

Université Paris-Saclay

Université de Versailles Saint-Quentin-en-Yvelines

M1 Mathématiques et interactions Site UVSQ

Présentation et Syllabus¹ (2017– 2018)

1. Les informations contenues dans le présent document sont susceptibles d'évoluer légèrement.

Table des matières

Présentation du Master 1 MINT	3
Contacts	7
Modalités de contrôle des connaissances	8
Calendrier provisoire	9
Tronc commun	11
Probabilités	12
Mathématiques assistées par ordinateur	13
Analyse d'algorithmes, programmation	15
Théorie de l'information	16
Projet	18
Anglais	19
Spécialisation "Algèbre appliquée"	20
Algèbre 1	21
Théorie des nombres et cryptographie	22
Cryptographie	23
Algèbre 2	25
Introduction aux courbes elliptiques	26
Calcul sécurisé	27
Spécialisation "Modélisation, Simulation"	28
Introduction à l'analyse fonctionnelle et aux équations aux dérivées partielles	29
Optimisation	29
Méthodes numériques	31
Mécanique des milieux continus – Fluides	32
Mécanique des milieux continus – Solides	33
Ondes et acoustique dans les fluides	35
Analyse des équations aux dérivées partielles	36
Méthodes numériques avancées et programmation	37
Stabilité et bifurcation	39
Corps professoral	40

Présentation

Le Master 1 « Mathématiques en Interaction » (MINT) de l'Université de Versailles Saint-Quentin-en-Yvelines est destiné à des étudiants désirant acquérir une formation solide et moderne dans le domaine des mathématiques et de leurs applications. Il fait partie du Master « Mathématiques et Applications » de l'Université Paris-Saclay.

L'objectif principal de ce master est de former des mathématiciens de haut niveau maîtrisant à la fois des techniques pointues d'algèbre et/ou d'analyse, ainsi que les outils de modélisation et de programmation qui leur ouvriront de nombreux débouchés professionnels.

La formation proposée dans le cadre du Master 1 « Mathématiques en Interaction » s'articule autour d'un tronc commun et de deux spécialisations au choix. Le tronc commun comporte un socle de connaissances fondamentales en mathématiques, en informatique et en modélisation. Les deux spécialisations proposées sont « Algèbre appliquée » et « Modélisation, Simulation ».

Après cette première année de Master, les deux spécialisations se poursuivent dans deux parcours : « Analyse, Modélisation et Simulation » et « Analyse, Arithmétique, Géométrie et Algèbre Appliquée », faisant tous deux partie de la deuxième année du Master « Mathématiques et Applications » (voir schéma ci-dessous).

Le présent document contient un descriptif des cours du tronc commun et de chacune des deux spécialisations. On y trouve en particulier le poids, le volume horaire le contenu et les objectifs de chaque cours. Une liste des enseignants qui interviendront dans ces cours est aussi présentée.

Spécialisation M1 "Algèbre appliquée"

Les étudiants qui se spécialiseront en algèbre appliquée suivront des cours approfondis en algèbre commutative, arithmétique, cryptographie et théorie algébrique des systèmes.

La spécialisation « Algèbre appliquée » ouvre à des débouchés académiques et privés : thèse dans un organisme public (universités, INRIA, etc.) ou en collaboration avec une entreprise privée, recherche en mathématiques fondamentales ou appliquées à la théorie du contrôle, à la cryptographie et à la sécurité informatique dans les milieux académique ou privé (Accenture, Dictao, Gemalto, Oberthur, Orange, etc.). Les étudiants pourront également s'orienter vers l'informatique théorique et les métiers d'ingénieurs dans le domaine des mathématiques appliquées à l'informatique (cryptologie, robotique).

Spécialisation M1 "Modélisation, Simulation"

Les étudiants qui suivront la spécialisation « Modélisation, Simulation » auront des cours ap-

profondis dans les domaines des équations aux dérivées partielles, de l'optimisation, du calcul scientifique et de la modélisation mécanique.

La spécialisation «Modélisation, Simulation» prépare les étudiants à de nombreux débouchés académiques et professionnels. Au terme de leurs deux années de Master, ils pourront par exemple candidater à une thèse dans un organisme public (universités, INRIA, CEA, Onera) ou en collaboration avec une entreprise privée. Ils pourront également postuler à des emplois dans le monde professionnel (Airbus, EDF, Renault, PSA, Safran, Thalès, etc.).

Cours M1 de tronc commun

- Probabilités (semestre 1, 3 ects)
- Mathématiques assistées par ordinateur (semestre 1, 6 ects)
- Analyse d'Algorithmes, Programmation (semestre 2, 5 ects)
- Théorie de l'information (semestre 2, 4 ects)
- Projet (semestre 2, 6 ects)
- Anglais (semestre 1, 3 ects)

Cours M1 de la spécialisation "Algèbre appliquée"

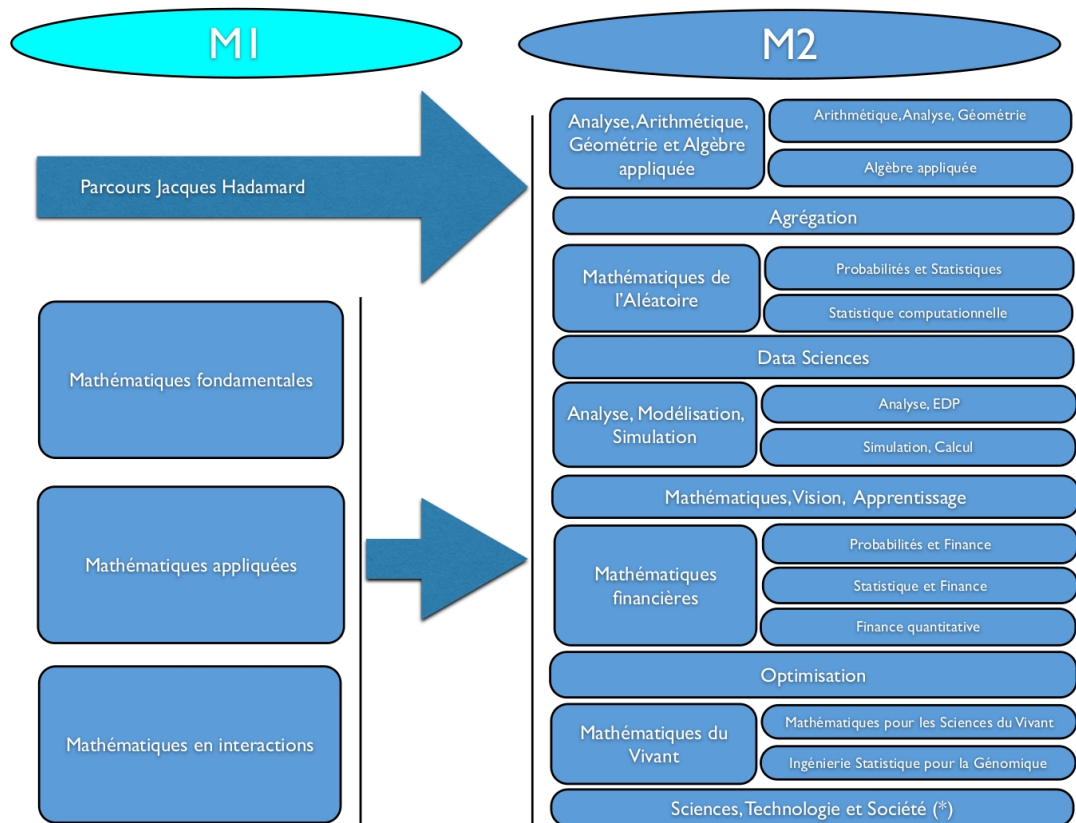
- Algèbre 1 (semestre 1, 6 ects)
- Théorie des nombres et cryptographie (semestre 1, 6 ects)
- Cryptographie (semestre 1, 6 ects)
- Algèbre 2 (semestre 2, 6 ects)
- Introduction aux courbes elliptiques (semestre 2, 6 ects)
- Calcul sécurisé (semestre 2, 3 ects)

