_1$.

$$\begin{aligned}(A_2 \setminus A_1) \cap B &= A_2 \cap A_1^{\complement} \cap B \\ &= (A_2 \cap B) \cap A_1^{\complement} \\ &= \underbrace{(A_2 \cap B)}_{\in m(\mathcal{E})} \setminus \underbrace{(A_1 \cap B)}_{\in m(\mathcal{E})} \in m(\mathcal{E})\end{aligned}$$

Donc $A_2 \setminus A_1 \in \mathcal{M}_1$.

(iii) Soit (A_i) une suite croissante d'éléments de $\mathcal{M}_1$. Soit $B \in \mathcal{E}$. On a $A_i \cap B \in m(\mathcal{E})$ pour tout $i \in \mathbb{N}$. Comme $(A_i \cap B)$ est une suite croissante de $m(\mathcal{E})$, on a

$$\bigcup_{i \in \mathbb{N}} (A_i \cap B) \in m(\mathcal{E})$$

On a donc $\left(\bigcup_{i \in \mathbb{N}} A_i\right) \cap B \in m(\mathcal{E})$ et ainsi $\left(\bigcup_{i \in \mathbb{N}} A_i\right) \in \mathcal{M}_1$.

Ainsi, on a

$$m(\mathcal{E}) \subset \mathcal{M}_1.$$

On pose à présent l'ensemble

$$\mathcal{M}_2 := \{B \in m(\mathcal{E}), \forall C \in m(\mathcal{E}), B \cap C \in m(\mathcal{E})\}$$

L'ensemble $\mathcal{M}_2$ est une classe monotone (quasiment même preuve que pour $\mathcal{M}_1$).

Montrons que $\mathcal{E} \subset \mathcal{M}_2$.

Soit $B \in \mathcal{E}$, il faut montrer que pour tout $C \in m(\mathcal{E})$, on a $B \cap C \in m(\mathcal{E})$.
Or $C \in m(\mathcal{E}) \subset \mathcal{M}_1$, donc puisque $B \in \mathcal{E}$, on a $C \cap B \in m(\mathcal{E})$ (par définition de $\mathcal{M}_1$).
Ainsi $\mathcal{E} \subset \mathcal{M}_2$.

Donc $m(\mathcal{E}) \subset \mathcal{M}_2$.
Ainsi $m(\mathcal{E})$ est stable par intersection finie.

Comme $m(\mathcal{E})$ est une tribu et que $\mathcal{E} \subset \sigma(\mathcal{E})$, alors

$$\sigma(\mathcal{E}) \subset m(\mathcal{E}).$$

D'où l'égalité $\sigma(\mathcal{E}) = m(\mathcal{E})$. □

Définition 3 (Probabilité)**.** Une probabilité est une mesure $\mathbb{P}$ sur $(\Omega, \mathcal{A})$ de mesure pleine égale à 1 (*i.e.* $\mathbb{P}(\Omega) = 1$) telle que

- $\mathbb{P}(\emptyset) = 0$
- $\mathbb{P}\left(\bigsqcup_{i=0}^{+\infty} A_i\right) = \sum_{i=0}^{+\infty} \mathbb{P}(A_i)$ pour $A_i \in \mathcal{A}$ disjoints

Définition 4 (Variable aléatoire)**.** Une variable aléatoire X est une fonction mesurable de $(\Omega, \mathcal{F}, \mathbb{P})$ vers $(E, \mathcal{B})$ et $\mathbb{P}_X(A) = \mathbb{P}(X \in A) = \mathbb{P}(X^{-1}(A))$ pour $A \in \mathcal{B}$. De plus, si $E = \mathbb{R}$ et $\mathcal{B} = \mathcal{B}(\mathbb{R})$ [4], on dit que X est une variable aléatoire réelle.

Définition 5. On dit que deux variables aléatoires X et Y ont même loi si les mesures $\mathbb{P}_X$ et $\mathbb{P}_Y$ sont identiques sur $(E, \mathcal{B})$.

Définition 6 (Fonction de répartition)**.** Soit X une variable aléatoire réelle, on appelle fonction de répartition F_X de X, la fonction suivante

$$\forall t \in \mathbb{R}, \quad F_X(t) = \mathbb{P}(X \leqslant t)$$

Théorème 2. Soit X et Y deux variables aléatoires réelles de mesures de probabilités $\mathbb{P}_X$ et $\mathbb{P}_Y$ respectivement. Si $F_X = F_Y$ alors $\mathbb{P}_X = \mathbb{P}_Y$ et donc X et Y sont de même loi.

Démonstration. On pose $\Lambda = \{A \in \mathcal{B}(\mathbb{R}), \mathbb{P}_X(A) = \mathbb{P}_Y(A)\} = \{A \in \mathcal{B}(\mathbb{R}), \mathbb{P}(X \in A) = \mathbb{P}(Y \in A)\} \subset \mathcal{B}(\mathbb{R})$. On pose $\mathcal{E}$ l'ensemble des intervalles de la forme $]-\infty, a]$ pour $a \in \mathbb{R}$.

On a alors $\mathcal{E} \subset \Lambda$ puisque $F_X = F_Y$.

Montrons que Λ est une classe monotone sur $\mathbb{R}$.

(i) On a $\mathbb{R} \in \Lambda$ car $\mathbb{P}(X \in \mathbb{R}) = 1 = \mathbb{P}(Y \in \mathbb{R})$.

(ii) Soit $A_1, A_2 \in \Lambda$ avec $A_1 \subset A_2$, on a donc $\mathbb{P}(X \in A_1) = \mathbb{P}(Y \in A_1)$ et $\mathbb{P}(X \in A_2) = \mathbb{P}(Y \in A_2)$. Donc

$$\begin{aligned}\mathbb{P}(X \in A_2 \backslash A_1) &= \mathbb{P}(X \in A_2) - \mathbb{P}(X \in A_1) \\ &= \mathbb{P}(Y \in A_2) - \mathbb{P}(Y \in A_1) \\ &= \mathbb{P}(Y \in A_2 \backslash A_1)\end{aligned}$$

D'où $A_2 \backslash A_1 \in \Lambda$.

(iii) Soit $(A_i) \in \Lambda^{\mathbb{N}}$ est une suite croissante pour l'inclusion. On a donc $\mathbb{P}(X \in A_i) = \mathbb{P}(Y \in A_i)$ pour tout $i \in \mathbb{N}$. On pose $B_i = A_i \backslash A_{i-1}$, de sorte que

$$\bigcup_{i=0}^{+\infty} A_i = \bigsqcup_{i=1}^{+\infty} B_i$$

D'où

$$\begin{aligned}\mathbb{P}\left(X \in \bigcup_{i=0}^{+\infty} A_i\right) &= \mathbb{P}\left(X \in \bigsqcup_{i=1}^{+\infty} B_i\right) \\ &= \sum_{i=1}^{+\infty} \mathbb{P}(X \in B_i) \\ &= \sum_{i=1}^{+\infty} \mathbb{P}(X \in A_i) - \mathbb{P}(X \in A_{i-1})\end{aligned}$$

4. désigne les boréliens de $\mathbb{R}$, *i.e.* la plus petite tribu engendrée par les intervalles

$$= \sum_{i=1}^{+\infty} \mathbb{P}(Y \in A_i) - \mathbb{P}(Y \in A_{i-1})$$
$$= \mathbb{P}\left(Y \in \bigcup_{i=0}^{+\infty} A_i\right)$$

Donc $\bigcup_{i=0}^{+\infty} A_i \in \Lambda$.

Donc on a $m(\mathcal{E}) \subset \Lambda$ puisque Λ est une classe monotone. Or $\mathcal{E}$ est stable par intersections finies. Donc par le théorème des classes monotones, on a

$$\sigma(\mathcal{E}) = m(\mathcal{E}).$$

Or par définition des boréliens, on a

$$\sigma(\mathcal{E}) = \mathcal{B}(\mathbb{R}).$$

Donc $\mathcal{B}(\mathbb{R}) \subset \Lambda$. On peut donc conclure que

$$\Lambda = \mathcal{B}(\mathbb{R})$$

Ce qui montre que les variables aléatoires X et Y suivent la même loi. □

Lien entre irréductibles de $\mathbb{Q}[X]$ et de $\mathbb{Z}[X]$

On dit qu'un polynôme de $\mathbb{Z}[X]$ est **primitif** si le pgcd de ces coefficients vaut 1. On dit qu'un polynôme P est **irréductible** sur $A[X]$, s'il est non nul, non inversible dans $A[X]$ et que toute réduction $P = QR$ où $Q, R \in A[X]$ implique que soit Q, soit R est inversible. On notera $c(P)$ le **contenu** de P, autrement dit le pgcd des coefficients de P. On suppose connu le lemme de Gauss, qui dit que $c(PQ) = c(P)c(Q)$.

Théorème 1. Si $P \in \mathbb{Z}[X]$ et primitif et irréductible sur $\mathbb{Q}$, alors il est irréductible sur $\mathbb{Z}$.

Démonstration. Si P est réductible sur $\mathbb{Z}$, on peut écrire $P = QR$ où $Q, R \in \mathbb{Z}[X]$, et deg Q, deg $R \geqslant 1$ car P est primitif. Alors P est réductible sur $\mathbb{Q}$, car $Q, R \in \mathbb{Q}[X]$ et Q, R non inversible dans $\mathbb{Q}[X]$. □

Contre exemple : Si P n'est pas primitif, le résultat est faux. Par exemple $P = 2X$ est irréductible sur $\mathbb{Q}$, alors qu'il est réductible sur $\mathbb{Z}$: $P = 2 \times X$ car 2 et X ne sont pas inversibles dans $\mathbb{Z}$.

Proposition 1. Si $P \in \mathbb{Z}[X]$ est unitaire, alors P est primitif.

Démonstration. Si P est unitaire, son coefficient dominant est 1 par définition. Ainsi le pgcd de ces coefficients est 1, donc P est primitif. □

Théorème 2. Si P est irréductible sur $\mathbb{Z}$, alors P est primitif et irréductible sur $\mathbb{Q}$.

Démonstration. Par contraposée, si P n'est pas primitif, *i.e.* le pgcd des coefficients (notons le d) n'est pas 1, on peut factoriser P par d et donc $P = d\tilde{P}$ où d et $\tilde{P}$ sont non inversibles. Donc P est réductible.

Si P est primitif et réductible sur $\mathbb{Q}$, on peut écrire $P = QR$ où Q et R sont dans $\mathbb{Q}[X]$. On note q (resp. r) le ppcm des dénominateurs des coefficients de Q (resp. de R). On a donc qQ, $rR \in \mathbb{Z}[X]$. On peut noter $qrP = qQrR$. On a

$$c(qrP) = qr$$

car P est primitif. D'autre part, on a

$$c(qQrR) = c(qQ)c(rR)$$

car $qQ, rR \in \mathbb{Z}[X]$ et par le lemme de Gauss.

Or $\dfrac{qQ}{c(qQ)} \in \mathbb{Z}[X]$ et $\dfrac{rR}{c(rR)} \in \mathbb{Z}[X]$, donc

$$P = \frac{qQ}{c(qQ)} \frac{rR}{c(rR)}$$

Donc P est réductible dans $\mathbb{Z}[X]$. □

Le polynôme minimal est irréductible

Théorème 1. Le polynôme minimal d'un élément algébrique sur un corps est irréductible.

Démonstration. Soit K un corps. Soit L/K une extension de K. Soit $\alpha \in L/K$ un élément algébrique sur $\mathbb{K}$. On regarde l'application

$$ev_\alpha : \begin{cases} K[X] & \to & L \\ P & \mapsto & P(\alpha) \end{cases}$$

Le noyau de ev_α est l'idéal qui contient tous les polynômes qui annulent α. Comme $K[X]$ est principal (car K est un corps), il existe un polynôme Π_α tel que

$$\ker(ev_\alpha) = (\Pi_\alpha)$$

En quotientant par le noyau, on a

$$K[X]/(\Pi_\alpha) \simeq K[\alpha] \subset L$$

Or L est intègre (car c'est un corps) donc $K[\alpha]$ est intègre. Ainsi l'idéal (Π_α) est un idéal premier, donc Π_α est premier dans $K[X]$ donc irréductible. □

On a utilisé la propriété suivante :

Proposition 1. Dans un anneau intègre, un élément premier est irréductible.

Démonstration. Soit p un élément premier d'un anneau A intrègre. On sait que si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Pour montrer que p est irréductible, on suppose que $p = ab$, on veut montrer que soit a est inversible, soit b est inversible. On a $p \mid ab$ d'où $p \mid a$ ou $p \mid b$, on suppose que $p \mid a$ sans perte de généralité. Ainsi $a = pk$ avec $k \in A$. Donc $p = pkb$, d'où

$$p(1 - kb) = 0$$

Or $p \neq 0$ car p est premier (par définition de être premier). Donc

$$1 - kb = 0$$

par intégrité de A. Donc $kb = 1$ et ainsi b est inversible. □

Equivalence des normes non respectée

On pose l'espace vectoriel

$$E = \{a + \sqrt{2}b, a, b \in \mathbb{Q}\}$$

est un espace vectoriel de dimension 2. Donc il est de dimension finie.

On choisit deux normes différentes :

— $N_1(a + \sqrt{2}b) = |a + \sqrt{2}b|$

— $N_2(a + \sqrt{2}b) = |a| + |b|$

Ce sont bien des normes [1].

On pose la suite

$$x_n = (1 - \sqrt{2})^n = a_n + b_n\sqrt{2}$$

On a le résultat suivant :

$$N_1(x_n) \xrightarrow[n\to\infty]{} 0 \text{ car } |1 - \sqrt{2}| < 1$$

De plus,

$$(1 + \sqrt{2})^n = a_n - b_n\sqrt{2}$$

On le voit en développant le binôme de Newton [2].

Ainsi

$$a_n = \frac{(1 - \sqrt{2})^n + (1 + \sqrt{2})^n}{2}$$

Donc $|a_n| \xrightarrow[n\to\infty]{} +\infty$.

Cela prouve que

$$N_2(x_n) \xrightarrow[n\to\infty]{} +\infty \text{ car } N_2(x_n) \geqslant |a_n|$$

Or si les normes N_1 et N_2 étaient équivalentes on aurait $\alpha, \beta > 0$ tels que

$$\alpha N_1(x) \leqslant N_2(x) \leqslant \beta N_1(x) \text{ pour tout } x \in E$$

Or

$$N_1(x_n) \xrightarrow[n\to\infty]{} 0 \text{ et } N_2(x_n) \xrightarrow[n\to\infty]{} +\infty$$

On aboutit à une contradiction ! Pourquoi ? Il n'y a donc pas équivalence des normes en dimension finie ? ? ?

Solution sur la page suivante

1. N_1 est liée à la valeur absolue, N_2 est la norme 1 usuelle, il suffit de faire les calculs pour s'en convaincre, mais c'est vrai !

2. $(1 + \sqrt{2})^n = \sum_{k=0}^{n} \binom{n}{k} \sqrt{2}^k$ et $(1 - \sqrt{2})^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k \sqrt{2}^k$, il faut séparer les k pair et impair.

Il y a équivalence des normes en dimension sur un $\boxed{\mathbb{R}\text{- espace vectoriel}}$
Et ici, on était sur $\mathbb{Q}$.

Le problème est que dans la preuve de l'équivalence des normes, on a besoin du caractère compact de $\mathbb{S}^1$, or sur $\mathbb{Q}$ ce n'est pas vrai !

En fait, il suffit que le corps de l'espace vectoriel soit complet. [3]

3. Et $\mathbb{Q}$ n'est pas complet ! Oui bon ça va, on a compris !

6.2 Informatique

Borne inférieure Complexité des tris par comparaisons

On veut calculer le nombre minimal de comparaisons d'un algorithme de tri par comparaisons.

Soit un algorithme $\mathcal{A}$ de tri par comparaisons.

On dessine l'arbre binaire des comparaisons pour une entrée à n éléments à trier, il faut pouvoir séparer les $n!$ permutations par l'algo $\mathcal{A}$, autrement dit

$$\#F \geqslant n!$$

(F est l'ensemble des feuilles de l'arbre)

On a les relations suivantes pour un arbre binaire (N est l'ensemble des noeuds et h la hauteur de l'arbre)

$$\#F = \#N + 1 \qquad \text{et} \qquad \#N \leqslant 2^h$$

On a donc

$$n! - 1 \leqslant 2^h$$

Autrement dit

$$h \geqslant \log_2(n! - 1)$$

Or $\log n! = \sum_{k=1}^{n} \log k = \Theta(n \log n)$ [1], donc

$$h \geqslant \Omega(n \log n)$$

.

