Université de Rennes
École Normale Supérieure
2025

Retours d'oraux

Agrégation 2025

Kylian Prigent

école
normale
supérieure
rennes

Table des matières

I Oral d'algèbre

I.A Couplage

— 156 Endomorphismes trigonalisables. Endomorphismes nilpotents.
— 181 Convexité dans $\mathbb{R}^n$.

Je choisi la leçon 156, l'autre était mon impasse.

I.B Note :

10

I.C Plan

J'introduit la leçon en disant qu'en algèbre et en mathématiques plus généralement on souhaite rendre les éléments les plus simples possibles pour les étudier, leur donner des formes systématiques et que sous condition d'extension de corps par exemple il est possible de se ramener à quelque chose de plus simple.

Mon plan se décomposait avec en 3 parties :

1. La 1^e concernant et les endomorphismes trigonalisables. Je commence avec une sous partie sur les sous-espace stables avec notamment le lemme des noyaux les noyers itérés qui amorce la sous-partie autour des endomorphismes cycliques de la partie suivante. En deuxième sous-partie je parle de la trigonalisation, de la trigonalisation automatique dans les corps algébriquement clos, je parle aussi de cotrigonalisation et du fait que la condition de commutation est suffisante non nécessaire.
2. Ensuite 2^e partie sur les endomorphismes nilpotents avec une première sous-partie autour la définition des des nilpotents la caractérisation en terme de polynômes caractéristiques, du polynôme minimale. J'ai aussi mis le dénombrement des matrices nulle nilpotente dans dans $\mathcal{M}_2(\mathbb{F}_q)$. Après je parlais d'endomorphismes cycliques, de la réduction de Frobenius et donc de la caractérisation des classes de similitude des nilpotents par la réduction de Frobenius j'ai décidé de ne pas proposer la réduction de Jordan dans le plan car c'est vraiment la même chose que Frobenius, d'ailleurs pendant les questions après que j'avais une réduction de Frobenius de nilpotents je parlais souvent de bloc de Jordan au lieu de matrices compagnons.
3. Enfin 3^e autour partie de la décomposition de Jordan-Chevalley-Dunford et applications donc première sous partie le théorème de Jordan-Chevalley, après avoir écrit la définition d'un corps parfait, des endomorphismes semi-simples, on a pu s'attaquer au théorème, s'en suivait une sous-partie consacrée à l'exponentielle de matrice donc avec les propriétés de base et la définition de l'exponentielle matricielle, propriétés de commutation puis le lemme qui dit que toute matrice unipotente est l'exponentielle d'une matrice nilpotente qui est un polynôme en cette matrice et enfin la surjectivité de $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$. Enfin le plan se concluait avec une 3^e sous partie autour des équations différentielles linéaires (en fait autonomes) avec la solution sous forme d'exponentielle et comme il ne restait pas beaucoup de place je n'ai pas pu parler de la résolvante (son expression, formule de Duhamel) et j'ai fait quelques dessins de stabilité ou non en fonction des valeurs propres dont dans le cadre d'une matrice 2×2 en fonction de la trace et du déterminant (le dessin qui est dans le dans le plan de Tiphaine) et 2 exemples qui se trouvent dans le dans le Meimné-Mansuy.

Globalement tous les résultats provenaient du Mneimné et de objectif agrégation pour les deux premières parties et du cours de Romagny et du Mneimné pour la troisième.

I.D Développement

— Réduction de Jordan-Chevalley-Dunford dans un corps parfait (Romagny).
— Lemme sur les matrices unipotentes et nilpotentes et surjectivité de l'exponentielle (Zavidovique + le lemme vient de la minerve de l'ENS).

Le jury choisit le premier. Tout se passe bien, juste une petite erreur "de vitesse" ou "de stress" que le jury me fait remarquer mais pas gênante car j'avais bien expliqué à l'oral. Comme pour ce développement on s'inspire de la méthode de Newton (idée de Chevalley), dans les notations je fais le parallèle avec

l'analyse (le jury a semblé avoir apprécié).

