Année 2018/2019

Métaplans d'Algèbre pour l'Agrégation

Pierre Le Barbenchon

ENS Rennes

TABLE DES MATIÈRES

CHAPITRE 1

PLANS DE LEÇONS

1.1 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

— Il 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 !

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

1.2 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 [8, p.49]

2) Espace affine

Angles orientés [36]

3) Isométries

Isométries du cube et du tétraèdre

Développements :

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

Références :

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

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

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

♥ - [36] 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 [37]
- 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 [37]
  1) Définitions
     Ordre
  2) Lagrange
     $|G| = [G : H]|H|$
  3) Actions de groupe

II - Groupes abéliens [11]
  1) Groupe cyclique

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

2) Théorème de structure

existence et unicité

III - Groupes non abéliens

1) Groupe symétrique [30]

Automorphismes de $\mathfrak{S}_n$

2) Géométrie

Groupes diédraux [37]

Isométries affines [8]

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 :

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

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

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

♥♥ - [8] 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 [6] [30]

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 $\mathfrak{A}_n$ [30]

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 [22]

Forme n-linéaire alternée

Définition du déterminant

Formule du déterminant

2) Action de groupes [8]

Groupe des isométries

Isométries du cube et du tétraèdre

Nombre de coloriages du cube

3) Polynomes symétriques [22]

Définition

Développements :

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

Références :

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

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

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

♥♥ - [22] Xavier GOURDON, *Algèbre*

♥♥ - [8] 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 [30] [24]
- 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 $SL(E)$ [30]
- 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 [8]

Dénombrement de $GL_n(\mathbb{F}_q)$

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

Isomorphismes exceptionnels [8, p.49]

IV - Groupe orthogonal [30]

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 :

♥♥ - [22] Xavier GOURDON, *Algèbre*

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

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

♥♥♥ - [8] 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 [30] [11]

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

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 [37]

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 [37] [6]

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 [30]

$SL(E)$ 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 :

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

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

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

♥♥♥ - [6] 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 [32]

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 [30]

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 [32] [27]

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 $\varphi(n)$ [30]

II - Arithmétique [27]

1) Résidus quadratiques [27]

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 [27]

Petit théorème de Fermat

Nombre de Carmichael

Thrm de Wilson

Système RSA et chiffrement

Primalité des nombres de Mersenne

Algorithme de Lehmer Lucas [34]

3) Résolution d'équations [27]

Système de congruence

Résolution d'équation

Réduction modulaire

Théorème de Fermat modulaire

Développements :

- Primalité des nombres de Mersenne
- Théorème de Fermat modulaire

Références :

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

♥♥♥ - [22] Xavier GOURDON, *Algèbre*

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

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

♥♥♥ - [34] 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 [22]

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 [18]

lien avec la fonction ζ

$\pi(x) \sim \frac{x}{\log x}$ [15]

II - Corps finis [30] [15]
  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 [34]
    Petit théorème de Fermat
    Def Nombres de Carmichael
  2) Nombres de Fermat [11] [34]
    Def
    Critère de primalité
  3) Nombres de Mersenne [34]
    Primalité des nombres de Mersenne
    Algo de Lehmer Lucas

Développements :

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

Références :

♥♥♥ - [26] Jean-Pierre LAMOITIER, *Arithmétique Classique*
♥♥ - [30] Daniel PERRIN, *Cours d'Algèbre*
♥♥ - [22] Xavier GOURDON, *Algèbre*
♥♥♥♥ - [15] Daniel DUVERNEY, *Théorie des Nombres*
♥♥ - [11] François COMBES, *Algèbre et Géométrie*
♥♥ - [18] Serge FRANCINOU, Hervé GIANELLA et Serge NICOLAS, *Oraux X-ENS, Analyse 1*
♥♥♥ - [34] 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 $\mathbb{F}_2[X]/(X^3+X+1)$ 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 [30]
- Caractéristique
- Morphisme de Frobenius
- Corps de rupture
- Inclusions des corps finis