Il faut donc au moins $n \log n$ comparaisons pour trier n élements.

1. car la moitié des termes sont supérieurs à $\log \frac{n}{2}$, donc on peut minorer la somme par $\frac{n}{2} \log\left(\frac{n}{2}\right)$ et majorer la somme par $n \log n$ donc on a le Θ

Algorithmes classiques

La plupart des algorithmes que je cite ci-dessous sont tirés du Cormen [CLRS10].

Algorithmes sur les **graphes** :

— Prim pour trouver l'arbre couvrant minimal
— Kruskal pour trouver l'arbre couvrant minimal
— Ford Fulkerson pour trouver le flot maximal ou la coupe minimal
— Bellman Ford pour trouver le plus court chemin entre deux sommets
— Dijkstra pour trouver le plus court chemin entre deux sommets
— Floyd Warshall pour trouver le plus court chemin entre toute paire de deux sommets
— Kosaraju pour trouver les composantes fortement connexes
— Tarjan pour trouver les composantes fortement connexes
— Tri Topologique

Algorithmes de **tri** :

— Tri Bulle
— Tri par sélection
— Tri par insertion
— Tri Rapide
— Tri Fusion
— Tri par tas
— Tri par dénombrement
— Tri par base
— Tri par paquets
— Tri externe
— Tri topologique

Algorithmes du **texte** :

— Morris Pratt pour trouver les motifs d'un texte
— Knuth Morris Pratt pour trouver les motifs d'un texte
— Cocke Younger Kasami pour montrer qu'un mot appartient à une grammaire algébrique
— Analyse LL(1) pour faire de l'analyse syntaxique
— Plus longue sous séquence commune
— Distance d'édition

Algorithme sur des **automates** :

— Hopcroft pour trouver l'automate minimal

Algorithme pour la **logique** :

— Algorithme d'unification pour trouve l'unificateur principal de deux termes de logique du premier ordre

Une structure de dictionnaire est une structure de données avec un type abstrait demandant les opérations de Recherche, d'Insertion et de Suppression.

Structure de **dictionnaire** :

— Liste
— Tableau trié
— Arbre Binaire de Recherche
— Arbre Binaire de Recherche Optimal
— AVL
— Arbre Rouge Noir
— Arbre Splay
— B-arbre

Schémas algorithmiques

Voici quelques exemples d'algorithmes qui utilisent les paradigmes suivants : diviser pour régner, programmation dynamique, algorithmique gloutonne.

Cela est très utile pour la leçon 931 : Schémas algorithmiques. Exemples et applications..

Algorithmes utilisant **"diviser pour régner"** :

— Tri fusion
— Tri rapide
— Dichotomie
— Multiplication de matrices par la méthode de Strassen
— Théorème de Savitch
— Exponentiation rapide
— Hopcroft pour le calcul de l'automate minimal (voir [CAR14])

Algorithmes utilisant la **"programmation dynamique"** :

— Cocke–Younger–Kasami
— Coefficient binomial
— Fibonacci
— Floyd Warshall
— Distance d'édition
— Plus longue sous-séquence commune
— Découpe d'une barre
— Arbre binaire de recherche optimal

Algorithmes utilisant une **"approche gloutonne"** :

— Dijkstra
— Prim
— Kruskal
— Algorithme LL(1)
— Codage de Huffman
— Rendu de monnaie (non optimal) [1]
— Coloration d'un graphe (non optimal)

Il existe d'autres paradigmes de programmation comme le backtracking ou le branch and bound ...

1. Par exemple, faire 40 avec les pièces 5, 10, 20, 25. L'algorithme glouton donne $40 = 25 + 10 + 5$ alors qu'on peut faire $40 = 20 + 20$

Propriétés de clôture des langages rationnels et algébriques

Langages rationnels (RAT)	stable par	étoile de Kleene intersection union complémentaire concaténation
	non stable par	inclusion

Langages algébriques (ALG)	stable par	étoile de Kleene union concaténation intersection avec un langage rationnel
	non stable par	intersection complémentaire

Langages rationnels :

Les propriétés de stabilité des langages rationnels sont présentes dans le livre de Carton [CAR14]

Un contre exemple pour l'inclusion qui n'est pas stable pour les langages rationnels est :

$$\{a^n b^n, n \in \mathbb{N}\} \subset (a+b)^*$$

Le langage de gauche est algébrique non rationnel (utilisation du lemme de l'étoile pour le prouver), le langage de droite est rationnel (c'est déjà une expression rationnelle)

Langages algébriques :

Les propriétés de stabilité des langages algébriques sont présentes dans le livre de Carton [CAR14]

Un contre exemple pour l'intersection qui n'est pas stable pour les langages algébriques est :

$$\{a^n b^n c^m, n, m \in \mathbb{N}\} \cap \{a^m b^n c^n, n, m \in \mathbb{N}\}$$

Le langage obtenu est $\{a^n b^n c^n, n \in \mathbb{N}\}$ qui n'est algébrique (lemme de l'étoile pour les langages algébriques) alors que les deux autres le sont [1]

Et si le complémentaire était algébrique, l'intersection le serait puisque

$$A \cap B = (A \cup B) \setminus ((A \setminus B) \cup (B \setminus A))$$

1. la première partie est engendrée par la grammaire

$$S \to AT$$
$$A \to aAb \mid \varepsilon$$
$$T \to cT \mid \varepsilon$$

et l'autre par la grammaire

$$S \to AT$$
$$A \to aA \mid \varepsilon$$
$$T \to bTc \mid \varepsilon$$

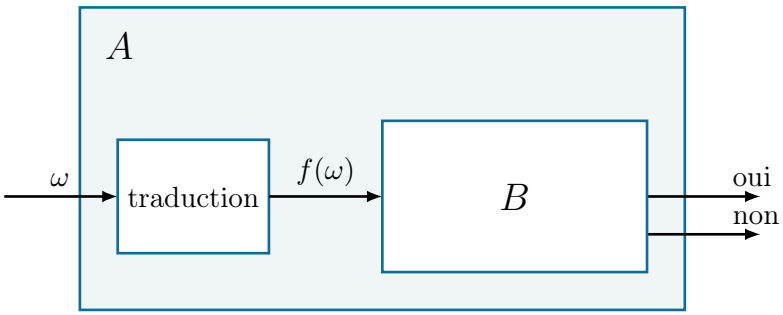
Problèmes NP-complets

On dit qu'un problème A est *dans NP* s'il existe une machine de Turing non nécessairement déterministe qui décide A en temps polynomial.

On appelle *réduction polynomiale* d'un problème A à un problème B, une fonction f calculable en temps polynomial par une machine de Turing déterministe telle que

$$w \text{ est une instance positive de A} \iff f(w) \text{ est une instance positive de B.}$$

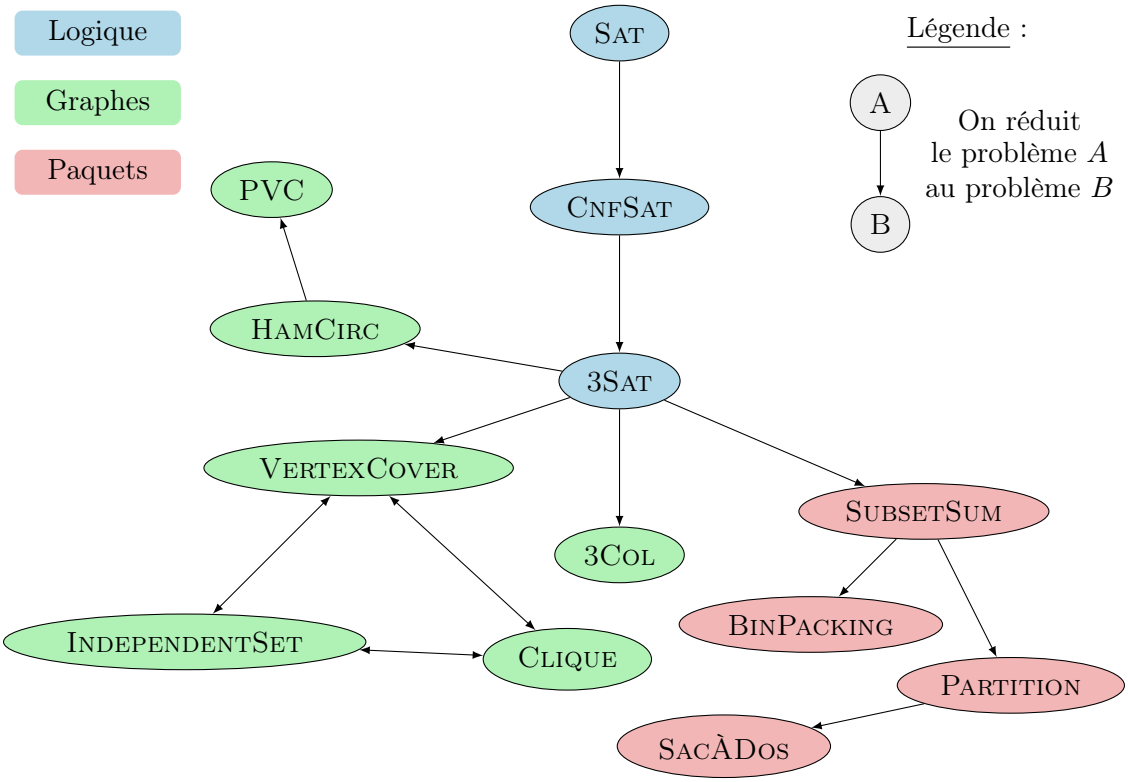
Si une telle réduction existe, on dit que A se réduit à B.



On dit qu'un problème A est *NP-dur* (ou *NP-difficile*) si, pour tout problème $L \in \mathsf{NP}$, L se réduit en temps polynomial à A.

Proposition 1. Si A est un problème NP-dur et qu'il existe une réduction de A à B, alors B est un problème NP-dur.

On dit qu'un problème A est *NP-complet* s'il est à la fois dans NP et NP-dur.



Exemple de schéma de réduction de problèmes NP-complets.

Sat
- entrée : une formule φ en calcul propositionnel ;
- sortie : oui si φ est satisfiable, non sinon.

CnfSat
- entrée : une formule φ en calcul propositionnel sous forme normale conjonctive ;
- sortie : oui si φ est satisfiable, non sinon.

3Sat
- entrée : une formule φ en calcul propositionnel sous forme normale conjonctive avec 3 littéraux par clause ;
- sortie : oui si φ est satisfiable, non sinon.

3Col
- entrée : un graphe $G = (S, A)$ non orienté ;
- sortie : oui s'il existe une application $c : S \to \{1, 2, 3\}$ telle que pour tout $(u, v) \in A$, $c(u) \neq c(v)$, non sinon.

VertexCover
- entrée : un graphe $G = (S, A)$ non orienté et un entier $j \leqslant |S|$;
- sortie : oui s'il existe $S' \subset S$ avec $|S'| \leqslant j$ telle que pour tout $(u, v) \in A$, $u \in S'$ ou $v \in S'$, non sinon.

IndependentSet
- entrée : un graphe $G = (S, A)$ non orienté et un entier $j \leqslant |S|$;
- sortie : oui s'il existe $S' \subset S$ avec $|S'| \geqslant j$ telle que pour tout $u, v \in S'$, $(u, v) \notin A$, non sinon.

Clique
- entrée : un graphe $G = (S, A)$ non orienté et un entier $j \leqslant |S|$;
- sortie : oui s'il existe $S' \subset S$ avec $|S'| \geqslant j$ telle que pour tout $u, v \in S'$, $(u, v) \in A$, non sinon.

HamCirc
- entrée : un graphe $G = (S, A)$ non orienté ;
- sortie : oui s'il existe un circuit qui passe une unique fois par chaque sommet (appelé circuit hamiltonien), non sinon.

PVC
- entrée : un graphe $G = (S, A)$ non orienté complet pondéré par des entiers relatifs et un entier $j \in \mathbb{Z}$;
- sortie : oui s'il existe un circuit hamiltonien de poids inférieur à j, non sinon.

SubsetSum
- entrée : un ensemble fini $A \subset \mathbb{N}$ et un entier $t \in \mathbb{N}$;
- sortie : oui s'il existe $A' \subset A$ tel que $\sum_{a \in A'} a = t$, non sinon.

BinPacking

$$\begin{cases} \underline{\text{entrée}} : & \text{un ensemble fini } A,\ w : A \to \mathbb{N} \text{ et deux entiers } c \text{ et } k \text{ de } \mathbb{N}\,; \\ \underline{\text{sortie}} : & \text{oui s'il existe une application } r : A \to [\![1;k]\!] \text{ telle que} \\ & \text{pour tout } j \in [\![1;k]\!],\ \displaystyle\sum_{a \in r^{-1}(j)} w(a) \leqslant c, \text{ non sinon.} \end{cases}$$

Partition

$$\begin{cases} \underline{\text{entrée}} : & \text{un ensemble fini } A \text{ et } w : A \to \mathbb{N}\,; \\ \underline{\text{sortie}} : & \text{oui s'il existe } A' \subset A \text{ tel que } \displaystyle\sum_{a \in A'} w(a) = \sum_{a \in A \setminus A'} w(a), \text{ non sinon.} \end{cases}$$

SacÀDos

$$\begin{cases} \underline{\text{entrée}} : & \text{un ensemble fini } A,\ w : A \to \mathbb{N},\ v : A \to \mathbb{N}, \\ & \text{un poids } P \text{ et une valeur } V\,; \\ \underline{\text{sortie}} : & \text{oui s'il existe } A' \subset A \text{ tel que } \displaystyle\sum_{u \in A'} w(u) \leqslant P \\ & \text{et } \displaystyle\sum_{u \in A'} v(u) \geqslant V, \text{ non sinon.} \end{cases}$$

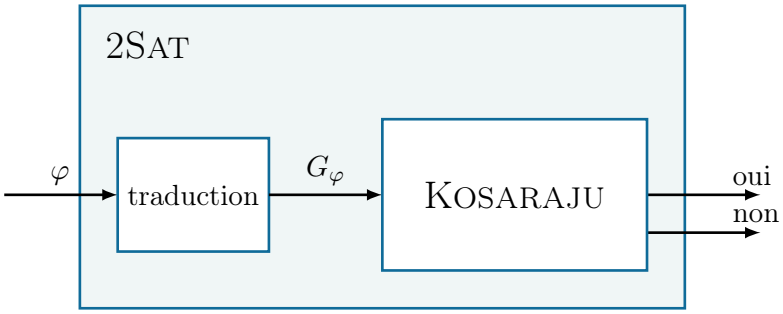
2SAT est dans P

On va étudier le problème 2SAT.

2SAT
- entrée : une formule φ en calcul propositionnel sous forme normale conjonctive avec 2 littéraux par clause ;
- sortie : oui si φ est satisfiable, non sinon.

Théorème 1. Le problème 2SAT est dans P.

Démonstration. On va réduire le problème 2SAT au problème des composantes fortement connexes. On peut trouver les composantes fortement connexes grâce à l'algorithme de Kosaraju.

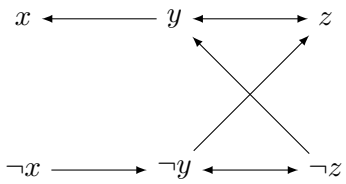


Soit φ une forme sous forme CNF avec 2 littéraux par clause. On pose le graphe $G_\varphi = (S, A)$ avec

$$S = \{x, \neg x, x \in VAR(\varphi)\}$$
$$A = \{(\neg a, b), (\neg b, a) \text{ pour } a \vee b \in \varphi\}$$

ici a et b sont des littéraux.

Exemple : La formule $\varphi = (x \vee \neg y) \wedge (\neg y \vee z) \wedge (y \vee \neg z) \wedge (y \vee z)$ donne le graphe G_φ suivant :



On veut montrer que

φ est satisfiable $\iff$ pour tout $x \in VAR(\varphi)$, x et $\neg x$ ne sont pas dans la même composante fortement connexe

$\boxed{\Longrightarrow}$ Soit ν une valuation satisfaisant φ.

Montrons que s'il existe un chemin de a à b et $\nu(a) = 1$, alors on a $\nu(b) = 1$, par récurrence sur la longueur n du chemin de a à b.

Initialisation : Pour $n = 1$, $(a, b) \in A$, donc $\neg a \vee b$ est une clause de φ. Comme $\nu(a) = 1$, on a $\nu(\neg a) = 0$, il faut donc que $\nu(b) = 1$ pour satisfaire φ.