Cours M1 de la spécialisation "Modélisation, Simulation"

- Introduction à l'analyse fonctionnelle et aux équations aux dérivées partielles (6 ects)
- Optimisation (semestre 1, 6 ects)
- Analyse des équations aux dérivées partielles (semestre 2, 6 ects)
- Méthodes numériques avancées et programmation (semestre 2, 6 ects)
- Stabilité et bifurcation (semestre 2, 3 ects)
- Mécanique des milieux continus - Fluides (semestre 1, 3 ects, optionnel)
- Mécanique des milieux continus - Solides (semestre 1, 3 ects, optionnel)
- Méthodes numériques (semestre 1, 3 ects, optionnel)
- Ondes et acoustique dans les fluides (semestre 1, 3 ects, optionnel)

Tous les cours sont obligatoires à l'exception des modules "Mécanique des milieux continus - Fluides", "Mécanique des milieux continus - Solides", "Ondes et acoustique dans les fluides" et "Méthodes numériques" dont il faudra choisir deux parmi les quatre.

Schéma du Master **Mathématiques et Applications**
de l'Université Paris-Saclay



Contacts

Enseignants responsables du master 1 MINT

- Spécialisation "Algèbre appliquée" : V. Sécherre et M. Krir
- Spécialisation "Modélisation, Simulation" : T. Z. Boulmezaoud
- Responsable global : V. Sécherre

Les coordonnées des professeurs responsables sont disponibles à la fin du présent document.

Secrétariat du département de mathématiques

Madame Liliane Roger
Bâtiment Fermat, 45 avenue des États-Unis,
78035 Versailles Cedex.
Téléphone : +33 1 39 25 46 46.
(coordonnées disponibles à la fin du présent document).

Scolarité

Bureau des Masters
Mme V. Delahaye, Mme M. Deschamps, Mme T. Diantantu
Bâtiment Fermat, 45 avenue des États-Unis,
78035 Versailles Cedex.

Master MMM (Méthodes Mathématiques pour la Mécanique)

Responsable : Mr. Paolo Vannucci.

Modalités de contrôle des connaissances 2017 - 2018

Chaque UE (Unité d'Enseignement) est évaluée par une note finale. Cette note est attribuée à chaque étudiant suivant cette UE en fonction de ses résultats aux contrôles de connaissances. Elle est calculée comme une moyenne pondérée de deux notes : une note de contrôle continu (CC) et une note d'évaluation terminale. Le poids de chacune de ces deux notes varie selon l'UE.

La note de contrôle continu synthétise des évaluations qui interviennent tout au long du semestre. Ce contrôle continu est organisé par l'équipe enseignante intervenant dans l'UE.

L'évaluation terminale (ou examen) est programmée après la fin des cours, lors de la première session d'examens. Pour l'année universitaire 2017-2018, la session d'examens du 1er semestre est prévue en janvier 2018, après les vacances de fin d'année. La session d'examens du second semestre est quant à elle prévue en mai 2018.

Une session de rattrapage est organisée en juin 2018 et porte sur les deux semestres. Son but est de donner une seconde chance à chaque étudiant concerné afin de valider des UE. L'évaluation de l'UE "Projet" (prévu au semestre 2) se fait sur la base de l'avis de l'encadreur, de la rédaction d'un mémoire et d'une soutenance orale. Cet UE n'est pas concerné par les sessions d'évaluations terminales.

Les étudiants sont invités à consulter les modalités de contrôle des connaissances pour chacune des deux sessions sur le site du master Mathématiques et applications de l'université Paris-Saclay.

Calendrier provisoire 2017 - 2018

Le calendrier ci-dessous est susceptible d'être modifié. Il concerne tous les cours du master M1 MINT à l'exception des quatre cours suivants :

- Méthodes numériques (S1)
- Mécanique des milieux continus - Fluides (S1)
- Mécanique des milieux continus - Solides (S1)
- Ondes et acoustique dans les fluides (S1)
- Stabilité et bifurcation (S2)

Ces cinq cours relèvent du calendrier du master Méthodes Mathématiques pour la Mécanique (MMM). Ils concernent les étudiants inscrits en master M1 MINT spécialisation "Modélisation, Simulation", ou Master 1 MMM.

Emploi du temps : consulter le lien <http://pubedt.uvsq.fr/VER/>

Calendrier du master 1 MINT

Début des cours :

lundi 18 septembre 2017.

Vacances de la Toussaint :

du samedi 28 octobre 2017 soir au dimanche 6 novembre 2016.

Vacances de la Noël :

du samedi 23 décembre 2017 soir au dimanche 7 janvier 2018.

Examens semestre 1 (1ère session) :

entre le lundi 8 janvier 2018 et le vendredi 19 janvier 2018.

Vacances d'hiver :

du samedi 24 février 2018 au dimanche 4 mars 2018.

Vacances de printemps :

du samedi 21 avril 2018 au dimanche 29 avril 2018.

Examens semestre 2 (1ère session) :

entre le lundi 2 mai 2018 et le mardi 22 mai 2018.

Examens de rattrapage semestre 1 et semestre 2 (2ème session) :

entre le vendredi 1 juin 2018 et le jeudi 30 juin 2018.

Programme des cours
du Master 1
Mathématiques en Interaction

Tronc commun

27 ECTS (12 ECTS en S1, 15 ECTS en S2)

Probabilités

Tutelle: Département de Mathématiques, UVSQ

Volume horaire: CM: 12h TD: 12h

ECTS: 3

Semestre: 1

Caractère: obligatoire

Intervenants: Catherine Donati-Martin

Lieu: UVSQ

Parcours: Modélisation, Simulation, Algèbre appliquée

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Calcul intégral et théorie de la mesure, Probabilités (cours L3)

Description

On reprend rapidement en les approfondissant les notions d'espace probabilisé et de variables aléatoires. On développe les différentes notions de convergence de variables aléatoires. On introduit la notion de processus stochastiques (famille de variables aléatoires indexées par le temps) qu'on illustre par l'étude des marches aléatoires et des chaînes de Markov.

Contenu

- Espaces de probabilités, variables aléatoires, indépendance
- Convergence de variables aléatoires, théorèmes limites
- Espérance conditionnelle
- Marches aléatoires
- Chaînes de Markov

Bibliographie

- P. Barbe et M. Ledoux, *Probabilité*, Belin, 1998.
- B. Bercu et D. Chafaï, *Modélisation stochastique et simulation. Cours et applications*, Dunod, 2007.
- R. Durrett, *Probability : Theory and Examples*, Duxbury, 2005.
- D. Foata et A. Fuchs : *Calcul des Probabilités : Cours, exercices et problèmes corrigés*, Dunod, 2003.
- Olivier Garet, Aline Kurtzmann, *De l'intégration aux probabilités*, Ellipses, 2011.
- P. Baldi, L. Mazliak et P. Priouret *Martingales et Chaînes de Markov*. Hermann, collection Méthodes, 1998.
- W. Feller, *An introduction to probability theory and its applications*, Wiley.