J'ai eu droit des questions sur Taylor-Lagrange : comment on peut appliquer Taylor-Lagrange dans le théorème (on utilise le fait que l'on a des polynômes et Taylor est exacte sur les polynômes puis on prend les termes qui nous arrange et on factorise le reste). Après autour de l'unicité j'avais eu aussi à savoir pourquoi s et u ($u = s + n$) commutaient et donc j'ai réexpliqué ce que j'avais dit au moment du développement comme quoi en fait le s et le n que je prenais sont construits par l'existence qui est constructive, autre question sur le développement, comment se sert-on de la perfection du corps ? (Je l'utilisait sur les irréductibles dans la décomposition de P, puis pour obtenir que P et premier à P' il faut juste écrire proprement P' en fonction des diviseurs irréductibles de P puis voir ce qui se passerait si un diviseur irréductible de P divisait P'). Après ça j'ai eu le droit une dernière question autour de développement (elle est arrivée à la fin en mode exo mais bon) : $M \in \mathcal{M}_n(\mathbb{R})$ a une décomposition de Jordan dans $\mathbb{C}$, est-ce que les matrices de la décomposition sont réelles ? (oui, il faut prendre le conjugué, vérifier que c'est encore une décomposition de J-C-D que l'on obtient et utiliser l'unicité du développement de JCD).

I.E Questions

J'ai eu beaucoup de questions sur les sous-espèces stables par les endomorphismes trigonalisables donc j'ai parlé d'espaces caractéristiques parce que c'est la plus immédiat et la chose qui m'est venue en premier mais j'avais un peu de mal parfois à voir où il voulait en arriver. Ensuite on a parlé aussi du cas nilpotents, endomorphismes induits demeurent nilpotents (trigo), de la décomposition de Frobenius et comment on peut savoir quel est l'ordre de nilpotence, la dimension du noyau de notre élément en fonction de la décomposition. J'ai répondu instinctivement la taille du plus grand bloc de Jordan, et pour le noyau, au début je ne savais plus vraiment comment il fallait faire donc j'ai donc pris le cas particulier ou l'indice de nilpotence est maximum pour voir que dans ce cas là en fait le noyau a dimension 1 et la réduction de Frobenius nous donne un seul bloc et donc en fait le noyau a pour dimension le nombre de blocs de Jordan.

II Oral d'analyse

II.A Couplage

— 215 Applications différentiables définies sur un ouvert de $\mathbb{R}^n$.
— 250 Transformation de Fourier.

Le couplage m'a bien plu, petite hésitation, je finis par prendre la 215

II.B Note :

15,25

II.C Plan

J'introduit la leçon en disant que dans les petites classes on travaille sur des fonctions d'une variable réelle est qu'il est naturel de se demander ce qu'il se passe quand on a une fonction de plusieurs variables, je parle de l'approximation du premier ordre avec la dérivée et du fait qu'on voudrait retrouver un équivalent en multiD.

Mon plan se décomposait avec en 3 parties :

1. La 1^e concernant différentes notions de dérivabilité. Je parle d'abord de dérivées directionnelles et dérivées partielles avec les implications et les contre-exemples à l'implication avec des exemples de dérivées directionnelles, je justifie de commencer par ces notions car elles sont plus "naturelles" (dérivée suivant x ou y). Ensuite je parle de la différentielle donc la définition avec l'application linéaire, ensuite je parle donc des implications : différentiel entraîne continue et les implications avec exemples et contre exemples entre les différentes notions de dérivation. Je rajoute des dessins pour montrer le lien avec la dimension 1 et l'approximation du premier ordre et je donne la définition de classe $\mathcal{C}^1$. Je conclut cette première partie avec la jacobienne et le fait que la jacobienne (et le jacobien son déterminant) sont utilisés notamment pour faire du changement de variables et le cas particulier du gradient pour une fonction d'une variable réelle, je parle de méthode en applications et enfin je fais une remarque sur la méthode de gradient à pas optimal.
2. Ensuite 2^e partie qui est la généralisation des théorèmes d'une variable réelle au cas multiD, à savoir la linéarité, la dérivation composée avec l'exemple de la norme issue d'un produit scalaire (le cas des formes bilinéaires et du produit scalaire ayant été présenté en première partie), je fais les remarques disant que ces propriétés s'illustrent bien avec les jacobiennes, je parle ensuite de l'inégalité des accroissements finis (lien entre différentielle nulle et être constante) et inégalité de Taylor reste intégral (je n'écrit que celle-ci par peur de manquer de temps et de place) parce que je l'utilise après dans le lemme de Morse.
3. Enfin 3^e qui tourne autour du théorème d'inversion locale avec toujours des dessins. Je commence par définir les $\mathcal{C}^1$-difféomorphisme puis je donne l'énoncé du théorème (avec dessin) et un contre exemple (avec dessin : $x \mapsto x + x^2 \sin(\frac{1}{x})$. J'ajoute ensuite le lemme de Morse comme application du TIL, il a aussi le droit à ses dessins puisqu'il peut permettre de savoir si un point critique est un extremum ou un point selle. Après cela je propose des généralisation du TIL, le TIG et le théorème d'Hadamard-Lévy. Ensuite j'aurais voulu mettre le théorème des fonctions implicites mais je n'ai pas eu le temps est j'ai donc commencé une sous-partie intitulée "quelques applications du TIL" dans laquelle je parle de racines k^e de matrice mais je n'ai pas eu le temps de mettre le TFI.