II - Etude sur les corps finis

1) Dénombrement et géométrie [8]
- 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 $\mathbb{F}_q$ [30]
- 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 $\mathbb{F}_q$ [30]

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 [34]

But : Trouver des nombres premiers très très grands

Primalité des nombres de Mersenne

Algorithme de Lehmer Lucas

Explication système RSA [27]

Développements :

- Primalité des nombres de Mersenne
- Loi de réciprocité quadratique

Références :

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

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

♥♥ - [22] Xavier GOURDON, *Algèbre*

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

♥♥♥ - [34] 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 [25]
- 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 $n \geqslant 3$ (Andrew 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 [25]), 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 $\mathbb{Z}$ [26]

$ax + by = c$

Bézout

Algorithme d'Euclide

Congruence

Equations diophantiennes linéaires

2) Equations linéaires modulaire [27]

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 [25]

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

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 $\mathbb{F}_q$ [8] [30]

$x^2 + py = q$

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 :

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

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

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

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

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

♥♥♥ - [8] 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 [22]
    Définition de polynômes
    Division euclidienne
  2) Critères d'irréductibilité [30]
    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 :

♥♥ - [30] Daniel PERRIN, *Cours d'Algèbre*
♥♥ - [22] Xavier GOURDON, *Algèbre*
♥♥♥ - [35] Ian STEWART et David TALL, *Algebraic Number Theory*
♥♥♥ - [7] 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 [24]

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 [7]

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 :

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

♥♥♥ - [22] Xavier GOURDON, *Algèbre*

♥ - [7] 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 [23]
   Théorème
   Exemple
2) Inégalité d'Hadamard
   Théorème des extrema liés
3) Volume [24]
4) Formes quadratiques [13]
   Discriminant

Développements :

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

Références :

♥♥♥♥ - [24] Joseph GRIFONE, *Algèbre Linéaire*
♥♥♥♥ - [22] Xavier GOURDON, *Algèbre*
♥♥ - [23] Xavier GOURDON, *Analyse*
♥♥ - [13] 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 :

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

♥♥♥ - [22] Xavier GOURDON, *Algèbre*

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

♥♥♥ - [10] 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 [22]

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 [33]

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 [3]

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 [19]

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 [20]

III - Applications aux équations différentielles [14] [4]

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 :

♥♥♥♥ - [22] Xavier GOURDON, *Algèbre*

♥♥♥ - [23] Xavier GOURDON, *Analyse*

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

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

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

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

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

♥♥ - [20] 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 :

♥♥♥♥ - [22] Xavier GOURDON, *Algèbre*

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

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

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

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

♥♥ - [1] 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 [24]

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 :

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

♥♥♥ - [22] Xavier GOURDON, *Algèbre*

♥♥ - [23] 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 **??**)

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

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

Développements :

- Méthode QR
- Méthode de gradient à pas optimal

Références :

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

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

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

♥♥♥ - [31] 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 :

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

♥♥ - [8] 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 [36]

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 :

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

♥♥♥♥ - [2] Michèle AUDIN, *Géométrie*

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

♥♥♥ - [5] 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 [8]
  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 [36] [5]
     Définition
     Action
  2) Isométries affines [8]
     Définition
     Isométries du cube et du tétraèdre
     Groupe icosaèdre

III - Géométrie projective [5]
  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 :

♥♥♥♥ - [2] Michèle AUDIN, *Géométrie*

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

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

♥♥♥ - [8] 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 [17] [12]

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 [30]
Indicatrice d'Euler
2) Séries formelles [21]
Nombres de Catalan
Nombres de Bell

III - Action de groupes
1) Coloriages
Théorème de Fermat modulaire [28]
2) Action de groupes [37]
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 [8]

Développements :

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

Références :

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

BIBLIOGRAPHIE

[1] Grégoire ALLAIRE and Sidi Mahmoud KABER. *Algèbre linéaire numérique*. Ellipses, 2002.