Mathématiques assistées par ordinateur

Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TP: 24h
ECTS: 6
Semestre: 1
Intervenants: Tahar Z. Boulmezaoud et Nicolas Perrin
Lieu: UVSQ
Caractère: obligatoire
Parcours: Modélisation, Simulation, Algèbre appliquée
Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: algèbre et analyse de licence

Description

Ce cours comporte essentiellement deux composantes de poids équivalents. La première composante est une initiation au Calcul formel (*Computer Algebra* en anglais). Celui-ci s'intéresse aux méthodes qui permettent de trouver des résultats de façon :

- Exacte (par opposition au Calcul numérique).
- Effective (par opposition aux théorèmes purement existentiels).
- Efficace (par opposition aux calculs dont la faisabilité est purement théorique).

L'outil de base est donc l'algorithme, dont on verra divers types. La question de l'efficacité donnera lieu à de petites études de complexité. Mais il ne s'agit aucunement d'un cours d'informatique, et aucun pré-requis n'est demandé dans ce domaine.

La deuxième composante du cours est dédiée à l'analyse numérique. Il s'agira essentiellement de la résolution de systèmes linéaires, d'équations différentielles et d'équations aux dérivées partielles. L'accent sera mis tout spécialement sur les méthodes numériques modernes.

Une partie non négligeable du cours se passera devant des ordinateurs, et sera consacrée à écrire en SAGE, MAXIMA ou SCILAB des algorithmes vus en cours.

Contenu

- **Calcul formel**
 - Objets de base : Les grands entiers, les polynômes à 1 variable.
 - Représentation. Addition et soustraction. Multiplication. Division euclidienne.
 - Algorithme d'Euclide : pgcd, identité de Bézout. Applications.
 - Arithmétique modulaire. Théorème chinois des restes.
 - Evaluation et interpolation (polynômes de Legendre). Changement de représentation.

- Multiplication rapide : Karatsuba ; transformée de Fourier discrète.
 - Division euclidienne rapide grâce à Newton.
 - Evaluation et interpolation rapides. Théorème chinois des restes rapide.
 - Algorithme d'Euclide rapide.
 - Algèbre linéaire rapide : multiplication de matrices selon Strassen.
 - Factorisation de polynômes sur un corps fini (Gauss).
- **Analyse numérique**
- Rappels sur les méthodes directes pour la résolution de systèmes linéaires
 - Méthodes itératives classiques (Jacobi, Gauss-Seidel, relaxation).
 - Méthodes itératives modernes. Méthodes de sous-espaces de Krylov.
 - Calcul de valeurs propres.
 - Schémas de résolution d'équations différentielles.
 - Résolution de problèmes aux limites 1D et 2D (différences finies, éléments finis).

Bibliographie

- J. Von zur Gathen & J. Gerhard, *Modern Computer Algebra*, 3rd Edition, Cambridge University Press (2013).
- V. Shoup, *A Computational Introduction to Number Theory and Algebra*, 2nd Edition, Cambridge University Press (2008).
- J. Stoer et R. Bulirsh, *Introduction to numerical analysis*, Springer (2nd edition).

Analyse d'algorithmes, Programmation

Tutelle: Département de Mathématiques, UVSQ

Volume horaire: CM: 20h TD: 20h

ECTS: 5

Semestre: 2

Intervenants: Luca De Feo

Lieu: UVSQ

Caractère: obligatoire

Parcours: Modélisation, Simulation, Algèbre appliquée, Informatique

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: non suggérés

Description

Introduction aux techniques de conceptions d'algorithmes et d'analyse de performances. TPs sur machine avec environnement Python/Sage.

Contenu

- Analyse d'algorithmes, modèles de complexité, complexité asymptotique, classes de complexité.
- Structures de données et algorithmes : ordonnancement, piles, files, tables de hachage, arbres, graphes.
- Programmation dynamique, programmation linéaire entière.
- Algorithmes arithmétiques : multiplication, pgcd, multiplication de matrices.
- Algorithmes géométriques : programmation linéaire, diagrammes de Vornoi

Bibliographie

- Thomas H. Cormen. Charles E. Leiserson. Ronald L. Rivest. Clifford Stein. Introduction to Algorithms. Third Edition. The MIT Press. Cambridge, Massachusetts.
- Christos H. Papadimitriou. Computational complexity. Addison-Wesley, 1994. 523 pages.

Théorie de l'information

Tutelle: Département de Mathématiques, UVSQ

Volume horaire: CM: 16h TD: 16h

ECTS: 4

Semestre: 2

Intervenants: Michaël Quisquater

Lieu: UVSQ

Caractère: obligatoire

Parcours: Algèbre appliquée, Modélisation, Simulation

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Algèbre linéaire. Quelques éléments d'algèbre. Théorie élémentaire des probabilités.

Description

Le but d'un système de communication est le transport d'information d'une source à un destinataire via un canal de communication. Ce canal possède en général des imperfections ce qui peut engendrer des erreurs de transmission. Aussi, le canal peut être sujet à des écoutes ce qui peut poser des problèmes de confidentialité. Finalement, l'utilisation d'un canal a un coût, il est donc important d'optimiser son usage.

Pour répondre à ces différentes exigences, on effectue un prétraitement de l'information ; il s'agit de la chaîne de codage. Celle-ci se divise en trois étapes : compression, chiffrement et ajout de redondance. Ces techniques font appel à la théorie des probabilités et à l'algèbre discrète. Ce cours présente les bases de la première et la troisième étape de la chaîne de codage, la seconde étant abondamment étudiée dans des cours de cryptographie.

Contenu

- Notions de base en théorie de l'information (entropie, information mutuelle).
- Algorithmes de compression sans perte (étape 1 de la chaîne de codage).
- Théorie des codes correcteurs d'erreurs (étape 3 de la chaîne de codage).
 - Canal sans mémoire à temps discret. Notion de capacité. Théorème de codage pour un canal bruyant. Principe de décodage par maximum de vraisemblance. Borne sur la probabilité d'erreur de décodage.
 - Théorie des codes correcteurs en blocs. Distance minimale et problématique des bornes sur la taille d'un code. Notion de code parfait.
 - Codes linéaires. Matrice génératrice et matrice de parité. Décodage par syndrome. Codes duaux. Polynôme énumérateur des poids. Identité de Mac-Williams.
 - Etude de certaines familles de codes linéaires (en bloc) et algorithmes de décodage.
 - Codes convolutionnels et algorithme de Viterbi.

Bibliographie

- The Theory of Error-Correcting Codes. F. J. MacWilliams, N. J. A. Sloane North Holland Publishing Co. 1977.
- Théorie des codes (Compression, cryptage, correction). J.-G. Dumas, J.-L. Roch, E. Tannier et S. Varrette, Dunod 2007.

Projet

Tutelle: Département de Mathématiques, UVSQ

ECTS: 6

Semestre: 2

Intervenants: Membres du département de Mathématiques

Lieu: UVSQ

Caractère: obligatoire

Parcours: Modélisation, Simulation, Algèbre appliquée

Evaluation: Appréciation de l'encadrant, rédaction d'un mémoire, soutenance orale (20 minutes + questions du jury).

Pré-requis: selon le sujet choisi.

Description

Ce module est l'occasion pour un binôme d'étudiants d'approfondir ses connaissances dans un thème choisi en accord avec un encadrant. Le sujet pourrait être la compréhension d'un résultat mathématique remarquable, l'étude d'un ouvrage particulier ou la réalisation d'un travail de recherche. Une collaboration avec le secteur économique et industriel pourrait aussi être envisagée.

Un enseignant suivra l'avancement du projet et orientera le binôme tout au long du semestre.