Hérédité : Soit un chemin $a_0 \to a_1 \to \cdots \to a_{n+1}$ avec $\nu(a_0) = 1$. Par hypothèse de récurrence au rang n, on a $\nu(a_n) = 1$, puis, comme pour l'initialisation, on trouve que $\nu(a_{n+1}) = 1$.

Conclusion : Pour tout chemin de a à b de G_φ avec $\nu(a) = 1$, on a $\nu(b) = 1$.

Par l'absurde, si pour un certain $x \in VAR(\varphi)$, x et $\neg x$ était dans la même composante fortement connexe, on aurait un chemin de x à $\neg x$ et un chemin de $\neg x$ à x.

Supposons que $\nu(x) = 1$, alors $\nu(\neg x) = 1$, contradiction avec le résultat de la récurrence. De même, si $\nu(\neg x) = 1$, on aurait $\nu(x) = 1$, contradiction.

$\boxed{\Longleftarrow}$ Supposons que pour tout $x \in VAR(\varphi)$, x et $\neg x$ ne sont pas dans la même composante fortement connexe.

On va créer une valuation qui satisfait φ.

1) • S'il existe un chemin de $\neg l$ à l (où l est un littéral), alors on pose $\nu(l) = 1$ et $\nu(\neg l) = 0$.
   • Pour tout $l' \in \varphi$ tel qu'il existe un chemin de l à l' (avec $\nu(l) = 1$), on pose $\nu(l') = 1$.

   On itère le procédé jusqu'à saturation.
2) S'il reste des variables $x \in VAR(\varphi)$ sans affectation, on lui assigne 1 ainsi qu'à tous les l' tel qu'il existe un chemin de x à l'.

Vérifions que c'est vraiment une valuation, autrement dit, que l'on n'a pas affecté 0 et 1 à la même variable.

Par l'absurde, si pendant la phase 1), on a mis des variables x à 0 et à 1, c'est que l'on a

$$\neg l_1 \to^* l_1 \to^* x$$
$$\neg l_2 \to^* l_2 \to^* \neg x$$

Or, on peut remarquer que si $a \to^* b \in G_\varphi$, alors $\neg b \to^* \neg a \in G_\varphi$. Ainsi, on a

$$\neg x \to^* \neg l_1 \quad \text{et} \quad x \to^* \neg l_2$$

Ainsi, en mettant bout à bout les chemins, on trouve

$$l_1 \to^* \neg l_1$$

Absurde, car par hypothèse l_1 et $\neg l_1$ ne sont pas dans la même composante fortement connexe et on avait déjà $\neg l_1 \to^* l_1$.

Pour la phase 2), on procède de la même façon.

Montrons maintenant que cette valuation satisfait φ.

C'est le cas puisque s'il existe un chemin de l à l' avec $\nu(l) = 1$, alors $\nu(l') = 1$. De plus, toute clause $a \vee b \in \varphi$, on a un chemin $\neg a \to b$ et un chemin $\neg b \to a$. Ainsi, la clause $a \vee b$ est satisfaite par ν. □

Remarques :

Pour être plus précis, le problème 2SAT est dans NL. Il est même NL-complet.

Réductions classiques

Classe x	NL	P	NP	PSPACE
Définition	NL = $\mathrm{NSPACE}(n \mapsto \log(n))$ Problèmes décidés par une machine de Turing non déterministe en espace logarithmique	P = $\bigcup_{k \geqslant 0} \mathrm{TIME}(n \mapsto n^k)$ Problèmes décidés par une machine de Turing déterministe en temps polynomial	NP = $\bigcup_{k \geqslant 0} \mathrm{NTIME}(n \mapsto n^k)$ Problèmes décidés par une machine de Turing non déterministe en temps polynomial	PSPACE = $\bigcup_{k \geqslant 0} \mathrm{SPACE}(n \mapsto n^k)$ Problèmes décidés par une machine de Turing déterministe en espace polynomial
Réduction associée	$A \leqslant_{log} B$ $f : \Sigma_A^* \to \Sigma_B^*$ calculable par une machine de Turing déterministe en espace logarithmique telle que $w \in L_A$ SSI $f(w) \in L_B$	$A \leqslant_{log} B$ $f : \Sigma_A^* \to \Sigma_B^*$ calculable par une machine de Turing déterministe en espace logarithmique telle que $w \in L_A$ SSI $f(w) \in L_B$	$A \leqslant_P B$ $f : \Sigma_A^* \to \Sigma_B^*$ calculable par une machine de Turing déterministe en temps polynomial telle que $w \in L_A$ SSI $f(w) \in L_B$	$A \leqslant_P B$ $f : \Sigma_A^* \to \Sigma_B^*$ calculable par une machine de Turing déterministe en temps polynomial telle que $w \in L_A$ SSI $f(w) \in L_B$
On dit qu'un problème B est **x-dur**, si pour tout problème A dans la classe x, il existe une réduction (celle associée à x) telle que A se réduit à B.				
Si un problème B est à la fois dans x et x-dur, on dit que B est **x-complet**.				
Exemple de problèmes x-complet	— 2-SAT — PATH (accessibilité dans un graphe — VIDE pour un automate fini déterministe ou non déterministe	— HORN-SAT — MAX-FLOT — VIDE pour une grammaire algébrique	(voir la section des problèmes NP-complets)	— QBF-SAT — UNIV pour un automate fini non déterministe

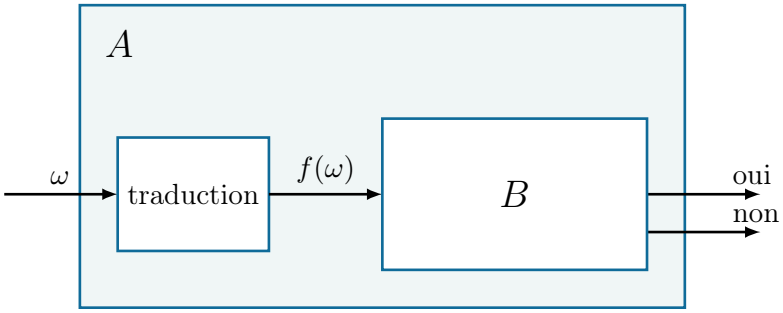
Problèmes indécidables et réduction

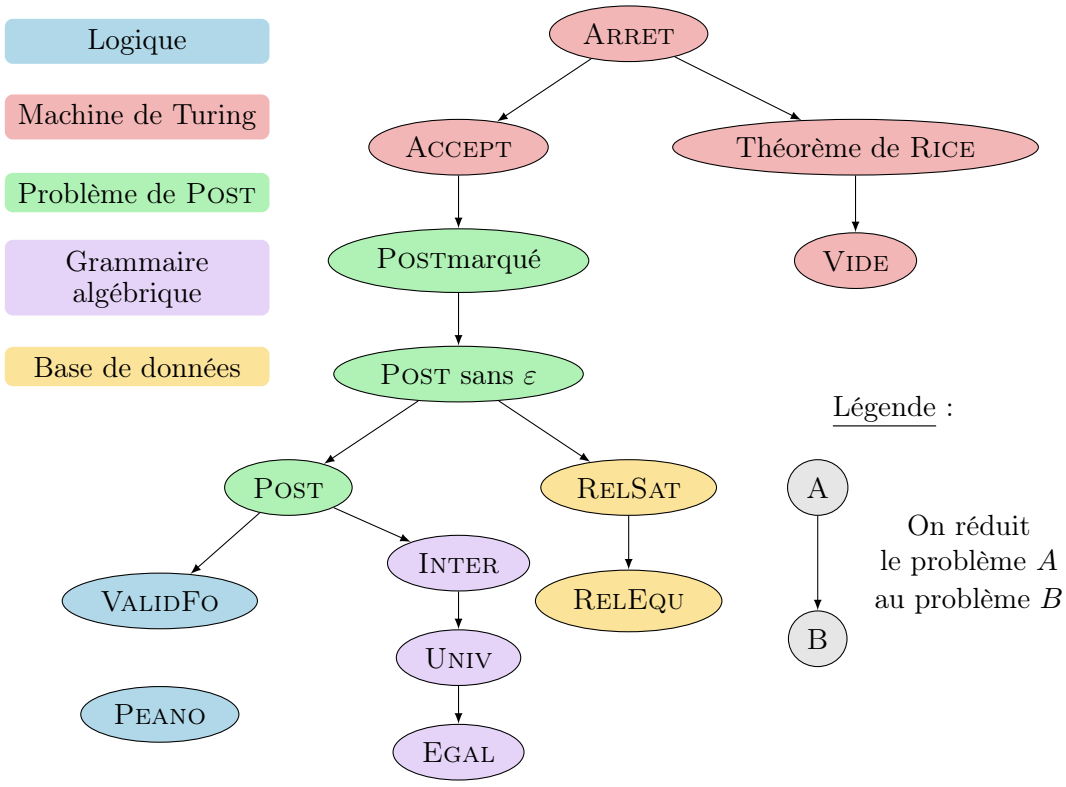
On dit qu'un problème A est *indécidable* s'il n'existe pas de machine de Turing qui décide le problème A.

On appelle *réduction* d'un problème A à un problème B, une fonction f calculable par une machine de Turing telle que

$$\omega \text{ est une instance positive de } A \iff f(\omega) \text{ est une instance positive de } B.$$

Si une telle réduction existe, on dit que A se réduit à B.





Le problème

Arret $\begin{cases} \underline{\text{entrée :}} \text{ une machine de Turing } M \text{ déterministe, un mot } w \\ \underline{\text{sortie :}} \text{ oui si } M(w) \text{ s'arrête, non sinon} \end{cases}$

est indécidable (construction d'une machine paradoxale) (voir le polycopié de calculabilité de François Schwarzentruber)

On réduit Arret à
ACCEPT { entrée : une machine de Turing M, un mot w
sortie : oui si M accepte w, non sinon
(voir le polycopié de calculabilité de François Schwarzentruber)

On réduit Accept à POSTmarqué

{ entrée : un alphabet fini Σ, un ensemble de tuiles fini $\left(\begin{array}{|c|}\hline u_i \\ \hline v_i \\ \hline\end{array}\right)_{i=1,\dots,n}$ avec $u_i, v_i \in \Sigma^*$
sortie : oui s'il existe $i_2, \dots, i_p \in \{1, \dots, n\}$ tels que $u_1 u_{i_2} \dots u_{i_p} = v_1 v_{i_2} \dots v_{i_p}$, non sinon
(voir le polycopié de calculabilité de François Schwarzentruber)

On réduit POSTmarqué à POST

{ entrée : un alphabet fini Σ, un ensemble de tuiles fini $\left(\begin{array}{|c|}\hline u_i \\ \hline v_i \\ \hline\end{array}\right)_{i=1,\dots,n}$ avec $u_i, v_i \in \Sigma^*$
sortie : oui s'il existe $i_1, \dots, i_p \in \{1, \dots, n\}$ tels que $u_{i_1} u_{i_2} \dots u_{i_p} = v_{i_1} v_{i_2} \dots v_{i_p}$, non sinon
(voir le polycopié de calculabilité de François Schwarzentruber)

On réduit Arret à $P_{\mathcal{P}}$ (Théorème de Rice) où $\emptyset \subsetneq \mathcal{P} \subsetneq RE$
$P_{\mathcal{P}}$ { entrée : une machine de Turing M
sortie : oui si $\mathrm{L}(M) \in \mathcal{P}$, non sinon
(voir le polycopié de calculabilité de François Schwarzentruber)

En prenant $\mathcal{P} = \{\emptyset\}$, on trouve l'indécidabilité de
VIDE { entrée : une machine de Turing M
sortie : oui si $\mathrm{L}(M) = \emptyset$, non sinon
(voir le polycopié de calculabilité de François Schwarzentruber)

On réduit Post à
VALIDFO { entrée : une formule close φ en logique du premier ordre
sortie : oui si φ est valide, non sinon
(voir Indécidabilité de la validité d'une formule du premier ordre)

On réduit Post à
INTER { entrée : deux grammaires algébriques G et G'
sortie : oui si $\mathrm{L}(G) \cap \mathrm{L}(G') = \emptyset$, non sinon
(voir Carton [CAR14, p.166])

On le réduit à
UNIV { entrée : une grammaire algébrique G
sortie : oui si $\mathrm{L}(G) = \Sigma^*$ où Σ est l'alphabet utilisé, non sinon
(voir Carton [CAR14, p.166])

On le réduit à

EGAL
- entrée : deux grammaires algébriques G et G'
- sortie : oui si $\mathrm{L}(G) = \mathrm{L}(G')$, non sinon

(voir Carton [CAR14, p.166])

On réduit POST à

POST sans ε
- entrée : des tuiles du problème de POST sans tuile contenant des ε
- sortie : oui si on peut trouver une suite de tuiles ayant le même mot en haut et en bas, non sinon

Je le fais plus bas

On réduit POST sans ε à

RELSAT
- entrée : une requête q en calcul relationnel
- sortie : oui si il existe $\mathcal{I}$ telle que $q(\mathcal{I}) \neq \emptyset$, non sinon

(voir Indécidabilité de la satisfiabilité d'une requête)

Le problème

RELEQU
- entrée : deux requêtes q et q' du calcul relationnel
- sortie : oui si q et q' sont sémantiquement équivalentes, non sinon

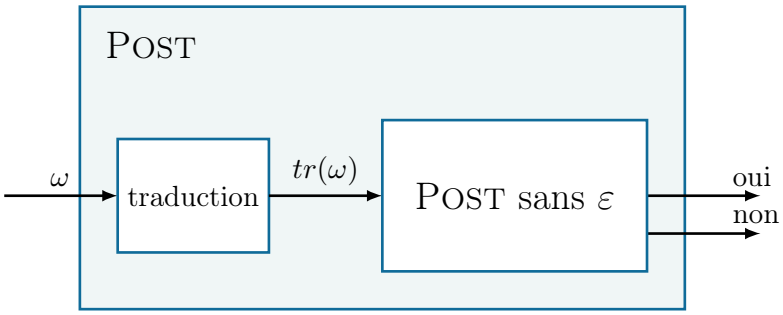
est indécidable.

Le problème

PEANO
- entrée : une formule φ close sur $L = \{0, 1, +, \times, =\}$
- sortie : oui si $\mathbb{N} \vDash \varphi$, non sinon

est indécidable. (preuve non triviale, non exigible à l'agrégation)

Réduction de POST à POST sans ε



Soit ω une instance de POST, i.e un nombre fini de tuiles $\begin{array}{|c|}\hline u_1 \\ \hline v_1 \\ \hline \end{array}, \ldots, \begin{array}{|c|}\hline u_N \\ \hline v_N \\ \hline \end{array}$ qui peut contenir des ε seulement en haut.

On veut trouver une instance $tr(\omega)$ de POST sans ε qui soit positive SSI ω est positive.

Pour toute tuile $\begin{array}{|c|}\hline \varepsilon \\ \hline a_1 \ldots a_k \\ \hline \end{array}$, on va mettre dans $tr(\omega)$ les tuiles :

$$\begin{array}{|c|}\hline \star \\ \hline \star a_1 \ldots a_k \\ \hline \end{array}, \begin{array}{|c|}\hline \star \\ \hline a_1 \star a_2 \ldots a_k \\ \hline \end{array}, \begin{array}{|c|}\hline \star \\ \hline a_1 a_2 \star a_3 \ldots a_k \\ \hline \end{array}, \ldots, \begin{array}{|c|}\hline \star \\ \hline a_1 a_2 \ldots a_k \star \\ \hline \end{array}$$

Et pour chaque tuile $\begin{array}{|c|}\hline b_1\dots b_l \\ \hline a_1\dots a_k \\ \hline \end{array}$, on va mettre dans $tr(\omega)$ les tuiles :

$$\begin{array}{|c|}\hline b_1\dots b_l \\ \hline \star a_1\dots a_k \\ \hline \end{array}, \begin{array}{|c|}\hline b_1\dots b_l \\ \hline a_1\star a_2\dots a_k \\ \hline \end{array}, \begin{array}{|c|}\hline b_1\dots b_l \\ \hline a_1a_2\star a_3\dots a_k \\ \hline \end{array}, \dots, \begin{array}{|c|}\hline b_1\dots b_l \\ \hline a_1\dots a_k\star \\ \hline \end{array}$$

et on met aussi la tuile $\begin{array}{|c|}\hline b_1\dots b_l \\ \hline a_1\dots a_k \\ \hline \end{array}$ dans $tr(\omega)$.

$\boxed{\Longrightarrow}$ Si $tr(\omega)$ est une instance positive de Post sans ε, on prend une succession de tuiles telle que le mot du haut est identique au mot du bas.