Beaucoup de livres peuvent être utilisés pour cette leçon, perso j'utilise Rouvière, Gourdon, Objectif agrégation et Benzoni-Gavage pour les définitions et les théorèmes, Rouvière et Objectif agrégation pour les exemples et applications et Bernis[2] pour Hadamard-Lévy, le Hauchecorne développe quelques contre-exemples et je l'ai regardé pour les détails du contre exemple $x, y \mapsto \begin{array}{ll} \frac{y^2}{x} & \text{si } x \neq 0 \\ y & \text{sinon} \end{array}$.

II.D Développement

— Lemme sur les formes quadratiques + lemme de Morse
— Théorème de Hadamard-Lévy (seulement l'implication difficile)

A nouveau le jury choisit le premier développement. Comme avec le stress je parle un peu vite pour combler je parle du fait que le lemme de Morse nous permet de savoir si le point critique est un extremum (plus précisément si c'est un maximum ou un minimum) ou s'il s'agit d'un point selle. A la fin, au moment de vérifier que la transformation $x \mapsto u$ que l'on a trouvé est un $\mathcal{C}^1$-difféomorphisme, et pour justifier qu'il y a un intérêt à montrer ceci en plus, je parle de la méthode de Laplace multidimensionnelle qui utilise le lemme de Morse comme changement de variables.

Ensuite questions sur le développement. Justifier que l'application $Q : x \mapsto \int_0^1 (1-t)\mathrm{d}^2 f(tx)\mathrm{d}t$ est continue bon je dis que c'est de la régularité sous l'intégrale, on me demande quel domaine des maths est en jeu, je ne vois pas trop ce que voulait le jury donc je réponds intégrale paramètre, il acquiesce. On m'a aussi demandé si la restriction d'une fonction $\mathcal{C}^\infty$ l'était encore (j'utilise ce résultat) je ne comprenais pas trop vers quoi il voulait m'amener, en fait la question portait sur le fait que l'espace est aplati par rapport à l'espace de départ. Je fais un petit dessin pour expliquer qu'on regarde la continuité sur l'espace sur lequel on a restreint et qu'on ne regarde pas les directions qu'on a perdu. On a passé un peu de temps là-dessus. La dernière question sur le développement en lui-même était de savoir pourquoi dans le premier lemme on montre que l'application est un $\mathcal{C}^1$-difféomorphisme (c'est pour que le changement de variable soit un $\mathcal{C}^1$-difféomorphisme).

Sinon le jury avait des questions sur des extensions du développement, on a donc parlé de ce qui se passait lorsque la différentielle seconde avait une valeur propre nulle, je fais un dessin pour dire ce qu'il se passe si ma fonction est nulle dans une direction (je réponds à une autre question en fait). Je ne voyais pas trop quelle conclusion on pouvait tirée, le jury me demande dans le cas d'une fonction d'une seule variable qu'est-ce qui peut se passer, je sors tout de suite notre application préférée ($x \mapsto x^3$) et bon globalement on comprends qu'on ne peut rien dire dans ce cas là.