Le binôme rédigera un mémoire final (d'une vingtaine de pages) et défendra son travail lors d'une soutenance orale comportant un exposé suivi de questions du jury.

Anglais

Tutelle: Institut d'Etudes Culturelles et Internationales

Volume horaire: CM: 0h TD: 27h

ECTS: 3

Semestre: 1

Caractère: obligatoire

Intervenants: Florian Leniaud et Jean-Baptiste Goyard

Lieu: UVSQ

Parcours: Modélisation, Simulation, Algèbre appliquée, Informatique

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis:

- Etre capable de comprendre à l'oral comme à l'écrit des supports d'anglais général et scientifique.
- Etre capable de faire des présentations orales et écrites sur des sujets d'actualité divers.
- Avoir d'importantes notions en grammaire anglaise.

Description

Dans un contexte à caractère professionnel, les cours en anglais Master visent à aider les étudiants à faire face aux exigences du monde du travail.

Contenu

- Job Interview
- Debating
- CV - Cover letter - Essay writing
- Listening Comprehension
- TOEIC training

Spécialisation "Algèbre appliquée"

33 ECTS (18 ECTS en S1, 15 ECTS en S2)

Algèbre 1

Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 1
Intervenants: Martin Andler
Lieu: UVSQ
Caractère: obligatoire
Parcours: Algèbre appliquée
Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Algèbre de licence

Description

Après de brèves révisions sur les structures fondamentales de l'algèbre : groupes, anneaux, corps, on étudie les anneaux de polynômes sur un anneau et sur un corps. Les deux domaines importants étudiés dans cette UE sont les modules, en particulier la structure de modules de type fini sur un anneau principal, et les extensions de corps et la théorie de Galois.

Contenu

- Anneaux de polynômes sur un anneau. Cas d'un corps ; théorèmes d'hérédité.
- Extensions de corps ; extensions algébriques.
- Groupe de Galois.
- Modules sur un anneau, modules de type fini ; modules sur un anneau principal.

Bibliographie

- Lang S., *Algebra*, Springer.
- Stewart I., *Galois Theory*, Chapman & Hall.
- Chambert-Loir A., *Algèbre corporelle*.

Théorie des nombres et cryptographie

Tutelle: Département de Mathématiques, UVSQ

Volume horaire: CM: 24h TD: 24h

ECTS: 6

Semestre: 1

Intervenants: Vincent Sécherre

Lieu: UVSQ

Caractère: obligatoire

Parcours: Algèbre appliquée

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Algèbre de Licence (groupes, anneaux, corps, polynômes et congruences)

Description

L'objectif de ce cours est de mettre en évidence la façon dont des propriétés algébriques (notamment les structures de groupe et d'anneau) peuvent servir à prouver des résultats arithmétiques, avec des applications à la cryptographie. Au début du cours, on rappelle brièvement les notions de théorie des groupes et des anneaux qui seront nécessaires dans la suite. On étudie notamment l'anneau des entiers relatifs et les anneaux de polynômes en une indéterminée à coefficients dans un corps, en insistant sur leurs propriétés algébriques communes. On étudie ensuite les propriétés arithmétiques des anneaux de congruence $\mathbb{Z}/n\mathbb{Z}$ et des corps finis, y compris la loi de réciprocité quadratique de Gauss, et on en déduit plusieurs tests de primalité. On introduit ensuite diverses propriétés de structure (anneaux euclidiens, principaux, factoriels, intégralement clos, etc.) et leurs conséquences en arithmétique (notamment le théorème des deux carrés). On introduit enfin la notion d'entier quadratique et on démontre le théorème des unités, qui permet de résoudre l'équation de Pell $x^2 + dy^2 = 1$.

Contenu

- Groupes et anneaux
- Entiers et polynômes en une indéterminée
- Congruences modulo un entier
- Corps finis
- Les entiers de Gauss et le théorème des deux carrés
- Anneaux euclidiens, principaux, factoriels
- Le théorème des unités et l'équation de Pell

Bibliographie

- M. Demazure, *Cours d'algèbre*, Cassini, 1997.
- M. Hindry, *Arithmétique*, Calvage et Mounet, 2008.
- K. Ireland et M. Rosen, *A classical introduction to modern number theory*, Graduate texts in mathematics **84**, Springer, 1990.
- D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

Cryptographie

Tutelle: Département d'Informatique et Département de Mathématiques, UVSQ

Volume horaire: CM: 20h TD: 20h

ECTS: 6

Semestre: 1

Intervenants: Louis Goubin

Lieu: UVSQ

Caractère: obligatoire

Parcours: Algèbre appliquée, Informatique

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Algèbre et algèbre linéaire de licence : arithmétique modulaire, calculs dans les corps finis. Rudiments de théorie des probabilités et de statistiques. Connaissances de base en algorithmique.

Description

Le but est de présenter un panorama des principaux algorithmes utilisés en chiffrement, authentification et signature électronique, ainsi que leur utilisation pour sécuriser les communications numériques.

A l'issue de ce cours, les étudiants devront pouvoir :

- utiliser l'arithmétique modulaire et les opérations de base sur les corps finis liées aux techniques cryptographiques
- décrire les concepts et algorithmes cryptographiques de base, incluant le chiffrement/déchiffrement, les fonctions de hachage et la cryptographie à clé publique
- évaluer la sécurité de primitives cryptographiques
- concevoir et analyser des protocoles pour des objectifs de sécurité variés

Contenu

- Cryptographie à clé secrète, Cryptographie à clé publique
- Attaques brutales, attaques par rejeu
- Attaques à chiffré seul, attaques à clair choisi, attaques à clair et chiffré choisis
- Attaques interactives et non interactives
- Chiffrement par flot, chiffrement par blocs
- Transposition et substitution, schémas de Feistel
- DES, AES
- Fonctions à sens unique, fonctions de hachage
- Algorithmes d'échange de clés
- RSA, Algorithmes zero-knowledge
- Applications

Bibliographie

- N. Koblitz, *A Course in Number Theory and Cryptography*, GTM 114, Springer, 1994.
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
- D. Stinson, *Cryptography : Theory and Practice*, Third Edition (Discrete Mathematics and Its Applications), CRC Press, 2005.
- S. Vaudenay, *A Classical Introduction to Cryptography : Applications for Communications Security*, Springer, 2005.

Algèbre 2

Tutelle: Département de Mathématiques, UVSQ

Volume horaire: CM: 24h TD: 24h

ECTS: 6

Semestre: 2

Intervenants: Vincent Cossart

Lieu: UVSQ

Caractère: obligatoire

Parcours: Algèbre appliquée

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Algèbre de Licence (groupes, anneaux, corps, polynômes et congruences), cours de théorie des nombres et cryptographie

Description

L'objectif de ce cours est de permettre aux étudiants d'aborder sereinement la géométrie algébrique et l'algèbre effective. Le cours est tourné vers l'étude des anneaux de polynômes. On cherche constamment à interpréter géométriquement les théorèmes d'algèbre abstraite : lemme de normalisation vs. projection sur un espace vectoriel, Nullstellensatz vs. recherche de l'idéal d'un fermé algébrique. Interprétation géométrique de la dimension de Krull.

Contenu

- Anneaux noethériens, théorème de la base de Hilbert.
- Topologie de Zariski de k^n .
- Correspondance entre idéaux et fermés algébriques.
- Anneaux de fractions, localisation.
- Extensions entières : going up et going down.
- Lemme de normalisation, degré de transcendance, dimension.
- Nullstellensatz.