S'il y a une $\star$ en haut, alors il suffit de placer la tuile $\begin{array}{|c|}\hline \varepsilon \\ \hline a_1\dots a_k \\ \hline \end{array}$ correspondante au bon endroit dans la succession de tuiles de ω. Sinon, il suffit de faire la même succession puisque toutes les tuiles sans $\star$ sont dans ω. Ainsi ω est une instance positive du problème Post.

$\begin{array}{|c|}\hline a \\ \hline ab \\ \hline \end{array}\begin{array}{|c|}\hline ba \\ \hline a\star b \\ \hline \end{array}\begin{array}{|c|}\hline \star \\ \hline ba \\ \hline \end{array}\begin{array}{|c|}\hline bbaa \\ \hline a \\ \hline \end{array}$ devient $\begin{array}{|c|}\hline a \\ \hline ab \\ \hline \end{array}\begin{array}{|c|}\hline ba \\ \hline ab \\ \hline \end{array}\begin{array}{|c|}\hline \varepsilon \\ \hline ba \\ \hline \end{array}\begin{array}{|c|}\hline bbaa \\ \hline a \\ \hline \end{array}$

$\boxed{\Longleftarrow}$ Si ω est une instance positive de Post, on prend une succession de tuiles telle que le mot du haut est identique au mot du bas. Si on a utilisé une tuile $\begin{array}{|c|}\hline \varepsilon \\ \hline a_1\dots a_k \\ \hline \end{array}$ alors on la remplace par $\begin{array}{|c|}\hline \star \\ \hline a_1\dots a_k \\ \hline \end{array}$ et on remplace la tuile où le ε serait en bas, par la même mais avec le $\star$ au bon endroit. Ainsi $tr(\omega)$ est une instance positive de Post sans ε.

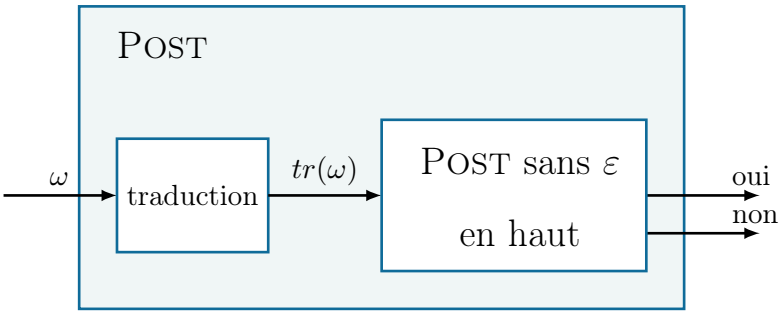
$\begin{array}{|c|}\hline a \\ \hline ab \\ \hline \end{array}\begin{array}{|c|}\hline ba \\ \hline ab \\ \hline \end{array}\begin{array}{|c|}\hline \varepsilon \\ \hline ba \\ \hline \end{array}\begin{array}{|c|}\hline bbaa \\ \hline a \\ \hline \end{array}$ devient $\begin{array}{|c|}\hline a \\ \hline ab \\ \hline \end{array}\begin{array}{|c|}\hline ba \\ \hline a\star b \\ \hline \end{array}\begin{array}{|c|}\hline \star \\ \hline ba \\ \hline \end{array}\begin{array}{|c|}\hline bbaa \\ \hline a \\ \hline \end{array}$

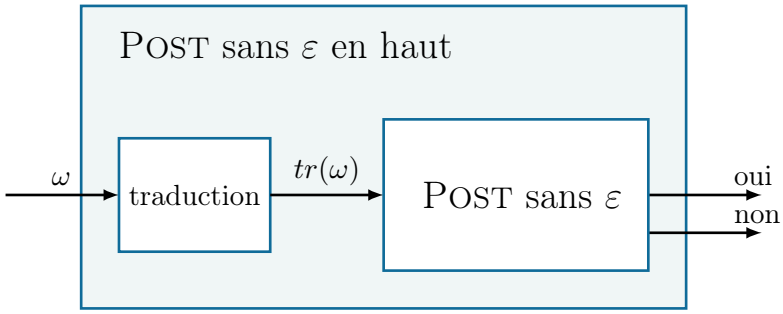
Ensuite si on a des ε en haut et en bas, on peut faire la réduction en deux temps, pour enlever les ε du haut puis ensuite ceux du bas.

Tout cela montre que Post sans ε est indécidable.

Remarques :

En fait, on peut voir ça comme deux réductions successives





Remarques :

En fait, si on regarde plus attentivement la réduction de ACCEPT à POSTmarqué et POSTmarqué à POST, on observe que l'on a pas de tuiles avec des ε ni en haut ni en bas, donc finalement, on avait déjà l'indécidabilité de POST sans ε, cependant c'est un bon exercice de savoir faire des réductions comme ça à partir de variantes de problème que l'on connait.

Fonctions primitives récursives usuelles

Les fonctions de base des fonctions primitives récursives :

$$\mathsf{zéro} : \begin{cases} \setminus & \to & \mathbb{N} \\ & \mapsto & 0 \end{cases} \quad \text{d'arité } 0$$

$$\mathsf{succ} : \begin{cases} \mathbb{N} & \to & \mathbb{N} \\ x & \mapsto & x+1 \end{cases} \quad \text{d'arité } 1$$

$$\pi_i^n : \begin{cases} \mathbb{N}^n & \to & \mathbb{N} \\ (x_1, \dots, x_n) & \mapsto & x_i \end{cases} \quad \text{d'arité } n$$

L'ensemble des fonctions primitives récursives est clos par composition :
Si φ est d'arité k et $\psi_1, \dots, \psi_k$ sont d'arité n, alors on peut définir

$$\mathsf{comp}(\varphi, \psi_1, \dots, \psi_k) : \begin{cases} \mathbb{N}^n & \to & \mathbb{N} \\ \vec{x} = (x_1, \dots, x_n) & \mapsto & \varphi(\psi_1(\vec{x}), \dots, \psi_k(\vec{x})) \end{cases} \quad \text{d'arité } n$$

On notera $\circ(\varphi, \psi_1, \dots, \psi_k)$ pour $\mathsf{comp}(\varphi, \psi_1, \dots, \psi_k)$

L'ensemble des fonctions primitives récursives est clos par récursion primitive :
Si f est d'arité n et g sont d'arité $n+2$, alors on peut définir

$$\mathsf{rec}(f,g) : \begin{cases} \mathbb{N}^n \times \mathbb{N} & \to & \mathbb{N} \\ (\vec{x}, k) & \mapsto & \begin{cases} f(\vec{x}) & \text{si } k = 0 \\ g(\vec{x}, k-1, \mathsf{rec}(f,g)(\vec{x}, k-1)) & \text{sinon} \end{cases} \end{cases} \quad \text{d'arité } n+1$$

Voici quelques fonctions primitives récursives que l'on peut construire :

- plus : $\begin{cases} \mathbb{N}^2 & \to & \mathbb{N} \\ (x,y) & \mapsto & x+y \end{cases}$ d'arité 2

$$\mathsf{plus} = \mathsf{rec}(\pi_1^1, \circ(\mathsf{succ}, \pi_3^3))$$

- mult : $\begin{cases} \mathbb{N}^2 & \to & \mathbb{N} \\ (x,y) & \mapsto & x \times y \end{cases}$ d'arité 2

$$\mathsf{mult} = \mathsf{rec}(\mathsf{zero}, \circ(\mathsf{plus}, \pi_1^3, \pi_3^3))$$

- power : $\begin{cases} \mathbb{N}^2 & \to & \mathbb{N} \\ (x,y) & \mapsto & x^y \end{cases}$ d'arité 2

$$\mathsf{power} = \mathsf{rec}(\mathsf{succ}(\mathsf{zero}), \circ(\mathsf{mult}, \pi_1^3, \pi_3^3))$$ [1]

- ▶ prédecesseur : $\begin{cases} \mathbb{N} & \to & \mathbb{N} \\ k & \mapsto & \begin{cases} k-1 & \text{si } k > 0 \\ 0 & \text{sinon} \end{cases} \end{cases}$ d'arité 1

$$\mathsf{pred} = \mathsf{rec}(\mathsf{zero}, \pi_2^3)$$

- ▶ diff : $\begin{cases} \mathbb{N}^2 & \to & \mathbb{N} \\ (x,y) & \mapsto & \begin{cases} x-y & \text{si } x-y > 0 \\ 0 & \text{sinon} \end{cases} \end{cases}$ d'arité 2

$$\mathsf{diff} = \mathsf{rec}(\mathsf{zero}, \circ(\mathsf{pred}, \pi_3^3))$$

Minimisation bornée :

- ▶ $\mu(i \leqslant .)(P(.))$: $\begin{cases} \mathbb{N} \times \mathbb{N}^n & \to & \mathbb{N} \\ (n, \vec{x}) & \mapsto & \begin{cases} \text{le plus petit entier } i \leqslant n \\ \text{tel que } P(\vec{x}) \text{ est vrai} \\ n+1 \text{ s'il n'existe pas} \end{cases} \end{cases}$ [2] d'arité $n+1$

$$\mu(i \leqslant n)(P(\vec{x})) = \sum_{i=0}^{n} \prod_{k=0}^{i} (1 - P(\vec{x}))$$

- ▶ division euclidienne : $\begin{cases} \mathbb{N}^2 & \to & \mathbb{N} \\ (x,y) & \mapsto & x//y \end{cases}$ d'arité 2

$$\mathsf{div}(a,b) = \mu(i \leqslant a)(a - i * b < 0) - 1$$

1. on a écrit ici $\mathsf{succ}(\mathsf{zero})$ pour $\circ(\mathsf{succ}, \mathsf{zero})$
2. P représente un prédicat primitif, on l'identifie à son indicatrice

- ▶ modulo : $\begin{cases} \mathbb{N}^2 & \to & \mathbb{N} \\ (x,y) & \mapsto & x\ [y] \end{cases}$ d'arité 2

  $\mathsf{mod}(a,b) = a - (a//b) * b$

- ▶ is_zero : $\begin{cases} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & \begin{cases} 1 & \text{si } n = 0 \\ 0 & \text{sinon} \end{cases} \end{cases}$ d'arité 1

  $\mathsf{is_zero} = \mathsf{rec}(\mathsf{succ}(\mathsf{zero}), \mathsf{zero})$

- ▶ egal_k : $\begin{cases} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & \begin{cases} 1 & \text{si } n = k \\ 0 & \text{sinon} \end{cases} \end{cases}$ d'arité 1

  $\mathsf{egal_k}(n) = (\mathsf{is_zero}(\mathsf{diff}(n,k)) + \mathsf{is_zero}(\mathsf{diff}(k,n)))//2$

- ▶ sign : $\begin{cases} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & \begin{cases} 1 & \text{si } n > 0 \\ 0 & \text{sinon} \end{cases} \end{cases}$ d'arité 1

  $\mathsf{sign} = \mathsf{rec}(\mathsf{zero}, \mathsf{succ}(\mathsf{zero}))$

- ▶ superieur : $\begin{cases} \mathbb{N}^2 & \to & \mathbb{N} \\ (x,y) & \mapsto & \begin{cases} 1 & \text{si } x > y \\ 0 & \text{sinon} \end{cases} \end{cases}$ d'arité 2

  $\mathsf{superieur}(x,y) = \circ(\mathsf{sign}, \mathsf{diff}(x,y))$

Bijection primitive récursive dont la réciproque l'est aussi :

► φ : $\left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N}^2 \\ k & \mapsto & (\mathsf{diag}(k) - \mathsf{ecart}(k), \mathsf{ecart}(k)) \end{array} \right.$

avec $\mathsf{diag}(k) = \mu(i \leqslant k+1)(\frac{i(i+1)}{2} > k) - 1$

$$\mathsf{ecart}(k) = k - \frac{\mathsf{diag}(k)(\mathsf{diag}(k)+1)}{2}$$

Sémantiques du langage de programmation IMP

On va étudier deux sémantiques différentes (la sémantique opérationnelle et la sémantique dénotationnelle) sur le langage IMP.

Pour introduire le langage IMP, on va avoir besoin de nombres, de variables, d'expressions arithmétiques, d'expressions booléennes munis de leur sémantique. Ainsi on pourra ensuite définir la syntaxe des instructions puis donner différentes sémantiques sur cette syntaxe.

On définit les nombres Num :
Syntaxe :

$$n ::= 0 \mid 1 \mid n0 \mid n1 \mid -n.$$

Sémantique :

$$\mathcal{N} : \mathsf{Num} \to \mathbb{Z}$$

définie par induction structurelle

$$\begin{aligned} \mathcal{N}[\![0]\!] &= 0; & \mathcal{N}[\![n0]\!] &= 2.\mathcal{N}[\![n]\!]; \\ \mathcal{N}[\![1]\!] &= 1; & \mathcal{N}[\![n1]\!] &= 2.\mathcal{N}[\![n]\!] + 1; \\ & & \mathcal{N}[\![-n]\!] &= -\mathcal{N}[\![n]\!]. \end{aligned}$$

On définit les variables Var par un ensemble de symboles $\{x, y, z, \dots\}$. On peut définir alors une mémoire

$$\mathsf{State} : \mathsf{Var} \to \mathbb{Z}.$$

On notera la mémoire $s = [x \mapsto 2, y \mapsto 7, \dots]$. On suppose qu'elle est totale.

On définit les expressions arithmétiques Aexp :
Syntaxe :

$$a ::= n \mid x \mid a_1 + a_2 \mid a_1 * a_2 \mid a_1 - a_2.$$

Sémantique :

$$\mathcal{A} : \mathsf{Aexp} \to (\mathsf{State} \to \mathbb{Z})$$

définie par induction structurelle

$$\begin{aligned} \mathcal{A}[\![n]\!]_s &= \mathcal{N}[\![n]\!]; & \mathcal{A}[\![a_1 + a_2]\!]_s &= \mathcal{A}[\![a_1]\!]_s + \mathcal{A}[\![a_2]\!]_s; \\ \mathcal{A}[\![x]\!]_s &= s(x); & \mathcal{A}[\![a_1 * a_2]\!]_s &= \mathcal{A}[\![a_1]\!]_s.\mathcal{A}[\![a_2]\!]_s; \\ & & \mathcal{A}[\![a_1 - a_2]\!]_s &= \mathcal{A}[\![a_1]\!]_s - \mathcal{A}[\![a_2]\!]_s; \end{aligned}$$

On définit les expressions booléennes Bexp :
Syntaxe :

$$b ::= \mathsf{true} \mid \mathsf{false} \mid a_1 = a_2 \mid a_1 \leqslant a_2 \mid \neg b \mid b_1 \wedge b_2.$$

Sémantique :

$$\mathcal{B} : \mathsf{Bexp} \to (\mathsf{State} \to \{tt, ff\})$$

définie par induction structurelle

$$\mathcal{B}[\![\mathsf{true}]\!]_s = tt; \qquad \mathcal{B}[\![\neg b]\!]_s = \begin{cases} tt & \text{si } \mathcal{B}[\![b]\!]_s = ff \\ ff & \text{si } \mathcal{B}[\![b]\!]_s = tt \end{cases};$$

$$\mathcal{B}[\![\mathsf{false}]\!]_s = ff; \qquad \mathcal{B}[\![b_1 \wedge b_2]\!]_s = \begin{cases} tt & \text{si } \mathcal{B}[\![b_1]\!]_s = \mathcal{B}[\![b_2]\!]_s = tt \\ ff & \text{sinon} \end{cases};$$

$$\mathcal{B}[\![a_1 = a_2]\!]_s = \begin{cases} tt & \text{si } \mathcal{A}[\![a_1]\!]_s = \mathcal{A}[\![a_2]\!]_s \\ ff & \text{si } \mathcal{A}[\![a_1]\!]_s \neq \mathcal{A}[\![a_2]\!]_s \end{cases};$$

$$\mathcal{B}[\![a_1 \leqslant a_2]\!]_s = \begin{cases} tt & \text{si } \mathcal{A}[\![a_1]\!]_s \leqslant \mathcal{A}[\![a_2]\!]_s \\ ff & \text{si } \mathcal{A}[\![a_1]\!]_s > \mathcal{A}[\![a_2]\!]_s \end{cases}.$$

Avant d'introduire la syntaxe des instructions du langage IMP, on va définir la substitution (opération syntaxique) :

On note la substitution $a_1[x \to a_2]$ définie par

$$\begin{aligned} n[x \to a] &= n; \\ x[x \to a] &= a; \\ y[x \to a] &= y \ (\text{si } y \neq x); \\ (a_1 + a_2)[x \to a] &= a_1[x \to a] + a_2[x \to a]; \\ (a_1 - a_2)[x \to a] &= a_1[x \to a] - a_2[x \to a]; \\ (a_1 * a_2)[x \to a] &= a_1[x \to a] * a_2[x \to a]; \\ \mathcal{A}[\![a[y \to a_0]]\!]_s &= \mathcal{A}[\![a]\!]_{(s[y \mapsto \mathcal{A}[\![a_0]\!]_s])}. \end{aligned}$$

On peut maintenant définir la syntaxe des instructions statement du langage IMP :

$$S ::= x := a \mid \mathsf{skip} \mid S_1; S_2 \mid \ \mathsf{if}\ b\ \mathsf{then}\ S_1\ \mathsf{else}\ S_2 \mid \mathsf{while}\ b\ \mathsf{do}\ S$$

où

- $x := a$ représente l'affectation de la valeur a à la variable x,
- skip représente l'instruction vide (qui ne fait rien),
- $S_1; S_2$ représente la séquence d'instructions (on va faire l'instruction S_1 puis l'instruction S_2),
- if b then S_1 else S_2 représente la conditionnelle,
- while b do S représente la boucle while.