II.E Questions

On passe aux questions sur le plan. On me demande la différentielle composée sur un exemple ($g : x, y \mapsto g(x, y)$ différentiable, quel est la différentielle de $h : t \mapsto g(2t, t^2 + 1)$ je vois qu'il s'agit de faire une différentielle composée j'écris explicitement la fonction f tel que $g \circ f = h$ et j'applique la formule de la différentiel composé, on me demande de l'exprimer en fonction des dérivées partielles de g, je m'exécute. Le jury me demande ensuite si je sais faire la différentielle du déterminant (elle est dans le plan), je la calcule en $X \in \mathrm{GL}_n(\mathbb{R})$ en factorisant par X, en faisant apparaître un polynôme caractéristique et en utilisant la formule de la comatrice. Pour passer à une matrice quelconque je dis qu'on utilise la densité de GL_n, on me demande quoi d'autre, je ne vois pas, on me dit de penser à $\mathbb{R}*$ et $\mathbb{R}$ et la fonction $x \mapsto 1/x$, je répond qu'on utilise aussi la continuité de $X \mapsto \mathrm{Com}(X)$.

On a terminé en parlant de différentielle seconde. On me demande ce que l'on peut dire de la différentielle seconde, je parle de la matrice hessienne, on me demande quelles propriétés elle a, je répond qu'elle est symétrique, on me demande pourquoi, je réponds Schwarz, on parle un peu d'analogie avec les formes quadratiques (en lien avec le lemme de Morse donc) et on me demande si dans le cas d'une fonction ayant seulement des dérivées partielles on peut continuer à intervertir les dérivées (le rapport dit "Les candidates et candidats solides peuvent s'intéresser la notion de différentielle seconde pour les fonctions de classe $\mathcal{C}^2$"), je commence par dire que je sais qu'on peut faire la preuve en utilisant Taylor-Young et qu'avoir une fonction deux fois différentiable suffit, ça ne répond pas vraiment à la question mais on a déjà abaisser les hypothèses, on finit par passer à autre chose. En dernière question on m'a demandé quelle était la différentielle seconde composée.

III Oral de modélisation

III.A Note :

15,75

III.B C 31 : Corps finis, polynômes, arithmétique.

III.C Mots-clefs

Corps finis, polynômes, arithmétique

III.D Résumé

On souhaite repérer des erreurs dans des mots de passe ou des identifiants lors de leur saisie manuelle.

Je fais une introduction sur les centres de vaccination où le personnel rempli à la main les numéros de sécurité sociales et où des erreurs peuvent donc apparaître. J'illustre aussi en parlant de partir en vacances avec un groupe d'amis et une personne avance les frais de transport, puis pour la rembourser on doit rentrer son IBAN et on souhaite que l'argent aille à notre ami.

Voici ce que je me rappelle du texte que j'ai travaillé le jour de l'oral :

1) Code de contrôle :

Lors de la saisie manuelle de codes, des erreurs peuvent survenir (IBAN, sécurité sociale, ...).

ERREURS LES PLUS FRÉQUENTES

1)	$\cdots a \cdots$	$\cdots b \cdots$	80%
2)	$\cdots ab \cdots$	$\cdots ba \cdots$	10%
3)	$\cdots abc \cdots$	$\cdots cba \cdots$	6%
4)	$\cdots aa \cdots$	$\cdots bb \cdots$	3%
5)	$\cdots aca \cdots$	$\cdots bcb \cdots$	1%

On se place dans $\mathbb{F}_q$ et on souhaite transmettre des suites finies de caractères $a_0, \cdots, a_{m-1}$. On ajoute un caractère qu'on appelle *clef de contrôle* tel que

$$f(a_0) + f^2(a_1) + \cdots + f^m(a_{m-1}) = 0$$

où f est une permutation de $\mathbb{F}_q$ fixée. Alors on peut détecter 1) et f est appelée permutation de contrôle.

Je reparle ici de notre numéro de sécurité social où l'on a à la fin une clef de contrôle de 2 chiffres.

Proposition :

f détecte les autres erreurs si et seulement si $(f - \mathrm{id}), (f + \mathrm{id}), (f^2 + \mathrm{id}), (f^2 - \mathrm{id})$ sont injectives.