Bibliographie

- Atiyah et Mac Donald, *An introduction to commutative algebra*, Addison-Wesley, 1969.
- Chambert-Loir *Algèbre commutative et introduction à la géométrie algébrique* <http://www.math.u-psu.fr>
- Cox, Little et O'Shea, *Ideal, varieties and algorithms*, Springer, 1991.
- Matsumura, Hideyuki *Commutative ring theory*. Cambridge University Press, 1986.
- C. Peskine *An algebraic introduction to complex projective geometry, I. Commutative algebra*, Cambridge University Press, 1996.
- D. Perrin, *Cours d'algèbre*, Ellipses, 1996.
- Samuel et Zariski, *Commutative algebra*, 2 volumes, Springer.

Introduction aux courbes elliptiques

Tutelle: Département de Mathématiques UVSQ

Volume horaire: CM: 24h TD: 24h

ECTS: 6

Semestre: 2

Intervenants: Mohamed Krir

Lieu: UVSQ

Caractère: obligatoire

Parcours: Algèbre appliquée

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Cours de Théorie des nombres et cryptographie, semestre 1 M1

Description

On donne les notions élémentaires introductives à la théorie des courbes elliptiques. L'accent sera mis sur l'aspect concret avec des exemples de calcul explicite. On introduit d'abord le plan projectif sur un corps, on définit ensuite les courbes elliptiques, la loi de groupe, les fonctions rationnelles et les diviseurs. La dernière partie sera consacrée aux notions de morphismes, isogénies, points de torsion et au théorème de Hasse.

Contenu

- Fonctions sur la droite projective
- Courbes elliptiques
- Fonctions rationnelles sur une courbe elliptique
- Diviseurs sur une courbe elliptique
- Morphismes entre courbes elliptiques
- Isogénies
- Points de torsion
- Couplage de Weil
- Théorème de Hasse

Bibliographie

- J. H. Silvermann, *The arithmetic of elliptic curves*, Springer 1986.
- *Tout autre livre introductif sur les courbes elliptiques*

Calcul sécurisé

Tutelle: Département d'Informatique et département de Mathématiques, UVSQ

Volume horaire: CM: 12h TD: 12h

ECTS: 3

Semestre: 2

Intervenants: Louis Goubin

Lieu: UVSQ

Caractère: obligatoire

Parcours: Algèbre Appliquée

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Cours de cryptographie (M1 MINT, 1er semestre)

Description

Traditionnellement, en cryptographie, on cherche à garantir la confidentialité, l'intégrité et l'authenticité de «messages», qui sont des objets «statiques» (stockés, ou transmis tels quels sur des canaux de communication non sécurisés). En revanche on ne considère pas la sécurité des algorithmes et protocoles cryptographiques eux-mêmes (qui sont en général des programmes, qui s'exécutent, et sont donc des objets «dynamiques»). Par exemple on ne s'intéresse pas :

- à la confidentialité des programmes (le principe de Kerckhoffs suppose qu'ils sont connus de tout le monde),
- ni à leur intégrité (on suppose qu'Alice et Bob exécutent ces algorithmes / protocoles / programmes correctement, sans aucune modification / erreur / bug),
- ni à leur authenticité (on suppose que les algorithmes / protocoles / programmes exécutés par Alice et Bob ont été installés par une autorité de confiance).

Dans l'UE «Calcul sécurisé», on verra qu'en réalité il est très important de sécuriser également les calculs (au sens d'algorithmes / protocoles / programmes).

Contenu

- Le cours couvrira des aspects pratiques de ces problèmes de sécurité (débordement de tampon, rétro-analyse de code, attaques par canaux auxiliaires, injection de fautes, ...)
- Ce sera aussi l'occasion d'approfondir des questions plus théoriques (modélisation de la notion de calcul, machines de Turing, garbled circuits, programmes auto-modifiants, obfuscation de code, ...), en montrant comment ces notions peuvent être utilisées pour prévenir les vulnérabilités du logiciel.
- Le cours et les TDs seront illustrés par de nombreux exemples, notamment issus de la sécurité des cartes à puce, de la virologie informatique, et des applications émergentes dans le «calcul en nuage» (cloud computing).

Spécialisation "Modélisation, Simulation"

33 ECTS (18 ECTS en S1, 15 ECTS en S2)

Introduction à l'analyse fonctionnelle et aux équations aux dérivées partielles

Tutelle: Département de Mathématiques, UVSQ

Volume horaire: CM: 24h TD: 24h

ECTS: 6

Semestre: 1

Caractère: obligatoire

Intervenants: Pierre Gabriel et Vahagn Nersesyan

Lieu: UVSQ

Parcours: Modélisation, Simulation, MMM

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Fonctions de plusieurs variables, Calcul différentiel, Calcul intégral, Espaces vectoriels normés

Description

Ce cours commencera par l'introduction à des outils d'analyse hilbertienne et au calcul des distributions. Ces outils seront ensuite employés pour analyser quelques équations aux dérivées partielles elliptiques issues de la physique et de la mécanique.

Contenu

- Rappels et compléments sur les espaces vectoriels normés.
- Espaces de Hilbert, projection orthogonale, base hilbertienne,
- Théorème de Riesz-Fréchet, Théorème de Lax-Milgram
- Éléments sur les distributions. Transformation de Fourier.
- Espace L^2 . Espaces de Sobolev H^m .
- Traces et formules de Green.
- Inégalités de Poincaré et de Poincaré-Wirtinger.
- Exemples d'équations aux dérivées partielles. Equation de Poisson. Solution fondamentale.
- Equations d'élasticité linéaire (stationnaires). Inégalité de Korn.

Bibliographie

- Pierre-Arnaud Raviart & Jean-Marie Thomas : Introduction à l'analyse numérique des équations aux dérivées partielles, Dunod, 1998.
- Haïm Brézis, Analyse fonctionnelle, Dunod, 1983.
- Lawrence C. Evans, Partial differential equations, Graduate Studies in Mathematics, Vol. 19, AMS.
- Laurent Schwartz, Méthodes mathématiques pour les sciences physiques, Hermann, 1961.

Optimisation

Tutelle: Département de Mathématiques, UVSQ

Volume horaire: CM: 24h TD: 24h

ECTS: 6

Semestre: 1

Caractère: obligatoire

Intervenants: Tahar Z. Boulmezaoud et Laurent Dumas

Lieu: UVSQ

Parcours: Modélisation, Simulation, MMM

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Fonctions à plusieurs variables, notions de calcul différentiel.

Description

De très nombreux problèmes en industrie, en physique et en économie consistent en la minimisation (ou la maximisation) d'une fonction objective. Ce cours vise à apporter quelques outils théoriques et numériques pour la résolution de ces problèmes.

La première partie du cours porte sur des résultats généraux concernant l'optimisation avec ou sans contraintes. La seconde partie est dédiée à la présentation de méthodes numériques, déterministes ou non, pour approcher en pratique les extremums. Le cours pourra comporter une implémentation sur machine de l'une ou plusieurs de ces méthodes.

Contenu

- Introduction. Exemples.
- Convexité : ensembles convexes, fonctions convexes, propriétés.
- Optimisation sans contraintes : conditions d'optimalité d'ordres 1 et 2.
- Optimisation avec contraintes : Théorème de Karush-Kuhn-Tucker, multiplicateurs de Lagrange. Cas d'un programme convexe.
- Programmation linéaire. Méthode du simplexe.
- Calcul de variations
 - Exemples
 - Conditions d'optimalité avec extrémités fixes. Equations d'Euler-Lagrange.
 - Cas d'extrémités libres. Conditions de transversalité.
- Méthodes numériques : méthodes de descente (de gradient, de quasi-newton,...etc), méthodes stochastiques (réduit simulé, algorithmes génétiques,...etc.).