On va maintenant définir des sémantiques différentes sur la syntaxe du langage IMP.

Sémantique opérationnelle à grands pas (ou sémantique naturelle) : On va définir les règles de dérivation de la sémantique à grands pas :

$$[\mathsf{skip}_{NS}] \qquad \langle \mathsf{skip}, s \rangle \to s$$

$$[\mathsf{ass}_{NS}] \qquad \langle x := a, s \rangle \to s\,[x \mapsto \mathcal{A}[\![a]\!]_s]$$

$$[\text{comp}_{NS}] \qquad \frac{\langle S_1, s\rangle \to s' \qquad \langle S_2, s'\rangle \to s''}{\langle S_1; S_2, s\rangle \to s''}$$

$$[\text{if}^{tt}_{NS}] \qquad \frac{\langle S_1, s\rangle \to s'}{\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \to s'} \text{ si } \mathcal{B}[\![b]\!]_s = tt$$

$$[\text{if}^{ff}_{NS}] \qquad \frac{\langle S_2, s\rangle \to s'}{\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \to s'} \text{ si } \mathcal{B}[\![b]\!]_s = ff$$

$$[\text{while}^{tt}_{NS}] \qquad \frac{\langle S, s\rangle \to s' \ \langle \text{while } b \text{ do } S, s'\rangle \to s''}{\langle \text{while } b \text{ do } S, s\rangle \to s''} \text{ si } \mathcal{B}[\![b]\!]_s = tt$$

$$[\text{while}^{ff}_{NS}] \qquad \langle \text{while } b \text{ do } S, s\rangle \to s \text{ si } \mathcal{B}[\![b]\!]_s = ff.$$

La sémantique à grands pas est donc définie par

$$\mathcal{S}_{ns}[\![S]\!]_s = \begin{cases} s' & \text{si on a } \langle S, s\rangle \to s' \\ undef & \text{sinon} \end{cases}.$$

Sémantique opérationnelle à petits pas :

On va définir les règles de dérivation de la sémantique à petits pas :

$$[\text{skip}_{SOS}] \qquad \langle \text{skip}, s\rangle \Rightarrow s$$

$$[\text{ass}_{SOS}] \qquad \langle x := a, s\rangle \Rightarrow s\,[x \mapsto \mathcal{A}[\![a]\!]_s]$$

$$[\text{comp}^{1}_{SOS}] \qquad \frac{\langle S_1, s\rangle \Rightarrow \langle S_1', s'\rangle}{\langle S_1; S_2, s\rangle \Rightarrow \langle S_1'; S_2, s'\rangle}$$

$$[\text{comp}^{2}_{SOS}] \qquad \frac{\langle S_1, s\rangle \Rightarrow s'}{\langle S_1; S_2, s\rangle \Rightarrow \langle S_2, s'\rangle}$$

$$[\text{if}^{tt}_{SOS}] \qquad \langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \Rightarrow \langle S_1, s\rangle \text{ si } \mathcal{B}[\![b]\!]_s = tt$$

$$[\text{if}^{ff}_{SOS}] \qquad \langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \Rightarrow \langle S_2, s\rangle \text{ si } \mathcal{B}[\![b]\!]_s = ff$$

$$[\text{while}_{SOS}] \quad \langle \text{while } b \text{ do } S, s\rangle \Rightarrow \langle \text{ if } b \text{ then } (S; \text{while } b \text{ do } S) \text{ else skip}, s\rangle.$$

La sémantique à petits pas est donc définie par

$$\mathcal{S}_{sos}[\![S]\!]_s = \begin{cases} s' & \text{si on a } \langle S, s\rangle \Rightarrow^* s' \\ undef & \text{sinon} \end{cases}.$$

Théorème 1. Pour toute instruction S du langage IMP, on a

$$\mathcal{S}_{ns}[\![S]\!] = \mathcal{S}_{sos}[\![S]\!].$$

La preuve de ce résultat fait l'objet du développement : Équivalence entre sémantiques opérationnelles.

Sémantique dénotationnelle :

On pose la fonction

$$\mathcal{S}_{ds} : \mathsf{statement} \to (\mathsf{State} \to \mathsf{State})$$

définie par

$$\begin{aligned} \mathcal{S}_{ds}[\![x := a\ ]\!]_s &= s[x \mapsto \mathcal{A}[\![a]\!]_s]; \\ \mathcal{S}_{ds}[\![\mathsf{skip}\ ]\!]_s &= \mathrm{Id}; \\ \mathcal{S}_{ds}[\![S_1; S_2\ ]\!] &= \mathcal{S}_{ds}[\![S_2\ ]\!] \circ \mathcal{S}_{ds}[\![S_1\ ]\!]; \\ \mathcal{S}_{ds}[\![\ \mathsf{if}\ b\ \mathsf{then}\ S_1\ \mathsf{else}\ S_2\ ]\!] &= cond(\mathcal{B}[\![b]\!], \mathcal{S}_{ds}[\![S_1]\!], \mathcal{S}_{ds}[\![S_2]\!]); \\ \mathcal{S}_{ds}[\![\mathsf{while}\ b\ \mathsf{do}\ S\ ]\!] &= \mathrm{Fix}F. \end{aligned}$$

avec

$$cond : (\mathsf{State} \to \{tt, ff\}) \times (\mathsf{State} \to \mathsf{State}) \times (\mathsf{State} \to \mathsf{State}) \to (\mathsf{State} \to \mathsf{State})$$

définie par

$$cond(f, \sigma_1, \sigma_2)s = \begin{cases} \sigma_1 s & \text{si } fs = tt \\ \sigma_2 s & \text{si } fs = ff \end{cases}$$

et

$$F : \begin{array}{ccc} (\mathsf{State} \to \mathsf{State}) & \to & (\mathsf{State} \to \mathsf{State}) \\ g & \mapsto & cond(\mathcal{B}[\![b]\!], g \circ \mathcal{S}_{ds}[\![S]\!], \mathrm{Id}) \end{array}.$$

L'opérateur Fix est un opérateur de point fixe.

$$\mathrm{Fix} : ((\mathsf{State} \to \mathsf{State}) \to (\mathsf{State} \to \mathsf{State})) \to (\mathsf{State} \to \mathsf{State}).$$

On développe cette théorie dans le livre [NN07].

Théorème 2. Pour toute instruction S du langage IMP, on a

$$\mathcal{S}_{sos}[\![S]\!] = \mathcal{S}_{ds}[\![S]\!].$$

Ainsi les trois sémantiques que l'on a vu sont équivalentes.

Logique de Hoare :

On va étudier la correction partielle de programmes sur le langage IMP grâce à la logique de Hoare.

Définition 2. On appelle triplet de Hoare le triplet suivant

$$\{P\}S\{Q\}$$

où P et Q sont des prédicats et S une instruction du langage IMP.

Il faut comprendre que P est un prédicat vrai avant le programme et Q est un prédicat vrai après l'exécution de l'instruction S.

On définit les règles de la logique de Hoare :

$$[\mathsf{skip}_H] \qquad \{P\}\ \mathsf{skip}\ \{P\}$$

$$[\mathsf{ass}_H] \qquad \{P[x \mapsto \mathcal{A}[\![a]\!]]\}\ x := a\ \{P\}$$

$$[\mathsf{comp}_H] \qquad \frac{\{P\}\ S_1\ \{Q\} \qquad \{Q\}\ S_2\ \{R\}}{\{P\}\ S_1; S_2\ \{R\}}$$

$$[\mathsf{if}_H] \qquad \frac{\{\mathcal{B}[\![b]\!] \wedge P\}\ S_1\ \{Q\} \qquad \{\neg\mathcal{B}[\![b]\!] \wedge P\}\ S_2\ \{Q\}}{\{P\}\ \mathsf{if}\ b\ \mathsf{then}\ S_1\ \mathsf{else}\ S_2\ \{Q\}}$$

$$[\mathsf{while}_H] \qquad \frac{\{\mathcal{B}[\![b]\!] \wedge P\}\ S\ \{P\}}{\{P\}\ \ \mathsf{while}\ b\ \mathsf{do}\ S\ \{\neg\mathcal{B}[\![b]\!] \wedge P\}}$$

$$[\mathsf{cons}_H] \qquad \frac{\{P'\}\ S\ \{Q'\}}{\{P\}\ S\ \{Q\}}\ \text{si } P \Rightarrow P' \text{ et } Q' \Rightarrow Q.$$

Définition 3. On note $\vdash_p \{P\}S\{Q\}$ si et seulement s'il existe un arbre correct aboutissant à $\{P\}S\{Q\}$ avec les règles ci-dessus.

C'est un aspect syntaxique.

Définition 4. On note $\vDash_p \{P\}S\{Q\}$ si et seulement si pour tout état s tel que $Ps = tt$, si $\langle S, s\rangle \to s'$, alors $Qs' = tt$.

C'est un aspect sémantique.

Théorème 3. Pour tout P, Q, S,

$$\vdash_p \{P\}S\{Q\} \iff \vDash_p \{P\}S\{Q\}.$$

Le sens direct correspond à la correction de la logique de Hoare. On le montre par induction sur la dérivation.

Le sens indirect correspond à la complétude de la logique de Hoare. La preuve fait l'objet du développement : Complétude de la logique de Hoare.

Règles de la sémantique opérationnelle à grands pas

(rédigé par Julie Parreaux)

$$[\mathsf{skip}_{\ NS}] \qquad \langle \mathsf{skip}, s\rangle \to s$$

$$[\mathsf{ass}_{\ NS}] \qquad \langle x := a, s\rangle \to s\,[x \mapsto \mathcal{A}[\![a]\!]_s]$$

$$[\mathsf{comp}_{\ NS}] \qquad \frac{\langle S_1, s\rangle \to s' \qquad \langle S_2, s'\rangle \to s''}{\langle S_1; S_2, s\rangle \to s''}$$

$$[\mathsf{if}^{\ tt}_{NS}] \qquad \frac{\langle S_1, s\rangle \to s'}{\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \to s'} \text{ si } \mathcal{B}[\![b]\!]_s = tt$$

$$[\mathsf{if}^{\ ff}_{NS}] \qquad \frac{\langle S_2, s\rangle \to s'}{\langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \to s'} \text{ si } \mathcal{B}[\![b]\!]_s = ff$$

$$[\mathsf{while}^{\ tt}_{NS}] \qquad \frac{\langle S, s\rangle \to s' \ \langle \mathsf{while}\ b\ \mathsf{do}\ S, s'\rangle \to s''}{\langle \mathsf{while}\ b\ \mathsf{do}\ S, s\rangle \to s''} \text{ si } \mathcal{B}[\![b]\!]_s = tt$$

$$[\mathsf{while}^{\ ff}_{NS}] \qquad \langle \mathsf{while}\ b\ \mathsf{do}\ S, s\rangle \to s \text{ si } \mathcal{B}[\![b]\!]_s = ff$$

Règles de la sémantique opérationnelle à petits pas

(rédigé par Julie Parreaux)

$[\mathsf{skip}_{SOS}]$ $\quad \langle \mathsf{skip}, s\rangle \Rightarrow s$

$[\mathsf{ass}_{SOS}]$ $\quad \langle x := a, s\rangle \Rightarrow s\,[x \mapsto \mathcal{A}[\![a]\!]_s]$

$[\mathsf{comp}^{1}_{SOS}]$ $\quad \dfrac{\langle S_1, s\rangle \Rightarrow \langle S_1', s'\rangle}{\langle S_1; S_2, s\rangle \Rightarrow \langle S_1'; S_2, s'\rangle}$

$[\mathsf{comp}^{2}_{SOS}]$ $\quad \dfrac{\langle S_1, s\rangle \Rightarrow s'}{\langle S_1; S_2, s\rangle \Rightarrow \langle S_2, s'\rangle}$

$[\mathsf{if}^{tt}_{SOS}]$ $\quad \langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \Rightarrow \langle S_1, s\rangle \text{ si } \mathcal{B}[\![b]\!]_s = tt$

$[\mathsf{if}^{ff}_{SOS}]$ $\quad \langle \text{ if } b \text{ then } S_1 \text{ else } S_2, s\rangle \Rightarrow \langle S_2, s\rangle \text{ si } \mathcal{B}[\![b]\!]_s = ff$

$[\mathsf{while}_{SOS}]$ $\quad \langle \text{while } b \text{ do } S, s\rangle \Rightarrow \langle \text{ if } b \text{ then } (S; \text{while } b \text{ do } S) \text{ else skip}, s\rangle$

Règles de la logique de Hoare

(rédigé par Julie Parreaux)

$[\mathsf{skip}_{\ H}]$ $\quad \{P\}\ \mathsf{skip}\ \{P\}$

$[\mathsf{ass}_{\ H}]$ $\quad \{P[x \mapsto \mathcal{A}[\![a]\!]]\}\ x := a\ \{P\}$

$[\mathsf{comp}_{\ H}]$ $\quad \dfrac{\{P\}\ S_1\ \{Q\} \qquad \{Q\}\ S_2\ \{R\}}{\{P\}\ S_1; S_2\ \{R\}}$

$[\mathsf{if}_{\ H}]$ $\quad \dfrac{\{\mathcal{B}[\![b]\!] \wedge P\}\ S_1\ \{Q\} \qquad \{\neg\mathcal{B}[\![b]\!] \wedge P\}\ S_2\ \{Q\}}{\{P\}\ \mathsf{if}\ b\ \mathsf{then}\ S_1\ \mathsf{else}\ S_2\ \{Q\}}$

$[\mathsf{while}_{\ H}]$ $\quad \dfrac{\{\mathcal{B}[\![b]\!] \wedge P\}\ S\ \{P\}}{\{P\}\ \ \mathsf{while}\ b\ \mathsf{do}\ S\ \{\neg\mathcal{B}[\![b]\!] \wedge P\}}$

$[\mathsf{cons}_{\ H}]$ $\quad \dfrac{\{P'\}\ S\ \{Q'\}}{\{P\}\ S\ \{Q\}}$ si $P \Rightarrow P'$ et $Q' \Rightarrow Q$

λ-calcul

Syntaxe :

Définition. Soit un ensemble $\{x, y, z, \ldots\}$ dénombrable de variables. On définit les *termes de λ-calcul* (ou *λ-termes*) par induction :

- les variables sont des termes ;
- si M et N sont des termes, alors (MN) est un terme ;
- si M est un terme et x une variable, alors $(\lambda x.M)$ est un terme.

On dit que M et N sont des *sous-termes* de (MN) et que M est un *sous-terme* de $(\lambda x.M)$

Exemple : les expressions $(\lambda x.(xy))$ et $((\lambda y.y)(\lambda x.(xy)))$ sont des termes. L'expression $(x.\lambda x)$ n'est pas un terme.

On s'autorisera à écrire MNP pour $((MN)P)$ où M, N et P sont des termes et $\lambda xy.M$ pour $(\lambda x.(\lambda y.M))$ où M est un terme et x, y des variables.

Définition. Dans un terme $\lambda x.M$, on dit que M et tous les sous-termes de M sont dans la *portée* de λx.

Définition. Dans un terme P, une occurrence x est

- *liée* si x est un sous-terme de P et que x est dans la portée d'un λx qui est dans P.
- *libre* si elle n'est pas liée.

Définition. Si un terme n'a pas de variable libre, il est dit *clos*.

Exemple : les termes $I = \lambda x.x$, $K = \lambda xy.x$ et $S = \lambda xyz.xz(yz)$ sont clos.