Preuve : (cas 2).

$$\begin{aligned} & f^R(a_R) + f^{R+2}(a_{R+1}) = f^R(a_{R+1}) + f^{R+2}(a_R) \\ \Leftrightarrow & (f - \mathrm{id})(f^R(a_R)) = (f - \mathrm{id})(f^R(a_{R+1})) \end{aligned}$$

Donc f détecte 2) $\Leftrightarrow f - \mathrm{id}$ est injective.

Je fais la démonstration pour le cas 3 à l'oral afin de montrer que j'ai réfléchi à la preuve et que je ne fais pas que la recopier.

■

Exemple :

$f_a : x \to ax, \quad a \in \mathbb{F}_q^\times$.
f détecte 2), 3), 4) et 5) $\Leftrightarrow a^2 \neq \pm 1$.

Ce problème reste ouvert, on s'intéresse à un cas particulier.

Par Lagrange (interpolation), on peut représenter une permutation par un polynôme.

J'ai parlé de cela, après j'ai eu une question du jury pour détailler un peu comment on fait Lagrange. Je parle des polynômes de Lagrange (les L_i) puis on prend $P = \sum_{u \in \mathbb{F}_q} f(u) L_u$. Le jury me demande si je ferais comme ça en pratique, je répond que non, on utilise plutôt la méthode de Lagrange rapide, basée sur une construction d'arbres et qui est en $\mathcal{O}(n(\log(n))^2)$ alors que la méthode de Lagrange est en $\mathcal{O}(n^2)$.

2) Polynômes du type $\mathcal{P}$.

Soit $P \in \mathbb{F}_q[x]$.

Définition :

On dit que P est de type $\mathcal{P}$. ($P \in \mathcal{P}$) si

$$\begin{array}{c} \mathbb{F}_q \to \mathbb{F}_q \\ u \mapsto P(u) \end{array} \text{ est bijective.}$$

Exemple :

(Il y avait ici deux exemples à suivre de polynômes de type $\mathcal{P}$, l'un dans $\mathbb{F}_{11}$ et de degré 9 il me semble, qui est de type $\mathcal{P}$ mais qui ne détecte pas les erreurs et un autre dans $\mathbb{F}_{17}$ ($x^9 - x$ ou quelque chose comme ça) je crois qui lui détecte les erreurs.

j'avais codé l'algorithme de détection d'erreurs et j'ai passé ces deux polynômes dedans afin d'illustrer ce que disait le texte. De plus j'avais programmé l'algorithme pour qu'il me donne une fonction de la première proposition qui n'est pas injective (il en renvoie une seule) et donc savoir quelle erreur on ne peut pas détecter.

Exemple :

Si R est premier avec $q-1$ alors x^R est de type $\mathcal{P}$ car le seul antécédent de 0 est 0.

Remarque

P est de type $\mathcal{P}$ si et seulement si $\prod_{u \in \mathbb{F}_q} (x - P(u)) = x^q - x$.

Remarque :

Il y a $\dfrac{q!}{q^n}$ polynômes de type $\mathcal{P}$ de degré $\leqslant q$ dans $\mathbb{F}_q[x]_{<q}$.

La preuve n'est pas donnée, je la fais à l'oral par manque de temps (j'ai passé pas mal de temps sur le début : modélisation et première partie) et je trace la proportion de tels polynômes par rapport au nombre de polynômes dans $\mathbb{F}_p$ pour p les nombres premiers jusqu'à 29. Je fais la remarque qu'on ne peut pas espérer en prenant un polynôme au hasard qu'il soit de type $\mathcal{P}$, contrairement à ce que l'on peut espérer avec les polynômes irréductibles dans les corps finis. Ceci motive à parler de la partie suivante du texte.

3) Caractérisation des polynômes de type $\mathcal{P}$

On cherche un critère :

Lemme

$a_0, \dots, a_{q-1} \in \mathbb{F}_q$ sont deux à deux distincts si et seulement si

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{si } 0 \leqslant t \leqslant q-2 \\ -1 & \text{si } t = q-1 \end{cases}$$

Preuve :

On considère

$$Q_i = 1 - \sum_{k=1}^{q-1} a_i^{q-1-k} x^k.$$

$\implies Q_i(u) = \begin{cases} 1 & \text{si } u = a_i \\ -1 & \text{sinon} \end{cases}$ Le texte ne détaille pas beaucoup plus, il invite à regarder $a_i^q - u^q = (a_i - u)\sum_{k=0}^{q-1} a_i^{q-1-k} - u^k$.