Bibliographie

- Ph. G. Ciarlet, Introduction à l'analyse numérique matricielle et Optimisation, Masson, 1988.
- J. F. Bonnans, Optimisation continue : cours et exercices, Dunod, 2006.
- H. B. Hiriart-Urruty and C. Lemaréchal, Convex analysis and minimization algorithms, Vol. I, II, Springer-Verlag, 1993.

Méthodes numériques

Tutelle: Département de physique, UVSQ

Volume horaire: CM: 13.5h TD: 7.5h TP: 6h

3 Semestre: 1

Lieu: Université de Versailles Saint-Quentin-en-Yvelines

Caractère: optionnel (en MINT)

Intervenants: Stéphanie Basseville

Parcours: Modélisation, Simulation, MMM

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Cours d'analyse numérique de licence de mécanique ou UE équivalentes. Notions de programmation.

Description

La simulation numérique a pris une place essentielle dans la majorité des domaines scientifiques, et en particulier dans celui de la mécanique, et sa maîtrise est devenue incontournable dans une formation axée autour des sciences de l'ingénieur et de la recherche. Plus précisément, ce cours apportera aux étudiants les connaissances de base, nécessaires au traitement numérique des équations aux dérivées partielles issues de la mécanique des milieux continus et introduira les principales méthodes permettant de résoudre ces équations, principalement les méthodes de différences, volumes et éléments finis.

Contenu

- rappels (éventuel) sur les outils numériques de base
- Présentation, classification et analyse d'équations aux dérivées partielles modèles, issues de la physique et/ou de la mécanique des milieux continus.
- Introduction des différentes méthodes numériques de résolution des équations aux dérivées partielles et éléments d'analyse pour caractériser ces méthodes (par exemple consistance, stabilité, convergence. . .) :
 - Méthode des différences finies
 - Méthode des volumes finis
 - Méthode des éléments finis.
- Le cours sera accompagné de travaux dirigés et de séances de TP. Ces dernières seront l'occasion de coder les méthodes numériques introduites pour les simulations numériques de quelques problèmes modèles.

Bibliographie

- R. Théodor, Initiation à l'analyse numérique, CNAM cours A, Masson, 1994.
- G. Allaire, Analyse Numérique et Optimisation, Editions de l'Ecole Polytechnique, 2012.
- Quarteroni, Numerical Models For Differential Problems, Springer Verlag, 2012.

Mécanique des Milieux Continus - Fluides

Tutelle: Département de physique, UVSQ
Volume horaire: CM: 15h TD: 12h
ECTS: 3
Semestre: 1
Lieu: Université de Versailles Saint-Quentin-en-Yvelines
Caractère: optionnel (en MINT)
Intervenants: Mireille Tixier
Parcours: Modélisation, Simulation, MMM
Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis:

Contenu

- Equations de conservation : Conservation de la masse, de la quantité de mouvement et de l'énergie ; expression du second principe de la thermodynamique.
- Lois de comportement : Loi d'état, loi de Fourier, loi rhéologique ; tenseur des contraintes ; fluides parfaits, newtoniens et non newtoniens, loi de Herschel-Bulkley ;
- Conditions aux limites : Conditions aux limites sur les champs de vitesse, contrainte et température ; tension de surface, loi de Laplace ;
- Classification des écoulements : Nombres sans dimension ; phénomènes de transport dans un fluide en écoulement ;
- Analyse dimensionnelle : Théorème de Vaschy-Buckingham ; similitudes ; solutions semblables ;
- Suspensions, milieux poreux Notions sur les suspensions et les milieux poreux ; loi de Darcy ;
- Applications : Couches limites ; propriétés de l'équation de Stokes ; écoulements parallèles et quasi-parallèles, lubrification ; écoulement compressible dans une tuyère.

Bibliographie

- E. Guyon, J.P. Hulin, L. Petit : Ce que disent les fluides. Editions Belin, Paris, 2011
- L. Landau, E. Lifschitz : Mécanique des fluides. MIR, Moscou, 1971
- S. Candel : Mécanique des fluides : cours. Dunod, Paris, 2001
- P. Chassaing : Mécanique des fluides : éléments d'un premier parcours. Cépaduès ed, Toulouse, 1997.

Mécanique des Milieux Continus - Solides

Tutelle: Département de physique, UVSQ
Volume horaire: CM: 15h TD: 12h
ECTS: 3
Semestre: 1
Lieu: Université de Versailles Saint-Quentin-en-Yvelines
Caractère: optionnel (en MINT)
Intervenants: Paolo Vannucci
Parcours: Modélisation, Simulation, MMM
Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Calcul Intégral et Théorie de la Mesure ; Probabilités (cours L3)

Description

Ce cours est une introduction aux notions fondamentales de la mécanique des milieux solides élastiques. Il constitue une étape préliminaire pour les développements qui sont fait dans d'autres modules concernant la modélisation des solides et des structures.

Contenu

- Analyse de la déformation :
Gradient et mesures de la déformation ; linéarisation : le tenseur des déformations infinitésimales.
- Analyse de la contrainte :
bilan mécanique, équation d'équilibre, tenseur de la contrainte de Cauchy, contraintes principales, états de contrainte particuliers.
- Lois de comportement :
objectivité, loi de Hooke, équations de Lamé.
- Résolution des problèmes d'élastostatique :
approche semi-inverse, cas notables.
- Poutres élastiques :
poutre rectiligne à la Euler-Bernoulli ; solution de Saint-Venant ; poutres curvilignes.

Bibliographie

- A. E. H. Love : *A treatise on the mathematical theory of elasticity*. Fourth edition. Dover, 1944.
- I. S. Sokolnikoff : *Mathematical theory of elasticity*. McGraw-Hill, 1946.
- S. Timoshenko, J. N. Goodier : *Theory of elasticity*. Second edition. McGraw-Hill, 1951.

- P. Germain, P. Muller : *Introduction à la mécanique des milieux continus*. Masson, 1980.
- M. E. Gurtin : *An introduction to continuum mechanics*. Academic Press, 1981.
- F. Hartmann : *The mathematical foundation of structural mechanics*. Springer, 1985.
- J. R. Barber : *Elasticity*. Kluwer Academic Publishers, 1992.
- P. Podio-Guidugli : *A primer in elasticity*. Journal of Elasticity, v. 58 : 1-104, 2000.
- W. S. Slaughter : *The linearized theory of elasticity*, Birkhäuser, 2002.
- P. M. Mariano, L. Galano : *Fundamentals of the Mechanics of Solids*, Birkhäuser, 2016.

Ondes et acoustique dans les fluides

Tutelle: Département de physique, UVSQ

Volume horaire: CM: 15h TD: 12h

ECTS: 3

Semestre: 1

Lieu: Université de Versailles Saint-Quentin-en-Yvelines

Caractère: optionnel (en MINT)

Intervenants: Stéphanie Basseville et Mireille Tixier

Parcours: Modélisation, Simulation, MMM

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis:

Contenu

- Notions de bases sur les ondes dans les fluides : Notions de bases sur les ondes dans les fluides : équation d'onde, relation de dispersion, vitesses de phase et de groupe, énergie; réflexion et transmission sur une interface; diffraction;
- Acoustique linéaire : Ondes planes progressives harmoniques; définition du dB; pondération A;
- Résonateurs de Helmholtz et applications
- Ondes de surface gravito-capillaires (théorie d'Airy)
- Etude de quelques phénomènes non linéaires (ondes solitaires, mascarets...)
- Ondes de choc
- Coup de bélier

Bibliographie

- A. Chaigne : Ondes acoustiques. Editions de l'école Polytechnique, Palaiseau, 2001
- L. Petit, E. Guyon, J.P. Hulin : Hydrodynamique physique. InterEditions, Paris, 1991
- V. Guinot : Ondes en mécanique des fluides. Lavoisier, Paris, 2006

Analyse des équations aux dérivées partielles

Tutelle: Département de Mathématiques, UVSQ

Volume horaire: CM: 24h TD: 24h

ECTS: 6

Semestre: 2

Caractère: obligatoire

Intervenants: Emmanuelle Crépeau

Lieu: UVSQ

Parcours: Modélisation, Simulation

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: Calcul intégral, calcul différentiel, notions de distributions, éléments de topologie

Description

Ce cours a comme ambition d'introduire quelques outils d'analyse des équations aux dérivées partielles. Il commencera par quelques notions et résultats de base en analyse fonctionnelle et concernant les espaces de Sobolev. On abordera ensuite l'étude de quelques équations fondamentales telles que l'équation des ondes et l'équation de Schrödinger.