Définition. Soient M, N des termes et x une variable. La *substitution* de x par N dans M, notée $M[x \to N]$, est le remplacement de chaque occurrence libre de x dans M par N en renommant si besoin les variables de M par des variables fraîches pour qu'elles soient libres dans $M[x \to N]$.

Exemple : l'expression $(\lambda y.xy)[x \to \lambda y.y]$ nécessite un renommage, $(\lambda z.(\lambda y.y)z)$ est alors l'expression obtenue.

Définition. On définit l'*α-conversion* comme la plus petite relation d'équivalence $\sim_\alpha$ satisfaisant :

- $\lambda x.M \sim_\alpha \lambda y.\,(M[x \to y])$ pour une variable fraîche y ;
- $\lambda x.M \sim_\alpha \lambda x.N$ si $M \sim_\alpha N$;
- $MN \sim_\alpha PQ$ si $M \sim_\alpha P$ et $N \sim_\alpha Q$.

Exemple : on a $\lambda xy.x(xy) \sim_\alpha \lambda uv.u(uv)$

β-réduction :

Définition. On définit la relation de *β-réduction*, notée $\to_\beta$, par induction sur les termes

- $(\lambda x.M)N \to_\beta M[x \to N]$;
- si $M \to_\beta M'$, alors $\lambda x.M \to_\beta \lambda x.M'$;
- si $M \to_\beta M'$, alors $MN \to_\beta M'N$;
- si $N \to_\beta N'$, alors $MN \to_\beta MN'$.

Exemples :

- si $I = \lambda x.x$ alors $IM \to_\beta M$;
- si $K = \lambda xy.x$ alors $(KM)N \to_\beta (\lambda y.M)N \to_\beta M$;
- si $S = \lambda xyz.xz(yz)$ alors $SMNP \to_\beta^3 MP(NP)$.

Définition. Un terme M est sous *forme normale* s'il ne peut pas être β-réduit.

Lemme.

- une variable x est sous forme normale ;
- si M est sous forme normale, alors $\lambda x.M$ est sous forme normale.

Lemme. Si $P \to_\beta^* P'$ et $Q \to_\beta^* Q'$ alors $Q[x \to P] \to_\beta^* Q'[x \to P']$.

Théorème.(Church-Rosser I) Si $P \to_\beta^* P_1$ et $P \to_\beta^* P_2$ alors il existe Q tel que $P_1 \to_\beta^* Q$ et $P_2 \to_\beta^* Q$. Cette propriété est nommée *confluence*.

Définition. On dit que P possède une forme normale s'il existe un terme M sous forme normale tel que $P \to_\beta^* M$. Par le théorème de Church–Rosser, si P possède une forme normale alors elle est unique.

Définition. On dit que M et N sont *β-équivalents*, noté $M \sim_\beta N$, s'il existe $M_1, M_2, \dots, M_n$ tels que $M_1 \sim_\alpha M$, $M_n \sim_\alpha N$ et pour tout $i \in [\![1; n-1]\!]$, on a $M_i \to_\beta^* M_{i+1}$ ou $M_{i+1} \to_\beta^* M_i$.

Théorème.(Church-Rosser II) Si $P \sim_\beta Q$ alors il existe T tel que $P \to_\beta^* T$ et $Q \to_\beta^* T$.

Corollaire.

- Si $P \sim_\beta Q$ et si Q est sous forme normale alors $P \to_\beta^* Q$.
- Si $P \sim_\beta Q$ alors soit ils ont la même forme normale, soit ils n'en ont pas.

Exemples :

On va maintenant définir différents termes de λ-calcul.

- $T := \lambda xy.x$
- $F := \lambda xy.y$
- $\mathsf{if\ then\ else} := \lambda bxy.bxy$

La terminologie est justifiée par le fait que si $X \sim_\beta T$, alors $\mathsf{if}\ X\ \mathsf{then}\ M\ \mathsf{else}\ N \sim_\beta T\ M\ N \sim_\beta M$, de même si $X \sim_\beta F$, alors $\mathsf{if}\ X\ \mathsf{then}\ M\ \mathsf{else}\ N \sim_\beta F\ M\ N \sim_\beta N$.

- $\langle M, N\rangle := \lambda x.(xMN)$
- $\mathsf{fst} := T$
- $\mathsf{snd} := F$

On a $\langle M, N\rangle \mathsf{fst} \sim_\beta T\ M\ N \sim_\beta M$

- $[M] := M$ (liste contenant uniquement l'élément M)
- $[M_1, \dots, M_{n+1}] := \langle M_1, [M_2, \dots, M_{n+1}]\rangle$
- $\pi_i^n := \lambda x_1 \cdots x_n.x_i$ (projection)

On note $M^n N = \begin{cases} N & \text{si } n = 0, \\ M(M^{n-1}N) & \text{si } n > 0. \end{cases}$

Représentation des entiers :

On veut pouvoir représenter les entiers et utiliser les opérations usuelles dessus.

Entiers de *Church* :

- $[\![0]\!]_C := \lambda sz.z$
- $[\![n]\!]_C := \lambda sz.s^n z$
- $[\![\mathsf{succ}]\!]_C := \lambda n.(\lambda sz.ns(sz))$

La terminologie est justifiée par le fait que

$$\begin{aligned}[\![\mathsf{succ}]\!]_C[\![n]\!]_C &\sim_\beta \lambda sz.[\![n]\!]_C s(sz) \sim_\alpha \lambda sz.(\lambda uv.u^n v)s(sz)\\ &\sim_\beta \lambda sz.s^n(sz) \sim_\alpha \lambda sz.s^{n+1}z \sim_\alpha [\![n+1]\!]_C.\end{aligned}$$

- $[\![+]\!]_C := \lambda n_1 n_2.\lambda sz.n_1 s(n_2 sz) = \lambda n_1 n_2.n_1[\![succ]\!]_C n_2$
- $[\![\mathsf{exp}]\!]_C := \lambda mn.mn$
- $[\![\mathsf{pred}]\!]_C := \lambda n.\mathsf{fst}(n(\lambda y.[\mathsf{snd}y, [\![\mathsf{succ}]\!]_C \mathsf{snd}y][[\![0]\!]_C, [\![0]\!]_C]))$

On incrémente n fois le couple $(k, k+1)$ jusqu'à $(n-1, n)$ puis on extrait la première coordonnée afin d'obtenir $n-1$.

- $[\![\mathsf{is_zero}]\!]_C := \lambda n.n(\lambda x.F)T$

La terminologie est justifiée par le fait que

$$\begin{aligned}[\![\mathsf{is_zero}]\!]_C[\![0]\!]_C &\sim_\beta [\![0]\!]_C(\lambda x.F)\ T\\ &\sim_\alpha (\lambda sz.z)(\lambda x.F)\ T \sim_\beta T\\ [\![\mathsf{is_zero}]\!]_C[\![n+1]\!]_C &\sim_\beta [\![n+1]\!]_C(\lambda x.F)\ T \sim_\alpha (\lambda sz.s^{n+1}z)(\lambda x.F)\ T\\ &\sim_\beta (\lambda x.F)^{n+1}\ T \sim_\alpha (\lambda x.F)^n((\lambda x.F)\ T)\\ &\sim_\beta (\lambda x.F)^n\ F \sim_\beta F\end{aligned}$$

Entiers de *Barendregt*

- $[\![0]\!]_B := I = \lambda x.x$
- $[\![n+1]\!]_B := \langle F, [\![n]\!]_B\rangle = \lambda x.(xF[\![n]\!]_B)$
- $[\![\mathsf{succ}]\!]_B := \lambda n.\langle F, n\rangle$
- $[\![\mathsf{pred}]\!]_B := \lambda n.nF$

La terminologie est justifiée par le fait que

$$\begin{aligned}[\![\mathsf{pred}]\!]_B[\![n+1]\!]_B &\sim_\alpha \lambda n.(nF)[\![n+1]\!]_B \sim_\beta [\![n+1]\!]_B\ F \sim_\alpha \lambda x.(xF[\![n]\!]_B)\ F\\ &\sim_\beta F\ F\ [\![n]\!]_B \sim_\alpha (\lambda xy.y)F\ [\![n]\!]_B \sim_\beta [\![n]\!]_B.\end{aligned}$$

- $[\![\mathsf{is_zero}]\!]_B := \lambda n.nT$

La terminologie est justifiée par le fait que

$$\begin{aligned}[\![\mathsf{is_zero}]\!]_B[\![0]\!]_B &\sim_\alpha (\lambda n.nT)[\![0]\!]_B \sim_\beta [\![0]\!]_B\ T\\ &\sim_\alpha (\lambda x.x)\ T \sim_\beta T\\ [\![\mathsf{is_zero}]\!]_B[\![n+1]\!]_B &\sim_\alpha (\lambda n.nT)[\![n+1]\!]_B \sim_\beta [\![n+1]\!]_B\ T\\ &\sim_\alpha \lambda x.(x\ F\ [\![n]\!]_B)\ T \sim_\beta T\ F\ [\![n]\!]_B \sim_\beta F\end{aligned}$$

Point fixe :

Définition. Un *point fixe* est un λ-terme Y tel que, pour tout terme G, on a

$$YG \sim_\beta G(YG).$$

Exemple : le point fixe de Turing est $\theta = AA$ avec $A = \lambda xf.f(xxf)$
En effet, pour tout terme G, on a

$$\begin{aligned}\theta G &\sim_\alpha AAG\\ &\sim_\alpha (\lambda xf.f(xxf))(\lambda xf.f(xxf))G\\ &\to_\beta (\lambda f.f((\lambda xz.z(xxz))(\lambda xz.z(xxz))f))G\\ &\to_\beta G((\lambda xz.z(xxz))(\lambda xz.z(xxz))G)\\ &\sim_\alpha G(AAG)\\ &\sim_\alpha G(\theta G).\end{aligned}$$

Exemple : le point fixe de Curry est $Y = \lambda f.((\lambda x.f(xx))(\lambda x.f(xx)))$
En effet, pour tout terme G, on a

$$\begin{aligned}YG &\to_\beta (\lambda x.G(xx))(\lambda x.G(xx))\\ &\to_\beta G((\lambda x.G(xx))(\lambda x.G(xx)))\\ &\leftarrow_\beta G(YG).\end{aligned}$$

λ-calcul et calculabilité :

Définition. Soit ϕ une fonction de $\mathbb{N}^p$ dans $\mathbb{N}$. La fonction ϕ est λ-*définissable* si et seulement s'il existe un λ-terme G tel que

$$\forall n_1, \dots, n_p \in \mathbb{N}, \quad G[\![n_1]\!] \dots [\![n_p]\!] \sim_\beta [\![\phi(n_1, \dots, n_p)]\!]$$

Théorème. Une fonction est μ-récursive si et seulement si elle est λ-définissable.

(voir μ-recursif $\implies$ λ-définissable)

On dit que deux ensembles $\mathcal{A} \subset \mathbb{N}$ et $\mathcal{B} \subset \mathbb{N}$ disjoints sont *récursivement séparables* s'il existe une fonction μ-récursive φ telle que

$$x \in \mathcal{A} \implies \varphi(x) = 0 \quad \text{et} \quad x \in \mathcal{B} \implies \varphi(x) = 1.$$

Après avoir transposé la définition de *récursivement séparable* pour les λ-termes, on peut démontrer le théorème suivant.
Théorème. Aucune paire d'ensembles non vides de termes clos par β-équivalence ne sont récursivement séparables.

(voir Théorème de Scott–Curry)

Bases de données

Je mets ci-dessous le bagage minimum sur les bases de données qu'il faut avoir en allant à l'agrégation. C'est organisé comme mon plan de la leçon 932.

Voici un exemple de base de données :

FILMS

Titre	Réalisateur	Acteur
Didier	A. Chabat	A. Chabat
Au Poste	Q. Dupieux	G. Ludig
Réalité	Q. Dupieux	A. Chabat
Astérix	A. Chabat	E. Baer

SÉANCES

Cinéma	Horaires	Titre
UGC	$12^{\text{h}}\,00$	Au Poste
Gaumont	$20^{\text{h}}\,50$	Didier
Pathé	$13^{\text{h}}\,30$	Réalité
Pathé	$13^{\text{h}}\,30$	Didier

On veut se poser les questions suivantes :

- Q_1 : Quels films ont été réalisés par A. Chabat ?
- Q_2 : Quels sont les films réalisés par A. Chabat ou Q. Dupieux ?
- Q_3 : Quels sont les films de Q. Dupieux dans lesquels A. Chabat ne joue pas ?

Donnons maintenant le formalisme que l'on met sur les bases de données.

I - Formalisme

Soient les ensembles dénombrables distincts suivants :

- de variables $\text{VAR} = \{x, y, z, \ldots\}$
- d'attributs ATT
- de domaines DOM
- de noms de schéma de relation RELNAME

Définition. On se donne une fonction

$$sort : \text{RELNAME} \to \mathcal{P}_f(\text{ATT})$$

qui a $R \in \text{RELNAME}$ associe un nombre fini d'attributs.

Définition. On dira que, pour $R \in \text{RELNAME}$, la quantité $|sort(R)|$ est l'arité de R.

Définition. Un élément $R \in \text{RELNAME}$ est un schéma de relation. On notera $R[U]$ où $U = sort(R)$.

Définition. Un nombre fini de schémas de relation $R^{(1)}[U^{(1)}], \ldots, R^{(n)}[U^{(n)}]$ est un schéma de base de données. On notera

$$\mathcal{R} = \{R^{(1)}[U^{(1)}], \ldots, R^{(n)}[U^{(n)}]\}.$$

Exemple.

$$\mathcal{R} = \{\textsc{Films}[\text{Titre}, \text{Réalisateur}, \text{Acteur}], \textsc{Séances}[\text{Cinéma}, \text{Horaires}, \text{Titre}]\}$$

Définition. Un tuple sur un schéma de relation $R[U]$ est une fonction

$$u : U \to \textsc{Dom}.$$

On notera le tuple par

$$\langle U_1 : u(U_1), \dots, U_n : u(U_n)\rangle$$

On s'autorisera à noter $\langle u(U_1), \dots, u(U_n)\rangle$ s'il n'y a pas ambiguïté des attributs.

Exemple. Voici un tuple sur le schéma de relation $\textsc{Films}[\text{Titre}, \text{Réalisateur}, \text{Acteur}]$.

$$\langle \text{Titre} : \text{Didier}, \text{Réalisateur} : \text{A. Chabat}, \text{Acteur} : \text{A. Chabat}\rangle$$

Définition. Un tuple libre sur un schéma de relation $R[U]$ est une fonction $u : U \to \textsc{Dom} \cup \textsc{Var}$.

Exemple. $\langle x, \text{A. Chabat}, y\rangle$ est un tuple libre.

Définition. Une relation I sur un schéma de relation $R[U]$ est un nombre fini de tuples sur $R[U]$.

Exemple. La table $\textsc{Films}[\text{Titre}, \text{Réalisateur}, \text{Acteur}]$ de l'exemple ci-dessus est une relation.

Définition. Une base de données $\mathcal{I}$ sur un schéma de base de données $\mathcal{R}$ est un ensemble fini de relations, où une relation I est sur un schéma de relation $R[U] \in \mathcal{R}$.

Exemple. L'ensemble des tables de l'exemple ci-dessus est une base de données.

On veut maintenant pouvoir effectuer des requêtes sur les bases de données afin d'en extraire des informations. Pour cela, on va donner plusieurs approches qui sont de plus en plus expressives.

II - Requêtes conjonctives

1) Règles conjonctives

Définition. Une règle conjonctive sur $\mathcal{R}$ est une expression de la forme

$$ans(u) \leftarrow R^{(1)}(u^{(1)}), \dots, R^{(n)}(u^{(n)})$$

où $u, u^{(1)}, \dots, u^{(n)}$ sont des tuples libres sur des relations $R^{(i)} \in \mathcal{R}$ et $ans \notin \mathcal{R}$.

Exemple. $ans(x) \leftarrow \textsc{Films}(x, \text{A. Chabat}, y)$ est une règle conjonctive.

Définition. Une valuation ν sur $\textsc{Var}$ est une fonction $\nu : \textsc{Var} \to \textsc{Dom}$. On la prolonge sur les tuples libres en imposant que $\nu_{|\textsc{Dom}} = \mathrm{Id}_{|\textsc{Dom}}$.