[2] Michèle AUDIN. *Géométrie*. EDP Sciences, 2006.

[3] Vincent BECK, Jérôme MALICK, and Gabriel PEYRÉ. *Objectif Agrégation*. H & K, 2005.

[4] Florent BERTHELIN. *Equations Différentielles*. Cassini, 2017.

[5] Pascal BOYER. *Algèbre et Géométries*. Calvage et Mounet, 2015.

[6] Josette CALAIS. *Éléments de Théorie des Groupes*. PUF, 1998.

[7] Josette CALAIS. *Extensions de Corps, Théorie de Galois*. Ellipses, 2006.

[8] Philippe CALDERO and Jerôme GERMONI. *Nouvelles Histoires Hédonistes de Groupes et de Géométries - Tome 2*. Calvage et Mounet, 2018.

[9] Philippe CIARLET. *Introduction à l'analyse numérique matricielle et à l'optimisation*. Dunod, 2006.

[10] Michel COGNET. *Algèbre Linéaire*. Bréal, 2000.

[11] François COMBES. *Algèbre et Géométrie*. Bréal, 1998.

[12] Jean DE BIASI. *Mathématiques pour le CAPES et l'Agrégation interne*. Ellipses, 2004.

[13] Clément DE SEGUINS PAZZIS. *Invitations aux formes quadratiques*. Calvage et Mounet, 2011.

[14] Jean-Pierre DEMAILLY. *Analyse numérique et équations différentielles*. EDP Sciences, 2016.

[15] Daniel DUVERNEY. *Théorie des Nombres*. Dunod, 2007.

[16] Jean-Denis EIDEN. *Géométrie analytique classique*. Calvage et Mounet, 2009.

[17] Dominique FOATA, Jacques FRANCHI, and Aimé FUCHS. *Calcul des probabilités*. Dunod, 2012.

[18] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Analyse 1*. Cassini, 2003.

[19] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Algèbre 2*. Cassini, 2009.

[20] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Algèbre 3*. Cassini, 2013.

[21] Serge FRANCINOU, Hervé GIANELLA, and Serge NICOLAS. *Oraux X-ENS, Algèbre 1*. Cassini, 2018.

[22] Xavier GOURDON. *Algèbre*. Ellipses, 2008.

[23] Xavier GOURDON. *Analyse*. Ellipses, 2008.

[24] Joseph GRIFONE. *Algèbre Linéaire*. Cépaduès, 2011.

[25] Marc HINDRY. *Arithmétique*. Calvage et Mounet, 2008.

[26] Jean-Pierre LAMOITIER. *Arithmétique Classique*. Ellipses, 2012.

[27] Jean-Pierre LAMOITIER. *Arithmétique Modulaire*. Ellipses, 2012.

[28] Bruce LANDMAN and Aaron ROBERTSON. *Ramsey Theory on the Integers*. AMS, 2003.

[29] Roger MANSUY and Rached MNEIMNÉ. *Algèbre Linéaire, Réduction des Endomorphismes*. Vuibert, 2016.

[30] Daniel PERRIN. *Cours d'Algèbre*. Ellipses, 1996.

[31] Alfio QUARTERONI, Riccardo SACCO, and Fausto SALERI. *Méthodes Numériques*. Springer, 2007.

[32] Jean-Jacques RISLER and Pascal BOYER. *Algèbre pour la licence 3 : Groupes, Anneaux, Corps*. Dunod, 2006.

[33] François ROUVIÈRE. *Petit guide de calcul différentiel*. Cassini, 2009.

[34] Philippe SAUX-PICART and Éric RANNOU. *Cours de calcul formel, Corps finis, Systèmes polynomiaux, applications*. Ellipses, 2002.

[35] Ian STEWART and David TALL. *Algebraic Number Theory*. Chapman and Hall, 2015.

[36] Patrice TAUVEL. *Géométrie*. Dunod, 2005.

[37] Félix ULMER. *Théorie des Groupes*. Ellipses, 2012.