Contenu

- Éléments d'Analyse fonctionnelle
- Compléments sur les espaces de Banach.
- Formes linéaires, dualité.
- Applications linéaires continues
- Théorème de Hahn-Banach. Théorème de l'application ouverte, théorème du graphe fermé.
- Convergences faible et faible \star .
- Espaces L^p et espaces de Sobolev. Formulation variationnelle.
- Equation des ondes.
- Equation de Schrödinger.

Bibliographie

- Haïm Brézis, Analyse fonctionnelle, Dunod, 1983.
- Claude Zuily, Distributions et équations aux dérivées partielles, Hermann, 2001.
- Lawrence C. Evans, Partial differential equations, Graduate Studies in Mathematics, Vol. 19, AMS.

Méthodes numériques avancées et programmation

Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 2
Caractère: obligatoire
Intervenants: Christophe Chalons et Pierre Gabriel
Lieu: UVSQ
Parcours: Modélisation, Simulation, MMM
Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: notions sur les distributions et les espaces de Sobolev (suggérés mais non obligatoires)

Description

L'objectif de ce cours est de proposer une introduction à l'analyse mathématique et à l'approximation numérique des solutions de certaines équations aux dérivées partielles (EDP). Ces équations interviennent de manière récurrente dans de nombreuses applications, qu'il s'agisse d'ingénierie mécanique et physique (aéronautique, nucléaire, ingénierie pétrolière, automobile...) ou de finance, d'économie, de chimie...etc.

Nous présenterons des résultats importants d'analyse théorique des EDP ainsi que les trois grandes classes de méthodes numériques associées (méthode des éléments finis, méthode des volumes finis et méthode des différences finies).

L'objectif de ce cours est également d'apporter aux élèves une première expertise numérique pour la résolution des équations aux dérivées partielles en leur proposant de programmer, de tester et de comparer différentes méthodes sur des problèmes concrets.

Contenu

- EDP elliptiques
 - Rappels sur les distributions et les espaces de Sobolev
 - Formulation variationnelle
 - Théorème de Lax-Milgram
 - Etude de la méthode des éléments finis en 1D et en 2D
- EDP hyperboliques
 - Equation de transport et équation des ondes
 - Introduction à la méthode des volumes finis
- EDP paraboliques
 - Equation de la chaleur
 - Introduction à la méthode des différences finies

Bibliographie

- 1 Pierre-Arnaud Raviart, Jean-Marie Thomas : Introduction à l'analyse numérique des équations aux dérivées partielles, éditions Dunod 1998.
- 2 Brigitte Lucquin : Equations aux dérivées partielles et leurs approximations, Ellipses, 2004.
- 3 E. Godlewski et P.-A. Raviart : Hyperbolic systems of conservation laws, Ellipses 1991.
- 4 Lawrence C. Evans : Partial differential equations, Graduate Studies in Mathematics, Vol. 19, AMS.
- 5 C. Strikwerda : Finite Difference Schemes and Partial Differential Equations, SIAM 2004.
- 6 L. Hörmander : Lectures on Nonlinear Hyperbolic Differential Equations, Springer 1997.
- 7 F. Lagoutière : Polycopié de cours sur les Equations aux dérivées partielles et leurs approximations, Université Paris-Sud.

Stabilité et bifurcation

Tutelle: Département de Mathématiques, UVSQ

Volume horaire: CM: 12h TD: 12h

ECTS: 3

Semestre: 2

Caractère: obligatoire

Intervenants: Paolo Vannucci

Lieu: UVSQ

Parcours: Modélisation, Simulation, MMM

Evaluation: voir "Modalités de contrôle des connaissances".

Pré-requis: éléments de base de calcul différentiel, algèbre tensorielle, calcul des variations, dynamique.

Description

La modélisation de très nombreux problèmes en physique, en mécanique, en biologie et en industrie conduisent à l'étude de l'évolution de solutions d'équations différentielles. Le but de ce cours est d'apporter quelques outils et techniques mathématiques modernes pour étudier les propriétés qualitatives de telles solutions. Ces propriétés concernent la dépendance par rapport aux conditions initiales, la stabilité près des points d'équilibre et la sensibilité par rapport aux paramètres. Le cours sera illustré par de nombreux exemples issus de modèles mécaniques, physiques ou biologiques.

Contenu

- Introduction et rappels :
Des exemples de stabilité et bifurcation : stabilité des orbites dans un champ de potentiel $1/r^2$; poutre rigide avec rotule élastique ; différentes approches. Notion de stabilité au sens de Hadamard. Bref historique. Rappels de notions de base : équations de Lagrange, conditions d'équilibre.
- Stabilité :
Espace des phases : trajectoires, classification des points d'équilibre. Notions de stabilité, attracteurs. Equation de Duffing, oscillateur de Van der Pol.
- Bifurcation :
Notions de base. Diagramme de branching. Points limites et points de bifurcation. Interprétations géométrique et algébrique. Snap-through, types de bifurcation. Modes de bifurcation.
- Bifurcation de Hopf :
Définition. Bifurcation de Hopf et stabilité. Equation de Lorenz. Types de branching.
- Stabilité à la Liapunov :
Définition. Théorème de stabilité de Liapounov. Méthode directe de Liapounov. Stabilité asymptotique.
- Stabilité de l'équilibre de systèmes conservatifs :
Equilibre comme point stationnaire du potentiel. Théorème de Lagrange-Dirichlet.

- Coefficients de stabilité de Poincaré. Effet des perturbations.
- Bifurcation et stabilité de l'équilibre de poutres élastiques :
La poutre d'Euler. Stabilité flexo-torsionnelle de Prandtl. Stabilité torsio-flexionnelle.
 - Approches énergétiques :
Principes généraux. Quotient de Rayleigh. Méthode de Ritz. Méthode de Galerkin.

Bibliographie

- S. Timoshenko, S. Gere : *Theory of elastic stability*. McGraw-Hill, 1961.
- N. Chetaev : *The stability of motion*. Pergamon Press, 1961.
- J.M.T. Thompson, G.W.Hunt : *A general theory of elastic stability*. Wiley, 1973.
- J.M.T. Thompson, G.W.Hunt : *Elastic instability phenomena*. Wiley, 1984.
- R. Seidel : *From equilibrium to chaos*. Elsevier, 1988.
- M. Pignataro, N. Rizzi, A. Luongo : *Stability, bifurcation and post critical behavior of elastic structures*. Elsevier, 1991.
- N. Q. Son : *Stabilité des structures élastiques*. Springer, 1995.