Définition. La sémantique d'une règle conjonctive q pour $\mathcal{I}$ sur $\mathcal{R}$ est donnée par

$$q(\mathcal{I}) = \left\{\nu(u) \ : \ \nu \text{ est une valuation sur } \textsc{Var}(q) \text{ et } \nu(u_i) \in \mathcal{I}(R^{(i)})\, \forall i \in [\![1; n]\!]\right\}$$

Exemple. $ans(x) \leftarrow \textsc{Films}(x, \text{A. Chabat}, y)$ a pour sémantique

$$\langle \text{Didier}, \text{A. Chabat}, \text{A. Chabat} \rangle$$
$$\langle \text{Astérix}, \text{A. Chabat}, \text{E. Baer} \rangle$$

Comme on demande l'information x, il faudra ensuite donner le titre des films, ici Didier et Astérix. On a répondu à la question Q_1.

Définition. Le domaine actif de $\mathcal{I}$ (resp. de q, $q(\mathcal{I})$), noté $adom(\mathcal{I})$ (resp. $adom(q)$, $adom(q(\mathcal{I}))$) est l'ensemble des éléments de $\textsc{Dom}$ présents dans $\mathcal{I}$ (resp. q, $q(\mathcal{I})$).

On remarque que l'on a $adom(q(\mathcal{I})) \subset adom(q) \cup adom(\mathcal{I})$.

2) Calcul conjonctf

Définition. Soit un schéma de base de données $\mathcal{R}$. Une formule du calcul conjonctif est de la forme

- $R[u]$, avec u un tuple libre sur $R[U]$ et $R[U] \in \mathcal{R}$;
- $\phi \wedge \psi$ avec ϕ et ψ des formules du calcul conjonctif ;
- $\exists x\, \phi$, avec $x \in \textsc{Var}$ et ϕ une formule du calcul conjonctif.

Définition. Une requête du calcul conjonctif q sur $\mathcal{R}$ est une expression de la forme

$$q = \{e_1, \dots, e_n \mid \varphi\}$$

où $\langle e_1, \dots, e_n \rangle$ est un tuple libre, φ une formule du calcul conjonctif et l'ensemble des variables libres de φ est $\{e_1, \dots, e_n\}$.

Définition. Soient un schéma de base de données $\mathcal{R}$, une formule du calcul conjonctif φ sur $\mathcal{R}$ et une valuation ν sur les variables libres de φ. On dit que la base de données $\mathcal{I}$ sur $\mathcal{R}$ satisfait φ pour ν, noté $\mathcal{I} \vDash \varphi[\nu]$, si

- pour $\varphi = R[u]$, on a $\nu(u) \in \mathcal{I}$;
- pour $\varphi = \phi \wedge \psi$, on a $\mathcal{I} \vDash \phi[\nu]$ et $\mathcal{I} \vDash \psi[\nu]$;
- pour $\varphi = \exists x\, \phi$, il existe $c \in \textsc{Dom}$ tel que $\mathcal{I} \vDash \phi[\nu \cup [x \mapsto c]]$.

Définition. La sémantique d'une requête q du calcul conjonctif est donnée par

$$q(\mathcal{I}) = \{\nu(\langle e_1, \dots, e_n \rangle) \ : \ \nu \text{ une valuation sur les variables libres de } \varphi \text{ et } \mathcal{I} \vDash \varphi[\nu]\}$$

Exemple. Pour répondre à la question Q_1, on écrit

$$q = \{x \mid \exists y\, \textsc{Films}(x, \text{A. Chabat}, y)\}$$

Théorème 1. Le calcul conjonctif et les règles conjonctives sont équivalentes.

Toutes les requêtes conjonctives sont finies.

III - L'algèbre SPC

Définition. On définit les trois opérations suivantes sur $I, J \in \mathcal{I}$ qui formeront l'algèbre SPC.

- la sélection : $\sigma_{j=a}(I) = \{t \in I, t(j) = a\}$ avec $j \in \text{Att}$, $a \in \text{Dom}$ et t un tuple. On peut aussi définir $\sigma_{j=k}(I) = \{t \in I, t(j) = t(k)\}$ avec $j, k \in \text{Att}$ et t un tuple.
- la projection : $\prod_{j_1,\dots,j_n}(I) = \{\langle t(j_1), \dots, t(j_n)\rangle, t \in I\}$ avec $j_1, \dots, j_n \in \text{Att}$.
- le produit carthésien : $I \times J = \{\langle t(1), \dots, t(n), s(1), \dots, s(m)\rangle, t \in I, s \in J\}$ avec $n = \text{arité}(I)$ et $m = \text{arité}(J)$.

Exemple. Pour répondre à la question Q_1, on écrit

$$\prod_{\text{Titre}} (\sigma_{\text{Réalisateur=A. Chabat}}(\text{Films}))$$

Proposition : On peut effectuer la jointure naturelle et l'intersection avec les trois opérations de l'algèbre SPC.

Toutes les requêtes de l'algèbre SPC sont finies mais ne sont pas forcément satisfiables.

Exemple. La requête $\prod_A \sigma_{A=0}\sigma_{A=1}(I)$ est insatisfiable.

Théorème 2. Il y a équivalence entre les requêtes par règles conjonctives, le calcul conjonctif et les requêtes satisfiables de l'algèbre SPC.

Pour l'instant, on ne peut pas répondre aux questions Q_2 et Q_3. C'est pourquoi on va introduire de nouvelles opérations.

IV - L'algèbre relationnelle et le calcul relationnel

1) Ajout de l'union

Définition. On ajoute l'union dans l'algèbre SPC (qui devient alors l'algèbre SPCU) en autorisant la sélection

$$\sigma_{j=a \text{ ou } j=b}$$

Définition. On ajoute le connecteur logique « ou », noté $\vee$, aux formules du calcul conjonctif.

Exemple. On peut donc maintenant répondre à la question Q_2.

$$\prod_{\text{Titre}} (\sigma_{\text{Réalisateur=A. Chabat ou Réalisateur=Q. Dupieux}}(\text{Films}))$$

On peut alors avoir des requêtes infinies.

Exemple. La requête $\{x, y \mid R(x) \vee R(y)\}$ avec $R(x_0) = 1$ pour $x_0 \in \text{Dom}$. En effet, pour tout $y \in \text{Dom}$, on a $R(x_0) \vee R(y) = 1$. Ainsi, pour un domaine infini, on a une requête infinie.

Définition. On dit qu'une requête est sûre si $|q(\mathcal{I})| < +\infty$ pour toute base de données $\mathcal{I}$ sur $\mathcal{R}$.

Le problème RelSure est indécidable.

RelSure
- entrée : une requête q en calcul relationnel ;
- sortie : oui si $|q(\mathcal{I})| < +\infty$ pour toute base de données $\mathcal{I}$, non sinon.

2) Ajout de la négation

Définition. On ajoute la différence ensembliste dans l'algèbre SPCU, notée \, qui devient alors l'algèbre relationnelle SPCUD.

Définition. On ajoute le connecteur logique de négation, noté ¬, aux formules afin d'obtenir le calcul relationnel.

On peut donc exprimer le quantificateur universel ∀.

Exemple. On peut donc maintenant répondre à la question Q_3.

$$\prod_{\text{Titre}} (\sigma_{\text{Réalisateur=Q. Dupieux}}(\textsc{Films}) \setminus \sigma_{\text{Acteur=A. Chabat}}(\textsc{Films}))$$

On peut de nouveau avoir des requêtes infinies.

Exemple. La requête $\{x \mid \neg R(x_0)\}$ pour $x_0 \in \textsc{Dom}$. En effet, pour tout $x \in \textsc{Dom} \setminus \{x_0\}$, on a $\neg R(x_0) = 1$. Ainsi, pour un domaine infini, on a une requête infinie.

Pour une base de données $\mathcal{I}$ sur $\mathcal{R}$, on restreint le domaine au domaine actif ainsi, pour une requête et une relation fixées, la requête sera finie.

Théorème 3. Restreints au domaine actif, l'algèbre relationnelle SPCUD et le calcul relationnel sont équivalents.

Les problèmes suivants sont indécidables :

RelSat
- entrée : une requête q en calcul relationnel ;
- sortie : oui s'il existe $\mathcal{I}$ telle que $q(\mathcal{I}) \neq \emptyset$, non sinon.

RelEqu
- entrée : deux requêtes q et q' du calcul relationnel ;
- sortie : oui si q et q' sont sémantiquement équivalentes, non sinon.

On montre l'indécidabilité de RelSat dans le développement Indécidabilité de la satisfiabilité d'une requête.

Remarques :
On peut chercher à optimiser les opérations d'écriture et de lecture dans la base de données. On peut par exemple utiliser des B-arbres comme il est montré dans le développement sur les B-arbres.

INDEX MATHÉMATIQUE

action de groupe, 219, 223, 227, 294, 413
automorphismes , 299
    intérieurs, 299

Bézout
    théorème de, 230
Baire
    théorème de, 242
Banach
    espace de, 242, 260
Banach-Steinhaus
    théorème de, 242

caractéristique, 217
Carathéodory
    théorème de, 305
Cauchy–Lipschitz
    théorème de, 260, 285
centralisateur, 300
Césaro
    réciproque partielle du théorème de, 251
    théorème de, 249
classes monotones, 472
compacité, 288, 466
connexité, 234, 469
connexité par arcs, 234, 469
convergence dominée
    théorème de, 254, 276
convergence en loi, 290
convergence normale, 320, 325, 330
convexe
    enveloppe, 305
    fonction, 247
corps
    de rupture, 215
    extension de, 477
    finis, 223, 226

D'Alembert Gauss
    théorème de, 469
décomposition
    de Dunford, 230
    LU, 312
    polaire, 302
    QR, 312
déterminant
    de Van Der Monde, 238
diagonalisation, 230, 239
Dirichlet
    intégrale de, 275
    noyau de, 242, 459
division euclidienne, 315
Dunford
    décomposition de, 230

enveloppe convexe, 305
équation
    de Fermat-Wiles, 309
    différentielle ordinaire, 260, 264, 273, 284
    diophantienne, 307
équivalent asymptotique, 286
espace
    de Schwartz, 320
    métrique compact, 288
espace vectoriel , 264
    normé, 242, 466, 478
exponentielle
    développement en série, 271
    matricielle, 234, 302
exposant d'un groupe, 416

famille sommable, 271
fonction
    caractéristique, 275, 291

convexe, 247
de répartition, 275, 474
Γ, 254, 405
lipschitzienne, 260
méromorphe, 256, 405
forme linéaire, 280, 288
forme quadratique, 226, 302
formule
d'inversion de la fonction caractéristique, 275
d'inversion de Pascal, 470
des classes, 227
des compléments, 254, 405
sommatoire de Poisson, 320, 325, 330, 458
Fourier
coefficient de, 243, 321, 326, 331, 459
formule d'inversion, 275, 322
série de, 243
transformée de, 275, 320, 325, 330, 458
Fubini
théorème de, 254, 277

générateurs
de $\mathrm{SL}_2(\mathbb{Z})$, 294
de $\mathfrak{S}_n$, 220, 299
de $\mathrm{GL}_n(\mathbb{Z})$, 413
géométrie du plan complexe, 294
$GL_n(\mathbb{F}_q)$, 223
Gronwall
lemme de, 260

Hadamard
inégalité de, 282
holomorphie, 254, 291, 328, 332, 405
hyperplan, 288

idéal
maximal, 217
propre, 288
inégalité
d'Hadamard, 282
de Kantorovich, 268
indicatrice d'Euler, 315
invariant de similitude, 419
isobarycentre, 238
isométries , 302
du cube, 220
du tétraèdre, 219

Kantorovich
inégalité de, 268

lemme
chinois, 215
de Gronwall, 260
de relèvement, 284
de Schur, 310
des noyaux, 230, 419
des tiroirs, 309
libre
famille, 265
Lie
algèbre de, 237
lipschitzienne
fonction, 260
logarithme complexe, 254
loi de réciprocité quadratique, 216, 226
loi normale, 291

méthode
de Newton, 246
du gradient à pas optimal, 267
matrice
circulante, 239
compagnon, 419
de dilatation, 413
de permutation, 413
de transvection, 413
diagonalisable, 230
nilpotente, 230
morphisme
d'algèbre, 288
de Frobenius, 217

Newton
méthode de, 246
nombre premier, 215, 226
nombres de Bell, 271
norme
d'opérateur, 242
noyau
de Dirichlet, 242, 459
noyaux
lemme des, 230, 419

optimisation, 246, 267, 280
orthogonalité, 264

Pascal
formule d'inversion, 470
Picard
théorème de point fixe de, 260
plan tangent, 280
polynôme
caractéristique, 224

cyclotomique, 315
d'endomorphisme, 230, 234, 419
irréductible, 230, 315, 420, 476, 477
minimal, 315, 419, 477
primitif, 476
probabilité, 275, 290, 472
projecteur, 230
prolongement analytique, 254, 292, 406

résidu quadratique, 216, 226
résidus
théorème des, 254, 405
racine $n^{\text{ième}}$
primitive de l'unité, 315
rang
théorème du, 305
relation orbite/stabilisateur, 224, 227

série , 251
de Fourier, 243
entière, 271, 325
Schur
lemme de, 310
$\mathfrak{S}_n$, 299
sous-variétés, 280
suite , 249, 269
de matrices, 312
récurrente, 238, 246
symbole de Legendre, 216, 228

Taylor–Lagrange, 246
théorème
central limite, 290
d'holomorphie, 291, 408
d'inversion locale, 234
de Bézout, 230
de Banach-Steinhaus, 242
de Césaro, 249
de Carathéodory, 305
de Cauchy–Lipschitz, 260, 285
de Cayley–Hamilton, 235
de convergence dominée, 254, 276, 406
de D'Alembert Gauss, 469
de Dirichlet, 320, 325, 330
de Fubini, 254, 277, 406
de point fixe de Picard, 260
de prolongement des caractères, 417
de structure, 416
des classes monotones, 472
des résidus, 254, 328, 332, 405
des sous-variétés, 280
du rang, 305
spectral, 267
de Baire, 242
tribu, 472

variables aléatoires, 275, 290, 474

zéro de fonction, 246, 284
$\mathbb{Z}/p\mathbb{Z}$, 309

INDEX INFORMATIQUE

algèbre
  relationnelle, 515
  SPC, 514
algorithme
  Construit (tas), 335
  Entasse, 334
  RechercheBArbre, 356
  TriParTas, 336
  TriTopologique, 363
  de CockeYoungerKasami, 360
  de KnuthMorrisPratt, 366, 423
  de saturation, 395
  du texte, 366, 423
algorithmes classiques, 481
algorithmique gloutonne, 483
α
  conversion, 508
analyse syntaxique, 395
arbre
  binaire de recherche, 356
arithmétique
  de Peano, 378
  de Presburger, 378
automate , 376
  des occurrences, 366
  minimal, 366

B-arbres, 356, 516
base de données, 355, 399, 491, 512
β
  équivalence, 509
  réduction, 508

calcul
  conjonctif, 514
  relationnel, 515
Chuch-Rosser
  théorème de, 509
codage de Gödel, 346, 392
combinateur de point fixe, 372, 392
complexité amortie, 424
complexité minimale des tris par comparaisons, 480
composante fortement connexe, 488

dictionnaire
  structure de, 355
diviser pour régner, 338, 483
domaine actif, 516

entiers
  de Barendregt, 510
  de Church, 510
équisatisfiabilité, 347

fonction λ-définissable, 372, 392
fonction μ-récursive, 344, 372, 392, 426, 511
fonction primitive récursive, 344, 372, 426, 496
forme normale , 509
  conjonctive, 347
  de Chomsky, 359

grammaire algébrique, 359, 395, 491
graphe, 363, 369

indécidabilité , 491
  du problème Valid, 340
  du problème de Post, 340, 399
  du problème de RelSat, 399, 516

λ
  calcul, 372, 392, 508
  définissable, 511
  terme, 508

langage
  algébrique, 484
  IMP, 382, 387, 500
  rationnel, 366, 376, 484
LL(1)
  analyse, 395
logique
  de Hoare, 387, 504, 507
  du premier ordre, 340, 376, 400, 491
  propositionnelle, 347, 370, 488

machine de Turing, 344, 351, 374, 394, 426, 485, 491
Master theorem, 338
matrices de Strassen, 339
modèle, 341
modèle de calcul, 346, 372

NL, 489, 490
NP, 485, 490
NP-complétude
  de 3Col, 369, 486
  de 3Sat, 353, 369, 486
  de BinPacking, 486
  de Clique, 486
  de CnfSat, 347, 353, 486
  de HamCirc, 486
  de IndependentSet, 486
  de Partition, 487
  de PVC, 486
  de SacÀDos, 487
  de Sat, 347, 351, 486
  de SubsetSum, 486
  de VertexCover, 486

P, 488, 490
parcours
  en profondeur, 363
point fixe
  combinateur de, 511
  de Curry, 511
  de Turing, 511
Post
  problème de, 491
Premier
  fonction, 395
Presburger
  théorie de, 376
problème
  2Sat, 488
  3Col, 369, 486
  3Sat, 353, 369, 486
  Accept, 492
  BinPacking, 486
  Clique, 486
  CnfSat, 347, 353, 486
  HamCirc, 486
  IndependentSet, 486
  Partition, 487
  Peano, 493
  PVC, 486
  RelEqu, 493
  RelSat, 399, 493, 516
  SacÀDos, 487
  Sat, 347, 351, 486
  SubsetSum, 486
  Valid, 340, 492
  VertexCover, 486
  Vide, 492
  de Post, 340, 399, 492
  de Presburger, 376
  de l'Arrêt, 394, 492
  du mot pour les grammaires algébriques, 361
programmation dynamique, 360, 483
PSpace, 490

récursivement énumérable, 392, 426, 511
réduction
  calculable, 340, 399, 491
  espace logarithmique, 490
  temps polynomial, 349, 369, 485, 490
résiduel, 367
règle conjonctive, 513
recherche de motif dans un texte, 366, 423
relation, 512
requête conjonctive, 513

sémantique
  à grands pas, 382, 387, 501, 505
  à petits pas, 382, 502, 506
  dénotationnelle, 386, 503
  naturelle, 501
  opérationnelle, 382, 387, 501, 505, 506
satisfiabilité d'une requête, 399
schéma algorithmique, 483
Scott–Curry
  théorème de, 392, 511

tas binaire, 334
terme
  de λ-calcul, 508
théorème
  de Church-Rosser, 509

de Rice, 492
de Scott–Curry, 394, 511
théorie, 343, 376
thèse de Church, 344, 372
transformation de Tseitin, 347
tri
fusion, 339
par comparaison, 480
par tas, 334
topologique, 363
Turing
machine de, 491

BIBLIOGRAPHIE

[AHV95] Serge ABITEBOUL, Richard HULL, and Victor VIANU. *Foundations of Databases.* Addison-Wesley Publishing Company, 1995.