On pose alors $Q = Q_0 + \cdots + Q_{q-1}$. Et on obtient $Q(u) = \sum_{i=0}^{q-1} \delta_{i,u} = \#\{i \in \{0, \dots, q-1\} \quad / \quad a_i = u\}$.

La condition du lemme équivaut à $Q(x) = 1 \ \forall x \Leftrightarrow P \in \mathcal{P}$ car $Q = \sum_{i=0}^{q-1} Q_i = -\sum_{k=1}^{q-1} \left(\sum_{i=0}^{q-1} a_i^{q-1-k}\right) x^k$ ■

Je détails bien la preuve de ce lemme au tableau, il est fondamental dans la démonstration du théorème qui suit et je n'ai plus le temps de faire la preuve du théorème.

Théorème

Soit $P \in \mathbb{F}_q[x]$. Alors

$$P \in \mathcal{P} \iff \begin{array}{ll} (1) & P \text{ admet exactement une racine dans } \mathbb{F}_q \\ (2) & \forall t \in \{1, \dots, q-2\} \text{ le degré de } P^t \text{ réduit modulo } x^q - x \text{ est } \leqslant q-2 \end{array}$$

Je ne suis plus tout-à-fait sûr de l'énoncé.

Preuve :

elle est en partie donnée est basée essentiellement sur le lemme précédent.

Corollaire :

si $d = \deg(P)$ et si $d|q-1$ alors $P \notin \mathcal{P}$.
sans preuve, mais elle est facile à faire

Exemple :

les deux exemples de la partie précédente sont bien des polynômes de type $\mathcal{P}$.

4) Des classes de polynômes de type $\mathcal{P}$

Définition :

$L(x) = \sum_{i=0}^{k} a_i x^{p^i} \in \mathbb{F}_q[x]$ où p est la caractéristique du corps.

Proposition :

$$L \in \mathcal{P} \iff 0 \text{ est l'unique racine de } L \text{ dans } \mathbb{F}_q$$

sans preuve mais il suffit de voir qu'on a des combinaisons linéaires d'itérées du Frobenius.

Théorème : (pas sûr de l'énoncé exact mais je crois bien que c'est ça)

Soit $r > 0$, soit $s > 0$ premier avec $q-1$. Supposons :
— $r|q-1$
— Q n'a que 0 comme racine dans F_q ou est sans racine.
Alors $P = x^r \left(Q(x^s)\right)^{\frac{q-1}{s}} \in \mathcal{P}$

Preuve :

Le texte suggère d'utiliser le théorème de la partie précédente et de distinguer (pour montrer (2) du théorème) les cas $s|t$ ou non.

Je n'avais plus de temps, donc plutôt que de présenter la preuve, j'ai présenté l'algorithme que j'ai écrit, et les exemples qui sont suggérés par le texte et que j'écrit juste après.

On peut définir un polynôme linéarisé par :

$$\begin{cases} P(0) = 0 \\ P \text{ est unitaire} \\ \text{si } \deg P < q-1 \text{ alors le monôme d'indice } \deg(P)-1 \text{ est nul} \end{cases}$$

Exemple :

Les seuls polynômes linéarisés de degré 4 de $\mathbb{F}_5[x]$ sont $x^4 + 3x$ et $x^4 - 3x$.

Il sufiit de remarquer qu'avec les conditions de la définition, il n'y a que 2 monômes de liberté et ensuite d'utiliser l'ordinateur pour faire le reste.

VI) Approche probabiliste et résultant.

Partie non traitée, elle parlait d'une méthode probabiliste pour trouver des polynômes de permutations en utilisant des calculs de résultants.

Suggestions :

— Des preuves non faites ou incomplètes.
— Utiliser l'ordinateur pour traiter quelques exemples.
— Implémenter le calcul de résultant comme dans le texte.