Corps professoral

Martin Andler

Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0)1 39 25 46 30
Mél : martin.andler@uvsq.fr
Web : <http://lmv.math.cnrs.fr/annuaire/andler-martin/>

Cours en master 1 :

- Algèbre 1

Stephanie Basseville

Adresse : Département des sciences physiques
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0) 1 39 25 30 26
Mél : stephanie.basseville@uvsq.fr
Web : <http://www.uvsq.fr>

Cours en master 1 :

- Ondes et acoustique dans les fluides
- Méthodes numériques

Tahar Z. Boulmezaoud

Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0)1 39 25 36 23
Mél : tahar.boulmezaoud@uvsq.fr
Web :

Cours en master 1 :

- Optimisation
- Mathématiques assistées par ordinateur

Christophe Chalons

Adresse : Laboratoire de Mathématiques de Versailles

Université de Versailles Saint-Quentin-en-Yvelines

45, Avenue des Etats-Unis

78035 Versailles Cedex.

Tél. : ++ 33 (0)1 39 25 30 68

Mél : christophe.chalons@uvsq.fr

Web : <http://chalons.perso.math.cnrs.fr/>

Cours en master 1 :

— Méthodes numériques avancées et programmation

Vincent Cossart

Adresse : Laboratoire de Mathématiques de Versailles

Université de Versailles Saint-Quentin-en-Yvelines

45, Avenue des Etats-Unis

78035 Versailles Cedex.

Tél. : ++ 33 (0)1 39 25 46 48

Mél : vincent.cossart@uvsq.fr

Web : <http://lmv.math.cnrs.fr/annuaire/vincent-cossart/>

Cours en master 1 :

— Algèbre

Emmanuelle Crépeau

Adresse : Laboratoire de Mathématiques de Versailles

Université de Versailles Saint-Quentin-en-Yvelines

45, Avenue des Etats-Unis

78035 Versailles Cedex.

Tél. : ++ 33 (0)1 39 25 30 63

Mél : emmanuelle.crepeau@uvsq.fr

Web : <http://lmv.math.cnrs.fr/annuaire/emmanuelle-crepeau/>

Cours en master 1 :

— Analyse des équations aux dérivées partielles

Luca De Feo

Adresse : PRISM

Université de Versailles Saint-Quentin-en-Yvelines

45, Avenue des Etats-Unis

78035 Versailles Cedex.

Tél. : ++ 33 (0) 1 39 25 40 35

Mél : luca.de-feo@uvsq.fr

Web : <http://defeo.lu/>

Cours en master 1 :

— Analyse d'algorithmes et Programmation

Alexis Devulder

Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0)1 39 25 46 28
Mél : alexis.devulder@uvsq.fr
Web : <http://lmv.math.cnrs.fr/annuaire/devulder-alexis/>

Cours en master 1 :

— Probabilités

Catherine Donati-Martin

Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0)1 39 25 30 61
Mél : @uvsq.fr
Web : <http://lmv.math.cnrs.fr/annuaire/donati-martin-catherine/>

Cours en master 1 :

— Probabilités

Laurent Dumas

Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0)1 39 25 30 66
Mél : laurent.dumas@uvsq.fr
Web : <http://dumas.perso.math.cnrs.fr/>

Cours en master 1 :

— Optimisation

Pierre Gabriel

Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0)1 39 25 30 64
Mél : pierre.gabriel@uvsq.fr
Web : <http://pgabriel.perso.math.cnrs.fr/>

Cours en master 1 :

— Introduction à l'analyse fonctionnelle et aux équations aux dérivées partielles
— Méthodes numériques avancées et programmation

Louis Goubin

Adresse : UVSQ - Laboratoire PRISM
Batiment Descartes
45 Avenue des Etats Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0)1 39 25 43 29
Mél : louis.goubin@uvsq.fr
Web : <http://www.prism.uvsq.fr/users/logo>
Cours en master 1 :

- Cryptographie
- Calcul sécurisé

Jean-Baptiste Goyard

Adresse : Institut d'Etudes Culturelles et Internationales
Université de Versailles Saint-Quentin-en-Yvelines
Bâtiment E
45, avenue des Etats-unis,
78000 Versailles.
Tél. : ++ 33 (0)1 39 25 42 50
Mél : jean-baptiste.goyard@uvsq.fr
Web : <http://www.ieci.uvsq.fr/>
Cours en master 1 :

- Anglais

Mohamed Krir

Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0)1 39 25 46 23
Mél : mohamed.krir@uvsq.fr
Web : <http://lmv.math.cnrs.fr/annuaire/krir-mohamed/>
Cours en master 1 :

- Introduction aux courbes elliptiques

Florian Leniaud

Adresse : Institut d'Etudes Culturelles et Internationales

Université de Versailles Saint-Quentin-en-Yvelines

Bâtiment E

45, avenue des Etats-unis,

78000 Versailles.

Tél. : ++ 33 (0)1 39 25 42 50

Mél : florian.leniaud@uvsq.fr

Web : <http://www.ieci.uvsq.fr/>

Cours en master 1 :

— Anglais

Vahagn Nersesyan

Adresse : Laboratoire de Mathématiques de Versailles

Université de Versailles Saint-Quentin-en-Yvelines

45, Avenue des Etats-Unis

78035 Versailles Cedex.

Tél. : ++ 33 (0)1 39 25 46 27

Mél : vahagn.nersesyan@uvsq.fr

Web : <http://nersesyan.disque.math.cnrs.fr>

Cours en master 1 :

— Introduction à l'analyse fonctionnelle et aux équations aux dérivées partielles

Alban Quadrat

Adresse : Inria Saclay - Île-de-France,

Projet DISCO, L2S,

Supélec, 3 rue Joliot Curie,

91192 Gif-sur-Yvette.

Tél. : ++ 33 (0)1 69 85 17 75

Mél : alban.quadrat@inria.fr

Web : <http://pages.saclay.inria.fr/alban.quadrat/>

Cours en master 1 :

— Automatique et Algèbre

Michael Quisquater

Adresse : UVSQ - Laboratoire PRISM

Batiment Descartes

3ème étage

Bureau 306B

45 Avenue des Etats Unis

78000 Versailles.

Tél. : ++ 33 (0)1 39 25 40 47

Mél : michael.quisquater@prism.uvsq.fr

Web : <http://www.prism.uvsq.fr/~mquis>

Cours en master 1 :

— Théorie de l'information

Vincent Sécherre

Adresse : Laboratoire de Mathématiques de Versailles

Université de Versailles Saint-Quentin-en-Yvelines

45, Avenue des Etats-Unis

78035 Versailles Cedex.

Tél. : ++ 33 (0)1 39 25 36 20

Mél : vincent.secherre@uvsq.fr

Web : <http://lmv.math.cnrs.fr/annuaire/vincent-secherre/>

Cours en master 1 :

— Théorie des nombres et Cryptographie

Mireille Tixier

Adresse : Département des sciences physiques

Université de Versailles Saint-Quentin-en-Yvelines

45, Avenue des Etats-Unis

78035 Versailles Cedex.

Tél. : ++ 33 (0) 1 39 25 45 19

Mél : mireille.tixier@uvsq.fr

Web : <http://www.uvsq.fr>

Cours en master 1 :

— Mécanique des milieux continus – Fluides

— Ondes et acoustique dans les fluides

Paolo Vannucci

Adresse : Laboratoire de Mathématiques de Versailles

45 Avenue des Etats Unis

78000 Versailles.

Tél. : ++ 33 (0)1 39 25 42 18

Mél : paolo.vannucci@uvsq.fr

Web : <https://sites.google.com/site/paolovannucciwebsite/home>

Cours en master 1 :

— Stabilité et bifurcation