[AK98] Luc ALBERT and Daniel KROB. *Cours et exercices d'informatique.* Vuibert, 1998.

[AK02] Grégoire ALLAIRE and Sidi Mahmoud KABER. *Algèbre linéaire numérique.* Ellipses, 2002.

[AM04] Eric AMAR and Etienne MATHERON. *Analyse complexe.* Cassini, 2004.

[AUD06] Michèle AUDIN. *Géométrie.* EDP Sciences, 2006.

[AUT92] Jean-MIchel AUTEBERT. *Calculabilité et décidabilité.* Masson, 1992.

[AUT97] Jean-Michel AUTEBERT. *Théorie des langages et automates.* Masson, 1997.

[BA12] Mordechai BEN ARI. *Mathematical Logic for Computer Science.* Springer, 2012.

[BAR12] Henk BARENDREGT. *The Lambda Calculus.* College Publications, 2012.

[BB18] Julien BERNIS and Laurent BERNIS. *Analyse pour l'agrégation de mathématiques, 40 développements.* Ellipses, 2018.

[BBC92] Danièle BEAUQUIER, Jean BERSTEL, and Philippe CHRETIENNE. *Éléments d'algorithmique.* Masson, 1992.

[BER17] Florent BERTHELIN. *Equations Différentielles.* Cassini, 2017.

[BFH12] Alain BRETTO, Alain FAISANT, and François HENNECART. *Éléments de théorie des graphes.* Springer, 2012.

[BG10] Sylvie BENZONI-GAVAGE. *Calcul différentiel et équations différentielles.* Dunod, 2010.

[BL07] Philippe BARBE and Michel LEDOUX. *Probabilité.* EDP Sciences, 2007.

[BMP05] Vincent BECK, Jérôme MALICK, and Gabriel PEYRÉ. *Objectif Agrégation.* H & K, 2005.

[BOY15] Pascal BOYER. *Algèbre et Géométries.* Calvage et Mounet, 2015.

[BP12] Marc BRIANE and Gilles PAGÈS. *Théorie de l'intégration.* Vuibert, 2012.

[BRE05] Haïm BREZIS. *Analyse fonctionnelle.* Dunod, 2005.

[BRU10] Richard BRUALDI. *Introductory Combinatorics.* Pearson, 2010.

[CAL98] Josette CALAIS. *Éléments de Théorie des Groupes.* PUF, 1998.

[CAL06] Josette CALAIS. *Extensions de Corps, Théorie de Galois.* Ellipses, 2006.

[CAN09] Bernard CANDELPERGHER. *Calcul intégral.* Cassini, 2009.

[CAR14] Olivier CARTON. *Langages Formels : Calculabilité et complexité.* Vuibert, 2014.

[CG17] Philippe CALDERO and Jerôme GERMONI. *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 1.* Calvage et Mounet, 2017.

[CG18] Philippe CALDERO and Jerôme GERMONI. *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2.* Calvage et Mounet, 2018.

[CGCDM05] Marie COTTREL, Valentine GENON-CATALOT, Christian DUHAMEL, and Thierry MEYRE. *Exercices de Probabilités.* Cassini, 2005.

[CHL01] Maxime CROCHEMORE, Christophe HANCART, and Thierry LECROQ. *Algorithmique du texte.* Vuibert, 2001.

[CIA06] Philippe CIARLET. *Introduction à l'analyse numérique matricielle et à l'optimisation.* Dunod, 2006.

[CL03] René CORI and Daniel LASCAR. *Logique Mathématique.* Dunod, 2003.

[CLRS10] Thomas CORMEN, Charles LEISERSON, Ronald RIVEST, and Clifford STEIN. *Algorithmique.* Dunod, 2010.

[COG00] Michel COGNET. *Algèbre Linéaire.* Bréal, 2000.

[COL11] Pierre COLMEZ. *Éléments d'analyse et d'algèbre.* École Polytechnique, 2011.

[COM95] Jean COMBES. *Suites et séries.* PUF, 1995.

[COM98] François COMBES. *Algèbre et Géométrie.* Bréal, 1998.

[CON95] John CONWAY. *Functions of One Complex Variable.* Springer, 1995.

[DB04] Jean DE BIASI. *Mathématiques pour le CAPES et l'Agrégation interne.* Ellipses, 2004.

[DEM08] Michel DEMAZURE. *Cours d'Algèbre.* Cassini, 2008.

[DEM16] Jean-Pierre DEMAILLY. *Analyse numérique et équations différentielles.* EDP Sciences, 2016.

[DIE97] Jean DIEUDONNÉ. *Calcul infinitésimal.* Hermann, 1997.

[DLL12] Stéphane DEVISMES, Pascal LAFOURCADE, and Michel LÉVY. *Logique et démonstration automatique - Introduction à la logique propositionnelle et à la logique du premier ordre.* Ellipses, 2012.

[DM85] Harry DYM and Henry McKean. *Fourier Series and Integrals.* Academic Press In, 1985.

[DNR04] René DAVID, Karim NOUR, and Christophe RAFFALLI. *Introduction à la logique : Théorie de la démonstration.* DUNOD, 2004.

[DPV06] Sanjoy DASGUPTA, Christos PAPADIMITRIOU, and Umesh VAZIRANI. *Algorithms.* McGraw-Hill, 2006.

[DSP11] Clément DE SEGUINS PAZZIS. *Invitations aux formes quadratiques.* Calvage et Mounet, 2011.

[DUP15] Jacques DUPARC. *Logique pas à pas.* PPUR, 2015.

[DUV07] Daniel DUVERNEY. *Théorie des Nombres.* Dunod, 2007.

[EA08] Mohammed EL AMRANI. *Analyse de Fourier dans les espaces fonctionnels.* Ellipses, 2008.

[EA11] Mohammed EL AMRANI. *Suites et séries numériques, suites et séries de fonctions.* Ellipses, 2011.

[EID09] Jean-Denis EIDEN. *Géométrie analytique classique.* Calvage et Mounet, 2009.

[FAR06] Jacques FARAUT. *Calcul Intégral.* EDP Sciences, 2006.

[FB94] Robert FLOYD and Richard BEIGEL. *The Language of Machines : An Introduction to Computability and Formal Languages.* W.H. Freeman & Company, 1994.

[FFF12] Dominique FOATA, Jacques FRANCHI, and Aimé FUCHS. *Calcul des probabilités*. Dunod, 2012.

[FGN03] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Analyse 1*. Cassini, 2003.

[FGN09] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Algèbre 2*. Cassini, 2009.

[FGN12] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Analyse 4*. Cassini, 2012.

[FGN13a] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Algèbre 3*. Cassini, 2013.

[FGN13b] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Analyse 2*. Cassini, 2013.

[FGN14] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Analyse 3*. Cassini, 2014.

[FGN18] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Algèbre 1*. Cassini, 2018.

[FGS90] Christine FROIDEVAUX, Marie-Claude GAUDEL, and Michèle SORIA. *Type de données et algorithmes*. McGraw-Hill, 1990.

[FIL09] Francis FILBERT. *Analyse numérique*. Dunod, 2009.

[GJ79] Michael GAREY and David JOHNSON. *Computers and Intractability : A Guide to the Theory of Np-Completeness*. Freeman, 1979.

[GOU08a] Xavier GOURDON. *Algèbre*. Ellipses, 2008.

[GOU08b] Xavier GOURDON. *Analyse*. Ellipses, 2008.

[GOU11] Thierry GOUDON. *Intégration*. Ellipses, 2011.

[GRI11] Joseph GRIFONE. *Algèbre Linéaire*. Cépaduès, 2011.

[GS09] Roland GROUX and Philippe SOULAT. *Les fonctions spéciales vues par les problèmes*. Cepadues, 2009.

[GT96] Stéphane GONNORD and Nicolas TOSEL. *Topologie et analyse fonctionnelle : Thèmes d'analyse pour l'agrégation*. Ellipses, 1996.

[HAN94] Chris HANKIN. *Lambda Calculi, a guide for computer scientists*. Clarendon Press Oxford, 1994.

[HAU07] Bertrand HAUCHECORNE. *Les contre-exemples en Mathématiques*. Ellipses, 2007.

[HIN08] Marc HINDRY. *Arithmétique*. Calvage et Mounet, 2008.

[HIRP05] Bernard HERON, Françoise ISSARD-ROCH, and Colette PICARD. *Analyse Numérique*. Dunod, 2005.

[HL99] Francis HIRSCH and Gilles LACOMBE. *Éléments d'analyse fonctionnelle*. Dunod, 1999.

[HMU12] John HOPCROFT, Rajeev MOTWANI, and Jeffrey ULLMAN. *Introduction to automata theory, languages and computation*. Pearson, 2012.

[HR04] Michael HUTH and Mark RYAN. *Logic in Computer Science*. Cambridge University Press, 2004.

[HS08] Roger HINDLEY and Jonathan SELDIN. *Lambda-Calculus and combinators, an introduction*. Cambridge University Press, 2008.

[JOL16] Paul JOLISSAINT. *Fonctions d'une variable complexe, théorie de Cauchy élémentaire et applications*. Ellipse, 2016.

[KNU11] Donald KNUTH. *The Art of Computer Programming, Vol.2*. Addison Wesley, 2011.

[LAF96] Jacques LAFONTAINE. *Introduction aux variétés différentielles*. PUG, 1996.

[LAL00] René LALEMENT. *Logique, Réduction, Résolution*. Masson, 2000.

[LAM12a] Jean-Pierre LAMOITIER. *Arithmétique Classique*. Ellipses, 2012.

[LAM12b] Jean-Pierre LAMOITIER. *Arithmétique Modulaire*. Ellipses, 2012.

[LDR93] Richard LASSAIGNE and Michel DE ROUGEMONT. *Logique et fondements de l'informatique logique du 1er ordre, calculabilité et lambda-calcul*. Hermes Science Publications, 1993.

[LES12] Ahmed LESFARI. *Distributions, analyse de Fourier et transformation de Laplace*. Ellipses, 2012.

[LES15] Ahmed LESFARI. *Équations différentielles ordinaires et équations aux dérivées partielles*. Ellipses, 2015.

[LMLBP20] Didier LESESVRE, Pierre MONTAGNON, Pierre LE BARBENCHON, and Théo PIERRON. *131 Développements pour l'oral*. Dunod, 2020.

[LR03] Bruce LANDMAN and Aaron ROBERTSON. *Ramsey Theory on the Integers*. AMS, 2003.

[LS15] Romain LEGENDRE and François SCHWARZENTRUBER. *Compilation : Analyse Lexicale et Syntaxique du Texte à sa Structure en Informatique*. Ellipses, 2015.

[MM16] Roger MANSUY and Rached MNEIMNÉ. *Algèbre Linéaire, Réduction des Endomorphismes*. Vuibert, 2016.

[NN07] Hanne Riis NIELSON and Flemming NIELSON. *Semantics with applications*. Springer, 2007.

[OUV98] Jean-Yves OUVRARD. *Probabilités 1*. Cassini, 1998.

[OUV00] Jean-Yves OUVRARD. *Probabilités 2*. Cassini, 2000.

[PAP93] Christos PAPADIMITRIOU. *Computational Complexity*. Pearson, 1993.

[PER96] Daniel PERRIN. *Cours d'Algèbre*. Ellipses, 1996.

[PEY04] Gabriel PEYRÉ. *L'algèbre discrète de la transformée de Fourier*. Ellipses, 2004.

[POM94] Alain POMMELET. *Cours d'analyse : Agrégation de Mathématiques*. Ellipses, 1994.

[QSS07] Alfio QUARTERONI, Riccardo SACCO, and Fausto SALERI. *Méthodes Numériques*. Springer, 2007.

[QUE16] Hervé QUEFFELEC. *Topologie*. Dunod, 2016.

[QZ07] Hervé QUEFFELEC and Claude ZUILY. *Analyse pour l'agrégation*. Dunod, 2007.

[RB06] Jean-Jacques RISLER and Pascal BOYER. *Algèbre pour la licence 3 : Groupes, Anneaux, Corps*. Dunod, 2006.

[RDO98] Edmond RAMIS, Claude DESCHAMPS, and Jacques ODOUX. *Cours de Mathématiques 3 : Topologie et éléments d'analyse*. Dunod, 1998.

[ROM04] Jean-Etienne ROMBALDI. *Éléments d'analyse réelle*. EDP Sciences, 2004.

[ROU03] Henri ROUDIER. *Algèbre Linéaire*. Vuibert, 2003.

[ROU09] François ROUVIÈRE. *Petit guide de calcul différentiel*. Cassini, 2009.

[RP02] Jacques RAPPAZ and Marco PICASSO. *Introduction à l'analyse numérique*. Ellipses, 2002.

[RUD98] Walter RUDIN. *Analyse réelle et complexe*. Dunod, 1998.

[RWM15] Jean-Pierre RAMIS, André WARUSFEL, and François MOULIN. *Mathématiques pures et appliquées : Algèbre et Géométrie*. De Boeck, 2015.

[SAK17] Jacques SAKAROVITCH. *Éléments de théorie des automates*. Vuibert, 2017.

[SCHa] François SCHWARZENTRUBER. *Polycopié sur la calculabilité*.

[SCHb] François SCHWARZENTRUBER. *Polycopié sur la logique*.

[SIP12] Michael SIPSER. *Introduction to the Theory of Computation*. South-Western College Publishing, 2012.

[SPR02] Philippe SAUX-PICART and Éric RANNOU. *Cours de calcul formel, Corps finis, Systèmes polynomiaux, applications*. Ellipses, 2002.

[ST15] Ian STEWART and David TALL. *Algebraic Number Theory*. Chapman and Hall, 2015.

[TAU05] Patrice TAUVEL. *Géométrie*. Dunod, 2005.

[TOU99] Paul TOULOUSE. *Thèmes de probabilités et statistique*. Dunod, 1999.

[ULM12] Félix ULMER. *Théorie des Groupes*. Ellipses, 2012.

[VAZ10] Vijay VAZIRANI. *Algorithmes d'approximation*. Springer, 2010.

[WCC+13] Benjamin WACK, Sylvain CONCHON, Judicaël COURANT, Marc DE FALCO, Gilles DOWEK, Jean-Christophe FILLIATRE, and Stéphane GONNORD. *Informatique pour tous en classes préparatoires aux grandes écoles*. Eyrolles, 2013.

[WIN93] Glynn WINSKEL. *The Formal Semantics of Programming Languages : An Introduction*. MIT Press, 1993.

[WOL06] Pierre WOLPER. *Introduction à la calculabilité*. Dunod, 2006.

[ZAV13] Maxime ZAVIDOVIQUE. *Un Max de Maths*. Calvage et Mounet, 2013.